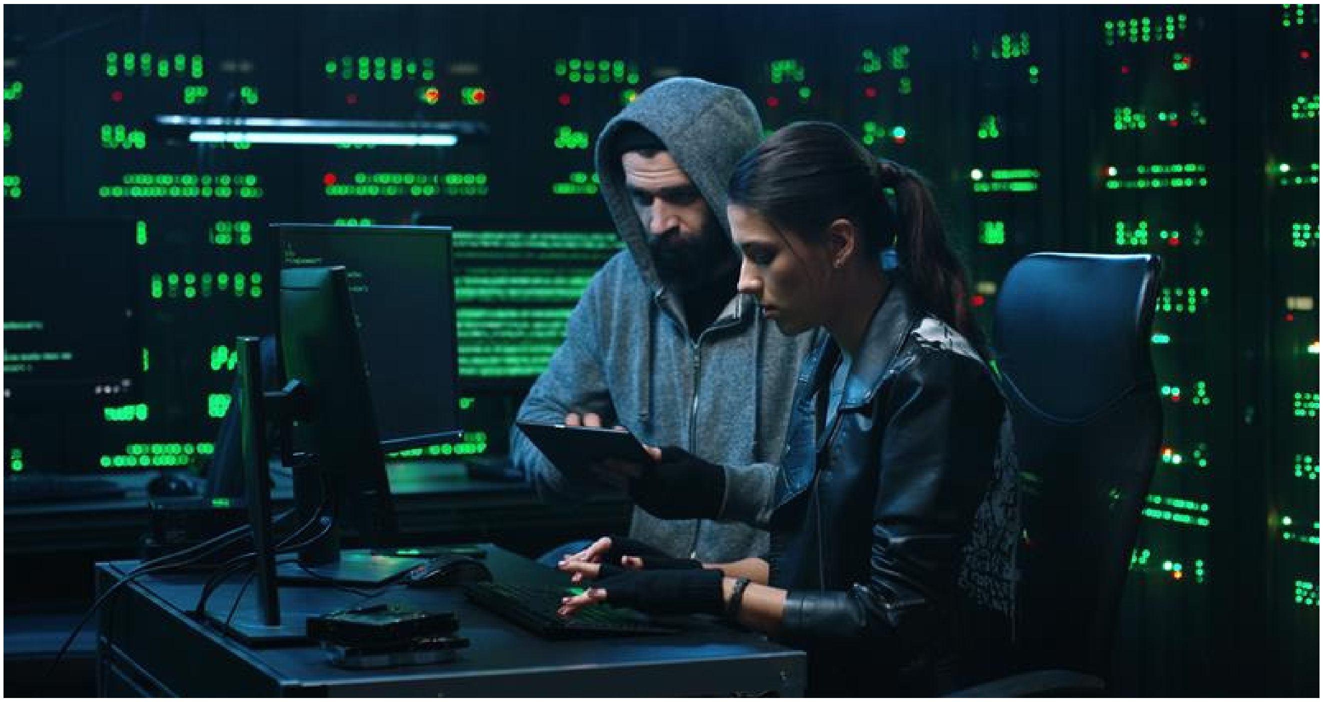
Ransomware as a Service: Enabler of Widespread Attacks

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks



By Fyodor Yarochkin

Additional insights by Janus Agcaoili, Byron Gelera, and Nikko Tamaña

Ransomware as a service (RaaS) can be credited as one of the primary reasons that ransomware attacks are proliferating rapidly. Simply put, RaaS involves selling or renting ransomware to buyers who are called affiliates.

In the past, ransomware attacks were mainly launched by the ransomware operators themselves. When RaaS entered the picture, however, it made it easier for a variety of attackers, even those who have little technical knowledge, to wield ransomware against targets.

Essentially, we observed an organized division of labor in groups using RaaS. As a result of this development, the participants of the cybercrime ecosystem gain higher proficiency and specialization with regard to specific tasks, with some focusing on penetrating networks and others on running the ransomware or conducting ransom negotiation with victims.

Such specialization, coupled with refined extortion techniques and technical strategies, makes modern ransomware a notorious threat. With the threat's ever-growing reach, it was predicted that ransomware attacks could cost billions in the next decade.

How RaaS operates: the underground as a breeding ground

While RaaS is based on the software-as-a-service (SaaS) model where software can be accessed online on a subscription basis, it also continues to evolve in its own ways, and this fully functional and independent ecosystem thrives in the underground with its key players.

Among these key players are the operators, or those who develop and peddle ransomware. They are usually organized in a group and have designated roles such as leader, developers, and infrastructure and system administrators. More advanced groups might also have other roles, such as recruiters, penetration testers (aka pentesters), victim analysts, and negotiators.

Some roles and tools might also be outsourced or acquired through affiliate programs. For instance, some operators avail of access-as-a-service (AaaS), which can provide various means of access to targeted organizations. Meanwhile, other groups could have strong penetration testing teams but might also lack the necessary ransomware software. Such penetration testing teams often participate as affiliates for RaaS and use affiliate program ransomware tools and infrastructure when a target is compromised. Affiliates might belong to organized gangs themselves or might operate independently.

