Evolution of Russian APT29 – New Attacks and Techniques Uncovered

avertium.com/resources/threat-reports/evolution-of-russian-apt29-new-attacks-and-techniques-uncovered

Executive Summary

In December 2020, the Texas-based IT management and monitoring platform company, SolarWinds, was compromised by the nation-state threat actor APT29 (also known as Nobelium, Cozy Bear, and Midnight Blizzard). The group managed to compromise the company by slipping a malicious code into Orion, a software program that monitors various components within the company's network, while it was being updated. The threat actors then used that update to deploy a massive cyberattack against the U.S.

When it comes to exceptionally sophisticated malware attacks, APT29 stands at the forefront. The SolarWinds breach marked only the beginning of persistent malware attacks carried out by the threat actor. Since the attack on SolarWinds, the APT has relentlessly persisted in its attacks on governments, defense entities, critical manufacturing organizations, and IT service providers. Their latest attacks involve exploiting lesser-known Windows features and specifically targeting diplomats stationed in Ukraine. Let’s examine APT29, their recent attacks, and what organizations can do to protect themselves.

TIR SNAPSHOTS

- Over the years, the Russian nation-state threat actor APT29 has led the way in highly sophisticated malware attacks and the SolarWinds breach was just the beginning of their persistence.
- In August 2021, APT29 attempted to exploit a cluster of Exchange vulnerabilities known as ProxyShell (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473).
- In October 2021, Microsoft issued a warning about APT29's renewed attacks on global IT supply-chains. This campaign initially surfaced in May 2021 and has resulted in 14 confirmed compromise cases, targeting 140 companies.
- APT29 was observed relying on various techniques, including password spray, API abuse, phishing, and token theft, to gain credentials and privileged access to victims' systems.
- In 2022, APT29, was linked to another "highly targeted" post-exploitation malware capable of maintaining persistent access to compromised environments. Dubbed MagicWeb by Microsoft's threat intelligence teams, this development reiterated APT29's commitment to developing and maintaining purpose-built capabilities.
- In 2022, the nation-state actor APT29 was discovered utilizing a lesser-known Windows feature called Credential Roaming. This exploit came to light after a successful phishing attack on an unspecified European diplomatic entity.

- APT29's April 2023 espionage campaign targeted NATO and EU member states' diplomatic and foreign ministries using previously undocumented malware. Poland's Military Counterintelligence Service and CERT Polska (CERT.PL) discovered the campaign, which involved APT29 sending spear phishing emails to specific personnel at diplomatic posts.

APT29's background

2021

Over the years, the Russian nation-state threat actor APT29 has led the way in highly sophisticated malware attacks and the SolarWinds breach was just the beginning of their persistence. In August 2021, APT29 attempted to exploit a cluster of Exchange vulnerabilities known as ProxyShell (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473). This vulnerability allowed threat actors to deploy web shells on unpatched Exchange servers for later access. Despite the availability of security patches, organizations remained vulnerable due to their failure to update their servers.

By 2021, APT29 shifted its focus to targeting software and cloud service resellers. Those attacks impacted 3,000 individual accounts across more than 150 organizations. Employing an established pattern of unique infrastructure and tools for each target, they enhanced their ability to evade detection for an extended period.

APT29 breached SolarWinds using the SUNBURST backdoor, TEARDROP malware, and GoldMax malware for their supply chain attack. They also breached nine U.S. government agencies (Department of Homeland Security, CISA, US Treasury, etc.) and 100 private companies with the same malware. After gaining access, APT29 employed a simple yet sophisticated strategy to delve deeper into their victims' networks, positioning themselves to compromise Microsoft 365 and Azure.

