



Cyber Threats 2021:

A Year in Retrospect

Contents

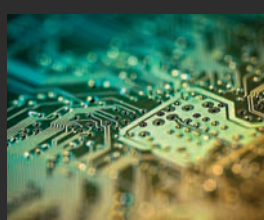


04
A perfect storm: 0-days, quatermasters, and surveillance

05 Year of the 0-day

05 An overview of quatermaster activity

08 An ever-watchful eye: surveillance and civil society



11
Cybercrime

12 Ransomware

25 Delivery and access



27
Regional activity

28 Asia-Pacific

42 Middle East

48 Europe and former Soviet Union



54
New threat actors spotlight

55 Red Dev 17

55 Blue Dev 6

55 Yellow Dev 23



59
Sectors spotlight

60 Telecommunications

60 Technology

61 Financial services

61 Retail

67 Conclusion

69 Endnotes

Introduction

Ransomware cemented its position as the most prominent cybersecurity threat faced by organisations across geographies and sectors, with increased momentum and impact throughout 2021.

PwC serves more than 200,000 clients in 156 countries. We use our vantage point as one of the largest and most global professional services networks to deliver one of the most global threat intelligence services to our clients. Our research underpins all of our security services, and is used by public and private sector organisations around the world to protect networks, provide situational awareness, and inform strategy. This annual report documents the overarching and thematic trends we observed in 2021, and is part of our contribution to help build a secure digital society.

Affiliate programmes and Ransomware-as-a-Service (RaaS) schemes fostered further growth of the cybercrime threat, and its hidden impact on lives was increasingly laid bare as schools, charities, public services, and critical infrastructure often bore the brunt of indiscriminate targeting. These schemes streamlined compromise-to-profit pipelines – providing financial incentives, reputation-based deals, and even furnishing operators with resources such as step-by-step intrusion playbooks. At the same time, ransomware schemes continued to strengthen mutualistic ties to the cyber criminal ecosystem surrounding them, including malware delivery systems (like TrickBot, IcedID, and QakBot), underground forums facilitating ransomware affiliate recruitment, and Access-as-a-Service (AaaS) markets.

While 2020 was dominated by the COVID-19 pandemic, its spread throughout the world and its impact in cyber space, a major trend in 2021 was the proliferation of cyber capabilities. 0-day vulnerabilities resumed as a major concern discussed

in cybersecurity conversations, with issues surrounding their research, disclosure, and exploitation attracting greater public scrutiny. These arose particularly in relation to indiscriminate targeting and issues of national security, as threat actors of all motivations and capabilities rushed to exploit high-profile vulnerabilities such as ProxyLogon and Log4Shell. The abuse of 0-day exploits also interlinked with two other phenomena: the impact of digital quartermasters on the cyber threat landscape (including that of commercial quartermasters), and surveillance activity against civilian targets.

Intelligence gathering operations, for the most part, remained aligned with geopolitical events. However, in 2021, more than any other year so far, we identified new and emerging clusters of activity pursuing objectives aligned with specific countries' strategic interests, including threat actors likely based in countries from which we had not previously observed offensive cyber activity originating.

The analysis in this report was conducted by the PwC Threat Intelligence practice, which is distributed across Australia, Italy, Germany, Netherlands, Sweden, United Kingdom, and the United States. It is based on our in-house intelligence datasets on cyberattacks and targeting from a wide variety of threat actors, intelligence gleaned from PwC's incident response engagements around the world, and our managed threat hunting services, as well as publicly available information.



A perfect storm:

0-days, quartermasters,
and surveillance



Year of the 0-day

0-day vulnerabilities, and particularly their research and disclosure, have been an ever-present topic of interest in the cybersecurity community. In 2021, several high-profile events, including highly targeted operations as well as mass exploitation of vulnerabilities, brought this topic yet again to the fore of strategic and tactical discussions, and into the public eye.

Rather than treating 0-days as an insurmountable threat, in this section we provide strategic context of this phenomenon.

Day by (0)day: a strategic overview of the zero-day landscape

Discussions about 0-days often revolve about the difficulty of avoiding them, based on the perception they might be even harder to defend against. In 2021, we saw coverage of this topic spilling into the mainstream, together with other high-profile topics like supply chain targeting (in the wake of the SolarWinds incident) and ransomware (following attacks on entities like Colonial Pipeline). The year 2021 also registered the largest number of 0-days disclosed in a single year¹, almost doubling 2020's figures. The reasons behind this surge are nuanced, and likely the result of a combination of factor, including:

- **A more overt element of national security:** While 0-days have been abused for years, 2021 saw several political displays of “0-day diplomacy”; that is, discussions about their usage on a national security level. As an example, Germany's newly elected coalition made a political statement on the embargo of government purchase of 0-days, citing their “highly problematic relationship to IT security and civil rights.”² The Cyberspace Administration of China (CAC) announced new laws surrounding domestic vulnerability disclosure.³ The new law also applies to vendors, which must ensure any vulnerabilities are mitigated in a timely manner and promptly disclosed to customers along with fixes, and encourages private organisations to set up bug bounty programs to financially incentivise vulnerability research.
- **The market for 0-days has expanded:** Over the past few years, there have been an increasing number of players operating in the vulnerability research space: from individual security researchers, to 0-day criminal brokers, to private espionage companies such as Hacking Team, FinFisher, NSO Group, and Candiru. Exploit brokers and private sector organisations, particularly, are among the most prominent players with regards to 0-day development and trading.

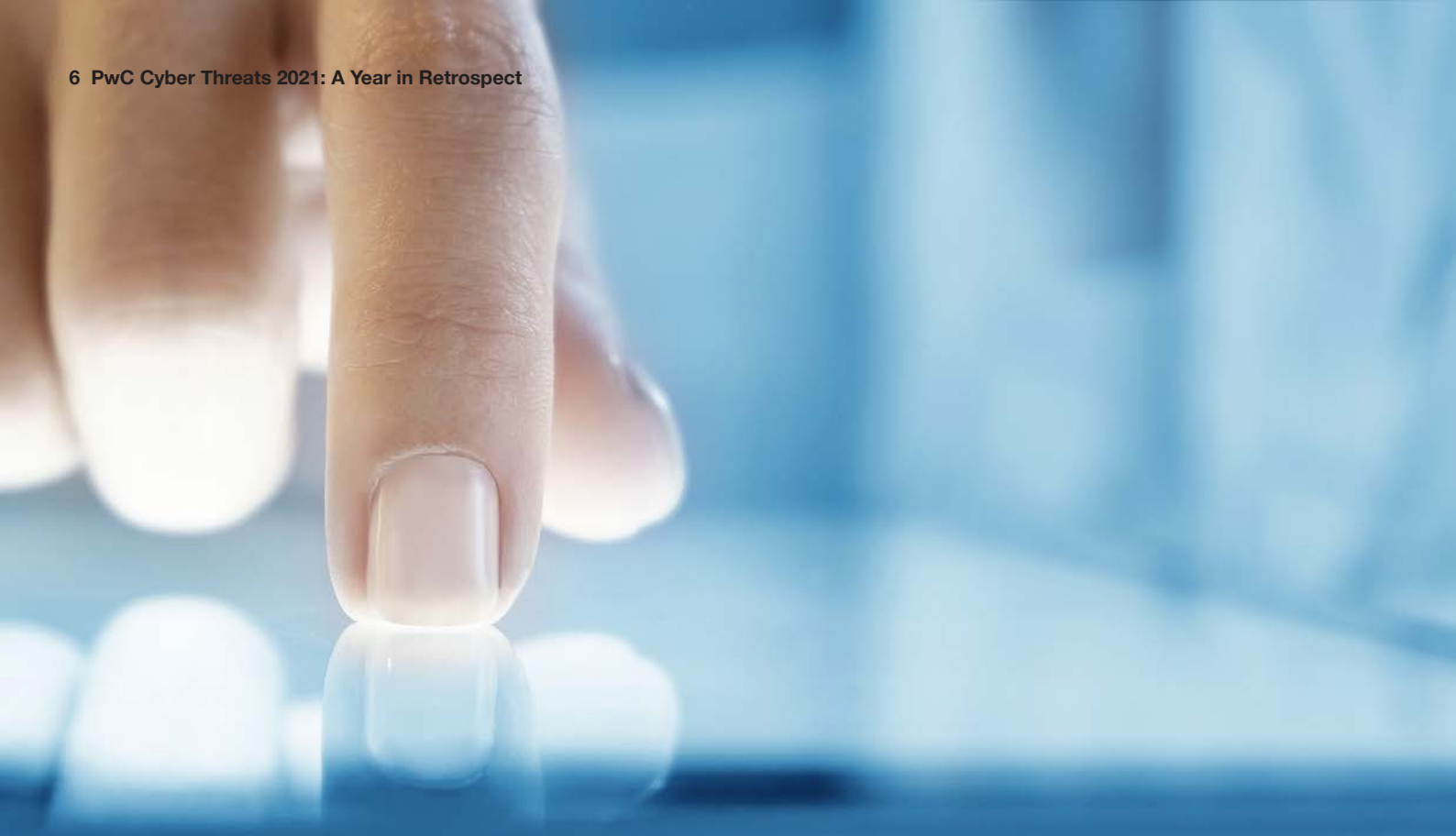
- **More incentives than ever before:** There are now increasing avenues for vulnerability researchers to compete and earn financial rewards for their exploit development work. These can be legitimate, such as the Tianfu Cup and Pwn2Own, or illegitimate, as has been the case with offensive research contests launched on Russian-language dark web forums.⁴ With this activity firmly rooted in the offensive security world, defenders have had to respond, dedicating resources to their own exploit development work for identification and disclosure purposes, such as with Google's Project Zero.⁵
- **A renewed focus on third-party infection:** Threat actors with a variety of motivations have begun targeting organisations involved in supply chains, often enabling access to multiple targets at once. This has led to an investment of resources into vulnerability research of widely used business technologies, such as email servers, or knowledge management software as key examples. This naturally increased the amount of 0-days discovered, and, with their disclosure (even where responsible and accompanied by vendor fixes and advisories), the amount of attempts at exploiting those very vulnerabilities.

Ultimately, preventing 0-days is not a trivial matter for software developers and vendors, let alone for their customer base. However, customers and defenders should not underestimate the capabilities and measures that can be put in place with a focus on detection and response to post-exploitation behaviours and activity. Coupled with robust core security hygiene, a solid detection and response function can make a difference in the impact that new 0-days might have on organisations.

An overview of quartermaster activity

The way threat actors procure and provision tools can affect not only attribution, but, more importantly, their capabilities and ability to pursue new target pools. The concept of a digital quartermaster is not new when it comes to cyber operations, but remains increasingly relevant. Quartermasters have been traditionally associated with supplying technology to military units. Consequently, digital quartermasters are more often thought of in the context of Advanced Persistent Threat (APT) actors gaining access to capabilities only shared among a select group of threat actors, or obtaining tools from a central entity in charge of distributing them and enabling their use.

However, PwC also defines the companies that sell offensive security solutions such as spyware, 0-day exploits, and related capabilities, to entities that then operate them as ‘Commercial Quartermasters.’ While traditional quartermasters often only provide tools to threat actors based in the quartermaster's own country, customers of commercial quartermasters might be based in several countries.



APT quartermasters

While it is not always possible to prove, the hypothesis that multiple APT groups operate under, or are resourced by, the same digital quartermaster cannot be ruled out for various sets of threat actors. In 2021, we continued to observe this phenomenon, whether through observations of shared capability (malware, techniques, exploits, and so on), or through overlaps in infrastructure (either through the same patterns observed on C2s, or the reuse of domains/IPs by other threat actors).

Of Shadows and Proxies: China-based threat actors sharing tools

The continued sharing of tools and techniques is a running theme among China-based threat actors. While not all of the China-based threat actors share tools with one another, and not all of them have access to the same tools, quartermaster arrangements (covered in more detail in a later section) continue to complicate attribution of activity. For example, the same malware families (such as PlugX, PoisonIvy, ShadowPad, Quarian, and the Winnti backdoor) are used by multiple China-based threat actors, and, as has become very well known in 2021 with the ProxyLogon incidents, some threat actors share exploits as well.

We note that while not all of these threat actors have been observed having access to the shared tools detailed below, these are prime examples of the dynamic described in this section.

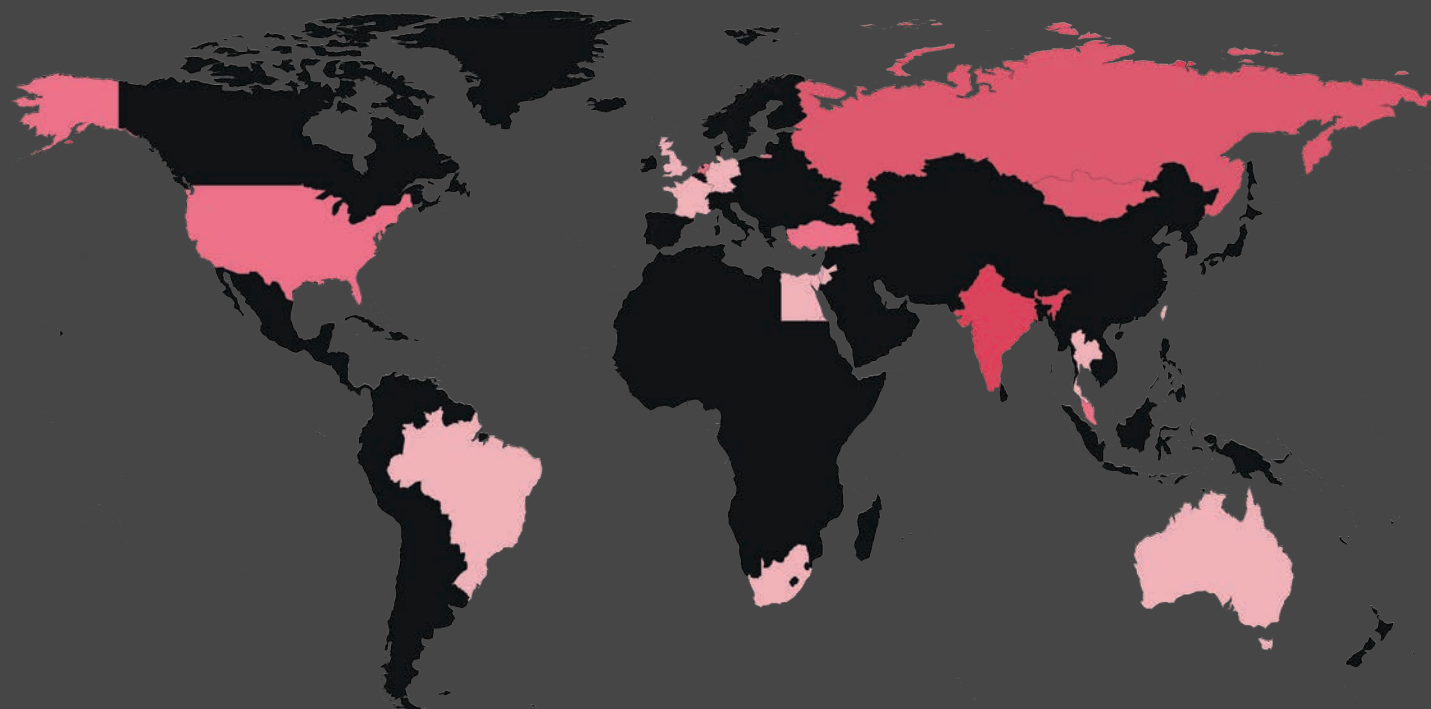
ShadowPad and Scatterbee

ShadowPad is a modular backdoor that allows a threat actor to customise the functionality delivered in an implant. Every ShadowPad sample that we have seen has a root module designed to orchestrate the next set of modules, including a plugins module that can then be customised depending on the functionality that the threat actor requires. The plugins can enable capabilities that may include, among others, C2 communications over HTTP or TCP, keylogging, screenshot gathering, port mapping, and system information gathering.⁶

In tracking “standard” ShadowPad samples in 2021, we identified and analysed a new variant, which we call ScatterBee: samples of ShadowPad that had been obfuscated using a custom technique.⁷ Likely in order to minimise detection on victim networks, the ScatterBee packing mechanism implements control flow obfuscation, string encoding, dynamic API resolutions, several anti-analysis techniques, as well as shellcode decoding/decrypting. We assess that one or more users of ShadowPad have access to ScatterBee, and have highly likely delivered some of these malicious payloads via watering hole attacks on sites that are used to deliver Adobe Flash update files. We assess that most ScatterBee payloads can be directly linked back to the threat actor we track as Red Dev 10 (aka Earth Lusca), and have been used to target organisations in the aerospace and defence sectors.

We assess ShadowPad to be highly likely used by at least 11 China-based threat actors.⁸ Our analysis into specific subsets of ShadowPad infrastructure allowed us to identify a wide set of victims, ranging from India-based entities in the telecommunications and oil and gas sectors, to East Asian branches of international humanitarian organisations.

Figure 1: Geographic distribution of ShadowPad victims observed until December 2021



Source: PwC

“Exchanging” Exchange: ProxyLogon

In early 2021, Red Dev 13 (aka HAFNIUM) began exploiting vulnerabilities in Microsoft Exchange, which became collectively known as ProxyLogon.^{9, 10, 11} While the initial activity surrounding ProxyLogon was associated exclusively with HAFNIUM, at the end of February/beginning of March 2021 (close but prior to the time of the first public disclosure of these campaigns), multiple China-based threat actors started exploiting the same vulnerabilities, on a mass scale versus precise targeting.

As we have already highlighted, it is not uncommon for these threat actors to share tools. However, the rapid sharing of these exploits ahead of the patching of the Microsoft Exchange vulnerabilities was unprecedented.

Iran-based developers working across multiple APTs

Threat actors are typically identified by the capabilities, infrastructure, targeting, and general TTPs they display. However, developers or operators behind campaigns working across multiple threat actors can muddy analysis and attribution.

This can occasionally be the case with Iran-based threat actors. For example, through researching phishing campaigns by Yellow Liderc (aka Tortoiseshell, TA456), we identified

a set of malicious PDF documents targeting the higher education sector. This targeting did not normally align with Yellow Liderc,¹² but matches that of Yellow Garuda (aka Charming Kitten, APT35, PHOSPHORUS, TA453, and ITG18). We have previously noted infrastructure overlaps between these two threat actors, raising the hypothesis that Yellow Liderc is an offshoot of Yellow Garuda.¹³ Based on several similarities between these threat actors, we assess there is a realistic probability that an operator has either spanned or transitioned between the two during 2021.

Commercial quartermasters

Commercial quartermasters differ from companies defined as hack-for-hire, like CyberRoot and BellTroX.¹⁴ Hack-for-hire companies are tasked with doing the actual hacking on behalf of a paying client, while commercial quartermasters only offer tools paid for by the client, which then are used by the client themselves to do the hacking. Early examples of commercial quartermasters include Hacking Team and FinFisher, both of which were at the centre of considerable public outrage and have since rebranded or gone bankrupt. Despite the fallout from these companies’ activities, PwC continues to observe threat actors, particularly those running surveillance operations, leveraging commercial quartermasters and their capabilities.¹⁵

The recent public spotlight on commercial quartermasters like NSO Group and Candiru has provided insight into a relatively secretive and growing industry that has implications for cybersecurity professionals and potential victims, including:

- difficulty in attributing threat actors that would otherwise not be capable of conducting such sophisticated operations;
- rapid enablement of a country to target both the private and public sector with advanced malware, such as a company, government body, or its personnel; and,
- the potential abuse of these tools to target journalists, activists, and civil society.

Additionally, the tools produced by commercial quartermasters are almost certainly used against a wide array of targets, which may also include government officials and private sector executives, warranting attention by organisations that might not think these types of threat actors fit within their threat profile.

An ever-watchful eye: surveillance and civil society

Whether armed by the rise of exploit brokers and surveillance software vendors, enhanced through quartermaster arrangements, or performed by state-sponsored groups, surveillance of civilian targets poses a significant threat to achieving a secure digital society for all. Minorities, civil rights activists, dissidents, politicians, and journalists, as well as civilians more broadly, frequently fall in the crosshairs of such state-sponsored espionage activity. Civil society targets often also include NGOs, social movements, coalitions, and faith-based organisations that may share common interests.

While surveillance activity often focuses on a person of interest, organisations associated with those individuals are sometimes found to be victims, where the organisation is considered a stepping stone to access the intended target. This factor is useful for contextualising threats to civil society as a shared problem.

Powering surveillance: from hacker-for-hire to commercial quartermasters

Candiru

In July 2021 Citizen Lab,¹⁶ Microsoft,¹⁷ and Google¹⁸ all exposed to varying degrees a commercial quartermaster called Candiru, which we track as Grey Mazzikim (aka SOURGUM). According to Microsoft, the actor's spyware is alleged to have been deployed against over 100 victims. Several domains associated with campaigns we tracked in 2021 indicated clear targeting of human rights activists and journalists; others aligned more with strategic interests of a nation-state, such as energy exports or government

organisations. The spyware sold by Grey Mazzikim is highly sophisticated and can infect and monitor iPhones, Androids, Macs, PCs, and cloud accounts.¹⁹ Once a target is infected with the spyware, the operator can exfiltrate the victim's private data from a number of apps and accounts including Gmail, Skype, Telegram, and Facebook, along with capturing browsing history and passwords.²⁰ The threat actor might also be able to turn on the target's webcam and microphone, or take screenshots.

Since Candiru is a supplier to multiple threat actors throughout the world, the complexity and scale of these attacks is quite extensive. In efforts to maximise coverage of and categorise these threats, PwC tracks Candiru as Grey Mazzikim and its customers, which currently consist of at least four different threat actors, separately where possible.²¹ There are a wide range of targets, but with a distinct focus on Europe and the Middle East.

NSO Group

NSO Group, which PwC tracks as Grey Anqa, was founded in 2010. The company is most widely known for its spyware called Pegasus, but also offers a range of other products, including geolocation software for cell phones and data analytics systems. Its primary services and product offerings focus on mobile devices and networks. Pegasus is known to infect the most recent versions of popular mobile operating systems via zero-click and 0-day exploits, including one of the most sophisticated exploits ever documented, known as FORCEDENTRY.^{22, 23}

NSO made headlines on multiple occasions for selling its Pegasus spyware to nation-states that ultimately abused the tools to spy on civil society.

The recognisable similarities between Grey Anqa and Grey Mazzikim are many: similar type of company, operating from the same country, recruiting from the same talent pools, with a similar customer base. In both cases, the readily available offensive capabilities for purchase highlight an industry that enables a consumer to wield sophisticated tools that have also been abused in targeting civil society on an international scale.

Pulling the plug: reaction to commercial quartermasters

2021 thrust commercial quartermasters into the public spotlight, and into courts of law in multiple countries. For example, several US technology companies are bringing lawsuits against commercial spyware providers on behalf of their customer base, and in some cases seeking to restrict the defendants' access to the companies' hardware and software. In 2021, we also observed the first high-profile action against commercial quartermasters at a state level: the US Commerce Department placed NSO Group and Candiru on its Entities List, citing a significant risk of them acting "contrary to the national security or foreign policy interests of the United States."²⁴

A first consequence of such action has been, for example, the Israeli government's move to restrict by two-thirds the list of countries to which Israeli security firms are allowed to sell surveillance and offensive hacking tools. As highlighted earlier, we note that commercial quartermasters operate in several countries internationally, with numerous brokers active in Europe^{25, 26} and in the US.²⁷

The likely enduring existence of commercial quartermasters brings forth a fresh set of challenges. It is relatively easy for a country to purchase bespoke and highly sophisticated offensive tooling that elevates the country's capabilities to that of an advanced persistent threat. The high sophistication of commercial quartermasters, together with their budgets for research and development, also implies their ability to retool while maintaining high operational security standards, both of which allow for end-users to continue to operate even after public exposure.

Advanced Persistent Watchers: APT surveillance activity

Red Dev Redemption

Red Dev 3 (aka DeepCliff, RedAlpha) is a threat actor active since at least 2015, which was first exposed in open source in 2018 by CitizenLab as targeting a specific community.²⁸ Throughout 2021 we observed Red Dev 3 set up hundreds of domains hosting credential phishing pages aimed at diverse pools of targets on an international scale.²⁹

Red Dev 3's domain naming convention imitates popular mail service providers, and the threat actor may also spoof login portals for the specific mail services of the organisations it is targeting.³⁰

Red Dev 3 also targeted or spoofed services including news outlets popular among diaspora communities and dissidents; NGOs with a focus on refugees as well as civil and human rights, such as Amnesty International; and think tanks and policy institutes.

Since April 2021, we observed a broadening focus of the threat actor's targeting from civil society to government entities, including Ministries of Foreign Affairs in at least five countries, as well as several government and political organisations worldwide.³¹ However, the threat actor also continued to brazenly and persistently target individual citizens and vulnerable communities, in relation to sensitive political and social topics.

Red Nue's new antics

Red Nue, active since at least 2017, is known for its use of the multi-platform LootRAT backdoor, also known as ReverseWindow.³² LootRAT has variants for Windows³³ and Macintosh³⁴ (reported in open source as Demsty), as well as an Android variant known as SpyDealer.³⁵ Red Nue has also used another Windows backdoor³⁶ known as WinDealer³⁷ since at least 2019, when it deployed it to targets as part of a watering hole campaign on a Chinese news website for the Chinese diaspora community.

In 2021, we observed the threat actor continue to iterate on LootRAT, deploying a Linux variant of the backdoor.³⁸ The new sample of the backdoor had the binary's comment section stripped, likely in an attempt to make analysis and understanding about the threat actor more difficult. All the victims that we observed from this campaign were based in Asia, and included a technology company providing simulation software.



The high sophistication of commercial quartermasters, together with their budgets for research and development, also implies their ability to retool while maintaining high operational security standards, both of which allow for end-users to continue to operate even after public exposure.”

Parts of Asia feature heavily in Red Nue's victimology. The threat actor has targeted individuals and universities with the Demsty MacOS variant of LootRat. For example, SpyDealer (the Android version of LootRAT) has the ability to steal information from over 40 mobile communications apps, including WeChat, Facebook, WhatsApp, Skype, Sina Weibo, Tencent Weibo, and Oupeng Browser, many of which are widely used in China.

White Dev 75 targeting Middle East and North Africa

White Dev 75 has been active since at least 2015, and PwC has determined that this threat actor is likely espionage-motivated. Its observed victims are primarily civil society members, who are likely being targeted in relation to political topics. White Dev 75 continues to be highly effective in compromising email accounts of journalists, dissidents, and politically-involved individuals located throughout the Middle East and North Africa.^{39, 40, 41}

Between at least April and October 2021, White Dev 75 registered dozens of new phishing domains that align with previous tactics and procedures observed in its campaigns, including one impersonating the Ministry of Foreign Affairs of a Middle Eastern country. White Dev 75 is particularly effective due to its ability to bypass MFA and leverage convincing social engineering techniques. The phishing emails White Dev 75 often uses are fake security alerts of abnormal login behaviour. The threat actor has also been observed abusing OAuth to circumvent MFA and passwords all together.⁴² OAuth is a common application allowing authentication of third-party services without the need to share passwords. The observed TTPs of White Dev 75 are not overly advanced but demonstrate a persistence and cleverness in its tradecraft that allows it to perpetrate these tactics against civil society.

40+

Apps that SpyDealer (the Android version of LootRAT) can steal information from



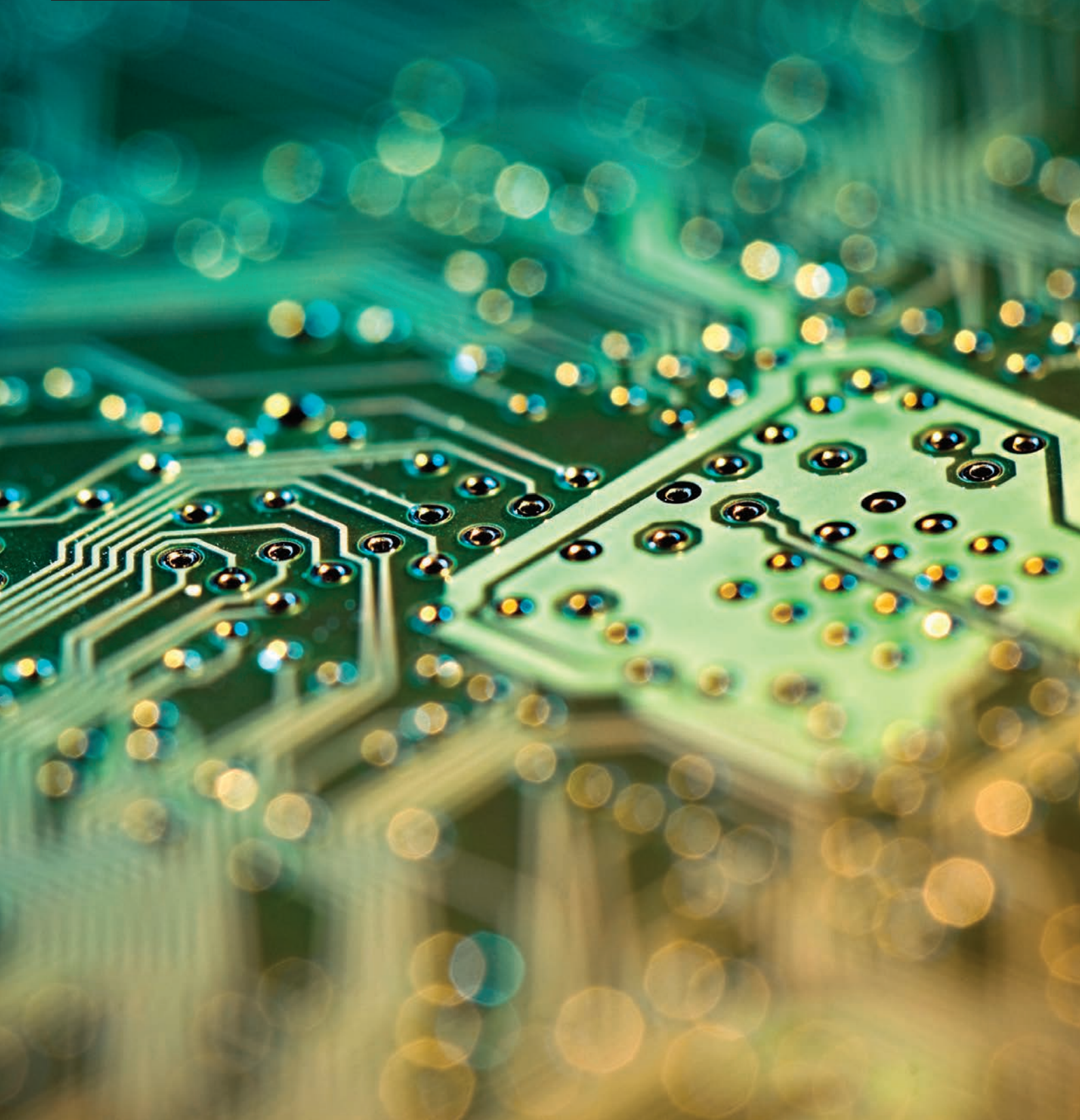
Yellow Garuda's domestic surveillance

Yellow Garuda (aka Charming Kitten, PHOSPHORUS, ITG18) is a versatile Iran-based threat actor which has been active since at least 2012. It was highly active throughout 2021, conducting a range of activity in a surveillance capacity.

We found evidence that Yellow Garuda conducted a targeted domestic surveillance campaign to extract data from a victim's Telegram account.⁴³ This included the exfiltration of messages, media files, details of group memberships, and the victim's contacts. Between September and October 2021, the threat actor compromised at least six Iran-based victims, based on data obtained by PwC along with copies of the actor's bespoke Telegram 'grabber' tool which was used to exfiltrate the data from victim accounts. We also uncovered an operational report written by the threat actor itself concerning surveillance on a seventh domestic victim; the data from this victim was more extensive and likely the result of exfiltration via mobile malware.

The addition of mobile malware in Yellow Garuda's toolset has been reported in open source⁴⁴ and correlates to our own analysis of an Android malware sample with multiple links to known Yellow Garuda infrastructure in early 2021.⁴⁵ This sample masqueraded as the messaging application WhatsApp and included the ability to record audio and video, take photos, access contacts, location data and SMS, and initiate calls. Its functionality and codebase was similar to an older sample of Android malware from 2018 which was reportedly used to target Iranian citizens, indicating that Yellow Garuda has likely had this capability for some time.