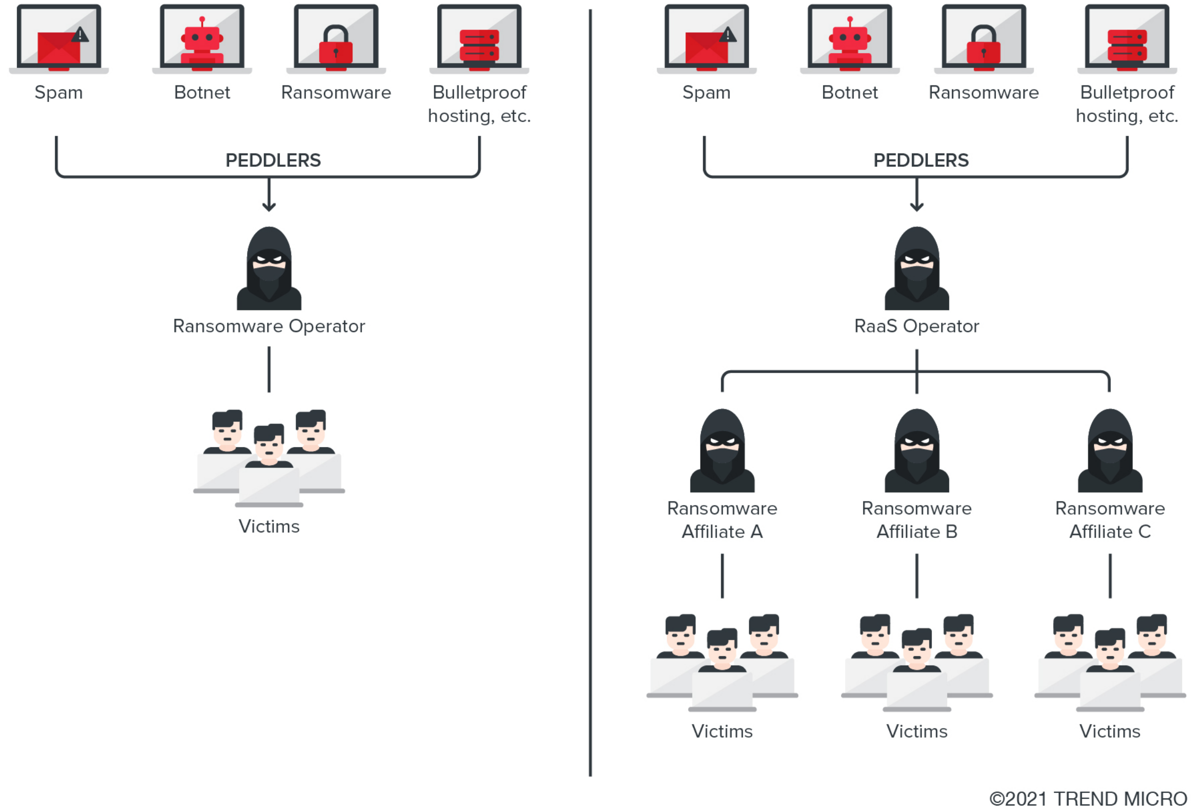


Figure 1. Comparison of direct ransomware operations (left) and RaaS operators (right)

With regard to the RaaS operation model, the RaaS-operating criminal group first needs to develop or acquire the ransomware software and infrastructure. They then proceed to recruit affiliates through online forums, Telegram channels, or personal connections, with some operators investing as much as US$1 million for recruitment efforts. Once enlisted, affiliates can then launch their own attacks.

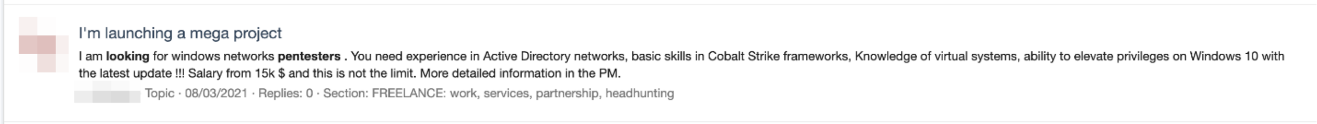
RaaS provides a win-win situation and a high payout for both operators and affiliates while allowing higher specialization in dedicated tasks. Affiliates can earn payouts without having to develop the ransomware themselves, while operators can directly make a profit from their affiliates. The payouts are normally organized using a revenue model for RaaS subscriptions. The possible revenue models besides subscription are one-time payments, profit sharing, and affiliate marketing. With such business models, the ransomware operators can fully focus on developing and improving their ransomware software and operations without needing to spend resources on other tasks, such as compromising targets or distributing the ransomware themselves. Instead, these tasks are delegated to the RaaS affiliates.

The cost of operations and its impact on ransom demands

It goes without saying that there are operational expenses for any ransomware group. As a ransomware group needs to spend money on tools, skilled personnel and monthly operational costs, ransomware attacks can indeed be expensive. A group leader thus needs to figure out how to cover the recurring cost of operation. In particular, the rental of network infrastructure has its own cost, and many of the group members receive monthly salaries that need to be paid even if the ransomware attack victims do not pay the ransom. A successful payout from an attack is therefore necessary to cover the recurring operational cost of keeping a ransomware group running.

The one-time purchases of tools naturally come with their own price tags. Ransomware groups and network penetration teams often do not develop the exploitation tools themselves but prefer to purchase tools for initial access into organizations from third-party software vendors and underground market software developers who offer varying prices, either for on-hand or customized tools.