Also, APT29 covertly integrated software backdoors into network-management programs distributed by SolarWinds, enabling spying activities. The attackers also introduced new Azure identities and elevated permissions for existing identities, manipulating Microsoft programs to facilitate email theft. As a result of their success, APT29 managed to infiltrate the Cybersecurity and Infrastructure Security Agency (CISA), a government organization tasked with protecting federal computer networks from attacks. This access allowed APT29 to steal, alter, and potentially destroy data. After gaining entry, APT29 meticulously erased all traces of their presence, complicating the efforts of investigators to attribute the breach to them.

In October 2021, Microsoft issued a warning about APT29's renewed attacks on global IT supply chains. This campaign initially surfaced in May 2021 and has resulted in 14 confirmed compromise cases, targeting 140 companies. During this time, APT29 was observed relying on various techniques, including password spray, API abuse, phishing, and token theft, to gain credentials and privileged access to victims' systems. Microsoft believes that APT29 employed a remote access malware known as FoggyWeb to establish persistence on compromised Active Directory Federation Services servers (AD FS). This backdoor persistence was first detected in the wild in April 2021.

2022

MagicWeb

In 2022, APT29, was linked to another "highly targeted" post-exploitation malware capable of maintaining persistent access to compromised environments. Dubbed MagicWeb by Microsoft's threat intelligence teams, this development reiterated APT29's commitment to developing and maintaining purpose-built capabilities.

MagicWeb, sharing similarities with another tool called FoggyWeb, was assessed to have been deployed to maintain access and block eviction during remediation efforts, but only after obtaining highly privileged access to an environment and moving laterally to an AD FS server. While FoggyWeb came with specialized capabilities to deliver additional payloads and steal sensitive information from Active Directory Federation Services (AD FS) servers, MagicWeb was a rogue DLL (a backdoored version of "Microsoft.IdentityServer.Diagnostics.dll") that facilitated covert access to an AD FS system through an authentication bypass.

The findings came on the heels of the disclosure of an APT29-led campaign aimed at NATO-affiliated organizations with the goal of accessing foreign policy information. Specifically, this involved disabling an enterprise logging feature called Purview Audit (previously Advanced Audit) to harvest emails from Microsoft 365 accounts. Another newer tactic used by the actor during that time was the use of a password guessing attack to obtain the credentials associated with a dormant account and enroll it for multi-factor authentication (MFA), granting it access to the organization's VPN infrastructure.

Windows Credential Roaming

Also, in 2022, the nation-state actor APT29 was discovered utilizing a lesser-known Windows feature called Credential Roaming. This exploit came to light after a successful phishing attack on an unspecified European diplomatic entity. Mandiant identified the use of Credential Roaming by the threat actor during their presence inside the victim network in early 2022. At that time, APT29 executed "numerous LDAP queries with unusual properties" against the Active Directory system.

Credential Roaming is a feature introduced in Windows Server 2003 Service Pack 1 (SP1) that enables users to securely access their credentials, such as private keys and certificates, across various workstations within a Windows domain. Microsoft explains that Credential Roaming stores user credentials in two attributes: ms-PKI-DPAPIMasterKeys and ms-PKI AccountCredentials. The latter is a multi-valued LDAP property containing encrypted credential objects in binary large objects (BLOBs).

Mandiant discovered an arbitrary file write vulnerability that could allow a threat actor to achieve remote code execution in the context of the logged-in victim. Tracked as CVE-2022-30170 (CVSS score 7.3), Microsoft addressed this issue as part of the September 13, 2022 Patch Tuesday updates. The company stated that exploiting the vulnerability requires a user to log in to Windows.

If successfully exploited, APT29 could have gained remote interactive logon rights to a victim's machine, which the victim's account would not normally have. Mandiant's research sheds light on why APT29 actively queries the related LDAP attributes in Active Directory.