Cyber crime



Ransomware

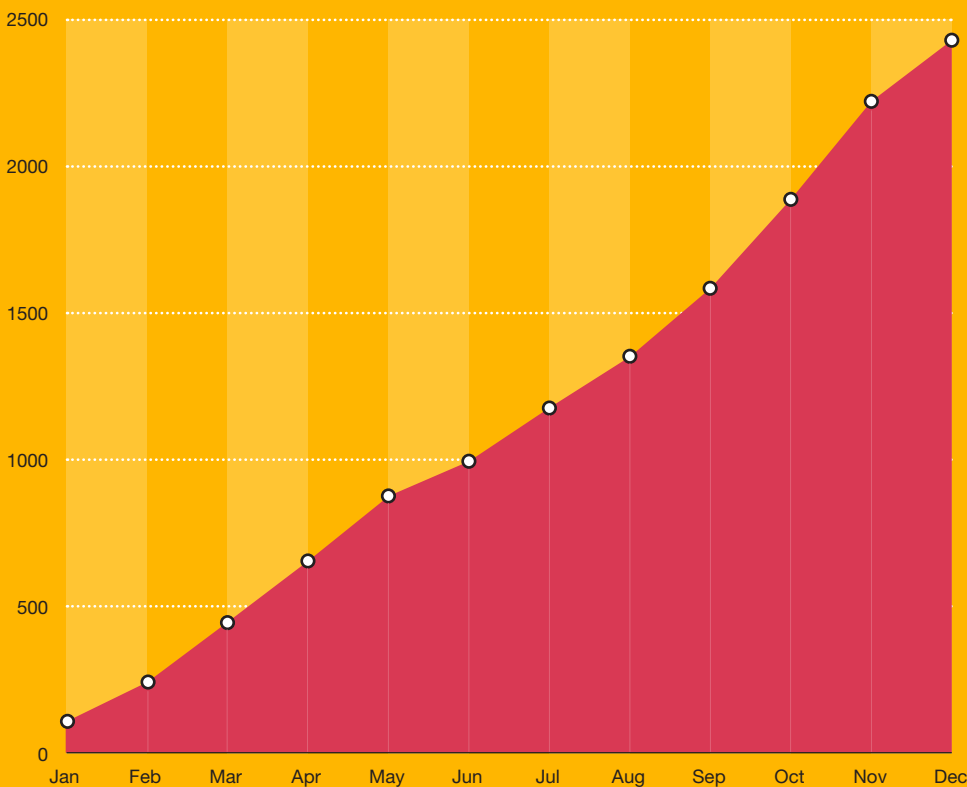
Ransomware remained the most significant cyber threat faced by most organisations in 2021. The contributing factors behind the ongoing trend remain applicable, with many amplified by the following observations:

- the number of threat actors engaged in ransomware operations increased, powered by the rise in prominence of Ransomware-as-a-Service (RaaS) arrangements and affiliate schemes;
- the pace and frequency of publicly reported attacks almost doubled; and,
- leaking of stolen data, or the threat to do so, became standard procedure for the majority of high profile threat actors adding privacy, regulatory, and reputational risks to the crisis of business disruption caused by data encryption.

The overwhelming majority of ransomware incidents were financially-motivated, with a limited set of attacks likely to have been politically-motivated and intentionally destructive.

In 2020, approximately 1,300 ransomware victims had their data exposed on leak sites. This almost doubled in 2021, with 2,435 victims exposed.

Figure 2: Running total of ransomware leaks in 2021

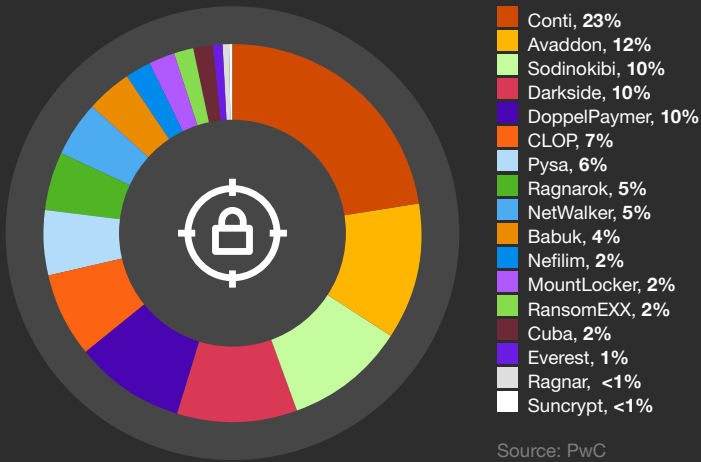


2,435

victims were exposed on leaked sites, nearly double the number exposed in 2020



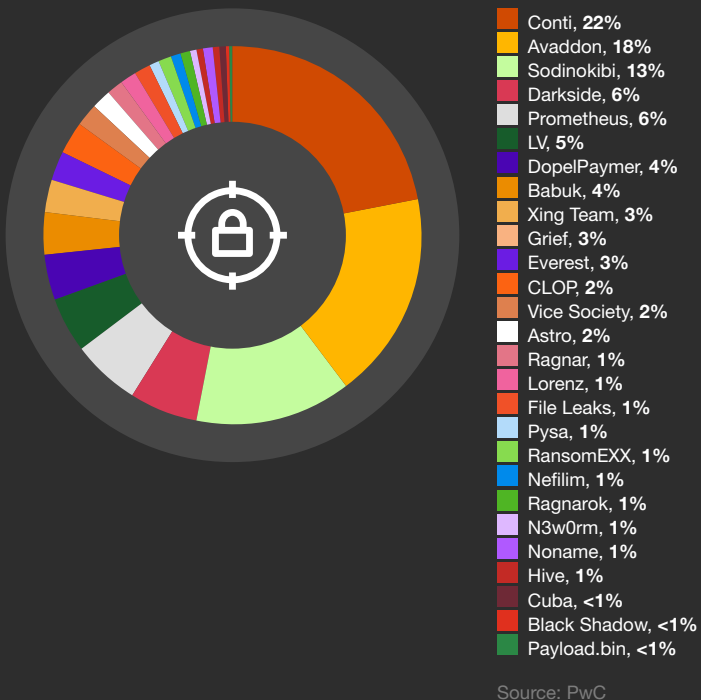
Figure 3: Ransomware incidents Q1 2021



The number of threat actors engaged in ransomware operations fluctuated, with prominent threat actors taking gaps, shutting down altogether, or re-emerging after a gap in activity under a new “brand”, as detailed in later sections. For example, in Q1 2021 PwC observed 17 threat actors leak data on approximately 440 victims, but 65% of these attacks were attributable to only five threat actors:

- White Onibi (aka Conti) - 23%
- White Dev 70 (aka Avaddon) - 12%
- White Apep (aka DarkSide) - 10%
- White Ursia (aka Sodinokibi, REvil) - 10%
- Blue Lelantos (aka DoppelPaymer) - 10%

Figure 4: Ransomware incidents Q2 2021

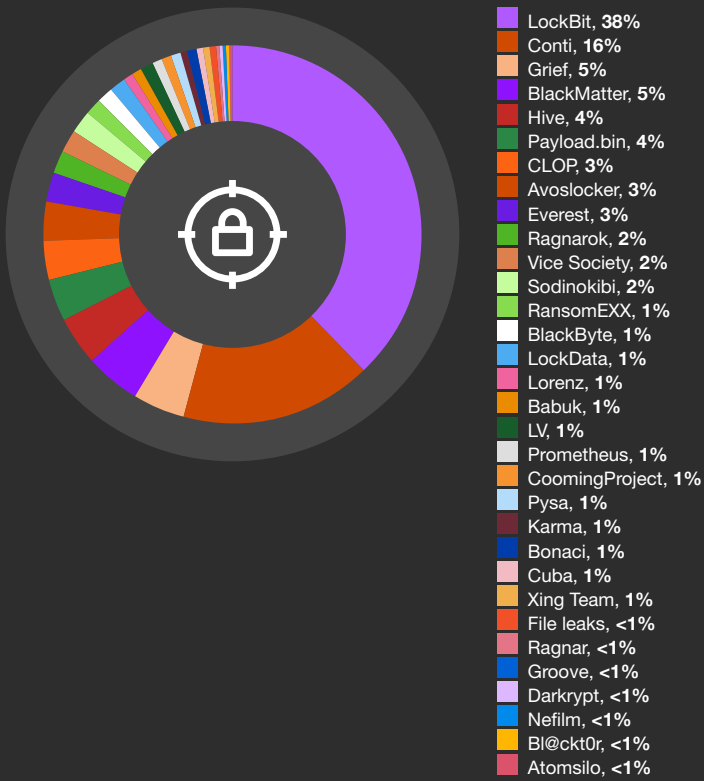


In Q2 2021, the number of threat actors observed conducting ransomware operations increased to 27, and the corresponding number of victims was over 500. However, activity was again dominated by a small number of ransomware families, with approximately 60% of incidents attributable to only four operations:

- Conti - 22%
- Avaddon - 18%
- REvil - 13%
- DarkSide - 6%

We assess that the notable reduction in DoppelPaymer operations in Q2 2021 was likely due to the threat actor rebranding its operations, before introducing the ransomware variant known as “Grief”.

Figure 5: Ransomware incidents Q3 2021

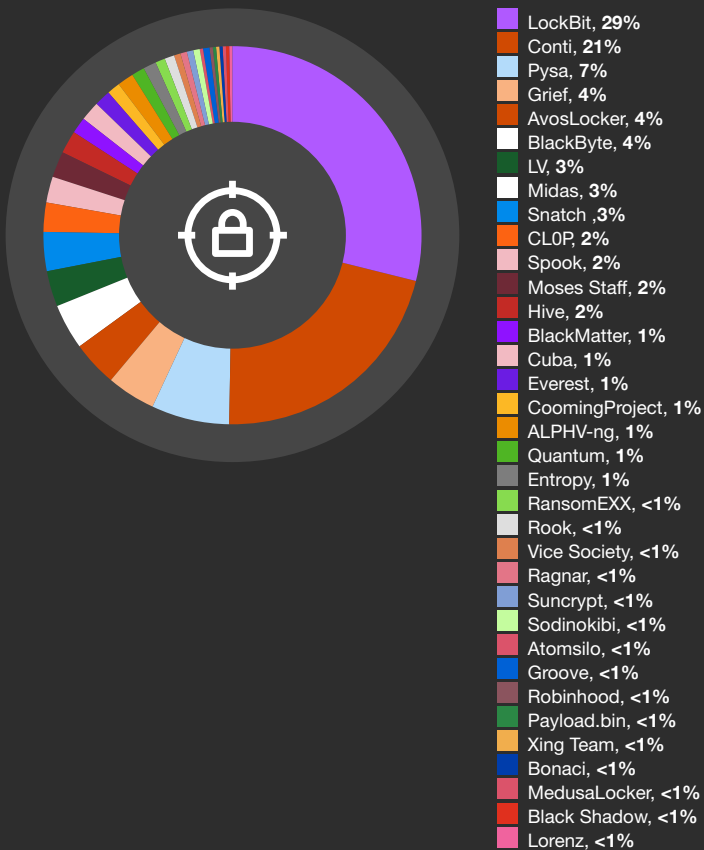


Source: PwC

By Q3 2021, significant changes in the ransomware marketplace were beginning to take effect. These were caused by the expulsion of affiliate programmes from their main recruitment sites, and the voluntary dissolution of some operations following high profile attacks. However, the most significant event impacting the ransomware marketplace during this period was the re-emergence of White Janus (aka LockBit) as LockBit 2.0 in July 2021. LockBit's original affiliate programme was inactive from late 2020 and did not re-emerge until July 2021, on the criminal forum RAMP, as White Janus reworked its ransomware.⁴⁶ The threat actor quickly established a high tempo operation, accounting for nearly 40% of observed incidents in Q3. This was likely the result of attracting affiliates from other ransomware schemes which closed down at the end of Q2 or the beginning of Q3. Overall in Q3, there were 32 threat actors leaking data accounting for almost 600 victims, with 64% of incidents again attributable to just four ransomware operations:

- LockBit - 38%
- Conti - 16%
- BlackMatter - 5%
- Grief - 5%

Figure 6: Ransomware incidents Q4 2021



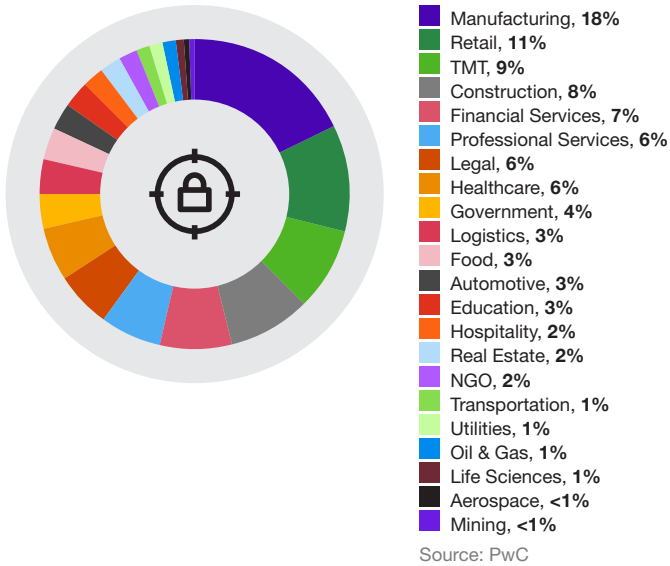
Source: PwC

In Q4 2021, the pace of attacks increased, with approximately 850 victims added to the tally of observed incidents. As with the previous quarter, the number of threat actors leaking data grew once more, with 35 leak sites active during the period. LockBit and Conti continued to dominate and 64% of observed incidents were attributable to just five actors:

- LockBit - 29%
- Conti - 21%
- White Thalia (aka Pysa) - 6%
- Grief - 4%; and,
- White Caerus (aka AvosLocker) - 4%

A spike in observed activity by Pysa was the result of an influx of data leaks on 10th November, which was more likely the result of the threat actor updating its often-neglected leak site rather than a surge in Pysa operations from that particular period.

Figure 7: Ransomware incidents by sector 2021



Sector breakdown

Ransomware operations are largely indifferent to the economic sector of organisations, although since the pandemic took hold, many threat actors have made public statements – to which they have not entirely adhered – that they would avoid targeting hospitals or other healthcare facilities. Where targeting objectives have been specified by threat actors, their focus has purely been on the size of the organisation (number of endpoints), its geographical location (with an emphasis on Canada, the EU, US, and UK) and its revenue.⁴⁷ As in 2020, few sectors were immune to attack, but some sectors experienced attacks more frequently than others, with the top six sectors accounting for 60% of all incidents noted:

- Manufacturing - 18%
- Retail and Consumer - 11%
- Technology - 9%
- Construction - 8%
- Financial Services - 7%
- Professional Services - 6%

The same top six sectors accounted for 66% of ransomware incidents in 2020.

We have not seen evidence that these sectors are specifically targeted by threat actors. However, if the healthcare sector is not included, these six sectors are a close match for the top six industry sectors by revenue in the United States.⁴⁸ For some of the most active threat actors – for example White Onibi – victim revenue is an important factor when determining whether to proceed with post-exploitation activity after initial access has been achieved. This may have some influence over the distribution of victims by sector.

60%
of all incidents noted were comprised of six sectors (Manufacturing, Retail and Consumer, Technology, Construction, Financial Services, and Professional Services)



Incident response case study:

HSE



The Republic of Ireland's Health Service Executive (HSE) commissioned a report by PwC on a Conti attack that disrupted HSE IT systems in May 2021. The HSE published this report on 10th December 2021, marking one of the first global instances of 'full disclosure' following such an incident.⁴⁹

On 14th May 2021, Conti ransomware was activated on over 3,500 workstations and 2,800 HSE servers, causing widespread and protracted disruption to healthcare services in Ireland, with some healthcare facilities unable to access patient data or schedule appointments via electronic systems. The origins of the attack dated back to March 2021, when a user opened a malicious attachment that had been delivered via email. There was a significant time gap between initial access to the network being achieved and post-exploitation activity. This was likely the result of the initial compromise being carried out by an Access-as-a-Service (AaaS) operation, before Conti assumed control of the compromised endpoint to progress the attack.

Conti is a "human-operated" ransomware system and is deployed through the manual execution of batch commands, rather than a malware that propagates through a network automatically, indiscriminately encrypting any infrastructure it encounters. The Conti operation followed known TTPs associated with the threat actor, including the deployment of Cobalt Strike to facilitate lateral movement and privilege escalation within the network; the use of other tools, including Mimikatz, to identify and compromise administrator-level accounts and systems, particularly Active Directories; and, the exfiltration of data prior to the encryption of files. The impact of the attack could have been much greater if Conti had been activated on medical systems as well as the victim's core IT estate. Many of the factors that contributed to the scale and impact of the incident are not unique to HSE. The report highlights lessons that all organisations need to consider in order to prepare for a similar cyberattack and to ensure they can mitigate and recover from one.

Affiliate programmes

Affiliate programmes continued to be a driving force behind the scale and pace of ransomware operations in 2021. Ransomware affiliate programmes generally offer access to a specific ransomware strain on a profit-sharing basis. In this scheme, a main threat actor, such as White Ursa, is responsible for the development and management of the malware, and it provides access to its affiliates, whose role is to conduct attacks. The funds extorted from victims are divided between the ransomware operators and their affiliates in pre-agreed, profit-sharing arrangements. This enables threat actors with network intrusion and exploitation skills to acquire access to ransomware and monetisation capabilities they could not easily develop themselves, reducing the barriers to entry.

Many of the most prolific ransomware operations, such as DarkSide, REvil and LockBit, openly ran ransomware affiliate schemes (Партнёрская программа); others, such as Conti, recruited “pentesters” without specifying their ultimate objectives. Affiliate programmes were mainly promoted in Russian-speaking criminal forums like Exploit and XSS. As the number and quality of affiliates (адвертов) were a defining factor in the revenue generated by many ransomware operations, competition between rival schemes intensified. Threat actors boosted their profile by:

- depositing large sums of cryptocurrency in their forum accounts, to demonstrate the financial success of their scheme;
- conducting media interviews promoting their operation’s success and revenue, many of which attracted positive coverage in the criminal forums where they recruited affiliates;
- posting links to media stories about their operations;
- offering competitive profit-sharing arrangements to their recruits; and,
- by claiming technical superiority over their competitors.

Figure 8: DarkSide affiliate recruitment advert

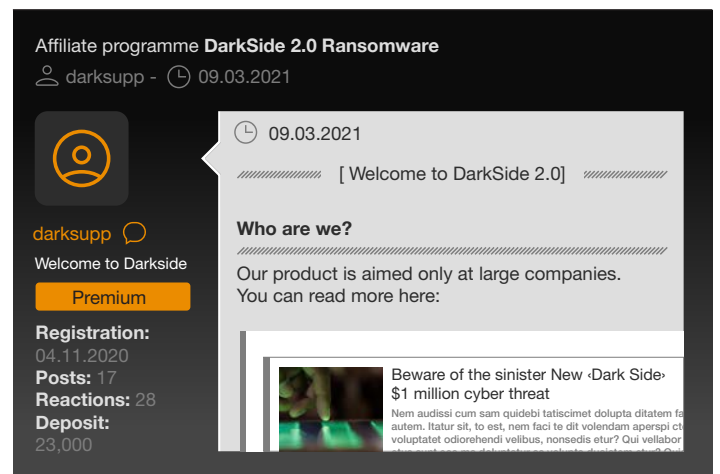


Figure 9: REvil

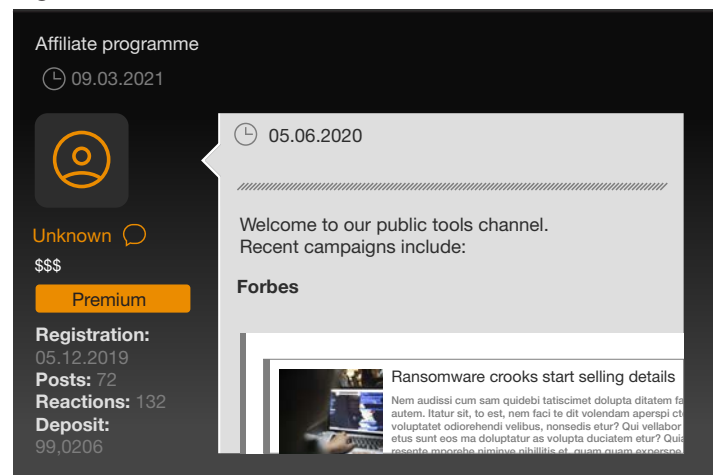


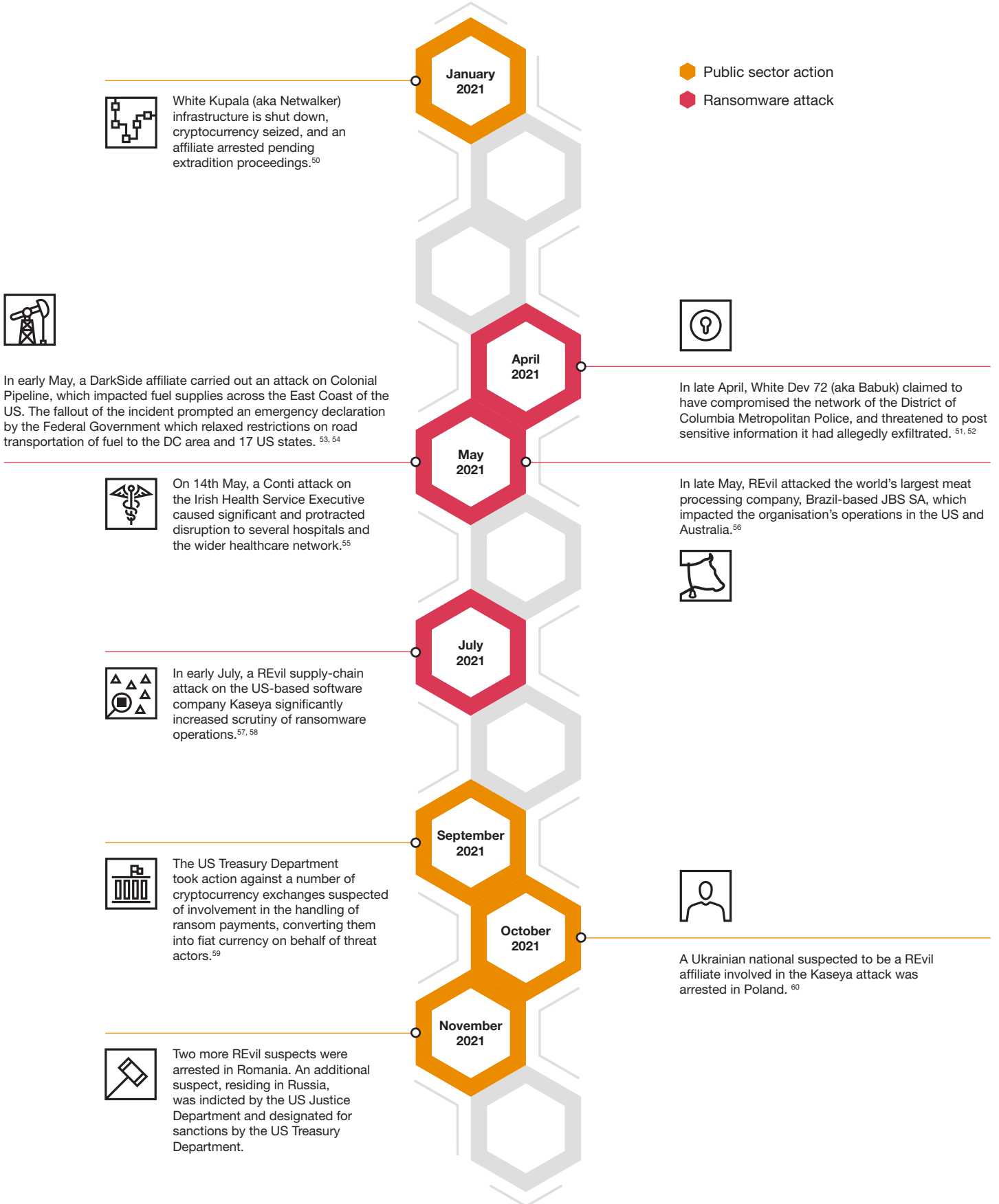
Figure 10: LockBit 2.0 advert claiming superior technical performance versus rival schemes

Encryption speed comparative table for some ransomware - 02.08.2021							
PC for testing: Windows Server 2016 x64 8 core Xeon E5-2680@2.40GHz 16 GB RAM SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 237472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	16H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec, 2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104 MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797

Getting political: legal and regulatory response

A series of incidents affecting mainly US organisations in the first half of 2021 significantly raised the profile of ransomware:

Figure 11: A timeline of high-profile ransomware attacks and public sector action



Mass expulsion of affiliate schemes

Increased focus and pressure on ransomware systems, especially as a consequence of the Colonial Pipeline incident, had an immediate impact on affiliate schemes. On 14th May, the administrators of the criminal forum XSS deleted posts relating to:

- Affiliate scheme recruitment;
- the rental of ransomware; and
- the sale of locker (ransomware) software.

Although the administrators cited several reasons for their actions, a key point was that ransomware had become “dangerous and toxic...and was being linked with geopolitics and state-sponsored attacks.” The other principal forum where affiliate schemes were operating, Exploit, also followed suit, citing similar reasons for its own ban.⁶¹

The ban on affiliate schemes did not result in an expulsion of ransomware threat actors from the forums themselves, although some did withdraw. For example, White Ursia announced that it would close its REvil affiliate scheme and “go private”; it subsequently canceled its forum memberships altogether. White Apep announced that it would shut down the DarkSide ransomware operation, and released decryption keys for the malware.⁶² However others, including White Janus (aka LockBit) retained their membership, and simply transferred their affiliate recruitment activities to their leak site.

Figure 12: XSS Administration bans ransomware activity on the site

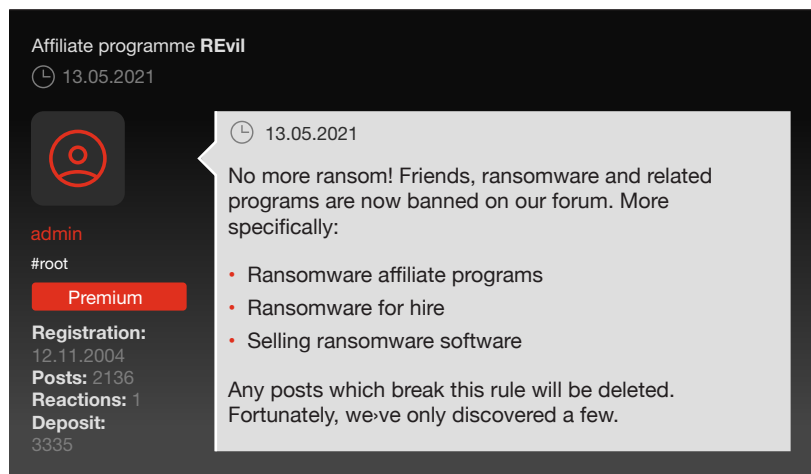


Figure 13: Exploit Administration does the same

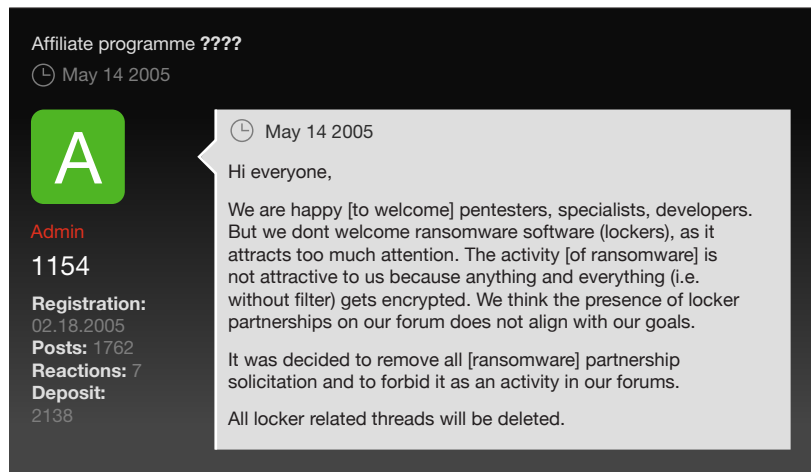
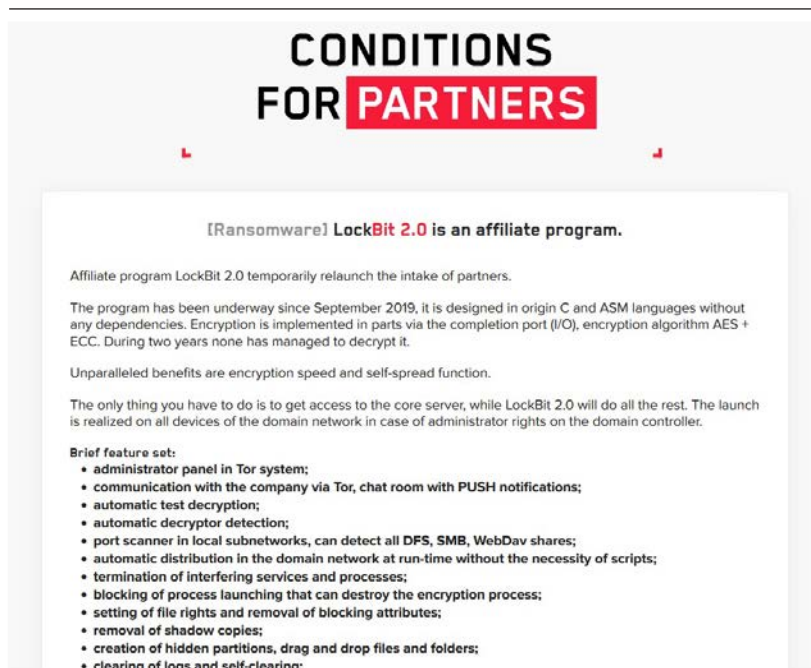


Figure 14: Affiliate recruitment advert in White Janus leak site

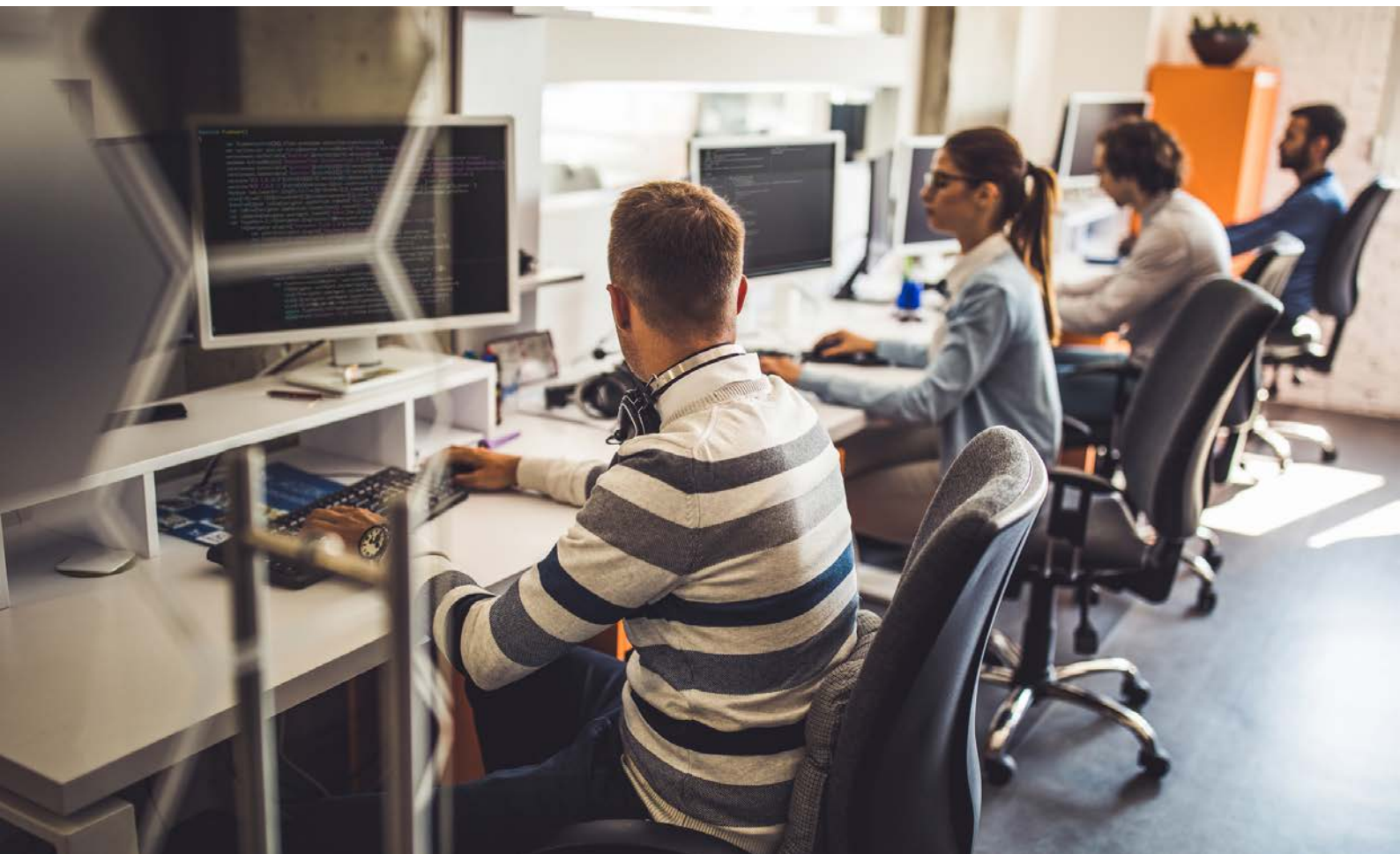


While overt affiliate recruitment schemes were the subject of the ban, the recruitment of “pentesters” continued without much disruption, with adverts in the “seeking work” or “freelance” sections of Exploit and XSS largely unaffected. The adverts did not openly state that recruitment was being conducted for ransomware operations, but the job specifications for many of the vacant positions bore similarities to previous affiliate scheme recruitment campaigns.