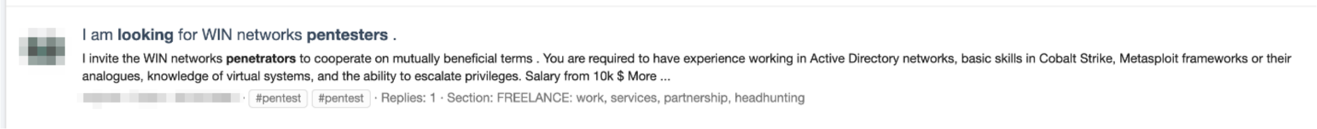
For groups following RaaS models and services with double extortion techniques, percentage payouts for kit sellers and RaaS partnership programs have risen, with some allocating for a full set of operations personnel such as pentesters, victim analysts, and negotiators, as advertised in ads in underground forums.



I'm launching a mega project

I am **looking** for windows networks **pentesters** . You need experience in Active Directory networks, basic skills in Cobalt Strike frameworks, Knowledge of virtual systems, ability to elevate privileges on Windows 10 with the latest update !!! Salary from 15k $ and this is not the limit. More detailed information in the PM.

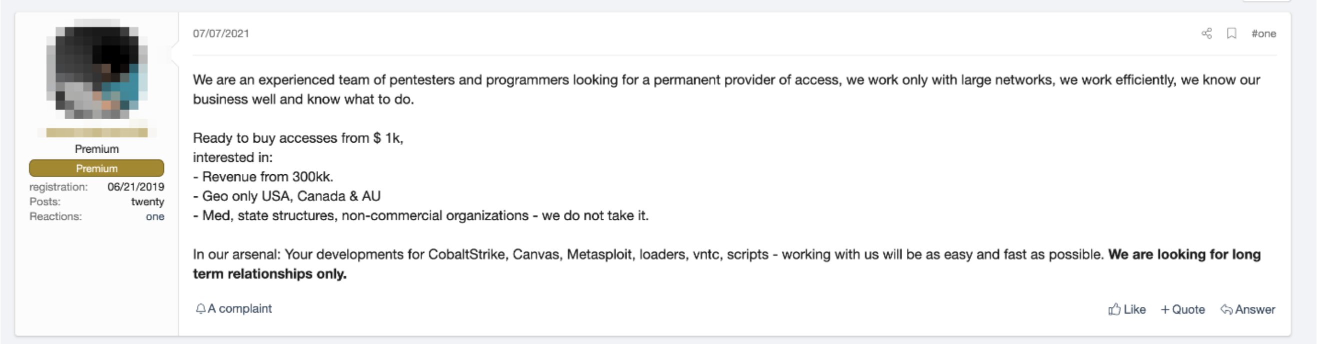
[redacted] Topic · 08/03/2021 · Replies: 0 · Section: FREELANCE: work, services, partnership, headhunting



I am **looking** for WIN networks **pentesters** .

I invite the WIN networks **penetrators** to cooperate on mutually beneficial terms . You are required to have experience working in Active Directory networks, basic skills in Cobalt Strike, Metasploit frameworks or their analogues, knowledge of virtual systems, and the ability to escalate privileges. Salary from 10k $ More ...

[redacted] · #pentest #pentest · Replies: 1 · Section: FREELANCE: work, services, partnership, headhunting



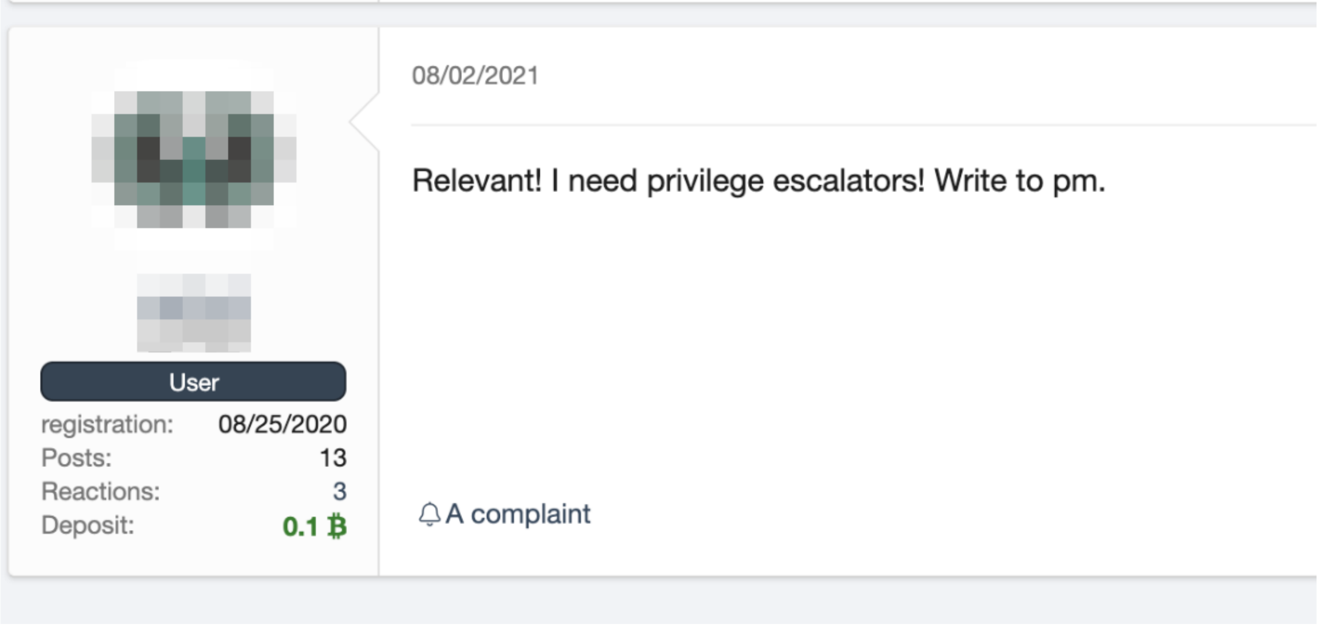
[redacted]
Premium
Premium
registration: 06/21/2019
Posts: twenty
Reactions: one