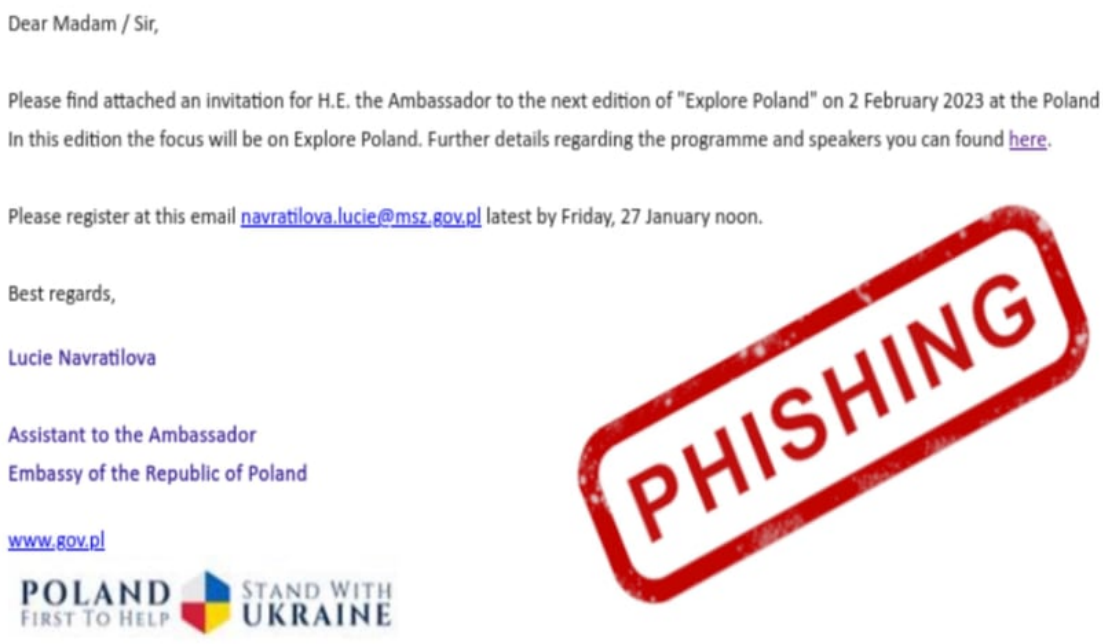
Recent Attacks

Polish Government

In April 2023, APT29 executed an espionage campaign directed at diplomatic and foreign ministries of NATO and EU member states. This ongoing operation utilized previously undocumented malware payloads. The campaign, discovered and investigated by Poland's Military Counterintelligence Service and CERT Polska (CERT.PL), involved APT29 hackers sending spear-phishing emails to specific personnel at diplomatic posts.

These emails were disguised as messages from European embassies, inviting recipients to meetings or collaboration on documents. The emails contained PDF attachments with links to seemingly external calendars, meeting details, or work files. Clicking on the links led to web pages that used JavaScript code to decode a payload, offering it for download. The script used HTML Smuggling, facilitating the transfer of files with .ISO, .ZIP, or .IMG attachments.

Image 1: Phishing Email



Dear Madam / Sir,

Please find attached an invitation for H.E. the Ambassador to the next edition of "Explore Poland" on 2 February 2023 at the Poland Embassy.
In this edition the focus will be on Explore Poland. Further details regarding the programme and speakers you can found here.

Please register at this email navratilova.lucie@msz.gov.pl latest by Friday, 27 January noon.

Best regards,

Lucie Navratilova

Assistant to the Ambassador
Embassy of the Republic of Poland

www.gov.pl

Source: CERT.pl

APT29 has employed .ISO files for malware distribution previously, but they have now introduced a new technique using .IMG (disk image) files. When these files are opened in Windows, they are automatically mounted as a virtual disk, allowing users to access the files within. In this case, the files were Windows shortcuts (LNK) that triggered a legitimate executable, which then loaded a malicious DLL.

This technique is referred to as DLL sideloading, where attackers deliver an executable file from a genuine application known to load a DLL library with a specific name from the same directory. The attackers simply provide a malicious DLL with the same name to accompany the file. By utilizing a legitimate file to load malicious code into memory, the attackers aim to evade detection by security tools that may have the file whitelisted.