Figure 15: Pentester recruitment advert by unidentified threat actor



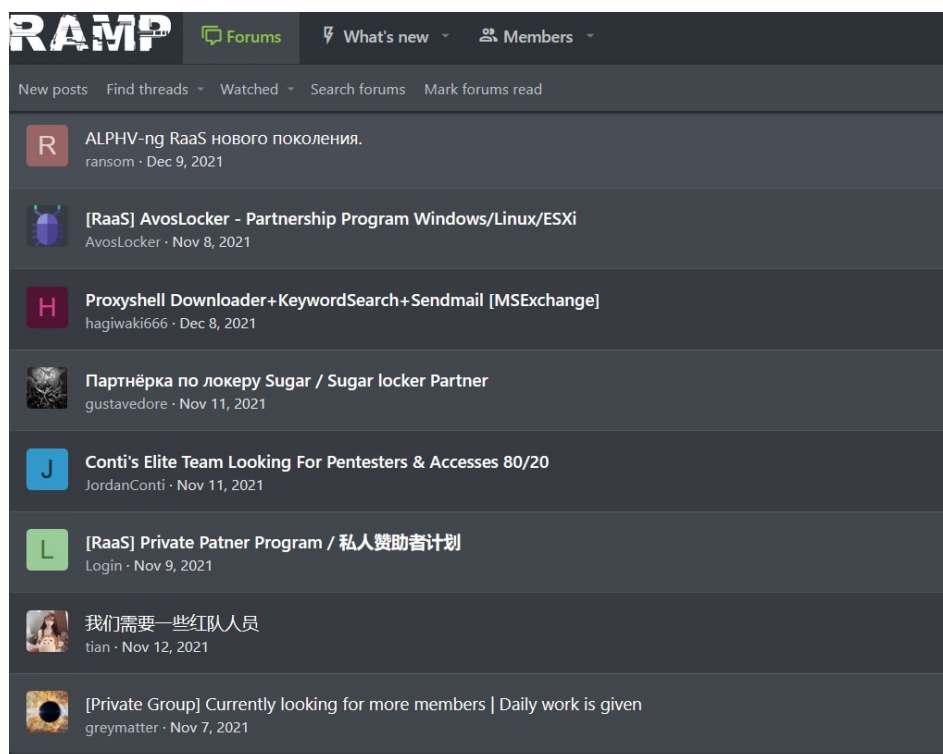
The screenshot shows a job advertisement titled "Need Pentester" posted on a platform. The ad is from a user named "kilobyte" and was posted on October 12. The job description states: "As the topic is not deleted, 1 pentester is required. Knowledge of Active Directories, Bloodhound. Experience of working with Cloud, Tape is required. Contact via private message. Salary \$5,000 to \$100,000". The ad was edited on October 25 by a user named "Seller". There are 7 views indicated by a green eye icon.



RAMPing it up

In response to the forum bans on affiliate recruitment, in mid-July a criminal forum was created that claimed to specifically cater to the needs of ransomware operations and affiliate programmes in particular. The site initially operated from the dark web address previously used by White Dev 72 (aka Babuk) for its leak site, and called itself RAMP, possibly intended as a reference to an earlier Russian-language dark web site that was involved in the sale of narcotics. The forum has a section specifically devoted to RaaS schemes as well as adverts recruiting pentesters and access to corporate networks. Prominent ransomware schemes currently active within RAMP include Conti, AvosLocker, and BlackCat.

Figure 16: Affiliate recruitment adverts on the RAMP forum



Ransomware rebranding

As another likely consequence of increasing legal and political pressure, in 2021 we observed one of the highest levels of ransomware rebrandings in recent years. Ransomware rebrands have three main benefits:

- allowing for established cybercrime threat actors to “reboot” their programme after suffering a setback. (for example, after the discovery of a flaw in their ransomware’s encryption routine results in the publication of a decrypter for the malware);
- providing an opportunity to lay low and reduce the spotlight on a specific group after a significant amount of activity or campaigns; and,
- preventing or delaying the attribution of attacks, where the threat actor perceives this to be an operational advantage.

Incident response case study:

New job, who this? Ransomware operator changes affiliate schemes



In February 2021, PwC's incident response team responded to a Sodinokibi/REvil attack on a France-based organisation in the agriculture sector. The intrusion began in mid-January, when a malicious attachment, delivered to the company's employees via a phishing email, led to the installation of QakBot on a victim workstation.

After achieving initial access, the threat actor deployed Cobalt Strike to strengthen its presence in the victim environment. It also started accessing LSASS credentials, relying on the Windows Remote Desktop Protocol (RDP) to move laterally across the network. The threat actor used a mix of BITS jobs, PowerShell and command-line interaction to install and execute payloads and fingerprint the network. RClone, open source software used to manage content on cloud storage systems, was used to exfiltrate data from the victim's local and cloud storages, before the ransomware was detonated.

Although the threat actor ultimately deployed Sodinokibi/REvil ransomware, the way it operated within the victim environment aligned more closely with techniques known to be adopted by affiliates of another ransomware programme which PwC tracks as White Samyaza (aka Egregor, Prolock). For example, while QakBot has also been observed leading to REvil infections⁶³, it is more strongly linked to White Samyaza operations⁶⁴. The command-line tool RClone is frequently, though not exclusively, used by Egregor/Prolock operators, particularly with the utility being renamed as "svchost.exe" to blend in with the victim environment⁶⁵. Additionally, the ransomware files observed during the incident response were labeled using the victim's name. This naming scheme is a characteristic unique to Egregor ransomware and is not typically observed in Sodinokibi/REvil ransomware (whose files are often named using a random naming scheme).



Based on the evidence we examined, we assess it is highly likely that an affiliate of White Samyaza moved to White Ursia, and deployed Sodinokibi/REvil using TTPs commonly observed with White Samyaza affiliates.

Blue Lelantos

In December 2019, members of the Russia-based crime group “Evil Corp” (tracked by PwC as Blue Lelantos) were indicted by US authorities and designated for sanctions.⁶⁶ Evil Corp operations continued throughout 2020, but changes to Evil Corp operations became apparent by the end of that year and increasingly noticeable in early 2021. Detections of WastedLocker,⁶⁷ one of Evil Corp’s principal ransomware systems, all but disappeared in late 2020. However, the WastedLocker operation continued throughout 2021, through a succession of rebrands. In late 2020, WastedLocker ransom notes began appearing as Hades ransomware, Phoenix Cryptolocker in March, Payloadbin in June, and Macaw in October.⁶⁸ Similarly, DoppelPaymer,⁶⁹ Evil Corp’s high profile “double extortion” operation, effectively ceased operations in May, with the last victim added to its leak site that month. In June, a new ransomware calling itself “Grief” or “PayorGrief” emerged and began posting victim data on its leak site from the outset. Analysis of Grief samples revealed extensive coding similarities between it and DoppelPaymer, with a major change being Grief’s use of the cryptocurrency Monero for ransom payments. We assess that Grief is yet another rebranding exercise by Evil Corp, and is unlikely to be its last.⁷⁰

Although we have no direct evidence of the reasons for the successive rebranding exercises undertaken by Evil Corp in 2021, we assess it is highly likely that these are a consequence of the group’s designation as a sanctioned entity by the US authorities:

- As with most ransomware operations, the majority of its victims are in the US;
- An organisation making or facilitating a ransom payment to a sanctioned entity would potentially place them in breach of US sanctions and therefore less likely to pay;
- Rebranding WastedLocker and DoppelPaymer made it more difficult, in the short term at least, to attribute a ransomware incident to a sanctioned entity; and,
- Rebranding existing code, rather than writing new ransomware variants from scratch, reduces Evil Corp’s opportunity costs and the time required to maintain its ransomware operations.

Figure 17: “Welcome to Darkside 2.0” announcement post

White Apep

DarkSide (aka BlackMatter), which PwC tracks as White Apep, has been in operation since at least August 2020, and had already undergone two rebrandings by the close of 2021. The first came in January 2021, two months after the launch of DarkSide’s affiliate programme, when security company Bitdefender developed and publicly released a decryption tool⁷¹ allowing DarkSide victims to recover their files. White Apep operations went on hiatus, likely to allow the threat actor to retool, and only resumed on 9th March 2021 under the rebranded banner of “DarkSide 2.0”. Its return was accompanied by a relaunch of its affiliate programme, and featured an updated version of the ransomware designed to avoid decryption by the existing tools.⁷²

It was after this first rebranding that one of DarkSide’s affiliates conducted one of the most damaging incidents observed in 2021, the successful attack on US-based Colonial Pipeline on 7th May. The attack led to a shutdown of operations on its 5,500 mile pipeline, used to supply almost half of the US East Coast’s fuel. Increased focus on DarkSide by the US government, and a subsequent infrastructure takedown, led the threat actor to announce in mid-May that it would be shutting down operations.⁷³

White Apep's second rebranding came in late July, in the form of a new RaaS system titled "BlackMatter". The new ransomware shared parts of its code, though not all, with DarkSide 2.0; these included code routines implementing privilege escalation, victim fingerprinting, and networking capabilities.⁷⁴

Growing pressure from law enforcement led to White Apep once again announcing its departure from the ransomware scene in November 2021. The decision was shortly followed by the US Justice Department announcing a US\$10m reward for any potential information on the group.⁷⁵ At the end of 2021, White Apep operations remained inactive. However, given the number of transformations White Apep's ransomware and overall operations have undergone, we assess that there is a realistic probability that this shutdown of operations is a chance for it to remain under the radar, only to re-emerge with yet another rebrand. There is circumstantial evidence that ALPHV-ng (aka BlackCat), which is currently tracked by PwC as White Dev 101, is yet another rebrand. The threat actor's affiliate scheme was launched on RAMP on 9th December 2021, and PwC's incident response team has responded to multiple BlackCat incidents conducted by a specific affiliate who was previously part of the BlackMatter scheme.

White Ursia

White Ursia was one of the most active ransomware threat actors in the first half of 2021. The public face of its operation, using the online identities 'UNKN' and 'Unknown' on Exploit and XSS respectively, maintained a high profile, conducting interviews and promoting REvil's affiliate programme. It is likely that mounting pressure on White Ursia,

after it found itself the subject of greater scrutiny following the Kaseya and JBS attacks, initiated its first offline move in 2021. 'UNKN' had already announced the decision to "go dark" following the expulsion of affiliate programmes from XSS and Exploit in May. White Ursia's "Happy Blog", the leak site used to publish compromised victim data, went offline in mid-July, as did its ransom payment infrastructure. REvil operations ceased and 'UNKN' no longer posted comments on XSS or Exploit after 4th July. The shutdown of REvil's payment infrastructure, as well as the disappearance of 'UNKN' damaged the reputation of the threat actor.

In September new online personas – 'REvil' on Exploit and '0_neday' on XSS – announced that, following 'UNKN's' disappearance, they had been able to restore REvil operations from backups. White Ursia resumed operations and posted data on six victims between 10th September and 14th October, before the site went down again, this time probably for good. '0_neday' claimed to have lost control of REvil infrastructure following a suspected cyberattack targeting the threat actor personally and had decided to lie low. On 14th January 2022, the FSB announced that they had detained 14 suspects and searched 25 premises connected with an investigation into the REvil operation.⁷⁶ Although at least some of the arrests occurred in early 2022, it is a realistic probability that elements of the REvil operation had been disrupted by the Russian authorities prior to the action taken in January 2022. Several criminal threat actors in XSS speculated that UNKN's disappearance in July and subsequent "radio silence" was also the result of FSB action. However, it is impossible to verify these claims.



Supply chain compromise: the new normal

Supply chain attacks have long been a tried and tested formula used by multiple threat actors. While they are traditionally associated with state-sponsored threat actors, financially motivated threat actors have also been successful in exploiting them. In early 2021 White Austaras (aka TA505), the threat actor in control of CL0P ransomware, was able to compromise multiple organisations that were using the legacy file transfer software Accellion FTA. White Austaras exfiltrated data from fewer than 25 victims, and threatened to expose it on the CL0P leak site if a ransom was not paid.^{77, 78}

In July 2021, White Ursia compromised multiple organisations that were clients of Kaseya, a US company specialising in network and IT management software, by abusing the company's VSA software to deliver malicious payloads. The attack was on a much greater scale than the Accellion incident, with as many as 1,400 organisations affected by REvil/Sodinokibi ransomware.⁷⁹

```

mirror_mod = modifier_ob.modifiers.new("mirror_ob")
mirror_ob = mirror_ob
mirror_ob.mirror_object = mirror_ob

operation = "MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
mirror_mod.use_z = False
operation = "MIRROR_Y":
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
operation = "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True

selection at the end -add back the deselected
mirror_ob.select= 1
mirror_ob.select=1
context.scene.objects.active = modifier_ob
selected = "selected" + str(modifier_ob) # modifier
mirror_ob.select = 0
key=context.selected_objects[0]
objects[one.name].select = 1

print("please select exactly two objects,
OPERATOR CLASSES -----

```

Delivery and access

Delivery systems

Malware delivery systems have proven to be a vital companion to ransomware threat actor arsenals. These are pieces of software specifically designed to house malicious payloads, which are later dropped by the threat actor to gain an initial entry onto a target system or network. In 2021, with both established players and new entrants active in the malware delivery market, cyber criminal threat actors had the option to flit between several and determine the most reliable and dependable option for their operations.

Emotet

Emotet, which PwC tracks as White Taranis, is one of the most prominent and long-running malware delivery systems. Early 2021 saw an international law enforcement takedown, named Operation LadyBird, of Emotet's botnet infrastructure. The operation, which saw over 700 devices used for Emotet's C2 systems seized, alongside arrests made in Ukraine,^{80, 81} impeded the threat actor from conducting its malicious spam and spear phishing email campaigns for a significant portion of the year.

However, in mid-November PwC observed Trickbot, the banking trojan operated by the group PwC tracks as White Magician, delivering malicious Emotet binaries to infected Trickbot machines, and executing them in memory. This was likely an attempt by the threat actor to help restore Emotet's command and control infrastructure. This technique is in line with similar activity associated with White Taranis, where Emotet was used as a means to help deliver Trickbot binaries after a similar takedown of Trickbot occurred in October 2020.

Alongside the delivery of Emotet binaries and the return of its command and control infrastructure, we also saw the introduction of two new spam delivery botnet servers, Epoch

4 and Epoch 5. This added to the three other botnet servers, Epoch 1, Epoch 2, and Epoch 3, which were previously used by White Taranis to infect machines. Further updates were also observed to Emotet's encryption capabilities, used to encrypt network traffic, and to its communication protocols.⁸² These additions to Emotet's arsenal underscore the significant capabilities that White Taranis has access to, and the continued threat it poses to organisations.

The absence of Emotet during most of 2021 saw a significant proportion of its client base forced to look at other forms of malware delivery. In 2021, malware delivery systems such as Buerloader, Bazar, SquirrelWaffle, and IcedID all significantly increased their activity, which was likely the result of the gap Emotet left following its takedown.

Colder than IcedID

The threat actor that PwC tracks as White Khione is behind the malware delivery system IcedID (aka Bokbot), which is associated with high profile ransomware systems such as Conti and Sodinokibi/REvil. First identified in 2017, IcedID was originally developed as a banking trojan, capable of stealing financial information. However, similar to other banking trojans, IcedID was later repurposed as a piece of modular malware designed to provide remote access to networks, which would later be sold to other users as part of the "Access as a Service" model.⁸³ In 2021, IcedID stepped up its capacity in Emotet's absence, proving one of the most consistent malware delivery systems. Its core capability lies within its consistent email spam campaigns, which are used to initiate the infection chain. Further capabilities include remote code execution and web browser injection, which enables IcedID to perform person-in-the-middle attacks with the intended goal of extracting financial information. However, IcedID is typically used to deploy further-stage payloads such as Cobalt Strike.

Access as a Service (AaaS)

Delivery systems, like Emotet and IcedID, have consistently been the choice of initial access for many cyber criminal threat actors. However, their availability and accessibility can be unreliable, with some systems being forced offline, while others require a long standing relationship in order to gain access to the malware delivery services. This has provided leeway for the Access as a Service (AaaS) marketplace to grow in 2021. These marketplaces allow the buying and selling of access to compromised hosts from a wide range of organisations and sectors, usually in the form of RDP and VPN access, as well as webshells. Various Russian-language criminal forums such as Exploit and XSS, and dedicated marketplaces such as Odin and MagBo, are used to advertise access listings.⁸⁴

A primary driver behind the rise in AaaS is the lower barrier of entry it provides for new threat actors. AaaS removes the need for threat actors to conduct complex intrusion or widespread phishing campaigns to gather credentials. With AaaS, the initial intrusion has already been completed, enabling the purchaser to transition straight into post-exploitation activity and ransomware deployment. In 2021, we witnessed several prolific ransomware threat actors or their affiliates making use of AaaS as a means of initial access, including White Janus (aka Lockbit 2.0) and White Apep (aka BlackMatter, DarkSide).

Figure 18: White Apep seeking access to corporate networks on the forum Exploit

Affiliate programme **BlackMatter**
 10.07.2021

BlackMatter
 Byte

B

Seller

Registration:
 07.19.2021
Posts: 3
Activity: Other
Deposit:
 4.000000

10.07.2021

Looking for corporate networks in the following countries:

- USA
- CA
- AU
- GB

=====

All sectors except:

- Medical
- State institutions

=====

Requirements:

- Zoom revenue from \$100 million
- 500 - 15,000 hosts
- We do not take networks which someone has already tried to exploit

=====

2 options for work:

- Buy: from 3 to 100k
- We take it to work (to be discussed individually)

=====

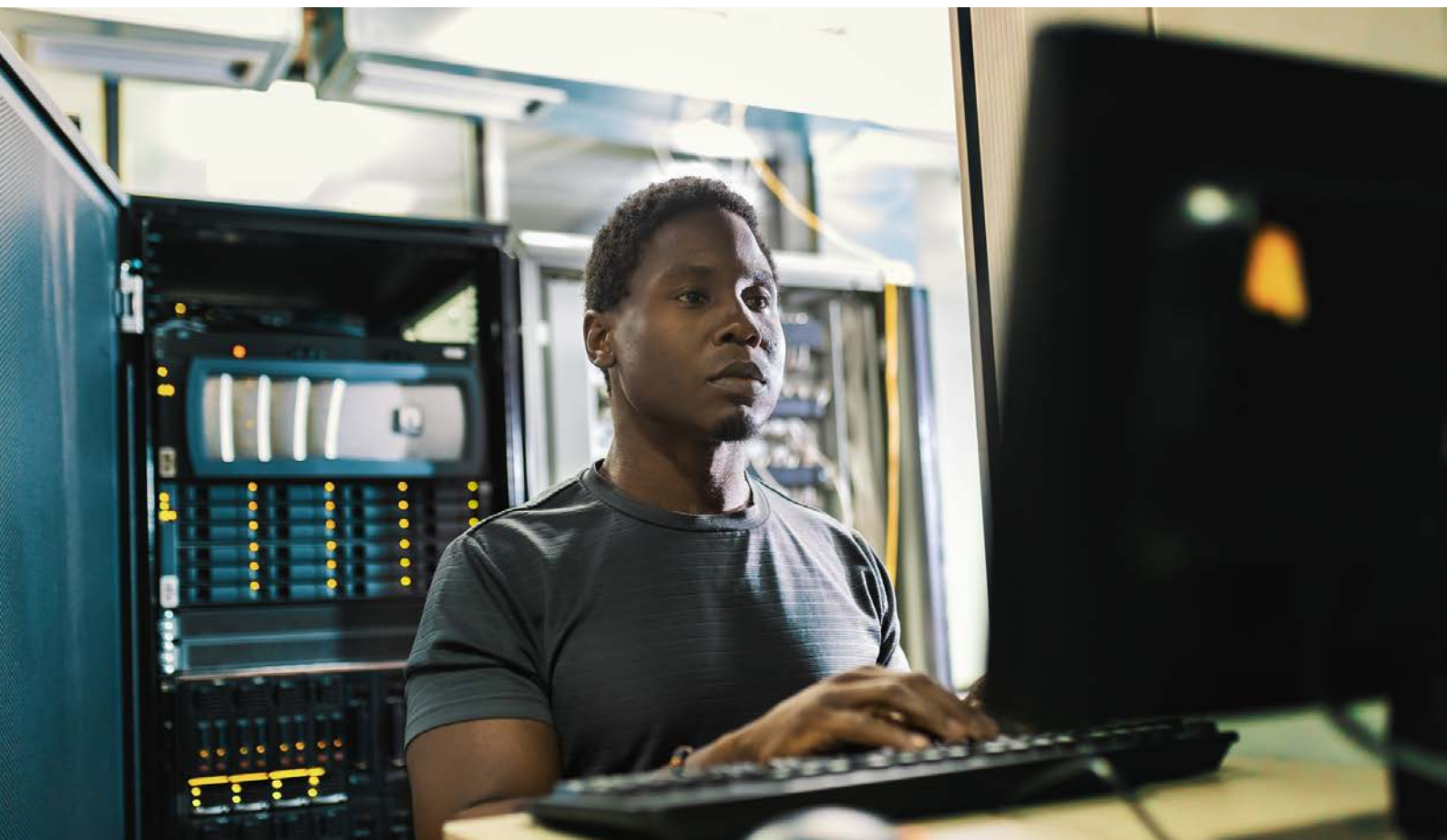
Work scheme:

- Choice of work option -> Transfer access
- > Verification -> We take it or not (in case of discrepancy)

=====

Deposit:

- 120k



Regional

activity

In this section, we describe campaigns conducted by the threat actors we believe to be based in specific geographic regions and ranging from intelligence-gathering operations (in support of political and/or national strategic objectives) to financially-motivated activity: both targeted and opportunistic. As in 2020, we continued to see the cyber threat landscape aligning with geopolitical circumstances, with real-world events influencing espionage- and sabotage-motivated operations alike. As in 2020, we continued to see the cyber threat landscape aligning to the geopolitical situation, with real-world events driving espionage and sabotage-motivated operations alike.



Asia-Pacific



Hard drive to survive

In North Korea, a centrepiece of Kim Jong-un's political doctrine is the country's continued development of its nuclear force, accompanied by a focus on national finances. Overall, cyber operations have highly likely been one of the North Korean state's main avenues for thwarting the impact of international sanctions and achieving its strategic objectives. Cryptocurrency in particular is a crucial source of income for North Korea's regime, with multiple North Korea-based threat actors targeting organisations and individuals involved with cryptocurrency, particularly cryptocurrency exchanges, since at least 2017.⁸⁵

Bitcoin is silver, compromise is gold: the newest North Korea-based threat actor(s)

Throughout 2021, we observed two main clusters of activity that we assess were highly likely conducted by North Korea-based threat actors, and which targeted entities dealing with cryptocurrency and the financial sector on an international scale. We initially tracked these two clusters separately, respectively as Black Alicanto (aka Dangerous Password, LeeryTurtle, CryptoMimic, CryptoCore, Operation SnatchCrypto)^{86, 87} and Black Dev 2 (aka Operation Gold Hunting, Operation SnatchCrypto). Ultimately, overlaps in capabilities, infrastructure, and victimology led us to assess that Black Alicanto and Black Dev 2 are likely to be the same North Korea-based threat actor. We further assess this threat actor to be highly likely an evolution of 'Black Artemis' (aka Lazarus Group, HIDDEN COBRA) financially-motivated subgroup Bluenoroff.

Below, we present Black Alicanto and Black Dev 2 individually to give an overview of the differing TTPs that we associated with the two clusters of activity.

Black Alicanto

Black Alicanto is financially-motivated, and has been active since at least 2018, targeting cryptocurrency organisations and entities in the financial services sector. While this threat actor often used lure documents themed around employee promotions or bonuses to induce targets into opening the payload, between September and December 2021 we observed Black Alicanto using lure documents presenting job descriptions for roles in companies in the finance and cryptocurrency sectors, including Goldman Sachs, J.P. Morgan, Commerz AG, SALT Lending, and Blockchain Intelligence Group.⁸⁸

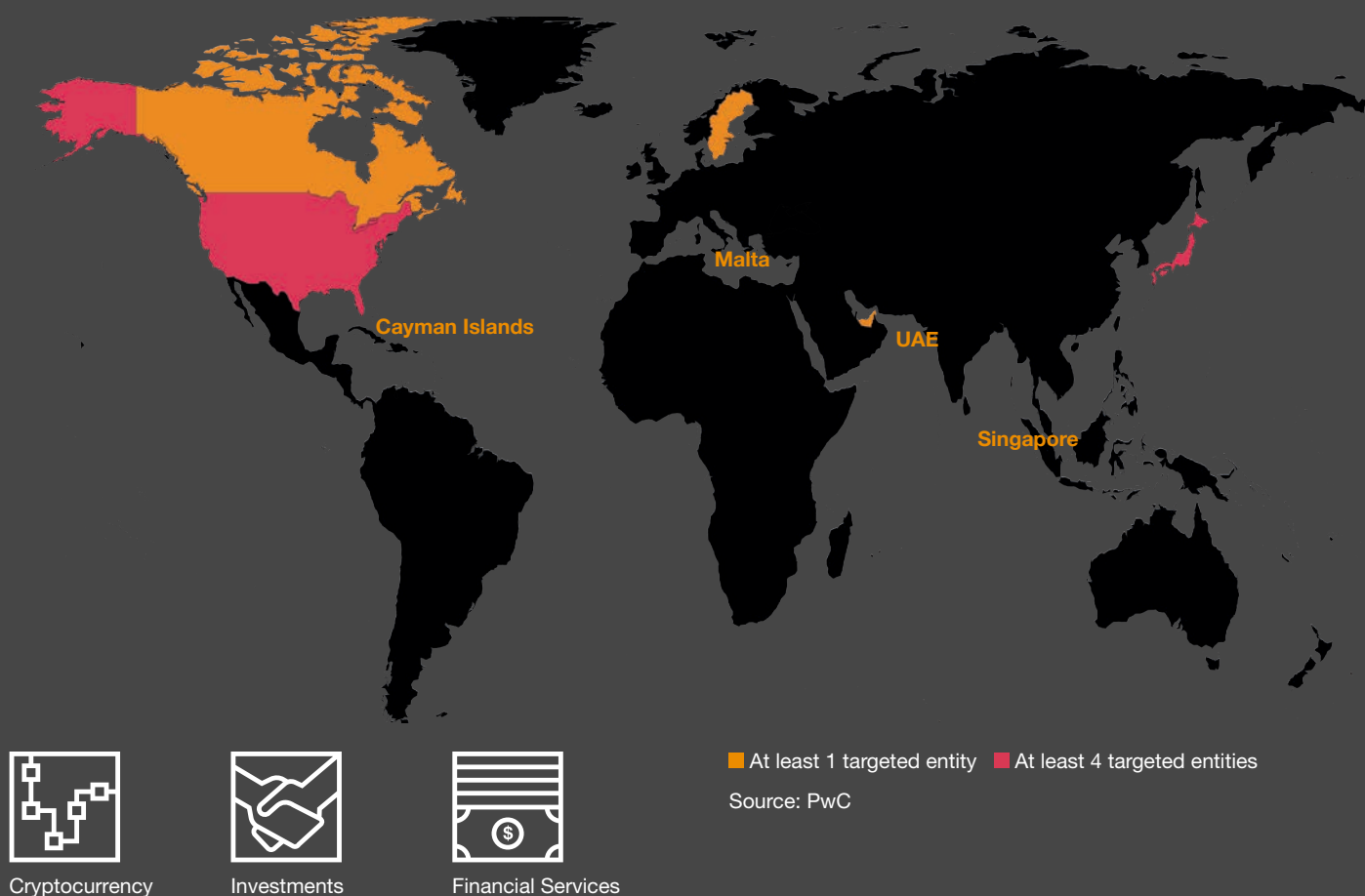
Black Alicanto initially sends targets spear phishing emails with attached compressed archives. These typically contain double-extension documents (.LNK files masquerading as Word or PDF documents) or, password-protected lure documents and malicious LNK files called Password.txt.lnk. The link files abuse Bit.ly URL-shortened links to lead the target to download malicious scripts from domains registered by the threat actor. Black Alicanto is careful to ensure that only actual targets, as opposed to security researchers, receive its payloads, and manually deploys later-stage payloads only to those.

One such payload is msoRAT^{89, 90}, a remote access trojan (RAT) that Black Alicanto manually deploys on victim systems of particular interest. msoRAT is an evolution of a backdoor that has been used for years by BlueNoroff.^{91, 92}

Black Dev 2

Since at least August 2020, we tracked a cluster of activity that we initially referred to as Black Dev 2⁹³, primarily targeting entities in the cryptocurrency and financial technology (FinTech) space, as well as venture capital (VC) firms, particularly ones funding cryptocurrency- and technology-related ventures.

Figure 19: Geographic distribution of entities targeted by Black Dev 2



The intrusions we associated with Black Dev 2 typically involved lure documents themed around a venture capital presentation or company pitch, or around non-disclosure agreements. The lure documents fetched a malicious remote template from a threat actor-registered domain. The remote template's macros would download a further payload – typically a malicious backdoor and victim profiler dynamic link library (DLL) - to be injected into another running process.

In timelining the creation and last modification times of malicious documents created by Black Dev 2, we identified a pattern matching that of an average working day, starting at around 8am and trailing off at around 6pm with a one or two-hour lunch gap in the middle, matching the GMT+9 timezone, which includes North Korea.

We also observed Black Dev 2 using a malware family that is likely a variant of msoRAT, on infrastructure overlapping with other msoRAT C2 servers used by Black Alicanto.⁹⁴ Based on the similarity in infrastructure setup and intrusion chains adopted by Black Dev 2 and Black Alicanto, and their common victimology, we assessed it likely that Black Dev 2 and Black Alicanto are the same North Korea-based threat actor, and an evolution of Bluenoroff.

Complementary missions

Beyond the imperative to continue generating funds for the regime, established North Korea-based threat actors have continued pursuing targets aligned with North Korean strategic objectives.