07/07/2021

We are an experienced team of pentesters and programmers looking for a permanent provider of access, we work only with large networks, we work efficiently, we know our business well and know what to do.

Ready to buy accesses from $ 1k,
interested in:
- Revenue from 300kk.
- Geo only USA, Canada & AU
- Med, state structures, non-commercial organizations - we do not take it.

In our arsenal: Your developments for CobaltStrike, Canvas, Metasploit, loaders, vntc, scripts - working with us will be as easy and fast as possible. **We are looking for long term relationships only.**


08/02/2021

Relevant! I need privilege escalators! Write to pm.

User

registration: 08/25/2020

Posts: 13

Reactions: 3

Deposit: 0.1 ₿

Figure 2. Job posts in underground forums for pentesters and programmers capable of accessing enterprise networks and performing privilege escalation

Regardless of successful payouts, most of these personnel require payment for services, whether such remuneration involves monthly salary or per-project payments.Estimating average monthly costs (such as salaries, servers, virtual private server rentals, service providers, tools, accesses, and infrastructure, among others), these groups might spend at least US$100,000 upward to keep operations running. If these groups target 10 companies at a time but only one victim can pay, that single organization carries the brunt of all the expenses that the groups make in addition to the profit they hope to have.

However, many organizations still refuse to pay ransom demands, either because of their internal policies, government regulations, or the assistance of authorities. Ransomware groups do not look kindly on these refusals for payment, and they find ways to retaliate against these companies. For example, Mespinoza operators threaten companies who refuse to pay, not just with the exposure of sensitive data but also with the threat of reporting the victim's illegal activities, such as tax fraud or evasion.

Avoiding certain targets

In the underground, ransomware operators also gradually developed a strategy for determining which targets to avoid. For instance, while the US remains one of the top targets for all kinds of malicious activities, some ransomware operators discuss avoiding the country. In the wake of high-profile ransomware attacks, authorities have been paying heightened attention to the threat. As a result, no-pay policies, government assistance to victims for ransom negotiation, and techniques to recover paid ransom could cause ransomware groups to have a harder time getting paid.

And while some groups have turned their attention to Asia, ransomware groups generally avoid, for example, going after Taiwanese companies because of the strict anti-money laundering policies that make it difficult to legally purchase cryptocurrency and keep organizations from paying the demanded ransom.

Other factors that can keep threat actors from attacking a certain region are the operators' patriotism, countries' poverty levels, or geopolitical situations that targets are in. For such locations that are struggling economically and politically, or for countries that operators feel a sense of loyalty to, threat groups opt to use other monetization activities, such as the sale or rental of compromised assets or the use of keyloggers for harvesting various credentials, which later on can be sold individually or through a "cloud of logs."

Recent updates on RaaS operations

This year, there were also momentary but noticeable changes in the underground. After DarkSide's attack on Colonial Pipeline, all topics related to ransomware were banned on many underground forums. Operators shifted to discreet advertising in underground forums for system administrators, pentesters, and other seemingly legitimate jobs without disclosing the purpose behind these ads. When it is discovered that the individuals behind these post are actually hiring for the purpose of operating ransomware, their accounts are banned.