The attack's initial payload, referred to as SNOWYAMBER by Polish researchers, is a lightweight custom malware dropper that gathers basic computer information and communicates with a command-and-control server on Notion.so, an online workspace collaboration service. The primary objective of this dropper is to download and execute additional malware, including Cobalt Strike and BruteRatel beacons, which are commercial post-exploitation frameworks initially intended for penetration testers but have been adopted by attackers as well.

Although a variant of SNOWYAMBER was publicly reported by Recorder Future in October 2022, the Polish researchers discovered a new variant with enhanced anti-detection routines in February 2023. APT29 also utilized another payload named HALFRIG, which, unlike SNOWYAMBER, decrypted Cobalt Strike from shellcode instead of relying on a command-and-control server for the download.

In March the hackers employed another tool named QUARTERRIG, sharing a portion of its codebase with HALFRIG. At this time, APT29’s list of targets included diplomatic entities (embassies, diplomatic staff, foreign ministries, etc.), government entities, international organizations, and non-governmental organizations. Although the attacks were primarily focused on EU and NATO entities, some targets were located in Africa.

Diplomats Stationed in Ukraine

By June 2023, APT29 initiated a targeted campaign aiming to breach the computers of numerous diplomats stationed at embassies in Ukraine. Palo Alto Networks' Unit 42 research division revealed that this extensive espionage activity focused on diplomats from at least 22 of the approximately 80 foreign missions in Kyiv, the capital of Ukraine.

In mid-April 2023, a diplomat within the Polish Ministry of Foreign Affairs sent out a legitimate flyer to various embassies advertising the sale of a used BMW 5-series sedan located in Kyiv. APT29 intercepted and duplicated the flyer, embedding it with malicious software, and distributed it to dozens of other foreign diplomats working in Kyiv.

The Polish diplomat said he had sent the original advertisement to various embassies in Kyiv, and that someone had called him back because the price looked "attractive". However, he realized that the price the individual was referring to appeared to be slightly lower. It turns out, the threat actor listed the diplomat's BMW for a lower price - 7,500 euros - in their fake version of the advertisement, to encourage more people to download malicious software that would give them remote access to their devices.

That software was disguised as an album of photographs of the used BMW. Attempts to open those photographs would have infected the target's machine. Twenty-one of the 22 embassies were targeted by the threat actors, but it’s not clear which embassies (if any) were compromised.

In 2021, U.S. and British intelligence agencies linked APT29 to Russia's foreign Intelligence Service, the SVR. Researchers at Unit 42 traced the fake car advertisement campaign back to the SVR, as the threat actors reused specific tools and techniques previously associated with the spy agency.

A New Campaign?

In May 2023, the researchers at Lab52 published their findings on a new campaign by an unknown threat actor using similar techniques to APT29, leading them to believe the new activity is from APT29. They named the campaign “Information” and stated that there was a new sample resembling QUARTERRIG, a malware previously analyzed by CERT.PL and connected to APT29, that was uploaded to VirusTotal. The analysis of the QUARTERRIG campaign referred to it as "Note". However, Lab52 has named the campaign “Information” so they can show the new features of the campaign.

The hash of the sample publicly available on VirusTotal is b422ba73f389ae5ef9411cf4484c840c7c82f2731c6324db0b24b6f87ce8477d and only 3 antivirus engines identified the sample as malicious at the time of Lab52’s findings. Lab52 reports that the new campaign exhibits a structure highly resembling the “Note” campaigns outlined in the CERT.PL report that we mentioned previously. The samples studied in the CERT.PL report date back to March 2023. However, Lab52 has observed a shift in the malware's operation since April 2023, noting variations in the injection method within the latest analyzed samples.