Black Banshee

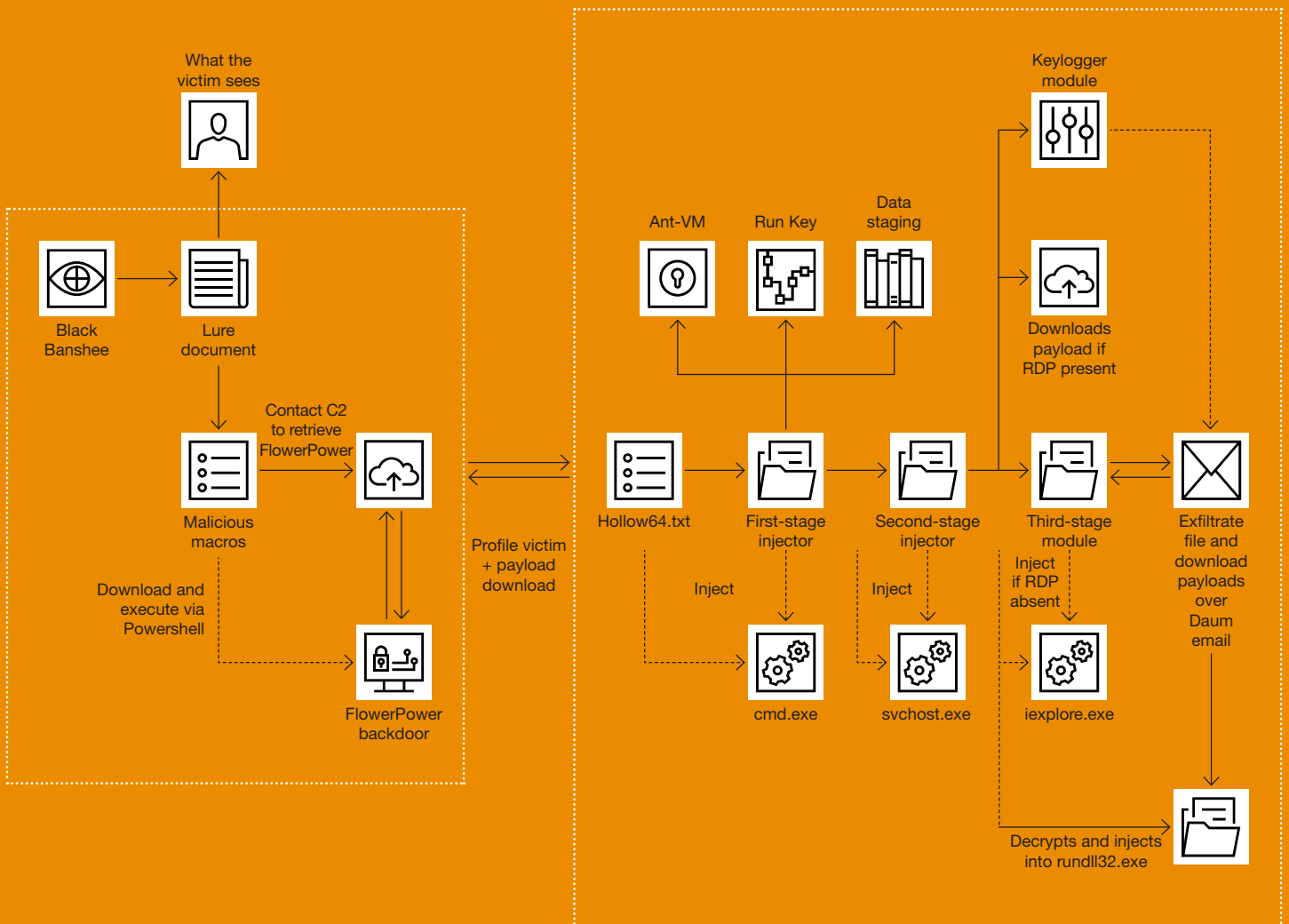
In 2021, Black Banshee's (aka Kimsuky, Velvet Chollima) core sectors of interest remained in line with the threat actor's historic targeting, and included:

- government and public sector;
- diplomacy and policy, including think tanks;
- academia (with particular attention to nuclear research and international policy);
- defence and aerospace;
- nuclear; and,
- targeting of civil society and specific groups such as journalists, NGOs, and religious groups active in relation to North Korea.

The BravePrince update

In 2021 we observed Black Banshee maintaining its focus largely on these priorities, and revamping tools from its previous arsenal in pursuit of its regional targets. For example, Black Banshee developed an updated version of its BravePrince backdoor, and used it to target South Korean victims.⁹⁵ The BravePrince backdoor acts as a victim profiler, keylogger, and information stealer, exfiltrating victim data over the South Korean email service Daum. The backdoor also has the ability to exfiltrate specific files of interest to Black Banshee, suggesting not only direct operator interaction with the implant, but also that the threat actor deployed the backdoor specifically to targets of interest. The campaign focused on South Korean entities; it likely aimed to attain diplomatic, political, and military intelligence about South Korea's stance in relation to North Korea, China, and Russia, as well as the United States. An update about this campaign published in November 2021⁹⁶ also detailed targeting of aerospace and defence material, as well as scientific research in specific fields such as aviation fuel.

Figure 19: Steps of a Black Banshee intrusion chain involving the BravePrince backdoor



Nuclear policy for BabySharks

Black Banshee also continued to run BabyShark campaigns for the most part of the year⁹⁷, maintaining its long-standing focus on nuclear, policy, and diplomacy topics. We identified and notified at least eight victims who Black Banshee had compromised since August 2021. These included diplomatic figures; current or former senior analysts at think tanks focused on the Asia-Pacific region; senior academics focusing on Asia-Pacific history, policy, and defence; and, employees at NGOs focused on the Korean peninsula. This targeting also aligned with previous campaigns operated by Black Banshee since at least late 2018, when we first observed the threat actor starting to target individual figures working at supranational organisations including the United Nations.

Black Artemis

Black Artemis (aka HIDDEN COBRA, Lazarus Group) continued heavily targeting the aerospace and defence sectors as part of a campaign that we track as ShowState.⁹⁸ The campaign persisted in 2021, relying on social engineering and spear phishing documents themed around job opportunities for aerospace and defence, expanding to include engineering and manufacturing companies.⁹⁹

A different campaign by Black Artemis in 2021, which targeted South Korean entities, also involved malicious documents with macros being used to achieve initial access. However, in this set of intrusions, the macros would drop to disk a PNG image containing malicious data in compressed format, making it harder to detect statically by antivirus software. The macro would then convert the PNG image to a BMP file, and execute it via mshta.exe. The embedded executable payload, a malware family we have called PaintJob¹⁰⁰, shares similarities with the encryption routine used by Dtrack, a well-known RAT which we attribute to the Black Artemis subgroup known as Andariel.

Black Artemis also persistently targeted offensive security and vulnerability researchers throughout the past year. In January 2021, Google¹⁰¹ and Microsoft¹⁰² reported a months-long social engineering campaign relying on Twitter profiles posing as security researchers, as well as on accounts on LinkedIn, Telegram, Discord, and Keybase. Black Artemis would reach out to targets under the false pretense of collaborating on a vulnerability research project. It would then send them a Visual Studio Project backdoored with malicious code executing the Comebacker dropper, that would ultimately lead to the installation of the Klackring backdoor.

The threat actor also maintained a security blog acting as a watering hole, and would direct targeted security researchers to it during conversation. When the targets visited the site, a 0-day Chrome exploit would lead to a malicious service being installed on their machine, together with an in-memory backdoor. Black Artemis could then exploit the access it had gained to security researcher systems to identify and steal offensive security research of interest.

A parallel effort by Black Artemis included specific targeting of Chinese offensive security researchers with Chinese-language malicious lure documents.¹⁰³ Compromise attempts against security researchers also involved a trojanized version of IDA Pro¹⁰⁴ - disassembly software widely used in cybersecurity research and particularly in vulnerability analysis and exploit development.

A year of China-based threat actor activity

Planning ahead

We have continued to observe significant China-based threat actor activity. Some of these threat actors, like Red Djinn, are focusing on specific industry sectors such as semiconductors, artificial intelligence, healthcare (which includes genetic research and biotechnology), quantum computing, and exploration across space, maritime, and polar arenas.¹⁰⁵ Others like Red Kelpie are pursuing (and in some instances enabling others to conduct) significantly broader targeting.

Beyond economic strategic objectives, we also continued to observe espionage-motivated activity focused against the public sector; Red Vulture (aka Ke3chang, APT15, APT25, NICKEL) and Red Keres (aka APT31, ZIRCONIUM) are both prominent examples of this kind of targeting focus.

Red Djinn

The China-based threat actor that we track as Red Djinn (aka BlackTech, Mobwork, Palmerworm) remained active in 2021, using known tools (such as PLEAD and TSCookie), and new ones (such as Consock, FlagPro and SpiderRAT).

In early 2021, we observed a series of Red Djinn campaigns using malware families known as PLEAD and TSCookie, including Linux variants of both backdoors to widen the variety of systems it could target. The targeting of these campaigns was on organisations based in parts of Asia, and included an IT and telecommunications company. The threat actor registered domains themed around cloud and VPN technologies, and the malware families contained campaign IDs likely indicating the targeting of the manufacturing and engineering sectors.

New Djinn

While Red Djinn has historically and consistently focused on targeting Asia’s largest economies, we have also previously observed broader targeting by the threat actor. For example, the threat actor previously targeted an overseas subsidiary of a managed service provider (MSP) to perform an ‘island-hopping’ attack to laterally move to the MSP’s main network.

Through our tracking of Conssock^{106, 107}, a custom Gh0stRAT variant associated with Red Djinn (also known as Gh0stTimes) we were able to identify the malware’s controller.

Figure 20: Times.exe, the controller for Red Djinn’s Conssock malware

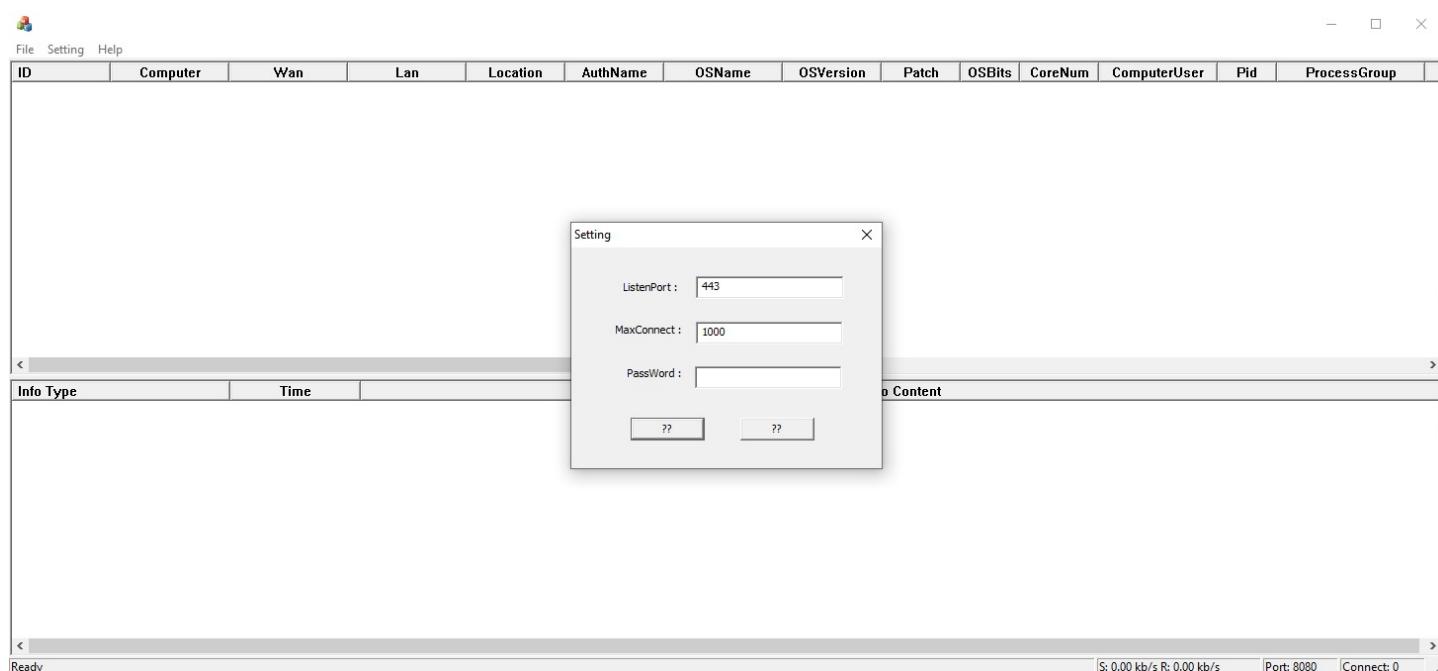
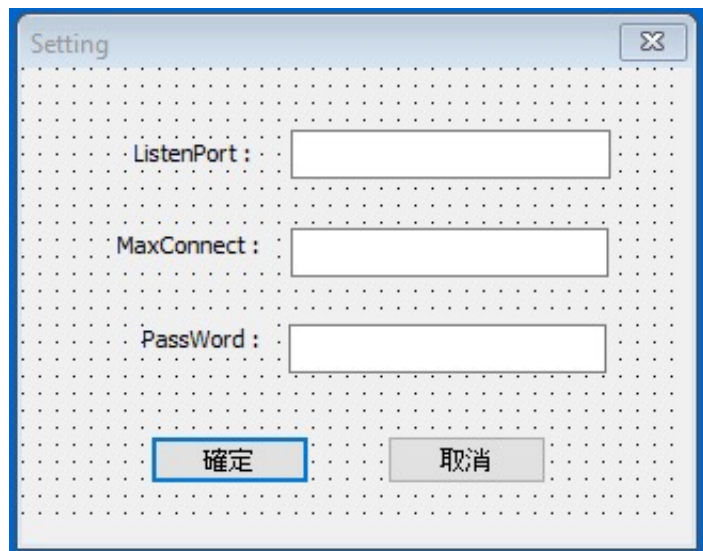


Figure 21: Times.exe was originally designed for Chinese-language systems



We also uncovered spear phishing lures used by the threat actor to deliver both Conssock, and also a new malware family which we named Flagpro.¹⁰⁸ We assess that Red Djinn highly likely used Flagpro in its targeting of the subsidiary of a Japanese IT Services provider and software developer operating across East and South Asia.

In our analysis of that campaign, we identified a series of exploit scripts which we assess were highly likely being used by Red Djinn for its operations. Metadata revealed some of them to have probably been taken or adapted from open vulnerability databases, such as Seebug. These were accompanied by folders containing data suggesting that Red Djinn had been performing reconnaissance for vulnerable systems on an international scale. In addition, we identified exploit code for Citrix and Mikrotik appliances that appeared to be still in development.¹⁰⁹ We also identified Red Djinn activity dating back to March 2021, exploiting the ProxyLogon vulnerabilities, after their initial disclosure, to deploy a new backdoor which we call SpiderRAT.^{110, 111}

Red Vulture

Red Vulture ramped up its operational tempo throughout 2021. We observed Red Vulture conducting regular reconnaissance on a variety of organisations across the year, across the following sectors:

- Government;
- Aerospace and Defence;
- Education; and,
- NGOs.

This reconnaissance mainly consisted of the threat actor browsing the websites and perimeter services (e.g. VPN, email) of targeted organisations. There has been evidence that the threat actor is mass scanning for vulnerabilities in public facing infrastructure.¹¹² Red Vulture's success in targeting victims in 2021 was often due to its prolific use of exploits against perimeter authentication systems (e.g. VPNs).

The observed reconnaissance was focused around the targeting of Ministries of Foreign Affairs (MFAs), with a consistent focus on Europe and South America.^{113, 114, 115}

Red Keres

In early 2021, the German Federal Office for the Protection of the Constitution (BfV) reported on Red Keres' targeting of institutions including "ministries and authorities, political organisations and foundations" across Europe.¹¹⁶

Analysing Red Keres infrastructure disclosed by the BfV, we also identified evidence suggesting that the threat actor had likely compromised, and was directly accessing, the email server of the Ministry of Foreign Affairs of a Southeast Asian government between at least December 2020 and February 2021.¹¹⁷ Around the same time, we observed similar activity involving the email server for the Ministry of Defence of a different Southeast Asian government.

In late 2021, France's Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) released a detailed report into Red Keres TTPs. The report detailed the threat actor's multilayered anonymisation infrastructure set-up, involving over a thousand Small Office/Home Office (SOHO) routers, a technique PwC has observed multiple other China based threat actors invest in throughout 2021. The report also highlighted the many different techniques that Red Keres deploys when attempting to gain initial access to a victim, ranging from spear phishing, to password brute-forcing and abuse of valid credentials, to exploitation of vulnerabilities such as ProxyLogon or in Virtual Private Network (VPN) products.

Red Kelpie

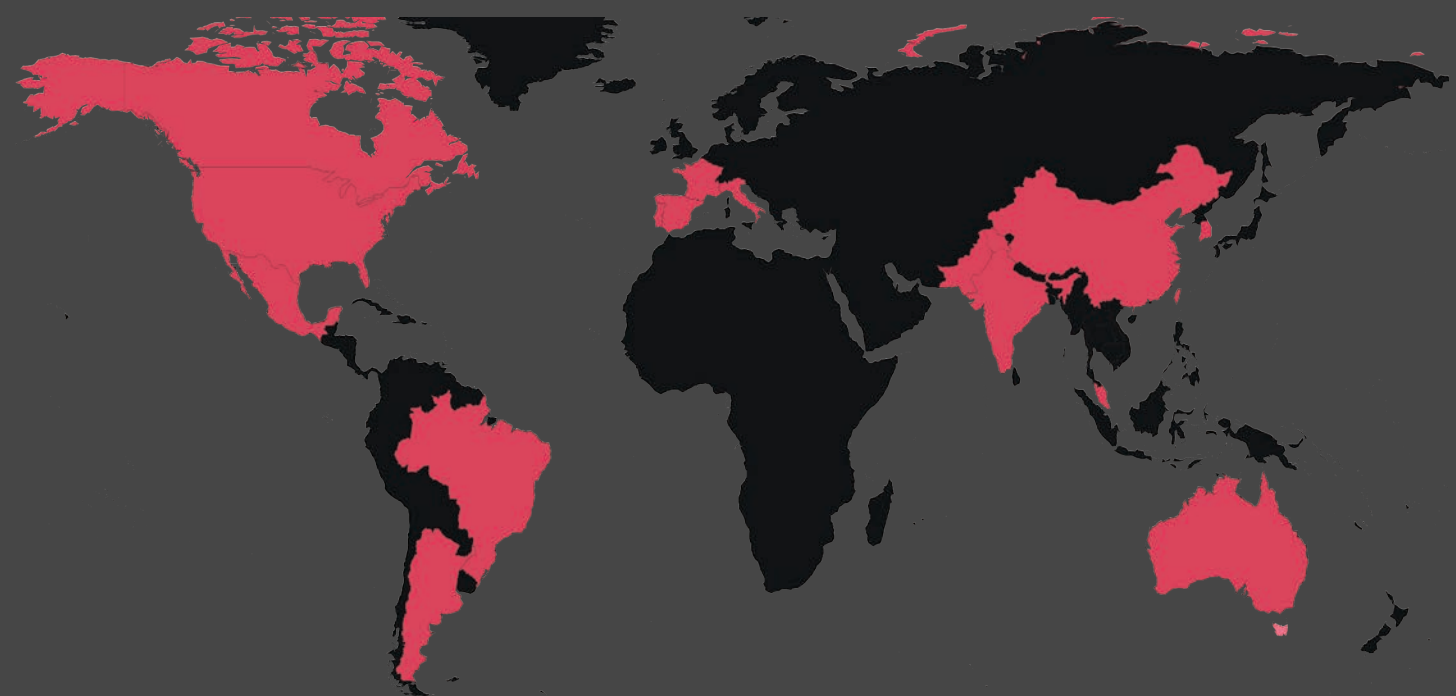
The threat actor that we track as Red Kelpie (which has overlaps with APT41 and BARIUM) relies on a wide variety of malware families including ShadowPad and CROSSWALK, as well as commodity tools like Cobalt Strike. It is prolific in its targeting, which encompasses several strategically important sectors.

ChaChaLoader

In 2021, Red Kelpie conducted a series of campaigns using the threat actor's well-known loader Motnug, and a likely evolution called ChaChaLoader. Motnug and ChaChaLoader were used to load Cobalt Strike, and in some rare cases, a newly observed backdoor which has been called SIDEWALK in open source, and which is a likely evolution of the CROSSWALK backdoor.¹¹⁸ It is plausible that the few cases where SIDEWALK was deployed instead of CobaltStrike were for high-value targets.

These campaigns targeted a variety of sectors including financial services, retail, telecommunications, manufacturing, and aviation.

Figure 22: Red Kelpie targeting in 2021



Financial Services



Retail



Telecommunications



Manufacturing



Aviation

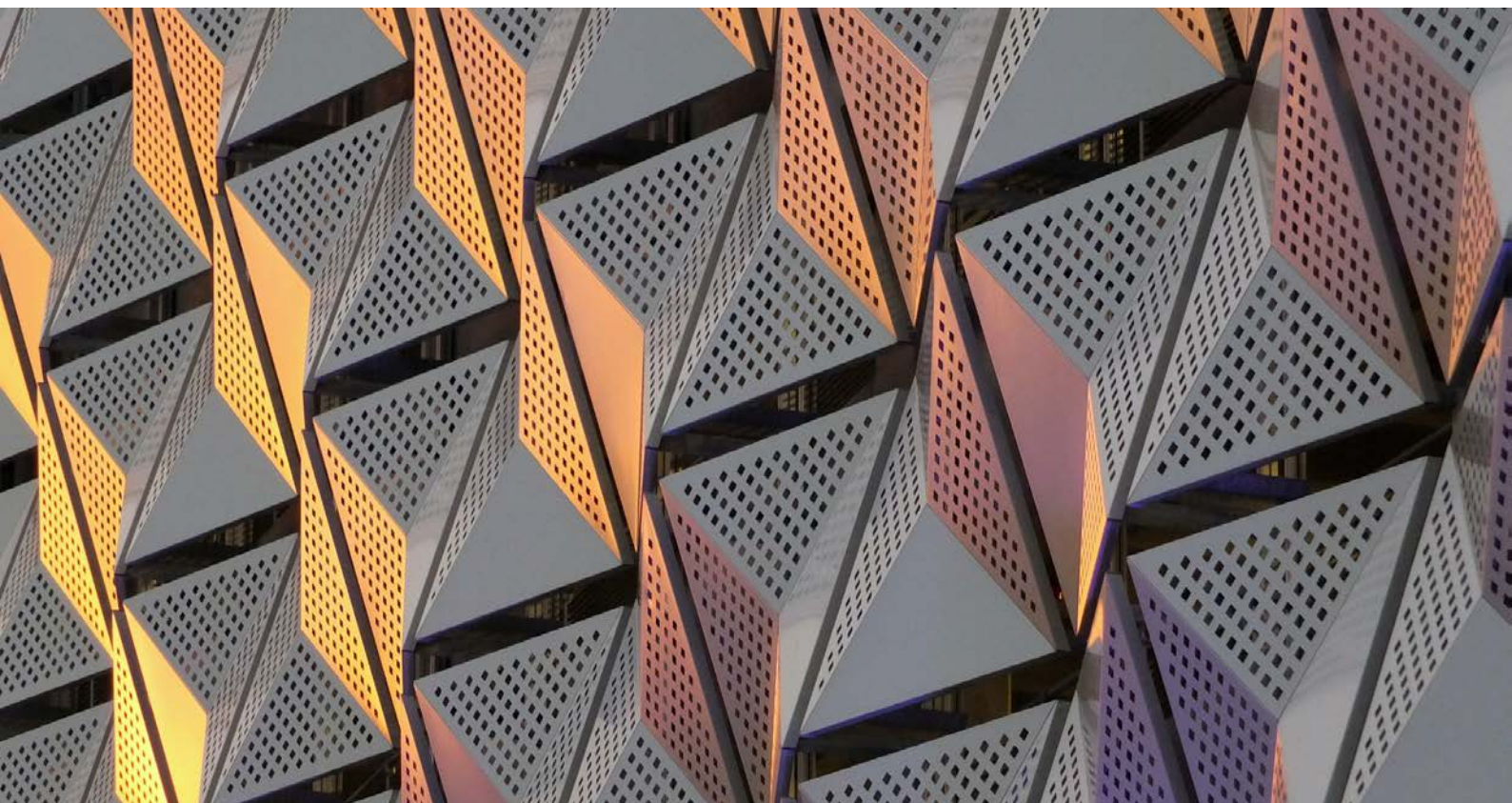
Confluence vulnerability

In prior years, Red Kelpie has mass-exploited vulnerabilities in public facing infrastructure to gain initial access, a tactic that we also noted in 2021. In particular, we observed Red Kelpie exploiting the Atlassian Confluence code execution vulnerability CVE-2021-26084 to drop a batch script and DLL used to load and execute Cobalt Strike.¹¹⁹ Red Kelpie has previously been observed using exploits for vulnerabilities in Citrix/Cisco software to deploy very similar batch scripts, which are also known to load and execute Cobalt Strike.¹²⁰

Active, despite indictments

In September 2020, the US Justice Department indicted seven individuals based in Asia alleging that these individuals were computer hackers, and that the intrusions they conducted were referred to in open source as APT41, BARIUM, Wintti, and so on.¹²¹

Despite these indictments, Red Kelpie activity continued throughout 2021. Perhaps the bigger cost to Red Kelpie due to the indictment was the seizing of accounts, servers, and domains being utilised by the threat actor, which forced it to change some of its operational tempo. We have tracked new sets of infrastructure being used by this threat actor across late-2020/2021, yet have still observed overlaps with older associated infrastructure attributed to that of APT41/BARIUM. The indictments of several of the operators behind the campaigns do not seem to have had any significant overall impact on the threat actor's operations.





Incident response case study:

Red Dev 14's FUNRUN

PwC responded to an intrusion into a think tank by a China-based threat actor, which we identified as Red Dev 14.¹²² Using the ProxyLogon exploits, the threat actor dropped a webshell onto an on-premises Exchange server. Initially, the threat actor attempted some reconnaissance via the webshell (mainly consisting of gathering system information like usernames and running processes), and ran commands to dump the memory of LSASS to obtain credentials via living-off-the-land binaries. The threat actor then utilised a variant of the backdoor called FUNRUN, which it used to drop ProcDump to dump the LSASS memory, as well as dropping Mimikatz to disk.

After successfully obtaining credentials, the threat actor moved laterally in the network via SMB remote shares, installing the FUNRUN backdoor to additional hosts. The threat actor also ran commands to search for other webshells on the Exchange server. This was likely done to test whether the Exchange server had already been compromised (likely

by ProxyLogon), which would inform Red Dev 14 if another threat actor was also present on the system. This has the potential to affect how it would achieve its goals.

From an attribution standpoint, we had previously observed the FUNRUN backdoor being used by the China-based threat actor we track as Red Pegasus (aka APT9).¹²³ However, a large amount of time has passed between when Red Pegasus was last observed using this backdoor (during 2014 and 2015), and the 2021 FUNRUN activity we observed. Based on this consideration, as well as on the fact that the loading mechanism was different for this backdoor compared to Red Pegasus' usage, and that there were no infrastructure overlaps with Red Pegasus, we decided to track this activity under the new name Red Dev 14.



Red Dev 14 compromised victims in multiple geographies as part of this campaign, primarily in agricultural sector.

Call me, maybe: China-based threat actors targeting telecommunications

Targeting of the telecommunications sector continues to be a focus for multiple China-based threat actors. Organisations in this sector hold a variety of high value information, including data from a telecommunications provider on its customers (which, depending on the provider, may be metadata around connections to websites, or call logs). This kind of information can then be exploited by threat actors for surveillance purposes, or to gather traditional intelligence about the activities of specific targets.

For example, as described above, we continued to see Red Kelpie targeting the telecommunications sector,¹²⁴ as well as the shared tool ShadowPad being used to compromise telecommunications providers.¹²⁵ We supported an incident response investigation to a telecommunications provider in Southeast Asia, where we observed a variant of the Evora backdoor used by the China-based threat actor Red Salamander (aka LotusBlossom).¹²⁶

Some things change, and some things stay the same for India-based threat actors

From our investigations into India-based threat actor operations, we continue to see a narrow focus on countries of strategic relevance to India, particularly on its near-neighbours, China and Pakistan. We observed almost all India-based espionage threat actors that we track using lure documents related to policy or political affairs of targeted countries, or otherwise themed around military and defence topics.

Orange Kala (Donot)

Orange Kala (aka Donot) maintained similar operational tempo and targeting focus in 2021 as in the previous year, with little variance in TTPs. In at least one case, the threat actor used a lure document related to missile technology.¹²⁷ This lure topic was not new for Orange Kala, as the content of several other lure documents since at least November 2020 was taken from both news articles and journals focusing heavily on missile defence technology. However, while most of the previous lure documents on this topic related to the United States, this campaign was the first instance where PwC observed Orange Kala focusing on missile technology within the Asia Pacific region. Both in this campaign, and throughout the year, Orange Kala relied heavily on the



Case study: Red Menshen targeting telecommunications providers

Throughout 2021 we tracked and responded to multiple intrusions attributed to a China-based threat actor that we have named Red Menshen.¹²⁸ This threat actor has been observed targeting telecommunications providers across the Middle East and Asia, as well as entities in the government, education, and logistics sectors using a custom backdoor we refer to as BPFDoor. This backdoor supports multiple protocols for communicating with a C2 including TCP, UDP, and ICMP allowing the threat actor a variety of mechanisms to interact with the implant.

Our research has shown that this threat actor uses a variety of tools in its post-exploitation phase. This includes custom variants of the shared tool Mangzamel (including Golang variants), custom variants of Gh0st, and open source tools like Mimikatz and Metasploit to aid in its lateral movement across Windows systems.^{129, 130} We also identified that the threat actor sends commands to BPFDoor victims via Virtual Private Servers (VPSs) hosted at a well-known provider, and that these VPSs, in turn, are administered via compromised routers based in Taiwan, which the threat actor uses as VPN tunnels.

Most Red Menshen activity that we observed took place between Monday to Friday (with none observed on the weekends), with most communication taking place between 01:00 and 10:00 UTC.¹³¹ This pattern suggests a consistent 8 to 9-hour activity window for the threat actor, with realistic probability of it aligning to local working hours.

Malware-as-a-Service (MaaS) tool WarzoneRAT. In one campaign, the threat actor deployed WarzoneRAT through a malicious DLL that would ultimately decode and execute a long series of hardcoded command-line commands in a batch script.¹³² Some lure documents involved in that campaign, and uploaded to an online multi-antivirus scanner from the UAE, were themed around new vessels in the Iranian Navy, and some around multinational naval exercises hosted by Pakistan, suggesting the threat actor's likely interest in military themes.

Sharing is caring

Over the year, we observed several crossovers in TTPs between Orange Kala and other India-based threat actors which we are still investigating, but which could be indicative of a greater degree of interconnection among India-based threat actors than had previously been considered. During February 2021, we tracked a campaign¹³³ involving a malicious RTF file template with links to both Orange Kala and Orange Dev 1 (aka CONFUCIUS) operations in 2020.¹³⁴ Links were also identified as far back as a 2017 campaign targeting Pakistan and known as Operation Shaheen¹³⁵. The 2021 activity centred on military and defence themes, with lure documents making reference to defence proposals, and, in one case, to the Royal Thai Navy. Orange Kala and Orange Dev 1 have both been known to target the defence and government sectors in the past. The 2021 campaign used different techniques from the similar activity reported in 2020¹³⁶, adding an extra layer into the attack chain, with the initial RTF documents downloading a second RTF on the victim machine, and using that second RTF as a downloader for a malicious DLL.

In June 2021, we observed a campaign by Orange Athos (aka Patchwork) involving VBA scripts that we had previously observed being used by Orange Kala as early as 2019.¹³⁷ The VBA macros were strikingly similar in the 2019 and 2021 activity, down to unique variable names; this suggests with realistic probability that they were not the product of a macro builder, but bespoke macros created by a threat actor and repurposed by another. While the malicious document was modelled after a Pakistani individual's biography taken from Scribd.com, the threat actor altered the original text to claim that the individual's father used to work for the Space and Upper Atmosphere Research Commission (SUPARCO),

the national space agency of Pakistan. The document was used to deliver the BADNEWS backdoor, a long-standing staple in Orange Athos' arsenal, to victims. Other open source reports^{138, 139} earlier in the year had discussed further malicious lure documents themed around SUPARCO; these delivered WarzoneRAT to targets and were attributed to India-based threat actor Orange Dev 1.

These campaigns display at least some modicum of shared tooling, or of cross-adaptation of simple tools, between India-based threat actors. However, we note we have only observed this at the level of initial access vectors, with India-based threat actors still largely differing in their choice of later-stage backdoors.

Orange Athos (Patchwork)

Orange Athos (aka Patchwork) continued to make heavy use of the BADNEWS backdoor (also known as BozokRAT) throughout different campaigns in 2021, with only minor changes to the malware's codebase since it was first reported on in open source as far back as 2016.¹⁴⁰

The threat actor maintained its previous focus¹⁴¹ on Chinese and Pakistani targets. In a campaign we observed in April 2021, the threat actor used a lure document relating to military cooperation between China and Pakistan.¹⁴² The document was a malicious DOCX file exploiting CVE-2017-0261, a Use-After-Free (UAF) vulnerability pertaining specifically to encapsulated postscript (EPS) images. This is a technique that we had observed the threat actor consistently rely on in several 2020 campaigns involving nearly identical tools, techniques, and procedures (TTPs), each with a focus on China-based targets.