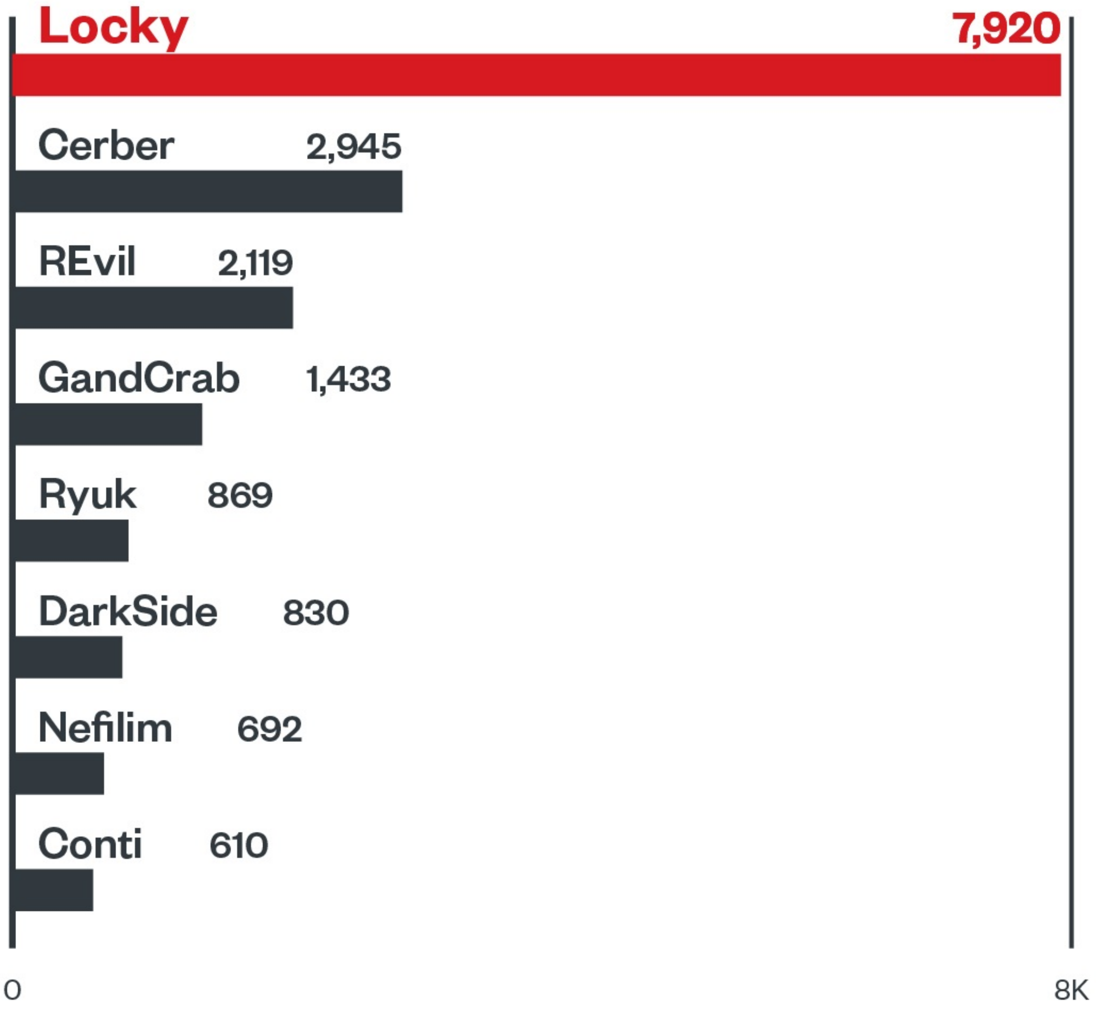
Ransomware operators have also become more selective of their targets. We observed discussions in public and private groups about being more careful when choosing potential victims and specifically avoiding political and critical infrastructure as well as the healthcare sector as targets.

Profit division has also changed. Profits used to be usually divided into 70% and 30% in favor of the affiliate when ransom demands were between five to six figures. Now, groups collecting up to seven figures allot a 20% "finder's fee" for access, while lateral movement and penetration testing are now done within the salaried group. This was the observed behavior for groups like Nefilim. Based on growing popularity in forum discussions, hiring more pentesters to become part of the salaried group and the continued professionalization of AaaS might likely continue to keep more of the profit intact and inside the main group.

The latest attacks also provide insight into where this is all heading. Based on REvil (aka Sodinokibi) and DarkSide's previous attacks on Linux-based VMware ESXi servers and network-attached storage (NAS), there is a likelihood that other RaaS groups will be expanding their targets and attacks to non-Windows servers, targeting other operating systems such as Linux CentOS, Linux RedHat, and other UNIX flavors, all of which are Portable Operating System Interface (POSIX) compliant.

Ransomware families used by RaaS operators and affiliates

Most modern ransomware families have adopted the RaaS model. In our midyear cybersecurity report, we found the top 10 most detected ransomware families. Interestingly, eight of these families have been used by RaaS operators and affiliates at some point. Some families, such as Locky, Cerber, and GandCrab, have been used in previous instances of RaaS operations, although these variants have not been actively employed for attacks recently. Nevertheless, they are still being detected in affected systems:



©2021 TREND MICRO

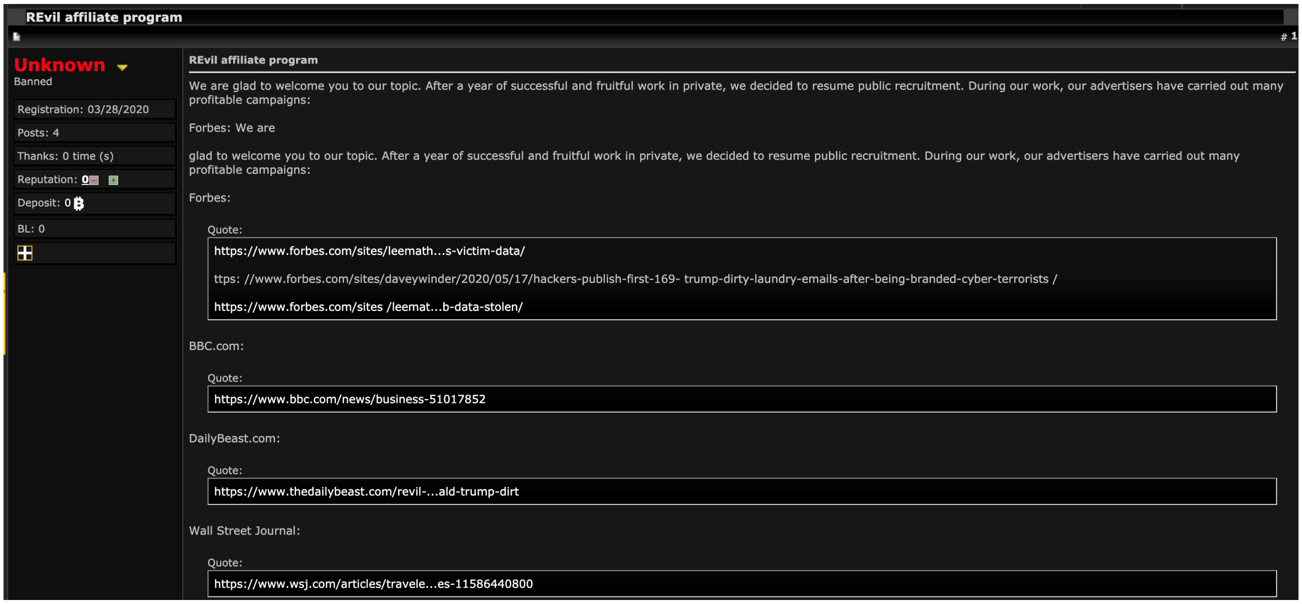
Figure 3. First half of 2021 data for most detected ransomware families that have been RaaS-operated at some point

Based on this list, here are some of the ransomware families used by RaaS operators and affiliates to launch critical attacks this year:

REvil

Before suddenly disappearing, REvil consistently made headlines this year due to its high-profile attacks, including those launched on meat supplier JBS and IT company Kaseya. It’s also the fourth overall most detected ransomware in our 2021 midyear data, with 2,119 detections. After disappearing for about two months, this group recently brought their infrastructure back and demonstrated signs of renewed activities.

This year, REvil demanded huge ransoms: US$70 million for the Kaseya attack (said to be record-breaking) and US$22.5 million (with US$11 million paid) for the JBS attack.



REvil affiliate program

1

Unknown
Banned

Registration: 03/28/2020

Posts: 4

Thanks: 0 time (s)

Reputation: 0

Deposit: 0 ₿

BL: 0

REvil affiliate program

We are glad to welcome you to our topic. After a year of successful and fruitful work in private, we decided to resume public recruitment. During our work, our advertisers have carried out many profitable campaigns:

Forbes: We are

glad to welcome you to our topic. After a year of successful and fruitful work in private, we decided to resume public recruitment. During our work, our advertisers have carried out many profitable campaigns:

Forbes:

Quote:

https://www.forbes.com/sites/leemath...s-victim-data/

ttps: //www.forbes.com/sites/daveywinder/2020/05/17/hackers-publish-first-169- trump-dirty-laundry-emails-after-being-branded-cyber-terrorists /

https://www.forbes.com/sites /leemat...b-data-stolen/

BBC.com:

Quote:

https://www.bbc.com/news/business-51017852

DailyBeast.com:

Quote:

https://www.thedailybeast.com/revil-...ald-trump-dirt

Wall Street Journal:

Quote:

https://www.wsj.com/articles/travele...es-11586440800

Figure 4. REvil affiliate recruitment in underground forums

Techniques

While most techniques used by ransomware gangs remain the same from our most recent update, they also employed some new techniques, such as the following:

Download and execution

- An attachment (such as a PDF file) of a malicious spam email drops Qakbot into the system. The malware will then download additional components and the payload.
- CVE-2021-30116, a zero-day vulnerability affecting the Kaseya VSA servers, was used in the Kaseya supply-chain attack.

Discovery

Additional legitimate tools, namely AdFind, SharpSploit, BloodHound, and NBTScan, are also observed to be employed for network discovery.

DarkSide

DarkSide has also been prominent in the news lately due to its attack on Colonial Pipeline. The targeted company was coerced to pay US$5 million in ransom. DarkSide ranked seventh with 830 detections in our midyear data on most detected ransomware families.

Operators have since claimed that they will shut down operations due to pressure from authorities. However, as with the case of some ransomware families, they might just lie low for a while before resurfacing, or come out with the threat's successor.

Techniques

As discussed in our earlier report, some of the notable techniques utilized by DarkSide are the following:

Reconnaissance

For this phase, DarkSide abuses various tools, namely PowerShell, Metasploit Framework, Mimikatz, and BloodHound.

Lateral movement

- For lateral movement, DarkSide aims to gain Domain Controller (DC) or Active Directory access. This is used to harvest credentials, escalate privileges, and gather valuable assets that will be exfiltrated.
- The DC network is then used to deploy the ransomware to connected machines.

Nefilim

Nefilim is the ninth most detected ransomware for midyear 2021, with 692 detections. Attackers that wield the ransomware variant set their sights on companies with billion-dollar revenues.

Like most modern ransomware families, Nefilim also employs double extortion techniques. Nefilim affiliates are said to be especially vicious when affected companies don't succumb to ransom demands, and they keep leaked data published for a long time.