This time, the shellcode is found in a file named "dbg.info," which differs from what was observed in previous campaigns. The "Information.iso" includes the following components:

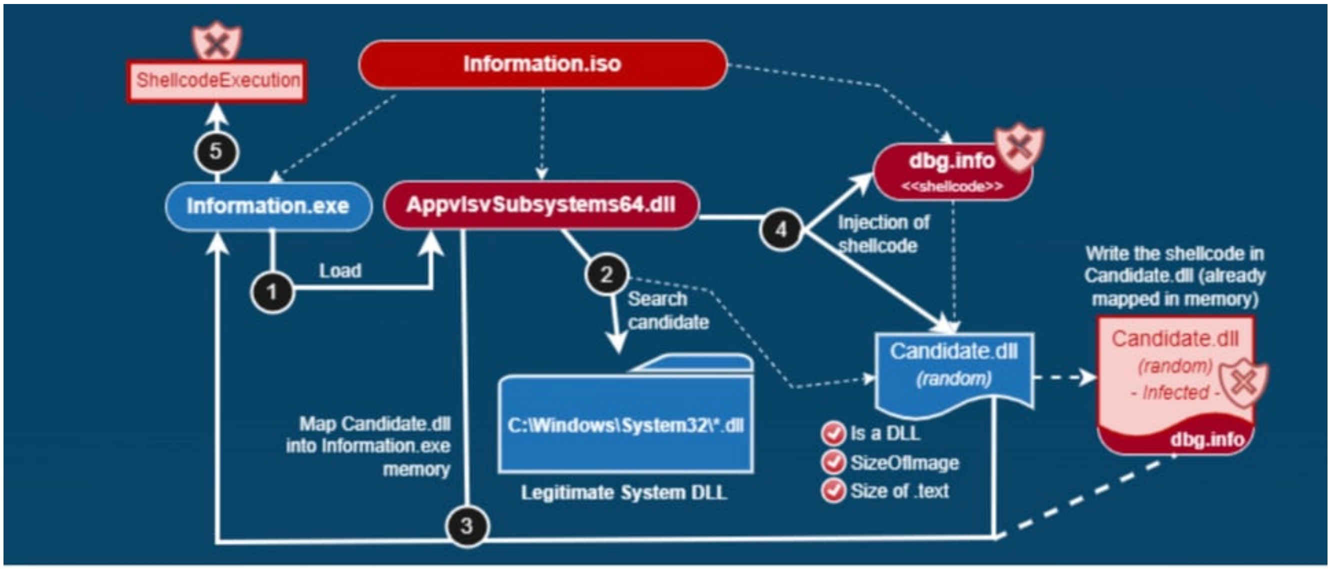
- AppvIsSubsystems64.dll – A DLL utilized to load a genuine system DLL and inject the shellcode into it.
- dbg.info – Contains the shellcode.
- Information.exe – A legitimate binary signed by Microsoft, intended to load AppvIsSubsystems64.dll via DLL Side-Load.

Lab52 also stated that the compilation date of AppvIsvSubsystems64.dll in this new campaign is more recent than in the previous one, indicating possible modifications made to improve the sample. The firm also stated that the most noticeable change between previous campaigns and the new one is the injection technique.

The objective remains unchanged: executing two DLLs using the executable (Information.exe). The first DLL, AppvIsvSubsystems64.dll, will be loaded during the process's execution. The second DLL will be loaded by AppvIsvSubsystem64.dll, but in this case, it will undergo careful modifications using different techniques to minimize detection methods.

Thus, Information.exe, a legitimate binary, will serve as the container for the malware to execute. To achieve this, it will load AppvIsvSubsystems64.dll, which will identify a suitable system DLL to be modified with the shellcode before loading into Information.exe. The main changes are found in AppvIsvSubsystems64.dll. Additionally, the command and control (C2) vary. Similar to how QUARTERRIG evolved from HALFRIG, APT29 has enhanced the sophistication of its dll loader "Applvsubsystem64.dll" in this new campaign.