Among separate intrusions, one¹⁴³ featured a lure purporting to be a form by the Federal Board of Revenue of Pakistan, asking employees of Pakistani federal government departments to input their personal details to be eligible to receive a special tax relief package. When victims opened the RTF, the same vulnerability mentioned above (CVE-2017-0261) would lead to the installation of the BADNEWS backdoor. With the continued exploitation of the specific vulnerability, and use of tooling that has been well documented in open source, it appears this is another threat actor that will persist with tried and tested TTPs.

Orange Yali (BITTER)

Throughout 2021, we identified several websites purporting to be legitimate Pakistani companies that we believe were most likely set up and maintained by India-based threat actor Orange Yali (aka BITTER) since 2020. The websites, which typically have little to no content or placeholder text, were used to stage payloads of the “rkftl” backdoor, sometimes packaged as an MSI installer, as well as utilities, such as the SSH and Telnet client PuTTY. Orange Yali also continued to use the malware family known as ArtraDownloader, and introduced the use of CHM (compiled HTML) files in a campaign specifically targeting Chinese entities.^{144, 145} Several reports also indicated that Orange Yali used at least two different 0-day exploits^{146, 147} throughout 2021, both of which were quite likely acquired from an exploit broker as opposed to developed in-house by the threat actor.¹⁴⁸ This indicates that at least one India-based, espionage-motivated threat actor has the resources to access the private 0-day market, something which we had not previously observed from threat actors active in the region.

Espionage doesn't pay: Pakistan-based threat actor activity

Throughout 2021, Green Havildar (aka APT36, Transparent Tribe, Gorgon Group) primarily continued operating in line with its likely main objective of gathering intelligence (including targeting of the military, government, and wider public sector, particularly in India). This threat actor relies on basic spear phishing for initial access, with lure documents varying from individuals' curriculum vitae to conference programmes, to several samples related to military and defence.¹⁴⁹

Green Havildar is known for its use of CrimsonRAT, which it continued to operate through a builder model: the RAT has a wide set of surveillance and exfiltration capabilities,

a consistent code obfuscation model, and the ability for the threat actor to flexibly change the ports over which C2 activity is conducted. Between April and July 2021, Team Cymru published reports exposing the setup of Green Havildar's C2 infrastructure, including the threat actor's management of it over RDP.^{150, 151}

In 2021, we observed increased activity by Green Havildar's financially-motivated, cybercrime-focused operations (reported in open source under the moniker Gorgon Group aka Aggah, MasterMana). As in 2020, the majority of Gorgon Group's spam campaigns involved PowerPoint document lures, and OneDrive links, delivering commodity RATs such as AgentTesla, Remcos, and Quasar. We additionally observed the use of two separate common injectors by the threat actor RunPE and HCrypt.

While Gorgon Group is also known to host multistage malicious scripts on public paste sites such as Pastebin and Blogspot, we also tracked a series of campaigns using accounts on The Internet Archive for similar purposes. In August 2021, it was reported¹⁵² that Gorgon Group was using compromised websites to stage next-stage malicious payloads and delivering Warzone RAT in place of paste sites, in an effort to avoid detection and takedown of its staged capabilities.¹⁵³

While Green Havildar's intelligence gathering operations focus primarily on India as well as occasionally on neighboring countries like Afghanistan¹⁵⁴, Gorgon Group's activity has an international reach not necessarily limited to political considerations. For example, from April 2021 we tracked a Gorgon Group campaign targeting organisations in the Netherlands and South Korea¹⁵⁵, including in the manufacturing sector (a frequent target of this threat actor). In contrast to Green Havildar, Gorgon Group is relatively indiscriminate in its targeting, and we have not observed it deploying any custom capabilities.

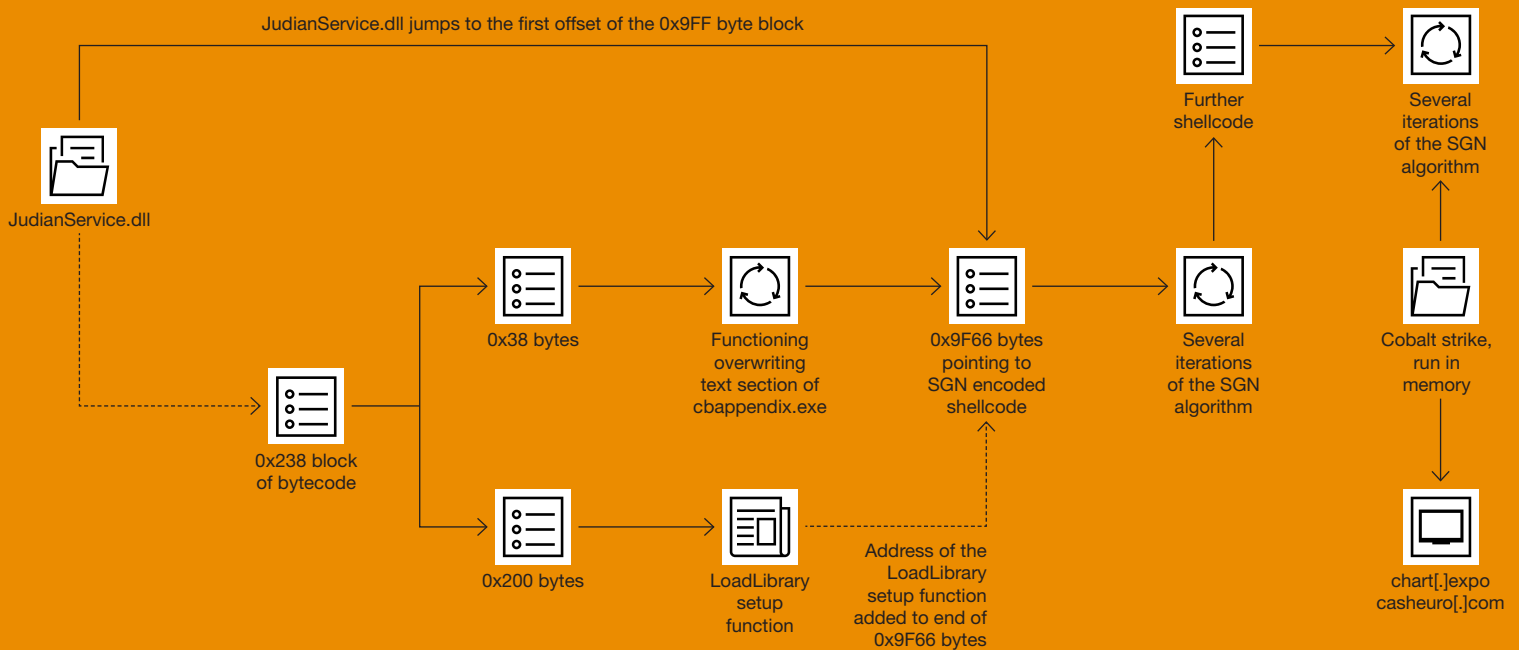
(Not) all is quiet on the Scarlet front: Vietnam-based threat actor activity

Following Facebook’s public attribution in December 2020 of Scarlet Ioke (aka Ocean Lotus, APT32) to CyberOne Group, a Vietnam-based IT company, we observed a drastic reduction in the threat actor’s operational tempo – at least with regards to known, ongoing campaigns. On the other hand, Chinese cybersecurity firms continued observing Scarlet Ioke targeting China over the past year, which is consistent with

the threat actor’s long-standing targeting focus. For example, Sangfor¹⁵⁶ reported in March on Scarlet Ioke activity using a loader commonly referred to as “DgBase.dll”. The Linux RotaJakiro¹⁵⁷ backdoor, which is also equipped with botnet functionality, was also attributed in open source to Scarlet Ioke, based on close code overlaps between RotaJakiro and the OceanLotus backdoor.

Between late 2020 and September 2021, we observed a campaign¹⁵⁸ involving DLL loaders for Cobalt Strike and Metasploit which used several layers of Shikata Ga Nai encoding to avoid detection. In some cases, the Cobalt Strike payloads used the Glitch web service to conduct C2 activity.

Figure 23: A suspected Scarlet Ioke attack chain loading CobaltStrike Beacon in memory

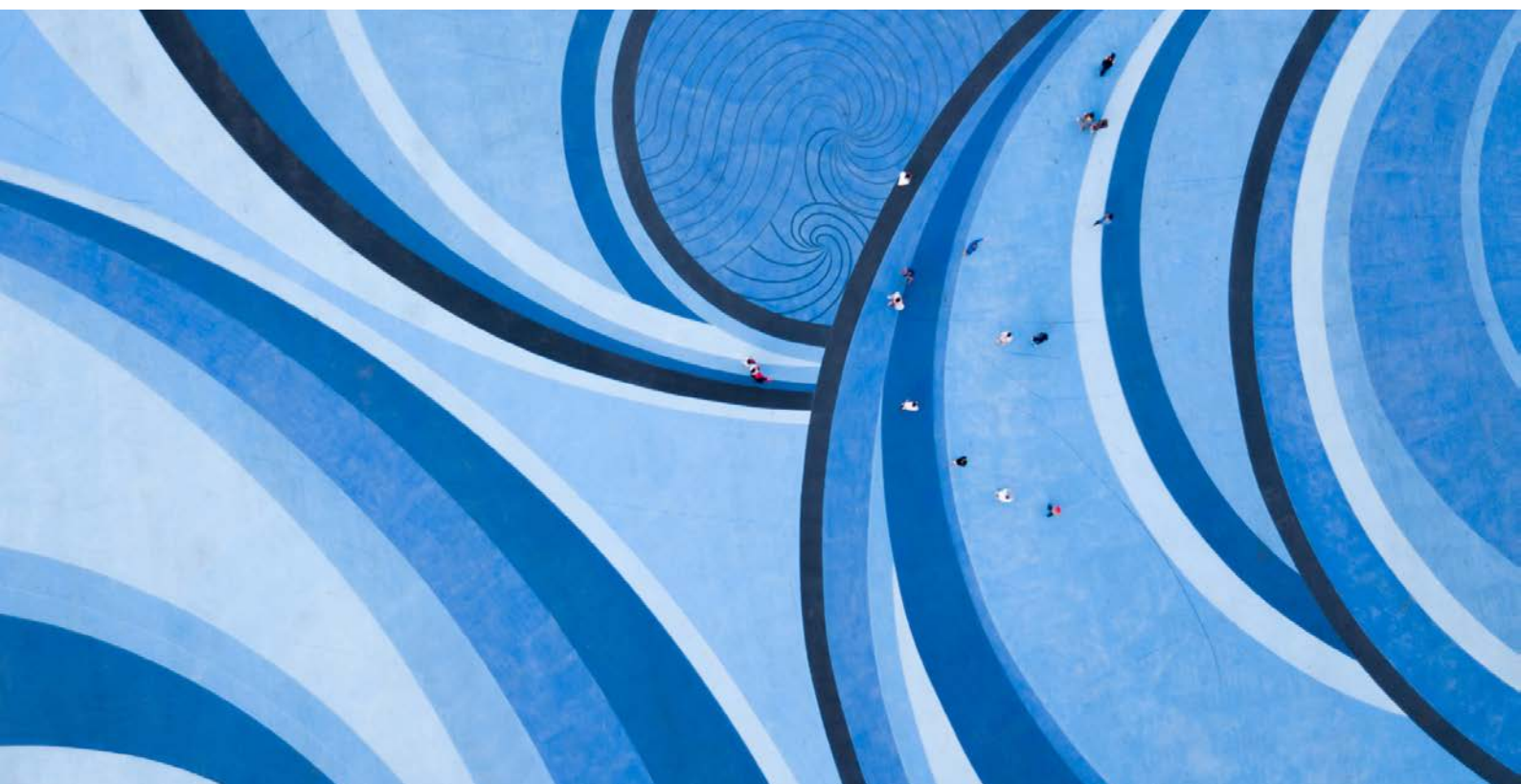


In at least one case, the DLL was sideloaded by a legitimate Kingsoft binary, a software predominately used in Mandarin Chinese-speaking countries. Furthermore, many of the Cobalt Strike samples that we identified were masquerading as Tencent's QQ service or as the Chinese search engine Sogou, a consistent tactic for Scarlet Ioke. This evidence suggests with realistic probability that the binaries were meant to target Chinese-speaking victims. Based on the TTPs and targeting that we observed in this campaign, we assess it is a realistic probability that it was conducted by Scarlet Ioke. Factors contradicting this assessment include the lack of direct links to previous Scarlet Ioke activity, as well as the use of typical penetration testing tools that could also be part of a domestic red team exercise.

Ultimately, threat actors respond differently to disclosure and attribution. Some, like Red Kelpie and Yellow Garuda, might continue operations with no alteration to their TTPs, while others may change tools and techniques or even undergo radical restructuring. Based on the observations we assess it unlikely that Scarlet Ioke has ceased operations. Rather, we assess it is likely that the threat actor is retooling and reorganizing, with plans to ramp up activity in new campaigns.



Threat actors respond differently to public disclosure of their activity. Some, like Red Kelpie and Yellow Garuda, continue operations with little to no changes to their TTPs, while others (possibly including Scarlet Ioke) may change tools and techniques, or even undergo radical restructuring.”



Middle East



Iran-based threat activity

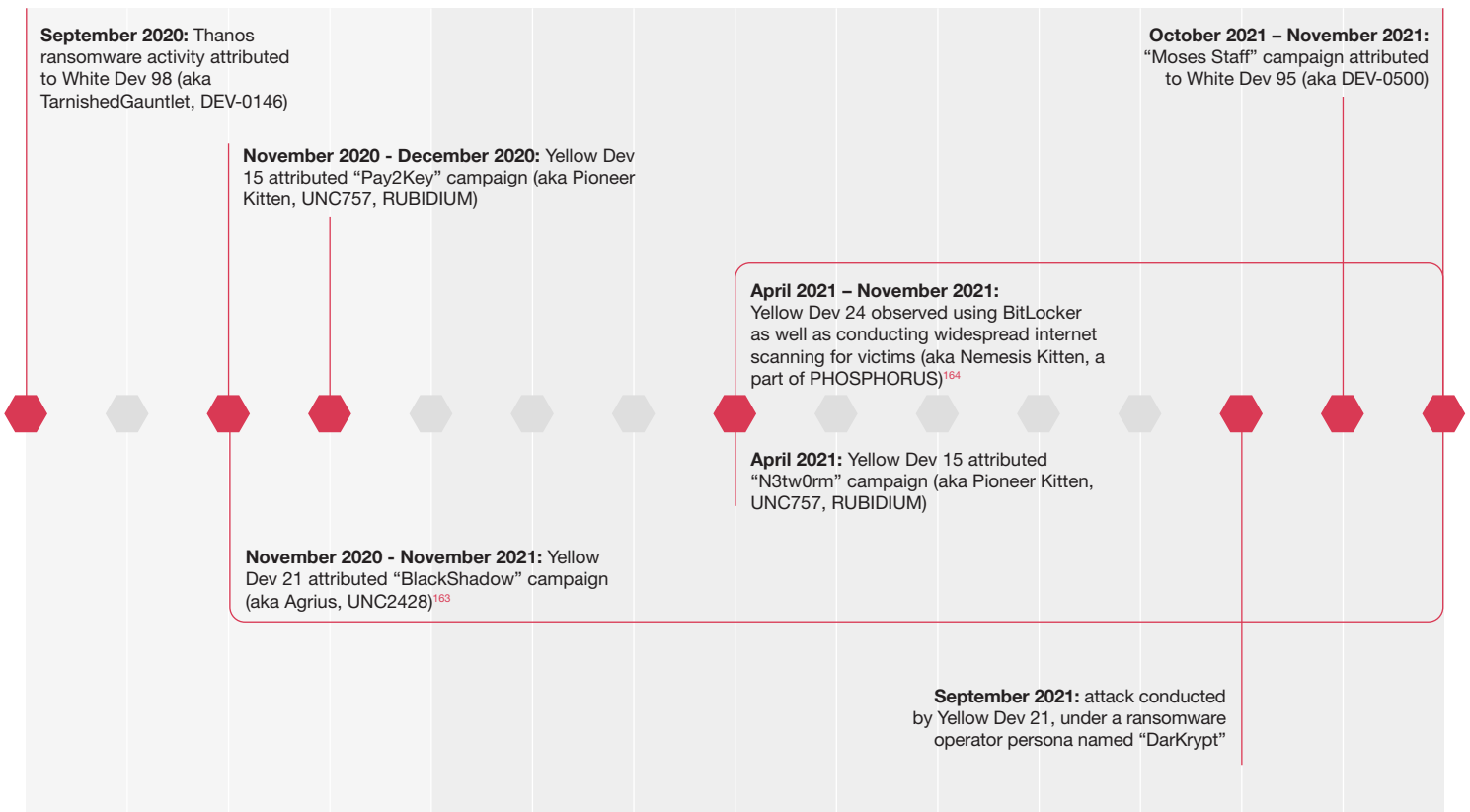
The changing face of sabotage operations

Iran-based threat actors have a long history of conducting sabotage attacks meant to destroy and disrupt victim organisations. Such attacks put the threat actors squarely under the spotlight, typically leading to attribution and scrutiny of their operations by the private and public sectors alike. In an attempt to mitigate unwanted attention, Iran-based threat actors often blame or pose as hacktivist collectives, a tactic that continues to be adopted by suspected Iran-based threat actors such as White Dev 95 (aka Moses Staff).¹⁵⁹

First emerging in late 2020 and rising to prominence in 2021, we observed a theme of Iran-based threat actors amplifying false motivation tactics, including Yellow Dev 15’s Pay2Key and N3tw0rm activity leveraging ransomware for sabotage rather than financial gain.¹⁶⁰ When used in conjunction with hacktivist behaviours, this can work to sow confusion about a threat actor’s true nature and intentions.

Iran-based threat actors such as Yellow Dev 15 and Yellow Dev 21 have also at times masqueraded as cyber criminals rather than hacktivists in their sabotage campaigns, where they also pretended to extort their victims.¹⁶¹ On one occasion, Yellow Dev 21 threatened to sell a victim’s data to third parties if a payment was not made.¹⁶²

PwC observed the following suspected Iran-based threat actors, with varying levels of confidence, leverage ransomware in their campaigns:





Case study: N3tw0rm

In late April 2021, a ransomware variant named N3tw0rm emerged targeting Israeli victims in the retail, logistics, NGO, and construction sectors. Technical analysis subsequently uncovered similarities between N3tw0rm and another ransomware variant named Pay2Key, is controlled by Yellow Dev 15, due to its lack of follow-through on providing decryption keys (as of December 2021, the bitcoin wallet listed on the N3tw0rm ransom note remained empty, which means no victim paid the ransom). The motivations behind the attacks appear to align with sabotage rather than financial.¹⁶⁶ As of December 2021, the bitcoin wallet listed on the N3tw0rm ransom note remained empty, which means no victim paid the ransom.



Case study: Moses Staff

Starting in September 2021, a threat actor calling itself “Moses Staff” started a destructive “lock and leak” campaign against Israeli organisations. We track the threat actor behind this campaign as White Dev 95. The majority of the campaign’s victims observed in late 2021 were Israeli organisations whose business footprints do not align to the threat actor’s mission statement exposing various crimes allegedly committed by the Israeli Government. They also span a diverse range of sectors: legal, logistics, retail, utilities, professional services, transport, construction, manufacturing, and financial services. This victimology suggests that targets were likely chosen somewhat opportunistically, with the focus solely on Israel as a target rather than on exposing any alleged wrongdoing.

White Dev 95 also displayed multiple similarities with a number of Israel-focused campaigns attributed to Iran-based threat actors that have taken place across 2021, and which specifically sought public attention in an attempt to build momentum towards their activities. To that effect, White Dev 95 operates multiple digital platforms to leak victim data, as well as directly engaging with them over Twitter. One of the key differentiators between the “Moses Staff” campaign and similar operations by Iran-based threat actors, is that White Dev 95 skips the extortion phase of its attacks, preferring instead to leak stolen data without warning. This likely contributes to the confusion caused to victims, maximising the destructive element of the campaign.

You can't teach an old threat actor new TTPs

The majority of Iran-based threat actors that we track emerged with new flavours of tooling this past year, while also continuing to rely on tried and tested techniques. Iran-based threat actors are often known for their use of open source tooling, particularly offensive security tools, as well as for their social engineering campaigns.

Open source tools

Yellow Nix (aka Static Kitten, MERCURY, MuddyWater) leveraged commercial remote administration tools consistently throughout 2021, including ConnectWise Control (aka ScreenConnect) and Remote Utilities, in order to gain initial access to victims.¹⁶⁷ We also saw Yellow Nix intermittently using macro-enabled Microsoft Office documents, including using them as a delivery mechanism for ConnectWise Control.¹⁶⁸

Both Yellow Dev 24¹⁶⁹ and Yellow Dev 15¹⁷⁰ have used the open-source FRP tool, which allows a system to provide network access to threat actor-controlled systems located outside of the victim network. Similarly, Yellow Orc (aka APT 33, Refined Kitten, Stonedrill) is well known for its use of PoshC2, an open source C2 framework used for post-exploitation and lateral movement. In 2021, we observed new Yellow Orc activity, which incorporated a similar publicly available C2 framework.¹⁷¹

Social engineering

A common denominator among many Iran-based threat actors is to use job or recruitment themed phishing lures, while relying on social media platforms to directly communicate and build trust with targets. In several fringe cases, phishing and social engineering techniques bypassed multi-factor authentication (MFA); however, from our observations, MFA remains highly effective in thwarting the majority of attacks.¹⁷²

Yellow Maero (aka APT34, OilRig, COBALT GYPSY) has a long history of social engineering; in January 2021, we observed it using a recruitment brochure branded as a legitimate US-based IT services provider and advertising a range of different IT, business, and engineering roles available in the Middle East.¹⁷³ The lure document is likely legitimate, though it was maliciously repurposed by the threat actor.

In July, the threat actor we track as Yellow Orc (aka APT33, Elfin) conducted a campaign involving job lures and a fake career finder website for positions primarily in the Middle East, with a focus on the following sectors: Oil & Gas, Chemicals, Energy, Life Sciences, Manufacturing, Mining, Infrastructure, and Government.¹⁷⁴ Open directory contents also show the threat actor likely began the year focusing on US targeting via malicious HTA files, and simultaneously conducted an operation leveraging a piece of malware that masqueraded as a COVID-19 tracker from the World Health Organization (WHO).¹⁷⁵ The open directory evidenced that Yellow Orc likely also used images of a female individual to socially engineer its targets.¹⁷⁶ The images bear resemblance to open source reporting on the “Marcella Flores” persona operated by the threat actor we track as Yellow Liderc.¹⁷⁷ Yellow Orc has been using job themed social engineering tactics since at least 2017.



Yellow Liderc (aka Tortoiseshell, TA456)¹⁷⁸ and a closely related threat actor we track as Yellow Dev 13 continued throughout 2021 to use LinkedIn and Facebook for social engineering, maintaining a network of fake recruitment companies and personas.^{179, 180} Both Microsoft and Meta documented Yellow Liderc's persistent yet patient process of using social media, often spanning multiple months between the initial connection with the target to the delivery of malicious content.^{181, 182}

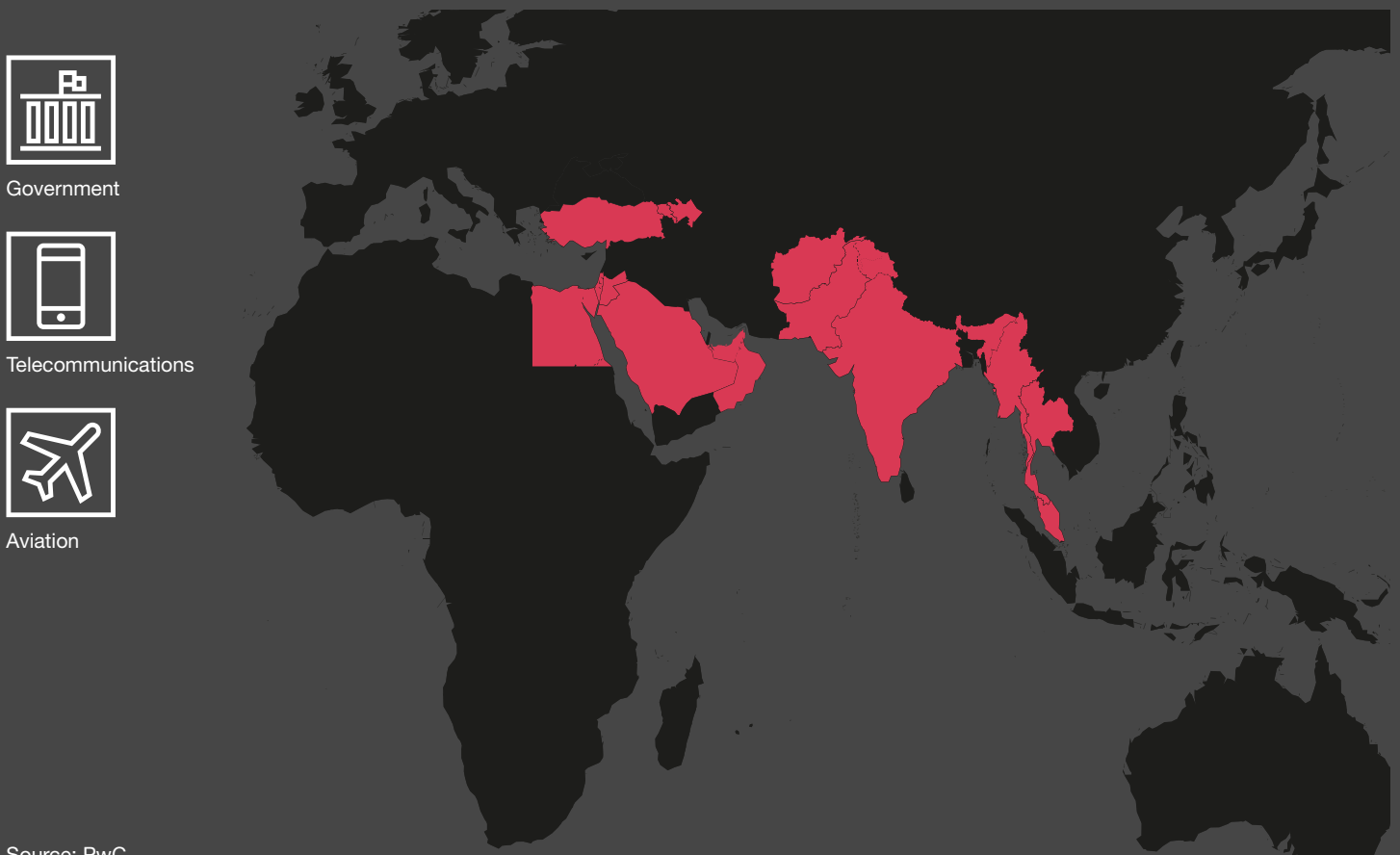
Broadening horizons

Yellow Nix

Yellow Nix continued to broaden its horizons beyond the geographic regions neighbouring Iran. Following a busy year in 2020, when it targeted Europe in multiple campaigns, in September 2021 we saw the threat actor shifting towards Southeast Asia. Its targeting of government, aviation, and telecommunications sectors in Malaysia, in particular, followed economic cooperation talks held between Iranian and Malaysian officials.¹⁸³ This is typically the case with Yellow Nix, with its activity often closely mirroring Iran's political and trade investments. Yellow Nix also appeared to direct increased levels of interest towards the aviation sector.

In September 2020, the United States sanctioned individuals associated with Yellow Mimas, a threat actor notorious for targeting global aviation and telecommunications sectors in order to monitor traveller movements. Since then, PwC analysts have not observed Yellow Mimas activity, and the threat actor has also been notably absent in open source threat reporting. It remains unclear if Yellow Mimas has entered a period of inactivity, but Yellow Nix's uptick in targeting aviation organisations demonstrates that its sponsor's requirement to obtain intelligence from this sector is likely being fulfilled, although the extent which Yellow Nix achieves this remains unclear. Yellow Nix's recent victimology also mirrors that of Yellow Mimas, and indicates that Yellow Nix may be engaged in conducting surveillance on individuals of interest.¹⁸⁴

Figure 24: Yellow Nix targeted geographies and sectors



Yellow Dev 9

First reported on by open sources in 2019, espionage-motivated Yellow Dev 9 (aka Lyceum, Siamese Kitten) shares similarities in its victimology, infrastructure, and tooling with another Iran-based threat actor we track as Yellow Maero. Yellow Dev 9 continued to be active in 2021 targeting African telecommunication and aviation sectors, socially engineering targets over LinkedIn, and hosting its recruitment themed malware on domains masquerading as information technology companies.¹⁸⁵ Despite multiple security researchers releasing public reports on Yellow Dev 9, the threat actor continued to develop new variants of malware, termed “Milan” and “Shark” backdoors, which use HTTP and DNS network connectivity. Yellow Dev 9’s infrastructure has a specific pattern, with the threat actor consistently registering command and control (C2) domains with DNS-, “update”, and CDN-themed names during 2021.¹⁸⁶ Yellow Dev 9 is known to reuse its historic infrastructure from its earlier campaigns.¹⁸⁷

Yellow Garuda

One of the most active and widely reported threat actors this past year was Yellow Garuda (aka Charming Kitten, PHOSPHORUS, ITG18). This threat actor is highly capable and persistent, increasing its operational tempo in 2021 while maintaining a sprawling network of phishing infrastructure. Yellow Garuda’s campaigns range from simple credential phishing¹⁸⁸ to compromising legitimate websites,¹⁸⁹ deploying mobile malware,¹⁹⁰ using Telegram bots to fingerprint victim devices,¹⁹¹ and doubling-down on social engineering efforts.

These operations translate into widespread targeting of victims around the globe and across multiple sectors. Victimology throughout 2021 included internal target sets within Iran, as well as neighboring countries throughout the Middle East, and typical targets in both the US and Europe.

Yellow Dev 19

An Iran-based threat actor, which PwC tracks as Yellow Dev 19, was observed targeting websites related to the 2020 United States presidential election, in what the US government assesses was an attempt to influence and interfere with the election.¹⁹² We assessed in May 2021 that Yellow Dev 19 was likely closely associated with the Iranian education sector, specifically in the form of a student or faculty member, which a November 2021 US indictment supports with the naming of two individuals aged 23-26¹⁹³. We also identified that Yellow Dev 19 likely is interested in targeting Saudi Arabian government entities.¹⁹⁴

According to the US government indictment, the alleged company responsible for leading the attempted campaign is Emennet Pasargad, a company acting in support of the Iranian government.¹⁹⁵ PwC analysts have also observed overlaps between this company, together with its sanctioned board members, and Yellow Liderc.¹⁹⁶ PwC assesses that Emennet Pasargad and/or its personnel is likely involved in other operations, such as ransomware for sabotage purposes, and is closely aligned with the Islamic Revolutionary Guard Corps.

Yellow Dev 24

Spanning from at least April to November 2021, PwC observed Yellow Dev 24 (aka Nemesis Kitten, a part of PHOSPHORUS) mass-scanning internet facing appliances, including Fortinet devices and Microsoft Exchange servers.¹⁹⁷ In some cases, Yellow Dev 24 subsequently deployed ransomware via BitLocker, while relying on open source tooling and living-off-the-land techniques. Yellow Dev 24 is one of several Iran-based threat actors who are adopting ransomware for sabotage purposes, while simultaneously capable of conducting espionage activity. Yellow Dev 24 is also opportunistic in its targeting selection, which makes this threat actor relevant to a global audience.¹⁹⁸

Victims in this campaign were geographically diverse, and included organisations in the US, Australia, the UAE, and South Africa,¹⁹⁹ as the threat actor reportedly compromised nearly 1,000 devices in just over six months.²⁰⁰ Slightly more targeted (though still opportunistic) activity occurred via password spraying US and Israeli defence technology companies, Arabian Gulf ports of entry, and global maritime transportation companies with business presence in the Middle East.²⁰¹

Threat activity across the Middle East

Teal Dev 2

Turkey-based threat actor Teal Dev 2 (aka StrongPity) continued to deploy its well-known backdoor StrongPity throughout 2021 although, from our observations, this activity slowed in the second half of the year. New Teal Dev 2 TTPs were brought to light, with open source reporting showing infrastructure links between StrongPity and Android malware, not previously known to be part of the threat actor's toolset, but which has likely been used since at least 2019.²⁰² Based on these observations, we assess that Teal Dev 2's apparent sparing use of specific tools and techniques has likely let them go undetected for several years, and is likely indicative of highly targeted campaigns.