Techniques

Nefilim makes use of a variety of techniques such as the following:

Initial access

- Nefilim can gain initial access through exposed RDPs.
- It can also use Citrix Application Delivery Controller vulnerability (aka CVE-2019-19781) to gain entry into a system.

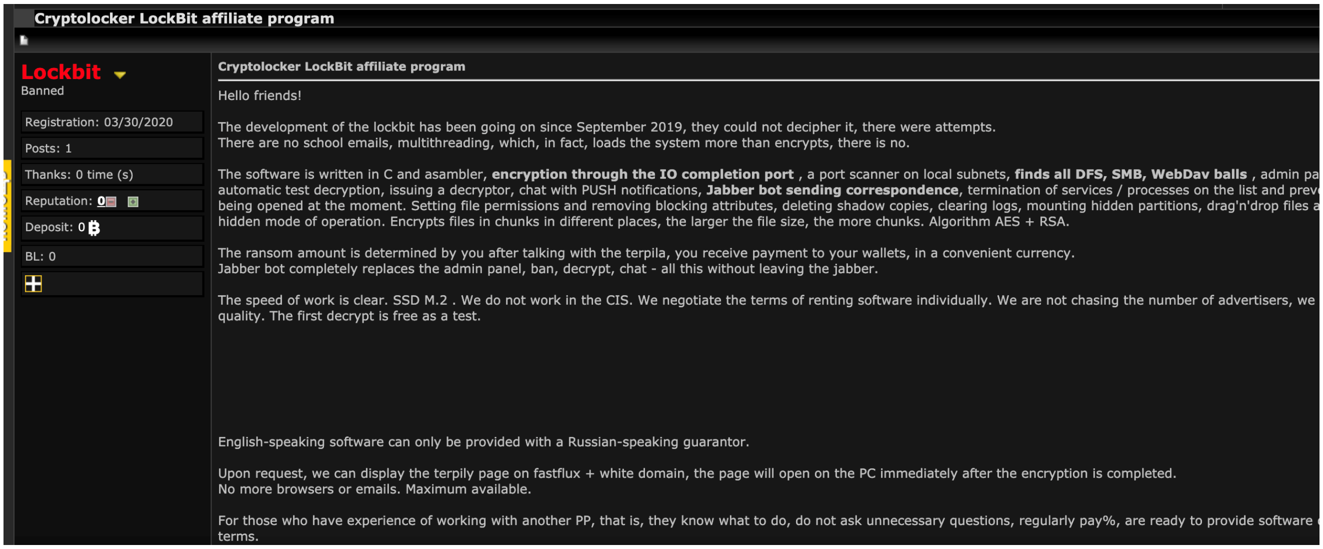
Lateral movement and defense evasion

- Nefilim is capable of lateral movement via tools such as PsExec or Windows Management Instrumentation (WMI).
- It performs defense evasion through the use of third-party tools like PC Hunter, Process Hacker, and Revo Uninstaller.

LockBit

LockBit resurfaced in the middle of the year with LockBit 2.0, targeting more companies as they employ double extortion techniques. Based on our findings, Chile, Italy, Taiwan, and the UK are among the most affected countries. In a recent prominent attack, ransom demand went up as high as US$50 million.

LockBit 2.0 claims to have one of the fastest encryption techniques among other ransomware. It also shows similarities with prominent ransomware families, Ryuk and Egregor.



Cryptolocker LockBit affiliate program

Lockbit
Banned

Registration: 03/30/2020

Posts: 1

Thanks: 0 time (s)

Reputation: 0

Deposit: 0 ₿

BL: 0

Cryptolocker LockBit affiliate program

Hello friends!

The development of the lockbit has been going on since September 2019, they could not decipher it, there were attempts.
There are no school emails, multithreading, which, in fact, loads the system more than encrypts, there is no.

The software is written in C and asambler, **encryption through the IO completion port** , a port scanner on local subnets, **finds all DFS, SMB, WebDav balls** , admin pa
automatic test decryption, issuing a decryptor, chat with PUSH notifications, **Jabber bot sending correspondence**, termination of services / processes on the list and preve
being opened at the moment. Setting file permissions and removing blocking attributes, deleting shadow copies, clearing logs, mounting hidden partitions, drag'n'drop files a
hidden mode of operation. Encrypts files in chunks in different places, the larger the file size, the more chunks. Algorithm AES + RSA.

The ransom amount is determined by you after talking with the terpila, you receive payment to your wallets, in a convenient currency.
Jabber bot completely replaces the admin panel, ban, decrypt, chat - all this without leaving the jabber.

The speed of work is clear. SSD M.2 . We do not work in the CIS. We negotiate the terms of renting software individually. We are not chasing the number of advertisers, we
quality. The first decrypt is free as a test.

English-speaking software can only be provided with a Russian-speaking guarantor.

Upon request, we can display the terpily page on fastflux + white domain, the page will open on the PC immediately after the encryption is completed.
No more browsers or emails. Maximum available.

For those who have experience of working with another PP, that is, they know what to do, do not ask unnecessary questions, regularly pay%, are ready to provide software
terms.

Figure 4. LockBit affiliate recruitment in underground forums

Techniques

Some of the updated ransomware’s techniques are the following:

Exfiltration

> Operators provide StealBit (detected by Trend Micro as TrojanSpy.Win32.STEALBIT.YXBHM), a tool that can automatically exfiltrate data, to their affiliates to help the latter harvest assets.