Image 2: Current Infection Chain for “Information” Campaign

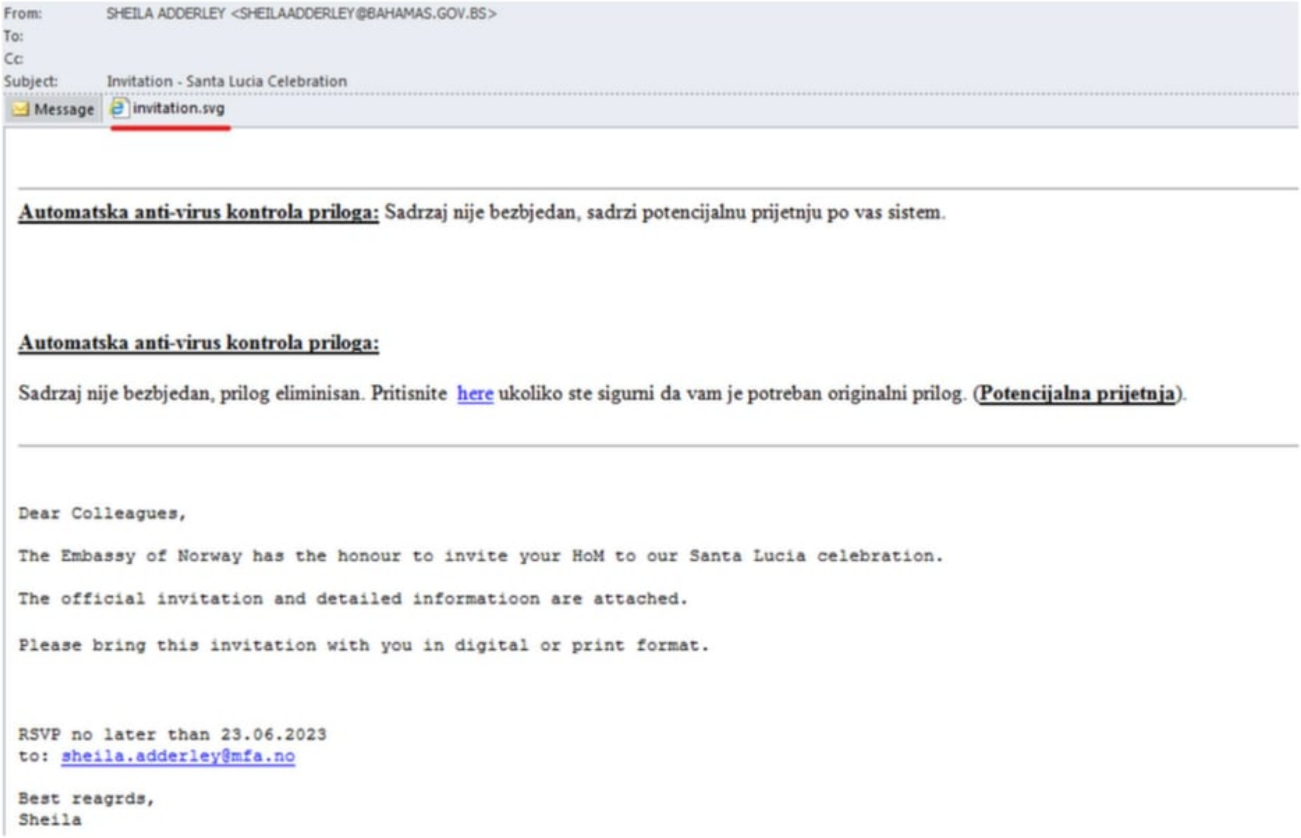


Source: Lab52

CCleaner

As of July 2023, Lab52 has reported the discovery of more advanced tactics used by APT29, which includes the usage of SVG Dropper, DLL for infection, and C2 behavior. The observed campaign's primary method of entry is through a phishing email with the subject "Invitation - Santa Lucia Celebration." This deceptive invitation is designed to impersonate the Norwegian embassy.