Grey Karkadann

Grey Karkadann (aka Arid Viper, APT-C-23, and part of the Gaza Cybergang) has continued using tried and tested techniques to target entities in the Middle East region, with a strong focus on Palestinian politics and Palestine-Israel relations. Over the course of 2021, this included the continued use of its Windows malware Micropsia,²⁰³ which is typically accompanied by decoy documents aligning with its main targeting themes. We also observed ongoing

development of its mobile malware, which is distributed via third party app stores or threat actor-controlled sites. Open source reporting notes that Grey Karkadann's arsenal now includes iOS malware in addition to its known Android implants.²⁰⁴ The threat actor's mobile malware contains extensive surveillance and stealth functionality, often masquerading as legitimate applications.²⁰⁵

White Dev 21

In May 2021, we observed a cluster of activity focused on Arabic speakers with an interest in Middle East affairs.²⁰⁶ The activity spanned back to at least 2019, and involved the use of macro-enabled documents with content covering a broad range of news and themes related to Palestine, Lebanon, and Iraq. This indicates that the threat actor has likely targeted multiple separate victims during this campaign. Open source reporting has linked this activity to a threat actor known as WIRTE, and highlighted the targeting of a number of high profile organisations in sectors including government and diplomatic entities, law firms, and financial institutions making the threat actor of concern to a wide variety of sectors.²⁰⁷ From our observations, WIRTE shares historic infrastructure overlaps with White Dev 21, a threat actor we observed in 2019 using election and diplomatic-relation themed lures related to Egyptian and Palestinian politics, and which we assess to likely be an offshoot of the Gaza Cybergang.^{208, 209}



Europe and former Soviet Union



Threat actors based in Russia continued their cyber operations in 2021, seeking to access confidential or sensitive information. This has included the targeting of government ministries across Europe, and Russia's near abroad. We saw the threat actor Blue Athena (aka Sofacy) take particular interest in the mining and natural resources sector in Central Asia.

We also continued to see the consistent targeting of entities in Ukraine by the Russia-based threat actor Blue Otso. We tracked Blue Otso activity targeting entities in eastern Ukraine, in the lead-up to the Ukrainian Security Service (SBU) eventually unmasking several alleged Blue Otso operators in November 2021.

Additionally, beyond Russia-based threat actors, our research also included tracking other malicious activity. White Tur is one example of an as-yet unattributed threat actor whose interest has focused on very specific sectors and geographies. Elsewhere, Georgia-based threat actor Rose Matsil has been observed in association with the targeting of medical organisations in Russia in 2021.

Blue Dev 5 - A 'noble' phisher

The Russia-based threat actor Blue Dev 5 (aka NOBELIUM²¹⁰, NobleBaron) was one of the most prolific and technically-sophisticated threat actors we tracked in 2021. Blue Dev 5 demonstrated careful tradecraft and novel techniques, including compromising Microsoft cloud environments and exploiting trust relationships between organisations.

Blue Dev 5 successfully compromised several cloud resellers and MSPs, leveraging cloud trust relationships held by these organisations with their customers to compromise customer cloud environments, and exploit the access provided to MSPs in order to pivot into their clients' networks. Once Blue Dev 5 gains access to victim organisations, it aims to gain long-term, stealthy, persistent access to Azure AD and Microsoft 365 instances, including privileged accounts and

sensitive data. Blue Dev 5 has demonstrated high levels of operational security, and has taken measures to evade detections and make it harder for victim organisations to investigate suspicious activity (for example, logging into compromised accounts at victim organisations from residential IP addresses).

We are not currently able to definitively link Blue Dev 5 with the threat actor behind the SolarWinds supply chain attacks that we track as Blue Nova^{211, 212}. However, we noted a significant overlap in techniques between the two, including in the techniques used to perform sophisticated identity-based attacks against Microsoft cloud environments. We also noted that both Blue Dev 5 and Blue Nova²¹³ leverage third-party trust relationships to gain access to organisations' IT environments.

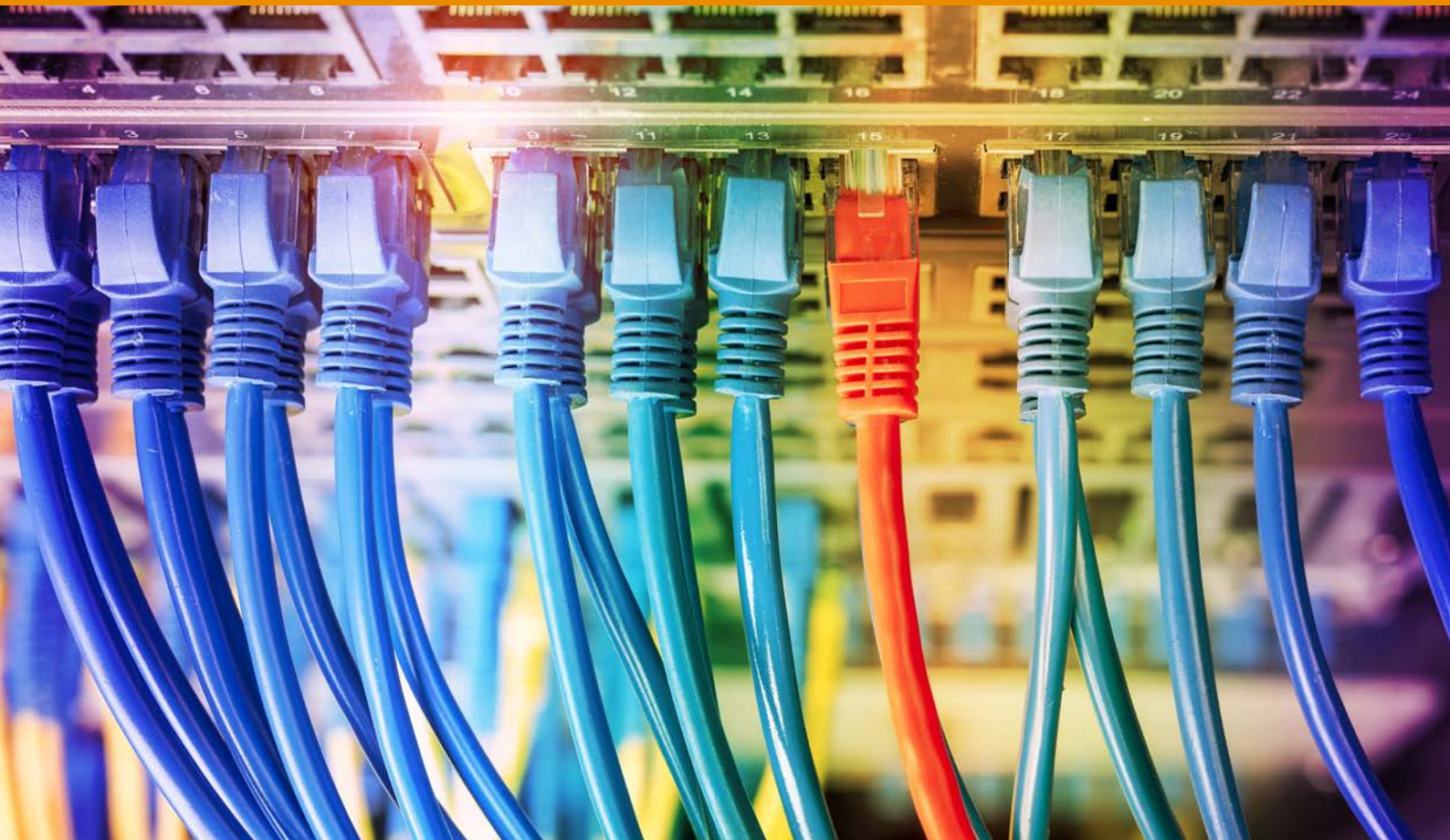
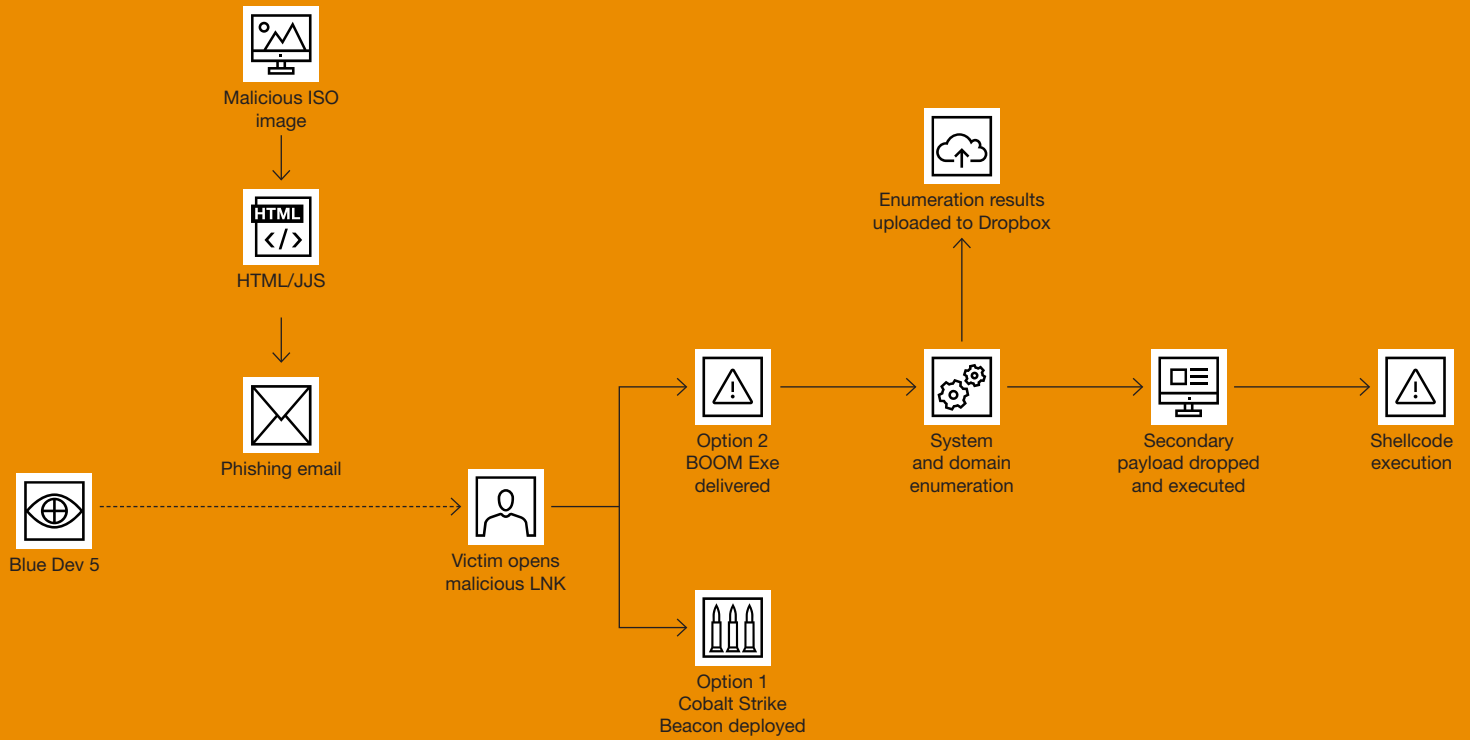
Organisations concerned about the threat of Blue Dev 5 should take steps to:

- Implement a robust privileged access strategy that includes using secure administration practices and stringent restrictions around the use of privileged access;
- Monitor Azure AD and Microsoft 365 logs for techniques used to compromise and abuse privileged accounts, persistence techniques, and for rare global events; and,
- Regularly audit cloud (Azure AD, Microsoft 365 and Azure) configurations and trust relationships.

Blue Dev 5 has also been observed using other well known techniques to gain access to organisations' environments, including password spraying and using compromised credentials.

Blue Dev 5 drew significant attention in May 2021, when it conducted a phishing campaign masquerading as USAID, in order to distribute Cobalt Strike Beacon malware packed with a custom loader. In this instance, we derived the following view of this activity:

Figure 25: A Blue Dev 5 intrusion chain involving Dropbox exfiltration

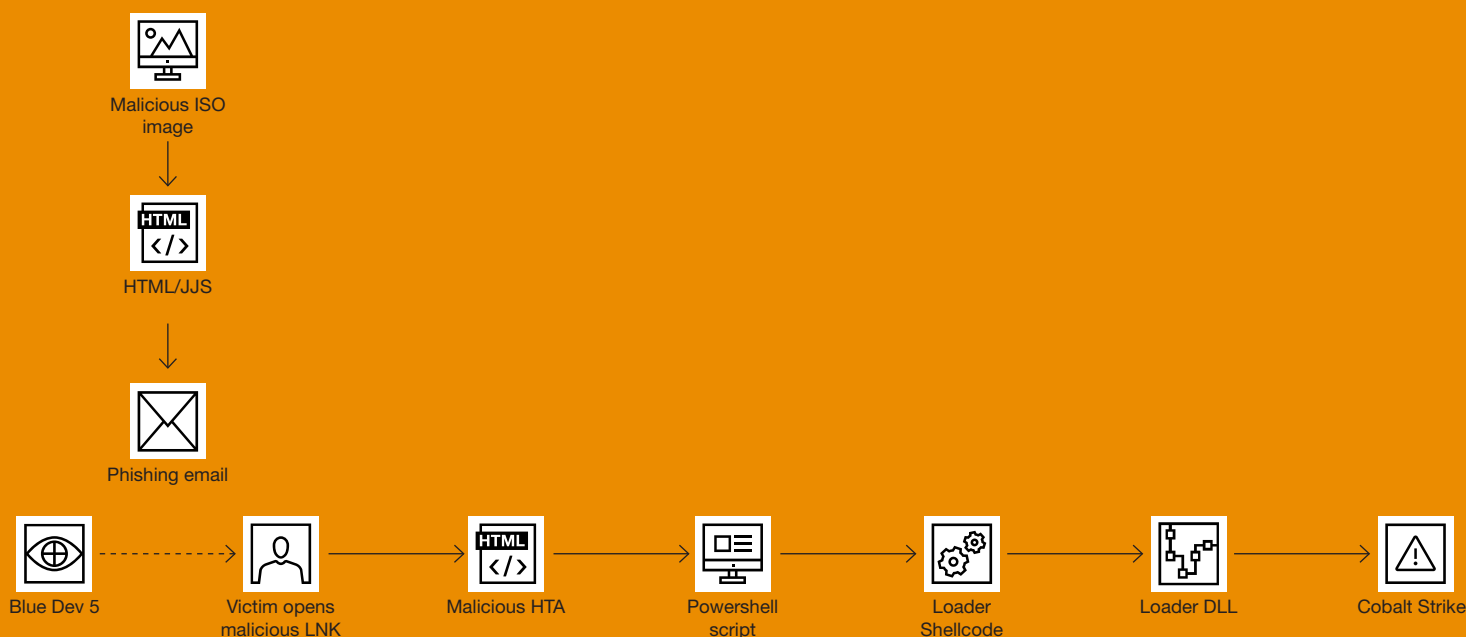


There is evidence that the first-stage HTML attachments were opened by individuals working at multiple embassies across Europe,²¹⁴ providing insight into the broader targeting conducted by this threat actor. Some payloads used by Blue Dev 5 appear to have been more targeted: one seen in March 2021²¹⁵ checked for environment variables which relate to the Ministry of Foreign Affairs of an Eastern European country; another impersonated an update for a Ukrainian government document management system.²¹⁶

By tracking Blue Dev 5's infrastructure over time, we also observed its TTPs grow more complex. For example, in a HTML lure which was likely created in November 2021, the threat actor had added several more stages between the initial HTML lure and the Cobalt Strike Beacon payload ultimately delivered to targets. In this case, as well as one other we identified, the lure document purported to notify the victim that an embassy was closed due to COVID-19.

We assess that it is highly likely that Blue Dev 5 will continue to remain active throughout the coming year, and that its TTPs will continue to evolve over time to better evade detection.

Figure 26: A variant of a Blue Dev 5 initial access intrusion chain





Spotlight on the Balkans: White Tur

In January 2021, PwC observed a phishing domain targeting the Serbian military.²¹⁷ Soon after, we identified additional related infrastructure that showed targeting of Serbian and Republika Srpska government and defence organisations ongoing since at least 2017, which we are tracking in association with a threat actor we call White Tur. Republika Srpska is one of the two federal entities within Bosnia-Herzegovina. This activity has taken place against a complex strategic backdrop as the wider Balkans region has a diverse, yet fractious, history. The targeting of both Serbia and Republika Srpska is of particular interest as, in recent months, there have been increasingly strong calls by some stakeholders for Republika Srpska to gain further autonomy, or indeed outright secession.²¹⁸

The additional infrastructure revealed previous activity that the Ministry of Interior for Republika Srpska disclosed in April 2020²¹⁹: a spear phishing campaign impersonating the prime minister of Republika Srpska, which led to a malicious HTA file executing PowerShell code from a C2 domain which we identified as connected to the Serbian military phishing domain.

Continued tracking of related infrastructure over the year identified targeting of Serbian research and development organisations closely aligned to military and defence.²²⁰ In September 2021, White Tur performed strategic web compromise on a website to host weaponised documents and archives with Republika Srpska and defence themes²²¹; previous to this, weaponised White Tur files had been hosted on dedicated threat actor-registered infrastructure.

In terms of capabilities, we observed White Tur using macro-weaponised documents leading to a JScript backdoor. Alternatively, White Tur deployed a Windows backdoor, packaged in a weaponised archive containing the open source project OpenHardwareMonitor, that used COM bittransfer objects to send information back to the C2.

Overall, we assess that White Tur is likely an espionage-motivated threat actor, and that it is likely to be aligned to a nation state. Based on regional tensions, there are a number of potential candidates for involvement in this activity, both within the Balkans and farther afield. At present, we do not have sufficient technical evidence to make a high confidence assessment as to the potential backers of White Tur. We do, however, assess that it is likely that the Balkans will remain a region of interest for threat actors of a variety of origins and motivations, White Tur among them. We explore White Tur further in [our blog](#).

Head in the clouds: Blue Odin

Blue Odin (aka CloudAtlas) is a threat actor known for its targeting of a variety of organisations across Russia and Russia-annexed regions of Ukraine using malicious documents, and for closely controlling the payloads these documents deliver in order to increase the difficulty researchers face in tracking it.

In 2021, we observed several new facets to Blue Odin's activity ranging from operational security (OPSEC) errors to new TTPs. In one instance, a malicious document used to target the Ministry of Defence of a country in Central Europe contained embedded links to an online translation service, which appear to have been used to translate the source of the lure contents from its original English to Ukrainian. This, in turn, suggests that the operator who prepared the document may speak Ukrainian as a first language.

Another observation was Blue Odin's use of Responder in early 2021. Responder is an open source tool used to conduct SMB Forced Authentication attacks. In this type of attack, the victim system attempts to authenticate to a threat actor-controlled server using NTLM, enabling the threat actor to capture challenge hashes. These may later be brute-forced offline in order to recover the victim's password. The malicious document in question likely targeted individuals associated with foreign affairs and diplomatic entities, and contained UNC paths to images on threat actor-controlled

servers which resulted in the forced authentication attack described above. Curiously, one of the IP addresses embedded in the document was likely a typo; the specified IP did not appear to be hosting a Responder server, but rather an IP address with a single character difference. This represents a departure from previous techniques used in the threat actor's malicious documents, which generally used remote template links. In other respects Blue Odin's activity remained very similar to that which has been observed previously: such as a malicious document observed in December 2021²²² that fetched a remote template containing an Equation Editor exploit, which downloads and executes an HTA, and in turn deploys a variant of VBShower. This chain is very similar to the exploit chain first documented by Kaspersky in 2019.²²³

From the activity we observed, we assess that there is a realistic probability that Blue Odin's targeting aligns with Ukrainian, rather than Russian, strategic priorities. For example, Blue Odin activity within Ukraine's borders seems to focus primarily on the self-proclaimed separatist regions in Eastern Ukraine, and on Crimea. We also observed Blue Odin targeting Russian organisations, including the energy and government sectors.²²⁴



Blue Otso's rollercoaster

Blue Otso (aka Gamaredon, Armageddon) has experienced both substantial successes and major setbacks in 2021, from wide-ranging compromises of sensitive systems, to exposure by the Security Service of Ukraine.

In February, the Ukrainian National Coordination Center for Cybersecurity reported that Blue Otso had compromised Ukrainian government document management systems known as SEI EB²²⁵ and ASKOD²²⁶. While the initial indicators of compromise were sparse, we identified a set of files which were likely uploaded to an online multi-antivirus scanner by an individual or individuals involved with incident response related to a single ASKOD server.²²⁷ These files included a variety of Blue Otso malware tools including downloader scripts, exfiltration tools, a VNC client, and a script used to add remote template references to Microsoft Word documents, which aligns with assessments made by the NCCC. These archives also included file modification timestamps, which we assessed are likely to be accurate to the times of deployment or modification on the victim machine. These timestamps suggest that the threat actor likely had access to the victim since at least 5th February 2021, several weeks before the incident was disclosed.

Blue Otso operations also faced notable disruptions in 2021. The first example of interest was made public by the Security Service of Ukraine in April, when they disclosed the arrest


of someone in relation to an individual sending messages to the personal numbers of SBU employees.²²⁸ These messages contained a link to a website that we later identified as murders-dkr[.]ru, which contained a link to an archive file purportedly containing lists of SBU officers who had bounties placed on them by one of the separatist entities. This was a first indicator available in open source that Blue Otso, previously thought to be a Russia-based threat actor, may well be supported by activities from non-occupied regions within the borders of Ukraine.

This was later expanded upon in November 2021, when the SBU disclosed the identities of a number of Blue Otso operators, and alleged that the threat actor's activity is tied to an FSB unit based in Crimea.^{229, 230} This unit is reportedly subordinate to the FSB's 18th Centre, otherwise known as the Centre for Information Security, a unit which has previously been linked to data breaches by the US Justice Department. Reportedly²³¹ the SBU first suggested Centre 18 involvement in 2015, at which time they also suggested the involvement of FSB Centre 16, better known for its association with Blue Python (aka Turla, Snake). Our analysis²³² noted that this announcement came amid reports of a Russian military buildup close to the shared Ukrainian/Russian border following large-scale military drills, prior to the war breaking out in Ukraine.

More recent analysis suggests that Blue Otso is undeterred by this disclosure; we assess that it is highly likely this threat actor will remain active in 2022 and onwards.

New Threat

Actors Spotlight



In this section, we spotlight specific cyber threat actors that we discovered in 2021. This does not mean that the threat actors were not previously active. However, as we continuously expand our tracking and identify new threat actors based on our visibility and collection, we think it valuable to give coverage in this report to lesser-known threat actors, and ones that we are still in the process of fully understanding. The threat actors we describe below have been included because they displayed interesting activity whether in their capabilities, targeting, links to other threat actors, or in the kind of operations they perform.



Red Dev 17

In 2021, we started tracking a series of intrusions under the moniker of Red Dev 17 that we assess were highly likely conducted by a China-based threat actor. Our analysis suggests Red Dev 17 has been active since at least 2017.

Red Dev 17's observed targets are mainly in India, and include the Indian military, a multinational India-based technology company, and a state energy company. We assess that it is highly probable that the threat actor behind intrusions associated with Red Dev 17 is also responsible for the campaign known in open source as Operation NightScout.

Red Dev 17 is a user of the 8.t document weaponisation framework (also known as RoyalRoad), and abuses benign utilities such as Logitech or Windows Defender binaries to sideload and execute Chinoxy or PoisonIvy variants on victim systems.

We identified capability and infrastructure links between Red Dev 17 and the threat actor we call Red Hariasa (aka FunnyDream APT), as well as infrastructure overlaps with Red Wendigo (aka Icefog, RedFoxtrot), and with ShadowPad C2 servers. At this time, we do not have sufficient evidence to directly link Red Dev 17 to any of these threat actors. However, we assess with realistic probability that Red Dev 17 operates within a cluster of threat actors that share tools and infrastructure, as well as a strong targeting focus on Southeast Asia and Central Asia.

Blue Dev 6

In October 2021, we observed several weaponised documents which used Cloudflare workers as a C2 channel. We assess that this activity was likely conducted by Blue Dev 6 (aka ReconHellCat), a threat actor first reported on by QuoIntelligence in August 2020.²³³ The weaponised documents used remote templates and macros to execute a payload downloaded from a Cloudflare worker C2. The payload, which was heavily obfuscated, had several similarities to BlackSoul malware (also known as BlackWater), including code used to iterate through browser folders and authenticate during C2 communication. The campaigns we analysed targeted a range of sectors including energy, defence, and government, as well as an international humanitarian organisation.

Yellow Dev 23

We tracked a new cluster of activity focusing on both the telecommunication and IT sectors as Yellow Dev 23 (aka Malkamak, DEV-0270). Open sources reported on this threat actor in late 2021 and described a campaign that focused heavily on Israel, specifically its IT and telecommunication sectors.^{234, 235} In addition to the open source reporting, we observed the threat actor typosquatting domains between February and July that spoofed Facebook and Office365 logins. Several of the malware samples attributed in open source to this threat actor overlap with another Iran-based threat actor we track as Yellow Liderc, which is known for targeting the IT sector in the Middle East.²³⁶

Incident response case study:

White Dev 89 calling



In 2021, we supported an incident response investigation at a health organisation involving a threat actor we named White Dev 89. This threat actor was observed performing opportunistic targeting, likely using malvertising campaigns, to deliver trojanised applications such as Zoom, AnyDesk, and Windscribe to its victims. These would install the respective legitimate applications, but at the same time drop and execute a malicious PowerShell script (likely a modified version of a PowerShellEmpire agent). This access allowed the threat actor to perform basic reconnaissance on the infected system. ²³⁷

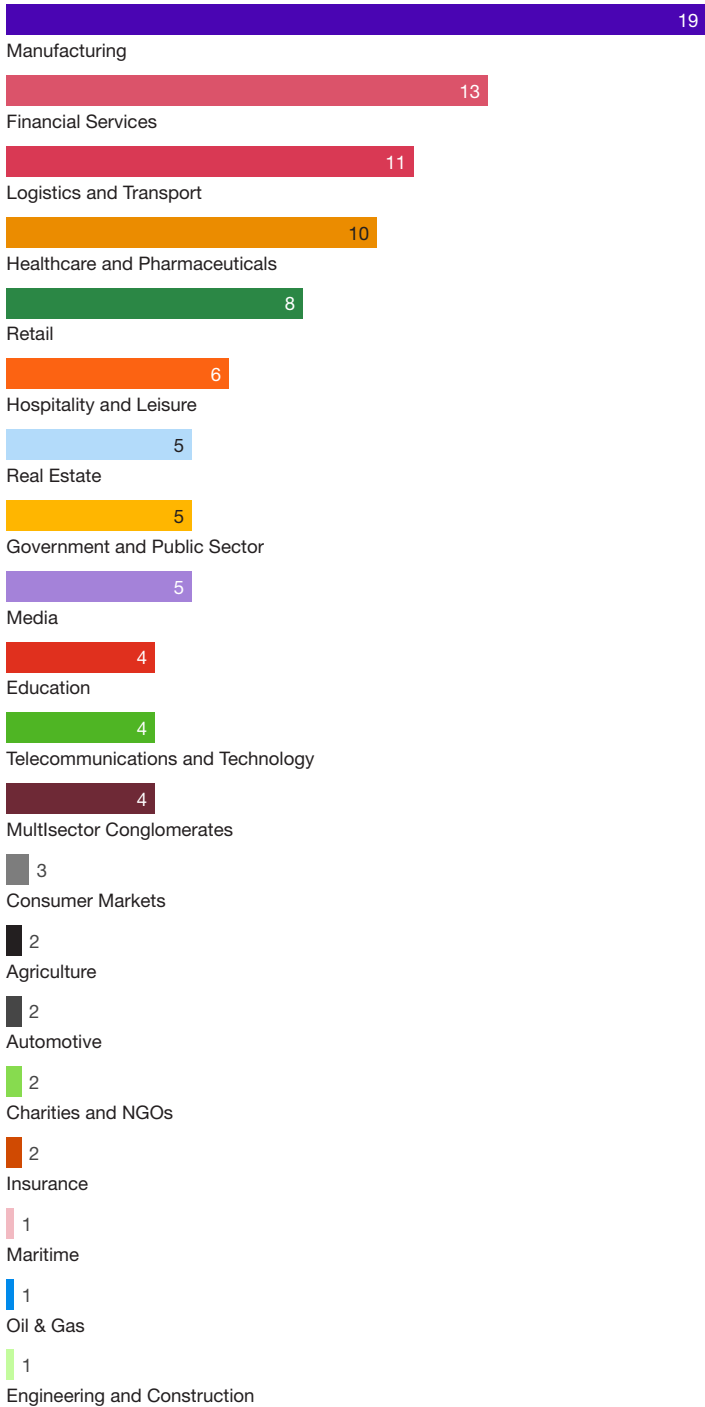
Once White Dev 89 profiled a compromised machine, we observed it dropping an additional PowerShell script to deploy Cobalt Strike Beacon. This kicked off further activity - including laterally moving via SMB to other systems on the network. Other lateral movement techniques that White Dev 89 used included compromising high-privilege accounts, running tools such as ADFind and BloodHound to map out the targeted network, and using 7-ZIP and SubInAcl during post-exploitation.



While the ultimate objectives of this threat actor are not clear, we found connections to other known campaigns. In particular, we found overlaps with infrastructure previously used in QakBot campaigns, leading us to hypothesise that either White Dev 89 is the same threat actor behind QakBot, or that it has previously used QakBot for initial access.