Defense evasion

To terminate processes and services, the following batch files are used:

- delsvc.bat (detected by Trend Micro as Trojan.BAT.KILLPROC.D) makes crucial processes (such as MySQL and QuickBooks) and services (such as Microsoft Exchange) unavailable.
- AV.bat (detected by Trend Micro as Trojan.BAT.KILLAV.WLDX) uninstalls the antivirus program ESET.
- LogDelete.bat (detected by Trend Micro as PUA.BAT.DHARMA.A) clears Windows event logs. Defoff.bat (detected by Trend Micro as Trojan.BAT.KILLAV.WLDX) disables Windows Defender features such as real-time monitoring.

Impact

> Devices are automatically encrypted across Windows through the abuse of Active Directory group policies.

Conti

Conti is probably one of the largest ransomware groups operating today. It is often said to be the successor of the Ryuk ransomware, as the former shares some similarities with the latter. For example, with regard to tactics, both Conti and Ryuk are distributed via Emotet, Trickbot, and BazarLoader. In our midyear roundup report data, Conti was the tenth most detected ransomware, as it amassed 610 detections.

Recently, the FBI and Cybersecurity and Infrastructure Security Agency (CISA) released an alert notice with regard to a surge in Conti ransomware attacks. Conti penetration-testing documents, which provide detailed information on the operators' preferred techniques, were also leaked.

Techniques

Some notable techniques of the Conti ransomware are as follows:

Initial access

- Conti can use malspam to gain entry into the system.
- It can also exploit known vulnerabilities for initial access.

Discovery, lateral movement, and persistence

  - Conti can use open-source and off-the-shelf commercial tools, such as PowerSploit, Metasploit, ADFind, and Cobalt Strike for discovery and lateral movement.
  - Other commercial tools, such as AnyDesk, can also be used by Conti to maintain persistence on compromised targets.

Exfiltration

Mega cloud storage can be used for the information exfiltration phase.

Defense evasion

- Defense evasion can be performed through the use of third-party tools like PC Hunter, Process Hacker, and Revo Uninstaller.
- Conti also disables some security tools found in compromised systems.

How to defend systems against ransomware

For enterprises to protect themselves from ransomware attacks, it would help to establish ransomware defense plans. These can be based on security frameworks, such as those from the Center of Internet Security (CIS) and the National Institute of Standards and Technology (NIST). These guidelines can help with prioritization and resource management for prevention, defense, and recovery from ransomware.

Beyond the technical means, it is important to understand that attackers will use any identified weakness within a target organization (such as customer data, mishandled personal identifiable information [PII], or accounting mistakes) as pressure points to leverage the ransom negotiation value and make the victim pay. Enterprises should therefore take these issues into account when evaluating their organizational readiness to protect themselves from ransomware attacks.

Some of the best practices from these frameworks are as follows:

Audit events and take inventory.

Take note of the following:

- Available assets and data
- Authorized and unauthorized devices and software
- Security events and incidents

Configure and monitor.

Manage and keep track of the following:

- Hardware and software configurations
- Admin privileges and access
- Activity in network ports, protocols, and services
- Network infrastructure devices, such as firewalls and routers, and their security configurations

Patch and update.

Regularly perform the following for software and applications:

- Vulnerability assessments
- Patching or virtual patching
- Version update

Protect systems and recover data.

Implement the following:

- Data protection, backup, and recovery measures
- Multifactor authentication (MFA)

Secure and defend layers.

Employ the following:

- **The defense in depth (DiD) principle.** This is done by creating multiple layers of defense against potential threats. One example of this is by blocking unused services not just on afirewall but alsoon actual servers.
- **Network segmentation and the least-privilege principle.** It is paramount to follow these when granting permissions to system users, services, and roles.
- **Email static and dynamic analysis.** Both of these work to examine and block malicious emails.
- **The latest version of security solutions to all layers of the system.** These layers include email, endpoint, web, and network.
- **Monitoring for early signs of an attack.** Identifying the questionable presence of various tools in the system can save organizations much time and effort in staving off possible attacks.
- **Advanced detection technologies.** In particular, technologies powered with AI and machine learning offer fortified protection.

Train and test.

Conduct the following regularly:

- Security skills assessment and training
- Red team exercises and penetration tests

Trend Micro Vision One™ helps detect and block suspicious activity, even those that might seem insignificant when monitored from only a single layer, through multilayered protection and behavior detection. It helps spot and block ransomware wherever it might be on the system.

Trend Micro Cloud One™ – Workload Security ensures real-time protection from both known and emerging threats that exploit vulnerabilities. This is made possible through virtual patching, machine learning techniques, and global threat intelligence.

Trend Micro™ Deep Discovery™ Email Inspector performs custom sandboxing and advanced analysis techniques. These effectively deter potential ransomware attacks that are coursed through malicious emails.

Trend Micro Apex One™, with the help of modern techniques, provides automated endpoint protection, threat detection, and quick response against a variety of security issues, including ransomware and fileless threats.

Updated on October 11, 2021 with additional details on most detected ransomware families that used RaaS previously or at present.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below.   2. Press Ctrl+A to select all.   3. Press Ctrl+C to copy.   4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Ransomware, ransomware as a service