Image 3: Phishing Email



From: SHEILA ADDERLEY <SHEILAADDERLEY@BAHAMAS.GOV.BS>
To:
Cc:
Subject: Invitation - Santa Lucia Celebration

Automatska anti-virus kontrola priloga: Sadrzaj nije bezbjedan, sadrzi potencijalnu prijetnju po vas sistem.

Automatska anti-virus kontrola priloga:

Sadrzaj nije bezbjedan, prilog eliminisan. Pritisnite here ukoliko ste sigurni da vam je potreban originalni prilog. (**Potencijalna prijetnja**).

```
Dear Colleagues,

The Embassy of Norway has the honour to invite your HoM to our Santa Lucia celebration.

The official invitation and detailed informatioon are attached.

Please bring this invitation with you in digital or print format.


RSVP no later than 23.06.2023
to: sheila.adderley@mfa.no

Best reagrds,
Sheila
```

Source: Lab52

After opening the file, an executed script initiates the process of mounting and downloading a file with a .iso extension, which holds the next stage of infection. This process transforms the .svg file into an HTML Smuggling technique, effectively infecting the victim, and dropping the next stage of the malware. Next, a download of an ISO file named "invitation.iso" is triggered, containing content similar to what Lab52 has previously observed in other APT29 campaigns.

The attention-grabbing file is invitation.lnk, a deceptive shortcut with a folder icon that executes the following command:

```
%windir%/system32/cmd.exe /q /c "robocopy . C:\Windows\Tasks /NODCOPY /NFL /NDL /NJH /NJS /NC /NS /NP > nul & start C:\Windows\Tasks\CCleanerReactivator.exe > nul"
```

Using Robocopy, all files are copied to the "C:\Windows\Tasks" folder, before CCleanerReactivator.exe is executed. CCleanerReactivator.exe is a digitally signed binary and remains undetected in VirusTotal. This software serves the legitimate purpose of freeing up computer space and can be downloaded legally.

Regarding C2 communications, Lab52 reported significant changes compared to previous campaigns. In the past, registration with C2 involved a POST request of an encrypted JSON containing the UserName and ComputerName. However, in this latest version, victim IDs in C2 have been streamlined to just 4 digits. Furthermore, the next stage (shellcode) is directly downloaded from C2 instead of being loaded locally.

It's important for cyber security professionals to pay close attention to established APTs just as much as they focus on newer ones. The example of APT29's espionage campaign in April 2023 targeting diplomatic and foreign ministries of NATO and EU member states demonstrates that even well-established threat actors can evolve their tactics and develop previously undocumented malware payloads.

By closely monitoring and analyzing the activities of known APT groups, security professionals can gain valuable insights into their methods, enabling better preparedness and proactive defense measures against their future attacks. Ignoring or underestimating established APTs could leave organizations vulnerable to highly sophisticated and evolving threats, potentially leading to significant data breaches, and compromising national security or sensitive information. A comprehensive approach to cybersecurity should include vigilant monitoring of both well-known and emerging threat actors to safeguard against constantly evolving cyber threats.

mitre map

Initial Access	Execution	Defense Evasion	Discovery
T1566: Phishing	T1102: Web Service	T1070: Indicator Removal of Host	T1057: Process Discovery
	T1055: Process Injection	T1176: Browser Extensions	

	T1574: Hijack Execution Flow
	T1134: Access Token Manipulation

avertium's recommendations

- Employee Training and Awareness: Conduct regular cybersecurity training sessions for employees to educate them about the dangers of phishing campaigns. Teach them how to identify suspicious emails, links, and attachments. Encourage a culture of reporting potential phishing attempts to the IT or security team.
- Robust Email Filtering: Implement advanced email filtering solutions that can detect and block phishing emails before they reach employees' inboxes. These filters can analyze email content, attachments, and sender reputation to identify and quarantine potentially malicious messages.
- Multi-Factor Authentication (MFA): Enforce the use of multi-factor authentication for accessing sensitive accounts and systems. MFA adds an extra layer of security by requiring users to provide a second form of verification (e.g., a one-time code sent to their mobile device) in addition to their password.
- Regular Security Patching and Updates: Ensure all software, operating systems, and security applications are up to date with the latest patches and updates. Cybercriminals often exploit known vulnerabilities in outdated software to launch phishing attacks. Regular updates help mitigate these risks and enhance overall cybersecurity posture.