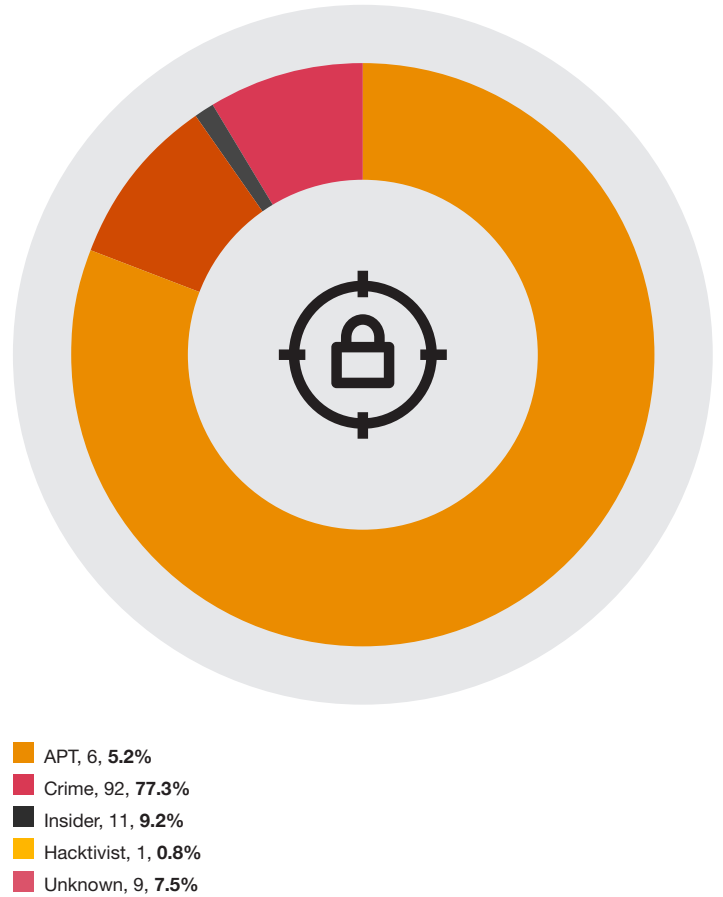
PwC Incident Response statistics

Figure 27: IR ransomware cases by sector 2021



Source: PwC

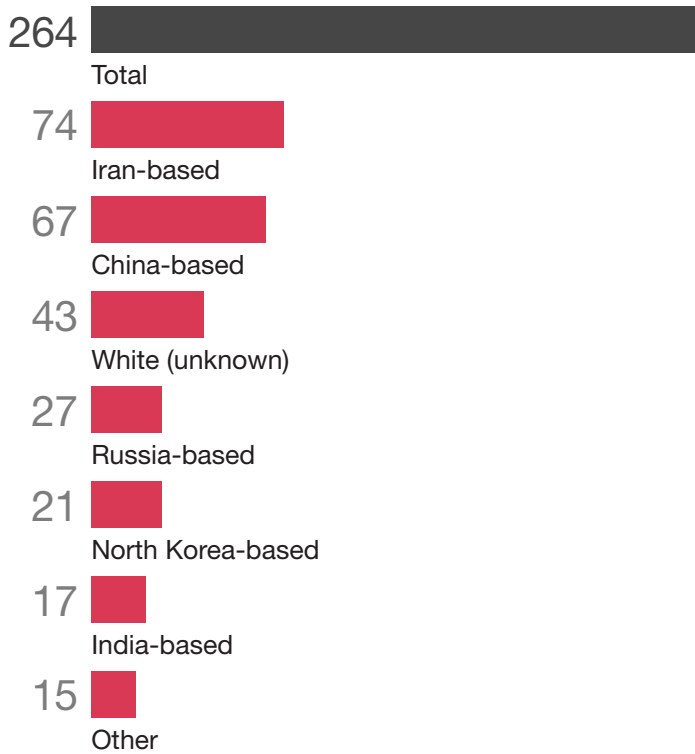
Figure 28: Incidents per type 2021



Source: PwC

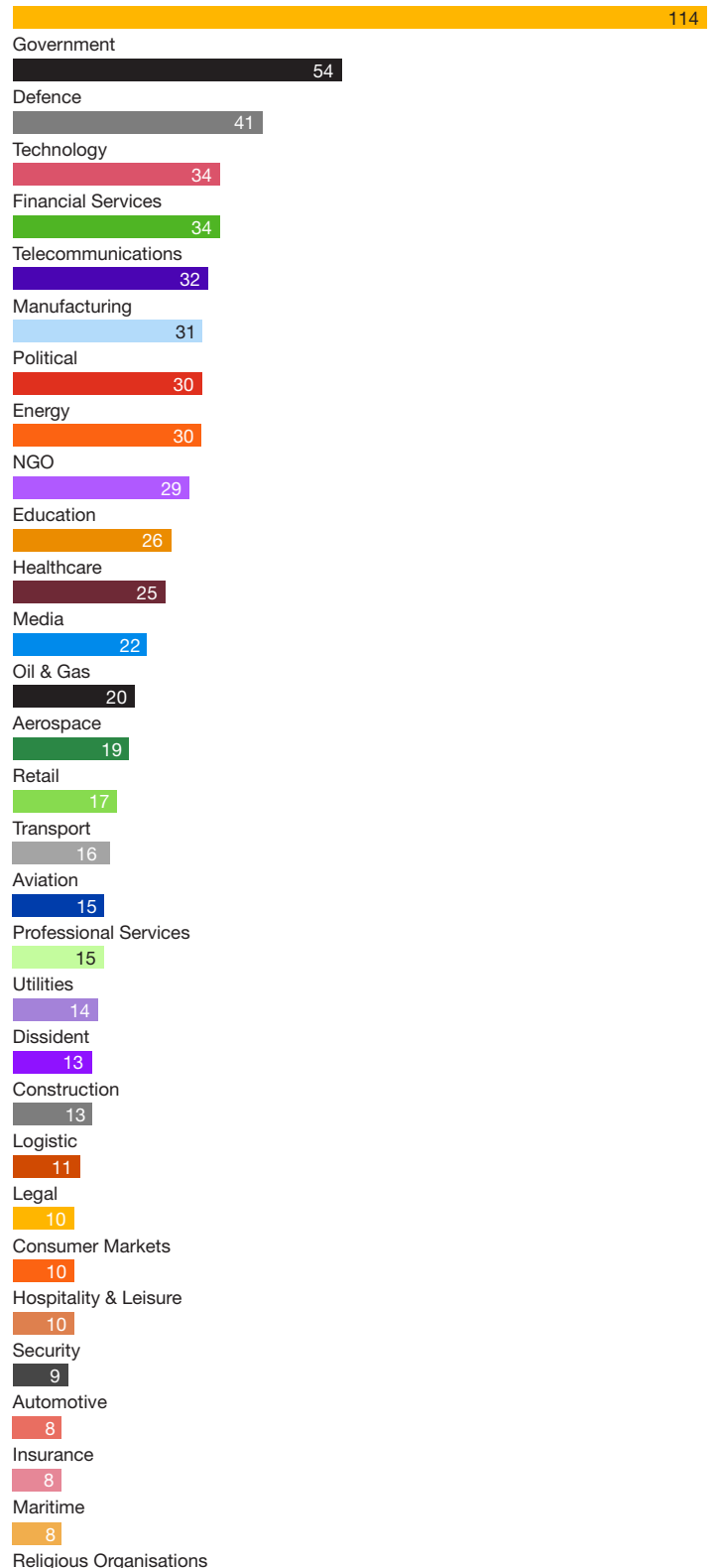
PwC Threat Intelligence reporting statistics

Figure 29: Reports per location of threat actor 2021



Source: PwC

Figure 30: Reports per sector 2021



Source: PwC

Sectors

spotlight

In this section, we highlight key cyber threats we observed in 2021 across a selection of sectors.





Telecommunications

2021 saw continued interest in the telecommunications sector by espionage-motivated threat actors, likely for the purposes of sensitive information collection as we have observed in previous years.²³⁸ We estimate that more than 80 telecommunications companies have been compromised by threat actors based in two countries.

As referenced earlier in this report, Red Menshen (formerly Red Dev 18) deployed its bespoke BPFDoor malware to multiple organisations in the Asia Pacific region, including telecommunication providers based in several countries.²³⁹

PwC has observed other China-based threat actors targeting the telecommunications sector, including Red Kelpie (aka APT41) using its Motnug loader malware on a Pakistan-based provider.²⁴⁰ This same victim also appears to have been targeted by Iran-based threat actor Yellow Mora²⁴¹: in the beginning of 2021, PwC analysed a campaign by Yellow Mora (aka Greenbug) targeting the telecommunication sector in South Asia.²⁴² Our analysis showed that Yellow Mora likely spent a prolonged period of time in the victim's environment, which aligns with public reporting on the way this threat actor operates.²⁴³ Similar activity by Yellow Nix (aka Static Kitten, MERCURY, MuddyWater), starting in January and continuing throughout the year, targeted a large number of telecommunication organisations in the Middle East, South Asia, Southeast Asia, and Central Asia.²⁴⁴ PwC assesses this targeting is likely intended, at least in part, to surveil and track individuals, which aligns with historical targeting of this sector by closely aligned groups like Yellow Mimas.²⁴⁵

Nor did this sector escape targeting by ransomware operations. Blue Lelantos's new Macaw ransomware, for example, was deployed against a US-based telecommunications company, while White Janus and White Apep – two of 2021's most active ransomware operators – also targeted multiple entities in this sector with Lockbit 2.0 and Darkside/BlackMatter ransomware, respectively. Overall, several state telecommunications companies, as well as high-profile private telecommunications providers, have fallen victim to ransomware in the past year, including Ecuador's Corporacion Nacional de Telecomunicacione, Schepisi Communications, and Spain's MasMovil.



Technology

Innovative technology is valuable to those looking to replicate products and services, and intellectual property continues to be sought after by threat actors. Technology companies themselves may be targeted in supply chain and island hopping attacks, particularly where they provide services (including IT and cybersecurity) to customers. In 2021, several airline companies (including members of the One Star Alliance and other individual airlines in the Asia Pacific region) were compromised through an initial breach of their shared communication technology suppliers: SITA.²⁴⁶ Open source analysis²⁴⁷ of this set of intrusions pointed to Red Kelpie as the likely perpetrator. We also observed Red Djinn attempting similar types of intrusions, with the threat actor targeting overseas subsidiaries of Japanese companies likely to move laterally and into the target's main network.

Threat actors were observed using technology company names in SSL certificates associated with their malicious infrastructure, as was identified with China-based threat actors where ShadowPad C2 infrastructure was identified masquerading as NVIDIA Corporation²⁴⁸. We also observed samples of HyperBro malware signed with a certificate belonging to a mobile app company. While there is evidence to suggest HyperBro malware might be shared among multiple China-based threat actors, its original user is Red Phoenix (aka APT27, Emissary Panda, Lucky Mouse). We observed Red Phoenix specifically continue targeting the technology sector, and identified its compromise of at least one US-based technology company.

Targeting against the technology sector was also initiated by cyber criminals, with Acer being compromised by REvil ransomware on two separate occasions: the second of which saw the company receiving a ransom demand of US\$50m, one of the highest publicly known to date.²⁴⁹

Finally, Israeli technology companies also found themselves receiving unwanted attention (purportedly a 'hacktivist' campaign) from White Dev 95, which we assess is very likely a sabotage-motivated threat actor conducting an information operation (IO) against Israel. Rather than using it for extortion, the threat actor encrypts its victims' networks and immediately proceeds to leak any stolen data—activity that bears the hallmarks of "lock and leak" operations.



Financial services

Organisations in the financial services (FS) sector remained a high-value target for cyber criminal threat actors. Across over three months of listings on criminal marketplaces RaidForums, XSS, and Exploit, the financial services entities consistently ranked in the top three most-affected sectors. They had a higher price relative to other impacted sectors, no doubt due to FS listings being of greater interest to buyers in terms of potential financial gains.

Established organised crime groups may specifically target FS entities due to the expectation of large ransom payments. For example, in early 2021 US insurance company CNA was initially compromised when employees executed a fake browser update. The organisation reportedly ended up paying a ransom of US\$40m. In May 2021, operators of the Avaddon ransomware leaked data belonging to Asia-based divisions of the AXA Group (including customer PII), and containing sensitive medical data; they also threatened to attack AXA websites with a Distributed Denial-of-Service (DDoS) attack if a ransom wasn't paid. More recently, in late November 2021 we observed a MirrorBlast campaign most likely conducted by White Austaras, involving spam emails that suggests the targeting of insurance companies based in Canada and France, as well as of a number of Asset and Wealth Management firms based in the US and Hong Kong.²⁵⁰

North Korea-based threat actors continued to pose a severe threat to FS organisations across the board, from investment and venture capital firms, to cryptocurrency exchanges (or any other organisation handling cryptocurrency). A February 2021 US Justice Department indictment of North Korean nationals (believed to be part of Black Artemis) states that the threat actor stole US\$11.8m from a New York financial institution using trojanized cryptocurrency trading applications.²⁵¹ Black Alicanto and Black Dev 2 have been consistently targeting FS entities, often sending spear phishing emails to targets as well as using lure documents related to cryptocurrency, or pretending to be legitimate joint venture pitches.



Retail

In 2021 ransomware operators continued to target the retail sector, exploiting retailers' need to maintain uninterrupted operational uptime—thereby effectively pressuring their victims to pay ransom, quickly. The rapid digitalisation of the retail sector has led to ransomware actors' ability to cripple endpoint payment systems, leading to revenue generation loss; further pressuring the organisation to meet the ransom demand.

Of the ransomware variants that have been observed targeting the retail sector Conti, operated by threat actor White Onibi, was the most active. This ransomware was used to successfully target retailers from clothing outlets to jewellery stores for either big ransom payouts or the theft of unique, sensitive information,^{252, 253, 254} that White Onibi auctioned in 2021.²⁵⁵

Other ransomware operators also targeted the retail sector. As part of the supply-chain attack against Kaseya, Sodinokibi ransomware infected the network of Visma Esscom, an IT supplier. As a result of the Visma Esscom infection, over 500 individual Coop stores across Sweden had to close after its payment systems were taken offline.²⁵⁶ In another example, in December 2021 a ransomware incident affecting retailer SPAR forced a reported 330 UK stores offline for – in some cases – several days. These incidents are just a few of the numerous ones afflicting the retail sector in 2021 and threatening normal business operations.^{257, 258, 259, 260}

Our analysis of listings on criminal marketplaces showed that, while the majority of listings for retail companies contained customer data, several (particularly on the Exploit forum) promised buyers the ability to redirect card payments on e-commerce websites. For brands that operate in the e-commerce space it's also worth remembering that credit card skimming operations known as "Magecart" are ongoing²⁶¹, with the UK NCSC notifying over 4,000 small-to-medium retailers just ahead of the Black Friday sales period that they were using compromised payment portals on their Magento e-commerce platforms.

Incident response case study:

DarkSide - from initial access to ransom demand in four hours



In April 2021, PwC Incident Response teams from multiple countries supported a global retail client that had fallen victim to a ransomware attack perpetrated by DarkSide (tracked by PwC as White Apep).

Analysis of the incident determined that the threat actor initially leveraged a remote access tool known as LogMeIn to gain access to the client's IT estate. This tool was used for legitimate purposes by one of the organisation's IT service providers to enable remote access for maintenance of retail store workstations and supporting systems. The initial intrusion used a functionality in the LogMeIn software whereby users with valid credentials can remotely access a system without any client employee needing to interact with it.

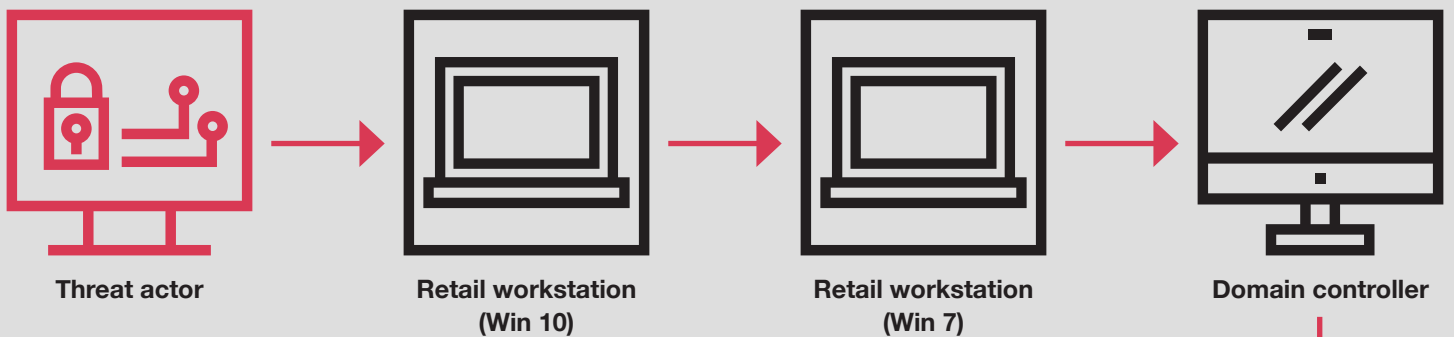
After compromising the retail store client in Country A, the threat actor downloaded administration tools, using them to perform internal reconnaissance on the client's network. Simultaneously, it elevated its privileges to a default administrative account used throughout the domain through LSASS memory dumping. Using the elevated privileges, the threat actor pivoted to systems in Country B which were end-of-life and not receiving updates.

The threat actor then used the credentials collected from these systems to create a Domain Administrator user, generating and storing the account password in a LastPass account belonging to the threat actor.

Once the threat actor had compromised the Domain Controller, it created a scheduled task and deployed it to all computers in the client's IT infrastructure, commanding them to download and run the ransomware. The time from the initial compromise to the ransomware being deployed was roughly four hours. While the ransomware operator demanded a US\$12m ransom, the client managed to establish manual business processes to keep the organisation operational throughout incident response and recovery efforts that spanned three weeks.

DarkSide


From initial access to ransom demand in four hours



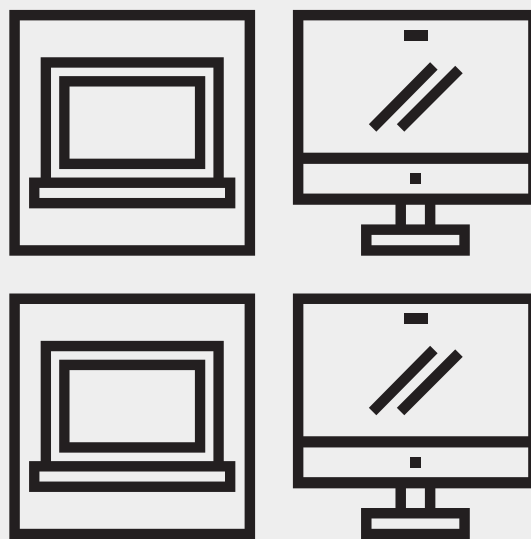
Threat actor compromises a retail store workstation in Country A, using the client's service provider's legitimate RDP credentials

After making a successful remote connection, the threat actor uses LOLbin to move laterally to a retail store workstation in Country B

The threat actor steals passwords, obtaining domain administrator privileges, and successfully compromises the domain controller in Country C



Using the privileges of and access to the domain controller, the threat actor deploys the ransomware on a shared network location to evade antivirus detection, and then deploys ransomware to the IT estate, rendering systems inoperable.



Incident response case study:

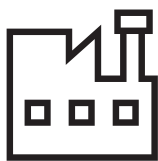
ShinyHunters hunting for treasure



In December 2021, PwC responded to an incident at an India-based retail client that had initially observed a spike in system resource utilisation across its cloud infrastructure, and subsequently received a ransom email from the cyber criminal threat actor we track as White Dev 100 (aka ShinyHunters).

Analysis revealed that the threat actor initially gained access to the network by using a compromised cloud access key belonging to a former C-Suite member of the organisation. The threat actor used the compromised credentials to gain web console access to the client's infrastructure. It was unable to access any of the instances, and proceeded to run reconnaissance commands to map the network.

The threat actor was able to create new instances and SSH keys, eventually injecting them into the SSH-authorized keys store. These actions, combined with the modifications to the security group, allowed the threat actor to freely SSH into the client environment. In addition, it accessed a number of .ssh directories and copied available private SSH keys to support its lateral movement. As the threat actor moved through the network it identified systems of interest, including testing and automation instances which it exploited for further access. During this time the threat actor maintained access to multiple terminal windows into the compromised environment. From analysis of the activity it has not been possible to determine if multiple operators were at work, or a single individual.



Manufacturing

For organisations in the manufacturing sector, any attack which can impact the availability or integrity of infected systems poses a critical risk to an organisation. These attacks cause operational downtime, production and delivery slowdowns resulting in lost revenue, as well as heavy remediation costs which add to the difficulties of returning to service. There are also knock-on issues such as delays in production deadlines, breach in supplier contracts, and reputational damage. Increasingly, the sector is experiencing significant and targeted attacks, ranging from disgruntled employees selling sensitive data to competitors to ransomware attacks conducted by sophisticated organised crime groups.

Operators of BlackMatter ransomware campaigns targeted manufacturing organisations more than any other sector between January and May 2021, in a series of sophisticated attacks which netted over GBP 17.5 million in bitcoin payments²⁶². Lockbit 2.0 also exhibited a heavy focus on the manufacturing organisations, with 21% of leak site data between January and September 2021 belonging to victims in the sector.

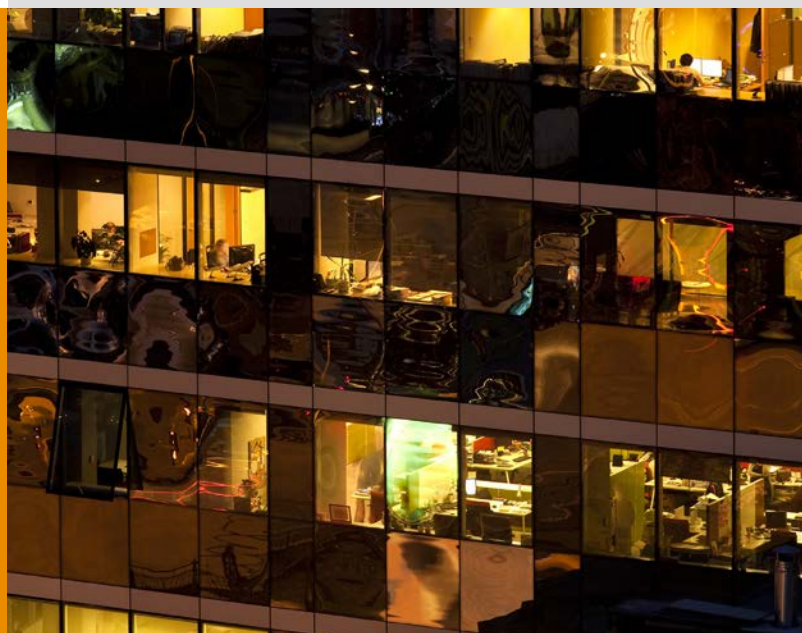
BEC attacks remain a substantial threat to all sectors, including manufacturing. In 2021, PwC observed a campaign most likely associated with Nigeria-based Bronze Dev 2 (aka SilverTerrier) targeting organisations in the manufacturing sector by sending spear phishing emails with a malicious attachment posing as an urgent budget document, which would deliver the commodity RAT AgentTesla.

Espionage remains prevalent within the manufacturing sector, and it has historically attracted high levels of interest from intelligence-gathering threat actors due to its associations with defence and aerospace customers. More widely, the technology investment taking place across the sector is likely to result in a renewed surge of interest. In April 2021 Black Artemis delivered weaponised lure documents, masquerading as job applications, to manufacturing companies which deployed malicious payloads onto the victim network²⁶³. The impact of a successful espionage attack can result in the loss of competitiveness in already tight international markets, as well as regulatory penalties if personal data is accessed in an intrusion.



Incident response case study:

Multinational manufacturing corporation facing LockBit



In March 2021, PwC responded to a ransomware incident affecting a multinational corporation operating in the industrial manufacturing sector, where a LockBit operator executed the ransomware on servers and workstations across ten different countries.

The incident analysis and investigation highlighted that starting from Q4 2020 the threat actor began gathering information about the client and preparing the attack. After gaining initial access, the threat actor used the file hosting service MEGA to download malware and conducted web searches to understand the location and nature of the infected systems. Subsequently, the threat actor downloaded and executed network scanner tools (Softperfect Network Scanner) and performed lateral movement using compromised accounts and supported by popular tools (including Mimikatz).

Throughout the following months, the threat actor compromised a domain controller in the United States, then moved to yet another server in the US, and in March 2021 leveraged a domain controller in Japan to distribute the ransomware.

In the final moments of the attack, the threat actor interacted with the client's antimalware solution to ensure that the ransomware would not be stopped, and ultimately distributed and executed the ransomware. Although the attack caused significant disruption to the victim organisation, there was no clear evidence of data exfiltration.

Conclusion

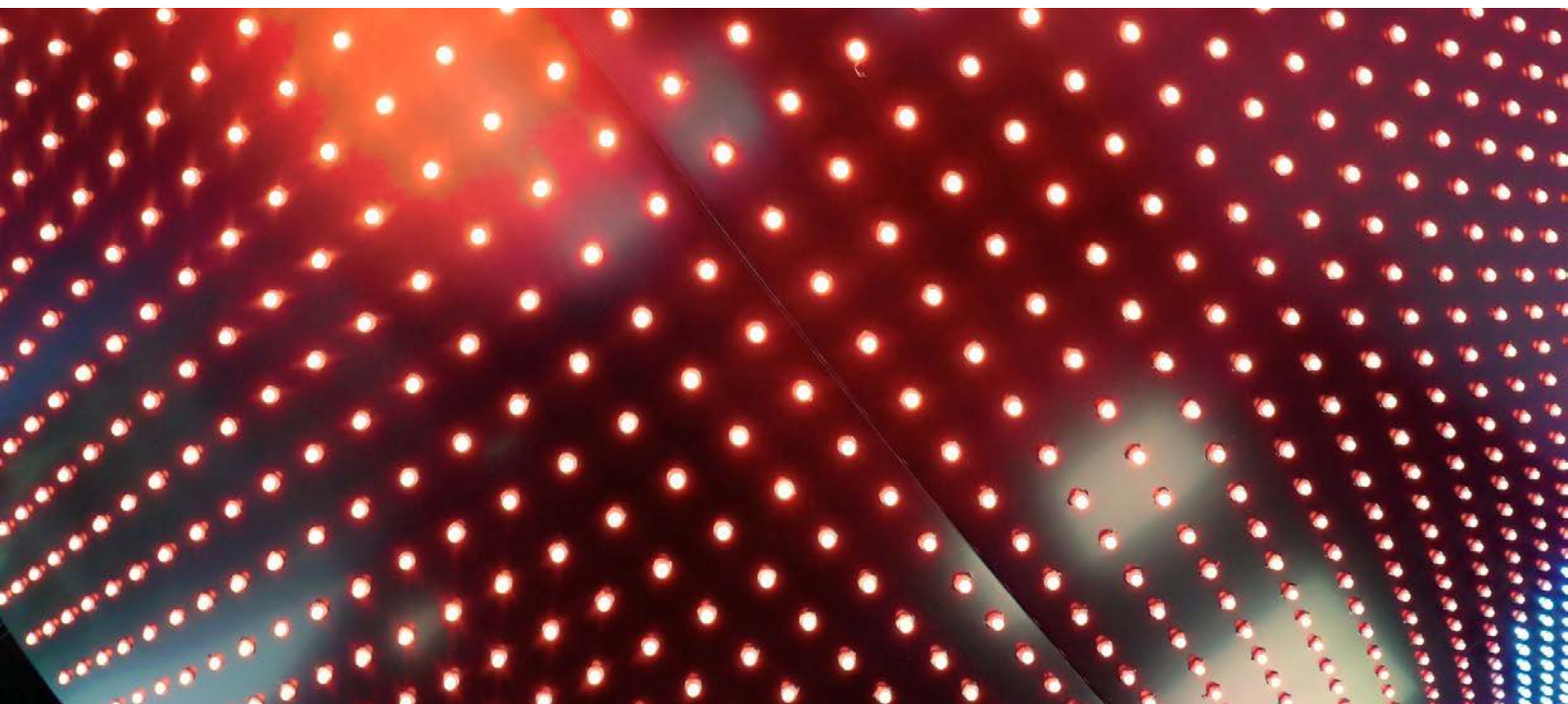
In 2021, the cyber threat landscape continued to see an increase in threat actors of all motivation and skill levels.

As in recent years, ransomware continues to be the most pervasive and immediately impactful threat to organisations of all sizes and sectors across the world, with ransomware developers continuing to grow their affiliate schemes in size, revenue, and capabilities. Supply chain attacks have now become part of the “new normal” of the cyber threat landscape, with cyber criminal threat actors incorporating them in their playbooks for maximum impact.

At the same time, a different type of threat to a secure digital society has been brought squarely into focus with the prominence and impact of digital quartermasters: both those traditionally aligned with state-sponsored operations, as well as commercial private sector brokers providing a wide range of clients with high-end offensive tooling and capabilities.

All these threats have culminated in a renewed focus on 0-day vulnerabilities - with several examples enabling both targeted operations and mass-scale attacks, and growing financial and strategic incentives pushing exploit research and development activity.

We assess that the themes that have emerged or have continued into 2021 – including ransomware and its surrounding criminal ecosystem, the importance of vulnerability and tools brokers, and the fallout of newly discovered vulnerabilities impacting unprepared victims – will continue into 2022. In the face of headline-grabbing vulnerabilities and incidents, cybersecurity becomes ever more present in the public eye, and it is even more important than ever for defenders to continue collaborating, sharing, and supporting organisations and society; focusing on prevention and detection measures, as well as incident mitigation and response plans that can stymie threat actors effectively.





PwC Cybersecurity

If you would like more information on any of the threats detailed in this report, please feel free to get in touch with us at threatintelligence@pwc.com.

PwC is globally recognised by industry analysts as a leader in cybersecurity; as a firm with strong global delivery capabilities, and the ability to address the security and risk challenges our clients face.

We underpin our board-level security strategy and advisory consulting services with expertise gleaned from the front lines of cyber defence across our niche technical expertise in services such as managed cyber defence, red teaming, incident response, and threat intelligence.

We differentiate ourselves with our ability to combine strategic thinking, strong technical capabilities, and complex engagement delivery with client service excellence. Our unique research and security intelligence, technical expertise, and understanding of cyber risk helps clients get the clarity they need to confidently adapt to new challenges and opportunities.

We bring together a team of specialists with expertise in security management, threat detection and monitoring, threat intelligence, security architecture and consulting, behavioural change, and regulatory and legal advice in our efforts to help our clients protect what matters most to them.

We specialise in providing the services required to help clients resist, detect, and respond to advanced cyberattacks. This includes crisis events such as data breaches, ransomware attacks, economic espionage, and targeted intrusions, including those commonly referred to as APTs. Our threat intelligence research underpins all of our security services, and is used by public and private sector organisations around the world to protect networks, provide situational awareness, and inform strategy.

Endnotes

1. '2021 has broken the record for zero-day hacking attacks', MIT Technology Review: Patrick Howell O'Neill, <https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/> (23rd September 2021)
2. 'New German government coalition promises not to buy exploits', Recorded Future, <https://therecord.media/new-german-government-coalition-promises-not-to-buy-exploits/> (8th December 2021)
3. Full (vulnerability) disclosure', PwC Threat Intelligence, CTO-SIB-20210810-01A
4. 'Play evil games, win evil prizes', PwC Threat Intelligence, CTO-SIB-20210625-01A
5. Google, 'Project Zero', <https://googleprojectzero.blogspot.com/>
6. 'Shining a light on ShadowPad usage throughout 2019', PwC Threat Intelligence, CTO-TIB-20200213-01A
7. 'Chasing Shadows', PwC Threat Intelligence, CTO-TIB-20211021-01A
8. 'My, My, MySQL tracking C2 infrastructure through certificate reuse', PwC Threat Intelligence, CTO-TIB-20210226-01B
9. 'HAFNIUM exploiting Exchange vulnerabilities', PwC Threat Intelligence, CTO-QRT-20210303-01A
10. 'HAFNIUM targeting Exchange Servers with 0-day exploits', Microsoft, <https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/> (2nd March 2021)
11. 'Operation Exchange Marauder: Active Exploitation of Multiple 0-day Microsoft Exchange Vulnerabilities', Volety: Josh Grunzweig, Matthew Meltzer, Sean Koessel, Steven Adair, Thomas Lancaster, <https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-0-day-vulnerabilities/> (2nd March 2021)
12. 'Eat, Sleep, Liderc, Repeat', PwC Threat Intelligence, CTO-TIB-20210730-01A
13. 'Caught in a .NET', PwC Threat Intelligence, CTO-TIB-20210211-02A
14. 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence
15. 'A closer look at commercial quartermasters', PwC Threat Intelligence, CTO-SIB-20210906-01A
16. 'Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus', Citizen Lab, <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/> (15th July 2021)
17. 'Protecting customers from a private-sector offensive actor using 0-day exploits and DevilsTongue malware', Microsoft, <https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/> (15th July 2021)
18. 'How we protect users from 0-day attacks', Google, <https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/> (14th July 2021)
19. 'Another commercial quartermaster', PwC Threat Intelligence, CTO-TIB-20210806-02A
20. 'Another commercial quartermaster', PwC Threat Intelligence, CTO-TIB-20210806-02A
21. 'A closer look at commercial quartermasters', PwC Threat Intelligence, CTO-SIB-20210906-01A
22. 'FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild', CitizenLab: Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, Ron Deibert, <https://citizenlab.ca/2021/09/forcedentry-nso-group-essage-zero-click-exploit-captured-in-the-wild/> (13th September 2021)
23. 'A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution', Google Project Zerolan Beer & Samuel Groß, <https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html> (15th December 2021)
24. 'Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities', United States Commerce Department, <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list> (3rd November 2021)
25. 'You Only Click Twice: FinFisher's Global Proliferation', CitizenLab: Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, <https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/> (13th March 2013)
26. 'FinSpy: Unseen Findings', Kaspersky, <https://securelist.com/finspy-unseen-findings/104322/> (28th September 2021)
27. 'Exclusive: An American Company Fears Its Windows Hacks Helped India Spy On China And Pakistan', Forbes: Thomas Bewster, <https://www.forbes.com/sites/thomasbrewster/2021/09/17/exodus-american-tech-helped-india-spy-on-china-and-pakistan/?sh=13286ba07009> (17th September 2021)
28. 'Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community', CitizenLab: Masashi Crete-Nishihata, Jakub Dalek, Etienne Maynier, John Scott-Railton, <https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/> (30th January 2018)
29. 'Red Dev Redemption', PwC Threat Intelligence, CTO-TIB-20210202-01A
30. 'Red Dev Redemption 2', PwC Threat Intelligence, CTO-TIB-20210223-01A
31. 'Red Dev Redemption 3', PwC Threat Intelligence, CTO-TIB-20210401-01A
32. "'LuoYu': The eavesdropper sneaking in multiple platforms", Team T5: Leon & Shui, https://jsac.jpCERT.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf (28th January 2021)
33. 'Red Dev 7 gets a Nue name', PwC Threat Intelligence, CTO-TIB-20201016-01A
34. 'APT trends report Q2 2017', Kaspersky, <https://securelist.com/apt-trends-report-q2-2017/79332/> (8th August 2017)
35. 'LootRAT deals four of a kind', PwC Threat Intelligence, CTO-TIB-20200130-02A
36. 'Threats under the Spotlight: February 2021', PwC Threat Intelligence, CTO-TUS-20210317-01A
37. 'Malware WinDealer used by LuoYu Attack Group', JPCERT: Yuma Masubuchi, <https://blogs.jpCERT.or.jp/en/2021/10/windealer.html#1> (26th October 2021)
38. 'Threats under the Spotlight: April 2021', PwC Threat Intelligence, CTO-TUS-20210511-01A
39. 'White Dev 75, like shooting phish in a barrel', PwC Threat Intelligence, CTO-TIB-20210303-01A
40. 'New White Dev 75 infrastructure', PwC Threat Intelligence, CTO-TIB-20211015-01A
41. 'When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users', Amnesty, <https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/> (19th December 2018)
42. 'Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa', Amnesty International, <https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/> (16th August 2019)
43. 'Yellow Garuda's VIP Telegram tool', PwC Threat Intelligence, CTO-TIB-20220110-01A

70 PwC Cyber Threats 2021: A Year in Retrospect

44. UNC788: IRAN'S DECADE OF CREDENTIAL HARVESTING AND SURVEILLANCE OPERATIONS, VB2021 localhost, <https://vbloglocalhost.com/uploads/VB2021-Haeghebaert.pdf> (October 2021)
45. 'A fresh bouquet of malware', PwC Threat Intelligence, CTO-TIB-20210511-02A
46. 'Lockbit 2.0', PwC Threat Intelligence, CTO-TIB-20211027-02A
47. CTO-TIB-20211209-01A - Nothing else BlackMatters, CTO-TIB-20210827-01A - How to be a ransomware operator
48. 'Economy of the United States by sector', Wikipedia, https://en.wikipedia.org/wiki/Economy_of_the_United_States_by_sector
49. <https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html>
50. 'Department of Justice Launches Global Action Against NetWalker Ransomware', US Department of Justice, <https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware>, 27th January 2021
51. 'Babuk - A new kid on the block', PwC Threat Intelligence, CTO-TIB-20210201-02A
52. 'Ransomware gang leaks data from Metropolitan Police Department', BleepingComputer: Sergiu Glatan, <https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-from-metropolitan-police-department/> (11th May 2021)
53. 'DarkSide', PwC Threat Intelligence, CTO-QRT-20210512-01A
54. 'Hackers Breached Colonial Pipeline Using Compromised Password', Bloomberg: William Turton, Kartikay Mehrotra, <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password> (4th June 2021)
55. 'Ransomware Attack on Health Sector - UPDATE 2021-05-16', Ireland National Cybersecurity Centre, https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf (16th May 2021)
56. 'JBS: Cyber-attack hits world's largest meat supplier', BBC, <https://www.bbc.co.uk/news/world-us-canada-57318965> (2nd June 2021)
57. 'Kaseya supply chain compromise', PwC Threat Intelligence, CTO-QRT-20210703-01A
58. 'Important Notice August 4th, 2021', Kaseya, <https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-August-4th-2021> (4th August 2021)
59. 'Treasury Takes Robust Actions to Counter Ransomware', US Department of Treasury, <https://home.treasury.gov/news/press-releases/jy0364>, 21st September 2021
60. 'Ukrainian Arrested and Charged with Ransomware Attack on Kaseya', US Department of Justice, <https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya>, 8th November 2021
61. 'Ransomware gets more ban for its buck', PwC Threat Intelligence, CTO-SIB-20210525-01A
62. 'DarkSide', PwC Threat Intelligence, CTO-QRT-20210512-01A
63. 'Understanding REvil: The Ransomware Gang Behind the Kaseya VSA Attack', Palo Alto Unit 42: John Martineau, <https://unit42.paloaltonetworks.com/revil-threat-actors/> (6th July 2021)
64. 'QakBot – a dip into the pond', PwC Threat Intelligence, CTO-TIB-20200515-02A
65. 'Egregor Meet the new boss', PwC Threat Intelligence, CTO-TIB-20201203-01A
66. 'Rezident evil: Dridex indictments', PwC Threat Intelligence, CTO-SIB-20200102-01A
67. 'WastedLocker - EvilCorp's new smoking gun', PwC Threat Intelligence, CTO-TIB-20200730-01A
68. 'New World, New Macaw', PwC Threat Intelligence, CTO-QRT-20211117-01A
69. 'A new DoppelPaymer', PwC Threat Intelligence, CTO-TIB-20200710-01A
70. 'Causing more Grief', PwC Threat Intelligence, CTO-TIB-20211028-01A
71. 'Darkside Ransomware Decryption Tool', Bitdefender, <https://www.bitdefender.com/blog/labs/darkside-ransomware-decryption-tool/> (11th January 2021)
72. 'Darkside', PwC Threat Intelligence, CTO-QRT-20210512-01A
73. 'DarkSide, Blamed for Gas Pipeline Attack, Says It is Shutting Down' New York Times, <https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html> (14th May 2021)
74. 'Nothing else BlackMatters', PwC Threat Intelligence, CTO-TIB-20211209-01A
75. 'Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice', US Department of State, <https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice/> (4th November 2021)
76. 'Moscow court arrests all REvil ransomware hackers detained after FBI request to Russia', TASS, <https://tass.com/russia/1388649> (15th January 2022)
77. 'Exploitation of Accellion File Transfer Appliance', Cybersecurity and Infrastructure Security Agency (CISA), <https://www.cisa.gov/uscert/ncas/alerts/aa21-055a>, 24th February 2021
78. 'Accellion Provides Update to FTA Security Incident Following Mandiant's Preliminary Findings', Accellion, <https://www.globenewswire.com/news-release/2021/02/22/2179666/0/en/Accellion-Provides-Update-to-FTA-Security-Incident-Following-Mandiant-s-Preliminary-Findings.html> (22nd February 2021)
79. 'Kaseya supply chain compromise', PwC Threat Intelligence, CTO-QRT-20210703-01A
80. 'Emotet is back', PwC Threat Intelligence, CTO-QRT-20211116-01A
81. 'World's most dangerous malware Emotet disrupted through global action', Europol, <https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action> (18th November 2021)
82. 'How the new Emotet differs from previous versions', Intel 471, "<https://intel471.com/blog/emotet-returns-december-2021>", 9th December, 2021
83. 'Colder than IcedID', PwC Threat Intelligence, CTO-TIB-20210511-01A
84. 'AaaS you like it', PwC Threat Intelligence, CTO-SIB-202108802-01A
85. 'Report of the Panel of Experts established pursuant to resolution 1874 (2009)', United Nations Security Council, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf (30th August 2019)
86. 'All LNKs lead back to Black Dev 1 Part 1', PwC Threat Intelligence, CTO-TIB-20210408-01A
87. 'All LNKs lead back to Black Dev 1 Part 2', PwC Threat Intelligence, CTO-TIB-20210525-01A
88. 'Who is Black Alicanto hiring', PwC Threat Intelligence, CTO-TIB-20210913-01A
89. 'All LNKs lead back to Black Dev 1 Part 1', PwC Threat Intelligence, CTO-TIB-20210408-01A
90. 'Unveiling the Cryptomimic', NTT Security: Hajime Takai, Shogo Hayashi, Rintaro Koike <https://vb2020.vbloglocalhost.com/uploads/VB2020-Takai-et-al.pdf> (2020)
91. 'Lazarus Group Campaign Targets Cryptocurrency Vertical', F-Secure, <https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-ttp-white-lazarus-threat-intel-report2.pdf> (18th August 2020)
92. 'Attributing Attacks Against Crypto Exchanges to LAZARUS – North Korea', ClearSky, <https://www.clearskysec.com/wp-content/uploads/2021/05/CryptoCore-Lazarus-Clearsky.pdf> (May 2021)
93. 'Capital injection', PwC Threat Intelligence, CTO-TIB-20210630-03A
94. 'Bitcoin is silver, compromise is gold: Emerging North Korea-based threat actors on the hunt for cryptocurrency', PwC: Sveva Vittoria Scenarelli, <https://www.youtube.com/watch?v=BOZecjABjSk>

71 PwC Cyber Threats 2021: A Year in Retrospect

95. 'The Banshee, The Flower, The Dragon and Prince', PwC Threat Intelligence, CTO-TIB-20210508-01A
96. 'North Korean attackers use malicious blogs to deliver malware to high-profile South Korean targets', Cisco Talos: Jung soo An, Asheer Malhotra, Kendall McKay, <https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html> (10th November 2021)
97. 'Nuclear Policy For BabySharks', PwC Threat Intelligence, CTO-TIB-20211014-01A
98. 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence (2020)
99. 'Your dream job awaits - just please enable editing', PwC Threat Intelligence, CTO-TIB-20210916-01A
100. 'Paint me like one of your BMP files', PwC Threat Intelligence, CTO-TIB-20210428-01A
101. 'New campaign targeting security researchers', Google, <https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/> (25th January 2021)
102. 'ZINC attacks against security researchers', Microsoft, <https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/> (28th January 2021)
103. 'North Korean Hackers Caught Snooping on China's Cyber Squad', The Daily Beast: Shannon Vavra, <https://www.thedailybeast.com/north-korean-hackers-caught-snooping-on-chinas-cyber-squad> (22nd November 2021)
104. @ESETresearch, Twitter, <https://twitter.com/ESETresearch/status/1458438155149922312?s=20> (10th November 2021)
105. 'China's 5-year plan has 7 technology targets' watch for responses', S&P Global, <https://www.spglobal.com/marketintelligence/en/newsinsights/latest-news-headlines/china-s-5-year-plan-has-7-technology-targets-watch-for-responses-63161384> (15th March 2021)
106. 'BlackTechs ELF-esteem', PwC Threat Intelligence, CTO-TIB-20210329-01A
107. 'BlackTech's Gh0st', PwC Threat Intelligence, CTO-TIB-20201113-01A
108. 'Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors', Symantec, <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt> (29th September 2020)
109. 'Red Djinn's red flags', PwC Threat Intelligence, CTO-TIB-20210903-02B
110. 'Back to Black(Tech): an analysis of recent BlackTech and an open directory full of exploits', PwC: Sveva Vittoria Scenarelli, Adam Prescott, <https://vblocalhost.com/conference/presentations/back-to-blacktech-an-analysis-of-recent-blacktech-operations-and-an-open-directory-full-of-exploits/> (7th October 2021)
111. 'Red Djinn's spider web', PwC Threat Intelligence, CTO-TIB-20211202-01A
112. 'NICKEL targeting government organizations across Latin America and Europe', Microsoft, <https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/> (6th)
113. 'Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity', US CISA, <https://us-cert.cisa.gov/ncas/alerts/aa20-258a> (24th October 2020)
114. 'A committee of vultures', PwC Threat Intelligence, CTO-SIB-20210722-01A
115. 'Okrum and Ketrican: An Overview of Recent Ke3chang Group Activity', ESET, July 2019, https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf
116. 'BfV Cyber-Brief Nr. 01/2021 - Bedrohung deutscher Stellen durch Cyberangriffe der Gruppierung APT31', Bundesamt für Verfassungsschutz, <https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-cyberabwehr/broschuere-2021-01-bfv-cyber-brief-2021-01> (18th January 2021)
117. 'Red Keres flows into South East Asia', PwC Threat Intelligence, CTO-TIB-20210211-01A
118. 'Learning to ChaCha with Red Kelpie', PwC Threat Intelligence, CTO-TIB-20210624-02A
119. 'Active exploitation of CVE-2021-26084', PwC Threat Intelligence, CTO-QRT-20210906-01A
120. 'This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits', Mandiant, <https://www.mandiant.com/resources/apt41-initiates-globalinvasion-campaign-using-multiple-exploits> (25th March 2020)
121. 'Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally', US Department of Justice, <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer> (16th September 2020)
122. 'Introducing Red Dev 14', PwC Threat Intelligence, CTO-TIB-20210412-01A
123. Mandiant, 'Advanced Persistent Threat Groups', <https://www.mandiant.com/resources/apt-groups>
124. 'Learning to ChaCha with Red Kelpie', PwC Threat Intelligence, CTO-TIB-20210624-02A
125. 'ShadowPad not a dead cert', PwC Threat Intelligence, CTO-TIB-20211116-02A
126. 'Inside a Red toolbox', PwC Threat Intelligence, CTO-TIB-20210518-01A
127. 'Orange Kala enters the Warzone', PwC Threat Intelligence, CTO-TIB-20210112-01A
128. 'Compromising Eurasian Telecoms justforfun', PwC Threat Intelligence, CTO-TIB-20210709-01A
129. 'A Window into Red Dev 18', PwC Threat Intelligence, CTO-TIB-20210831-02A
130. 'Of Gh0sts and Golang', PwC Threat Intelligence, CTO-TIB-20211011-01A
131. 'Red Dev 18 Further Developments', PwC Threat Intelligence, CTO-QRT-20210727-01A
132. 'Batch scripts back alright', PwC Threat Intelligence, CTO-TIB-20210223-02A
133. 'Orange Kala or Orange Dev 1 - you decide', PwC Threat Intelligence, CTO-TIB-20210520-01A
134. 'BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps', BlackBerry Cylance, <https://www.blackberry.com/us/en/forms/enterprise/bahamut-report> (October 2020)
135. 'The White Company: Inside the Operation Shaheen Espionage Campaign', Cylance, <https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf> (18th March 2021)
136. 'BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps', BlackBerry Cylance, <https://www.blackberry.com/us/en/forms/enterprise/bahamut-report> (October 2020)
137. 'Sharing is Caring', PwC Threat Intelligence, CTO-TIB-20210818-01A
138. 'Confucius APT deploys Warzone RAT', Uptycs: Abhijit Mohanta, Ashwin Vamshi, <https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat> (12th January 2021)
139. 'Warzone RAT - Beware of the Trojan malware stealing data triggering from various Office documents', Quickheal: Ayush Puri, <https://blogs.quickheal.com/warzonerat-beware-of-the-trojan-malware-stealing-data-triggering-from-various-office-documents/> (1st July 2021)
140. 'Monsoon - Analysis of an APT campaign', Forcepoint <https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysisreport.pdf>
141. 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence
142. 'Orange Athos has BADNEWS for its adversaries', PwC Threat Intelligence, CTO-TIB-20210204-02A
143. 'Threats under the Spotlight October 2021', PwC Threat Intelligence, CTO-TUS-20211118-01A

72 PwC Cyber Threats 2021: A Year in Retrospect

144. 'Orange Yali continues to set up shop in Pakistan', PwC Threat Intelligence, CTO-TIB-20210527-02A
145. 'Operation "Magichm": CHM file release and subsequent operation of BITTER-organization', QiAnXin, <https://ti.qianxin.com/blog/articles/%22operationmagichm%22:CHM-file-release-and-subsequent-operation-of-BITTER-organization/> (15th March 2021)
146. 'Windows kernel 0-day exploit (CVE-2021-1732) is used by BITTER APT in targeted attack', DBAPPSecurity, <https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/windows-kernel-0-day-exploit-is-used-by-bitter-apt-in-targeted-attack/> (10th February 2021)
147. '0-day vulnerability in Desktop Window Manager (CVE-2021-28310) used in the wild', Kaspersky: Boris Larin, Costin Raiu, Brian Bartholomew, <https://securelist.com/0-day-vulnerability-in-desktop-window-manager-cve-2021-28310-used-in-the-wild/101898/> (13th April 2021)
148. 'APT trends report Q2 2021', Kaspersky, <https://securelist.com/apt-trends-report-q2-2021/103517/> (29th July 2021)
149. 'CrimsonRAT - Green Havildars premium export', PwC Threat Intelligence, CTO-TIB-20210310-02A
150. 'Transparent Tribe APT Infrastructure Mapping Part 1: A High-Level Study of CrimsonRAT Infrastructure October 2020 – March 2021', Team Cymru: Joshua Picolet, <https://team-cymru.com/blog/2021/04/16/transparent-tribe-apt-infrastructure-mapping/> (16th April 2021)
151. 'Transparent Tribe APT Infrastructure Mapping Part 2: A Deeper Dive into the Identification of CrimsonRAT Infrastructure October 2020 – June 2021', Team Cymru: Joshua Picolet, <https://team-cymru.com/blog/2021/07/02/transparent-tribe-apt-infrastructure-mapping-2/> (2nd July 2021)
152. 'Aggah Using Compromised Websites to Target Businesses Across Asia, Including Taiwan Manufacturing Industry', Anomali, <https://www.anomali.com/blog/aggahusing-compromised-websites-to-target-businesses-across-asia-including-taiwan-manufacturing-industry> (12th August 2021)
153. 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence
154. 'Threats under the Spotlight - December 2020', PwC Cyber Threat Intelligence, CTO-TUS-20210111-01A
155. 'Not Enough Mana to Conduct that Operation', PwC Threat Intelligence, CTO-TIB-20210630-02A
156. '针对性伪装攻击，终端信息安全的间谍--海莲花 APT', Sangfor, https://mp.weixin.qq.com/s/WnKc0JbjA5_IsjPFSzFoYA (31st March 2021)
157. 'RotaJakiro: A long live secret backdoor with 0 VT detection', 360 Netlab, https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/ (28th April 2021)
158. 'Youre not Shikata Ga Nai believe this', PwC Threat Intelligence, CTO-TIB-20211102-02A
159. 'Whose campaign is it anyway', PwC Threat Intelligence, CTO-TIB-20211121-01A
160. 'Ransomware or sabotage, that is the question', PwC Threat Intelligence, CTO-SIB-20210927-01A
161. 'Ransomware or sabotage, that is the question', PwC Threat Intelligence, CTO-SIB-20210927-01A
162. 'Whose campaign is it anyway', PwC Threat Intelligence, CTO-TIB-20211121-01A
163. 'New Version Of Apostle Ransomware Reemerges In Targeted Attack On Higher Education', SentinelOne, <https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/#:~:text=New%20Version%20Of%20Apostle%20Ransomware%20Reemerges%20In%20Targeted%20Attack%20On%20Higher%20Education,-Amitai%20Ben%20Shushan&text=SentinelLabs%20has%20been%20tracking%20the,destructive%20attacks%20starting%20December%202020.> (30th September 2021)
164. 'Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021', Microsoft, <https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/> (16th November 2021)
165. 'Sharp dressed threat actor', PwC Threat Intelligence, CTO-TIB-20211222-02A
166. 'Pay2Key to N3tw0rm', PwC Threat Intelligence, CTO-TIB-20210513-01A
167. 'Missed connections', PwC Threat Intelligence, CTO-TIB-20210216-01A
168. 'A blast from the past', PwC Threat Intelligence, CTO-TIB-20210622-01A
169. 'Scanning the internet for vulnerabilities', PwC Threat Intelligence, CTO-TIB-20211118-01A
170. 'The mysteries of Pay2Key', PwC Threat Intelligence CTO-SIB-20210113-01A
171. 'The [redacted] sheds light on a campaign', PwC Threat Intelligence, CTO-TIB-20210712-01A
172. 'White Dev 75, like shooting phish in a barrel', PwC Threat Intelligence, CTO-TIB-20210303-01A
173. 'Yellow Maeros Art Attack', PwC Threat Intelligence, CTO-TIB-20210226-02A
174. 'New job, same malware', PwC Threat Intelligence, CTO-TIB-20210806-01A
175. 'The [redacted] sheds light on a campaign, PwC Threat Intelligence, CTO-TIB-20210712-01A
176. 'The [redacted] sheds light on a campaign, PwC Threat Intelligence, CTO-TIB-20210712-01A
177. 'I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona', Proofpoint, <https://www.proofpoint.com/us/blog/threat-insight/iknew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media> (28th July 2021)
178. 'Of course Im real...', PwC Threat Intelligence, CTO-SIB-20210818-01A
179. 'Eat, Sleep, Liderc, Repeat', PwC Threat Intelligence, CTO-TIB-20210730-01A
180. 'Iran-based threat actor responses to rising geopolitical tensions', PwC Threat Intelligence, CTO-SIB-20200108-01A
181. 'Taking Action Against Hackers in Iran', Meta, <https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/> (15th July 2021)
182. 'Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021', Microsoft, <https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021> (16th November 2021)
183. 'Yellow Nix shifts south east', PwC Threat Intelligence, CTO-TIB-20211015-03A
184. 'Yellow Nix has a complaint', PwC Threat Intelligence, CTO-TIB-20211216-02A
185. 'New Iranian Espionage Campaign By "Siamesekitten" – Lyceum', ClearSky, <https://www.clearskysec.com/siamesekitten> (17th August 2021)
186. 'Finding Yellow Dev 9, PwC Threat Intelligence, CTO-TIB-20211028-02A
187. 'Lyceum calling', PwC Threat Intelligence, CTO-TIB-20200605-01A
188. 'Get your shine on Yellow Garuda', PwC Threat Intelligence, CTO-TIB-20210514-01A
189. 'Only if your invited', PwC Threat Intelligence, CTO-QRT-20210907-01A
190. 'A fresh bouquet of malware', PwC Threat Intelligence, CTO-TIB-20210511-02A
191. 'Charming Kittens Telegram bot', PwC Threat Intelligence, CTO-TIB-20210909-01A
192. 'Alert (AA20-304A) Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data', US CISA, <https://us-cert.cisa.gov/ncas/alerts/aa20-304a>
193. 'Learning on the job with Yellow Dev 19', PwC Threat Intelligence, CTO-TIB-20201118-02A
194. 'Learning on the job with Yellow Dev 19', PwC Threat Intelligence, CTO-TIB-20201118-02A
195. 'Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election', United States Department of the Treasury, <https://home.treasury.gov/news/press-releases/jy0494> (18th November 2021)
196. 'New leaks and possible IRGC links', PwC Threat Intelligence, CTO-SIB-20210809-01A

73 PwC Cyber Threats 2021: A Year in Retrospect

197. 'Scanning the internet for vulnerabilities', PwC Threat Intelligence, CTO-TIB-20211118-01A
198. 'Scanning the internet for vulnerabilities', PwC Threat Intelligence, CTO-TIB-20211118-01A
199. 'Scanning the internet for vulnerabilities', PwC Threat Intelligence, CTO-TIB-20211118-01A
200. 'Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021', Microsoft, <https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021> (16th November 2021)
201. 'Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021', Microsoft, <https://www.microsoft.com/security/blog/2021/11/16/evolvingtrends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021> (16th November 2021)
202. 'StrongPity APT Group Deploys Android Malware for the First Time', Trend Micro, https://www.trendmicro.com/en_us/research/21/g/strongpity-apt-group-deploysandroid-malware-for-the-first-time.html (21st July 2021)
203. 'Threats under the Spotlight November 2021', PwC Threat Intelligence, CTO-TUS-20211203-01A
204. 'Taking Action Against Arid Viper', Facebook, <https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf> (April 2021)
205. 'Hiding in plain sight', PwC Threat Intelligence, CTO-TIB-20211126-01A
206. 'Phishing in the Middle East', PwC Threat Intelligence, CTO-TIB-20210629-02A
207. 'WIRTE's campaign in the Middle East 'living off the land' since at least 2019', Kaspersky, <https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044/> (29th November 2021)
208. 'Elections in Palestine – on the campaign trail', PwC Threat Intelligence, CTO-TIB-20191216-02A
209. 'There's a (Houdini)RAT in the Embassy', PwC Threat Intelligence, CTO-TIB-20191112-01A
210. Note: we do not currently cluster Blue Dev 5 activity with the same threat actor that conducted the SolarWinds activity, which we track as Blue Nova, due to differences in observed TTPs.
211. The UK NCSC assessed it is highly likely this actor was Russia's Foreign Intelligence Service (SVR).
212. 'UK and US call out Russia for SolarWinds compromise', NCSC, <https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise> (15th April 2021)
213. Blue Nova targeted Mimecast to gain access to the keys used to authenticate service accounts to victim mail servers, as well as targeting the software developed by SolarWinds.
214. 'Blue Dev 5 - The Roots of Targeting', PwC Threat Intelligence, CTO-TIB-20210608-01A
215. 'Blue Dev 5 - Mysteries of Foreign Affairs', PwC Threat Intelligence, CTO-TIB-20210527-01A
216. "NobleBaron | New Poisoned Installers Could Be Used In Supply Chain Attacks", Volexity, <https://www.sentinelone.com/labs/noblebaron-new-poisoned-installerscould-be-used-in-supply-chain-attacks/> (1st June 2021)
217. '(Darth) Vladars under attack Part 1', PwC Threat Intelligence, CTO-TIB-20210310-01A
218. 'Bosnia is in danger of breaking up, warns top international official', The Guardian, <https://www.theguardian.com/world/2021/nov/02/bosnia-is-in-danger-of-breakingup-warns-eus-top-official-in-the-state> (2nd November 2021)
219. 'MINISTARSTVO UNUTRAŠNJIH POSLOVA REPUBLIKE SRPSKE', Republika Srpska Ministry of Interior, <https://mup.vladars.net/lat/index.php?vijest=vtk&id=23325&vrsta=aktuelnosti> (24th April 2020)
220. '(Darth) Vladars under attack Part 2', PwC Threat Intelligence, CTO-TIB-20210423-01A
221. '(Darth) Vladars under attack Part 3', PwC Threat Intelligence, CTO-TIB-20210903-01A
222. 'Hunting Blue Odin Servers', PwC Threat Intelligence, CTO-TIB-20211215-01A
223. 'Recent Cloud Atlas activity' Kaspersky, <https://securelist.com/recent-cloud-atlas-activity/92016/> (12th August 2019)
224. 'Exploring Blue Odin', PwC Threat Intelligence, CTO-TIB-20210308-01A
225. 'The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies', NCCC, <https://www.rnbo.gov.ua/en/Diialnist/4823.html> (24th February 2021)
226. 'The NCCC at the NSDC of Ukraine has updated information on the document management system of state bodies', NCCC, <https://www.rnbo.gov.ua/en/Diialnist/4824.html> (25th February 2021)
227. 'Inside the ASKOD Compromise', PwC Threat Intelligence, CTO-TIB-20210319-01A
228. 'SBU finds hacker hunting for personal information of employees', Security Service of Ukraine, <https://ssu.gov.ua/en/novyny/sbu-vyiyavla-khakeri-yakyi-poliuvav-napersonalni-dani-spivrobitnykiv-sluzhby> (23rd April 2021)
229. 'SSU identifies FSB hackers responsible for over 5,000 cyber attacks against Ukraine', Security Service of Ukraine, <https://ssu.gov.ua/en/novyny/sbu-vstanovyakhakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy> (4th November 2021)
230. 'Ukraine discloses identity of Gamaredon members, links it to Russia's FSB', The Record: Catalin Cimpanu, <https://therecord.media/ukraine-discloses-identity-ofgamaredon-members-links-it-to-russias-fsb/> (4th November 2021)
231. 'Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare', Looking Glass Cyber, https://web.archive.org/web/20190921173500/https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf (28th April 2015)
232. 'Blue Otsos Armageddon', PwC Threat Intelligence, CTO-SIB-20211210-01A
233. 'ReconHellcat Uses NIST Theme as Lure To Deliver New BlackSoul Malware', QuoIntelligence, <https://quointelligence.eu/2021/01/reconhellcat-uses-nist-theme-aslure-to-deliver-new-blacksoul-malware/> (6th January 2021)
234. 'Operation GhostShell: Novel RAT Targets Global Aerospace and Telecoms Firms', Cybereason, <https://www.cybereason.com/blog/operation-ghostshell-novel-rattargets-global-aerospace-and-telecoms-firms> (6th October 2021)
235. 'Iran-linked DEV-0343 targeting defense, GIS, and maritime sectors', Microsoft, <https://www.microsoft.com/security/blog/2021/10/11/iran-linked-dev-0343-targetingdefense-gis-and-maritime-sectors/> (11th October 2021)
236. 'Tortoiseshell Group Targets IT Providers in Saudi Arabia in Probable Supply Chain Attacks', Symantec, <https://symantec-enterprise-blogs.security.com/blogs/threatintelligence/tortoiseshell-apt-supply-chain> (18th September 2019)
237. 'A Zoom call with White Dev 89', PwC Threat Intelligence
238. 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence
239. 'Compromising Eurasian Telecoms, justforfun', PwC Threat Intelligence, CTO-TIB-20210709-01A
240. 'Learning to ChaCha with Red Kelpie', PwC Threat Intelligence, CTO-TIB-20210624-02A
241. 'Yellow Mora is listening', PwC Threat Intelligence, CTO-TIB-20210426-01A
242. 'Yellow Mora is listening', PwC Threat Intelligence, CTO-TIB-20210426-01A
243. 'Sophisticated Espionage Group Turns Attention to Telecom Providers in South Asia', Symantec, <https://symantec-enterprise-blogs.security.com/blogs/threatintelligence/greenbug-espionage-telco-south-asia> (19th May 2020)

74 PwC Cyber Threats 2021: A Year in Retrospect

244. 'Yellow Nix working overtime remotely', PwC Threat Intelligence, CTO-TIB-20210309-01A
245. 'Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry', US Department of the Treasury, <https://home.treasury.gov/news/press-releases/sm1127> (17th September 2020)
246. 'Global Cyber Bulletin - June 2021', PwC Threat Intelligence, CTO-GCB-20210706-01A
247. 'Big airline heist: APT41 likely behind a third-party attack on Air India', Group-IB: Nikita Rostov ev, https://blog.group-ib.com/columntk_apt41 (10th June 2021)
248. 'ShadowPad not a dead cert', PwC Threat Intelligence, CTO-TIB-20211116-02A
249. 'Acer confirms second cyber attack in 2021', ZDNet: Jonathan Greig, <https://www.zdnet.com/article/acer-confirms-second-cyberattack-in-2021/> (14th October 2021)
250. 'Well its been a MirrorBlast', PwC Threat Intelligence, CTO-TIB-20211025-01A
251. 'Billion Dollar Baby', PwC Threat Intelligence, CTO-SIB-20210322-01A
252. 'Conti ransomware rakes in over \$25 million in just four months', Acronis, <https://www.acronis.com/en-us/cyber-protection-center/posts/conti-ransomware-rakes-in-over-25-million-in-just-four-months/> (23rd November 2021)
253. 'Retailer Fat Face Pays \$2 Million Ransom to Conti Gang', Bank Info Security, <https://www.bankinfosecurity.com/retailer-fat-face-pays-2-million-ransom-to-contigang-a-16277> (26th March 2021)
254. 'Graff multinational jeweller hit by Conti gang. Data of its rich clients are at risk, including Trump and Beckham', Security Affairs, <https://securityaffairs.co/wordpress/123980/cyber-crime/conti-ransomware-graff-jeweller.html> (31st October 2021)
255. 'Conti Ransom Gang Starts Selling Access to Victims', Krebs on Security, <https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/> (25th October 2021)
256. 'Coop supermarket closes 500 stores after Kaseya ransomware attack', Bleeping Computer, <https://www.bleepingcomputer.com/news/security/coop-supermarketcloses-500-stores-after-kaseya-ransomware-attack/> (3rd July 2021)
257. 'Hundreds of SPAR stores forced to shut following a major cyber incident', Teiss, <https://www.teiss.co.uk/spar-supermarket-cyber-incident/> (13th December 2021)
258. 'NCSC statement on cyber incident affecting Spar stores', NCSC, <https://www.ncsc.gov.uk/news/spar-stores-incident> (10th December 2021)
259. 'Canadian retailer Home Hardware hit by ransomware', ITWorld Canada, <https://www.itworldcanada.com/article/canadian-retailer-home-hardware-hit-byransomware/445416> (2nd April 2021)
260. 'Office Depot parent expects over \$20M loss due to malware attack', Retail Dive, <https://www.retaildive.com/news/office-depot-parent-expects-over-20m-loss-dueto-malware-attack/597544/> (30th March 2021)
261. 'The many tentacles of Magecart Group 8', Malwarebytes: Jérôme Segura, <https://blog.malwarebytes.com/threat-intelligence/2021/09/the-many-tentacles-ofmagecart-group-8/> (13th September 2021)
262. 'Nothing else BlackMatters', PwC Threat Intelligence, CTO-TIB-20211209-01A
263. 'Your dream job awaits, just please enable editing', PwC Threat Intelligence, CTO-TIB-20210916-01A



pwc.com/cyber-security

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees, and agents do not accept or assume any liability, responsibility, or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2022 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.