How Avertium is Protecting Our Customers

- Avertium’s Capability Management Team is implementing several SIEM detections for activity related to APT29:

  Please Note: These detections could have a high volume of false positives and are not a replacement for a proper security policy.

UNC2452 Process Creation Patterns	Detects specific process creation patterns as seen used by UNC2452
APT29 Command Line	Detects suspicious PowerShell command line combination as used by APT29.
Mimikatz keywords	Detects specific keywords in process fields indicative of mimikatz usage.

- Avertium offers Vulnerability Management to provide a deeper understanding and control over organizational information security risks. If your enterprise is facing challenges with the scope, resources, or skills required to implement a vulnerability management program with your team, outsourced solutions can help you bridge the gap.

- Fusion MXDR is the first MDR offering that fuse together all aspects of security operations into a living, breathing, threat-resistant XDR solution. By fusing insights from threat intelligence, security assessments, and vulnerability management into our MDR approach, Fusion MXDR offers a more informed, robust, and cost-effective approach to cybersecurity – one that is great than the sum of its parts.
- Minimizing the impact of a successful ransomware attack requires detecting it as early in the attack as possible. A Security Information and Event Management (SIEM) system can help an organization to accomplish this. Avertium offers a comprehensive SIEM-based approach that increases the potential for detecting a ransomware infection before it deploys. SIEM provides a holistic overview of a company's IT environment from a single point of view in terms of its specific security events, empowering teams to detect and analyze unusual behavior.

indicators of compromise

- The espionage campaign related to SnowyAmber has several IoCs published by the Polish government. These IoCs can help build detections for known malware samples. The IoCs are located in their advisory.

- **"Information" campaign File Hashes**
    - Information[.]iso
      B422BA73F389AE5EF9411CF4484C840C7C82F2731C6324DB0B24B6F87CE8477D
    - Information[.]exe
      6C55195F025FB895F9D0EC3EDBF58BC0AA46C43EEB246CFB88EEF1AE051171B3
    - AppvIsvSubsystems64[.]dll
      E7C49758BAE63C83D251CACBFADA7C09AF0C3038E8FF755C4C04F916385805D8
    - Dbg[.]info

      5F6219ADE8E0577545B9F13AFD28F6D6E991326F3C427D671D1C1765164B0D57

- **CCleaner**
    - MD5 File Hash
      f29083f25d876bbc245a1f977169f8c2
    - SHA 1 File Hash
      a61b35a9a9650396223bb82aad02c0ec1f1bb44b
    - SHA26 File Hash
        - 4875a9c4af3044db281c5dc02e5386c77f331e3b92e5ae79ff9961d8cd1f7c4f
        - 59e5b2a7a3903e4fb9a23174b655adb75eb490625ddb126ef29446e47de4099f
        - 7fc9e830756e23aa4b050f4ceaeb2a83cd71cfc0145392a0bc03037af373066b
        - 966e070a52de1c51976f6ea1fc48ec77f6b89f4bf5e5007650755e9cd0d73281
        - a8ae10b43cbf4e3344e0184b33a699b19a29866bc1e41201ace1a995e8ca3149
        - af1922c665e9be6b29a5e3d0d3ac5916ae1fc74ac2fe9931e5273f3c4043f395
        - d7bda5e39327fe12b0c1f42c8e27787f177a352f8eebafbe35d3e790724eceff
    - URL
      hxxps://kefas[.]id/search/s[.]php
    - Domain
      Kefas[.]id

Supporting DocumentationS

- Russian cyberspies hit NATO and EU organizations with new malware toolset | CSO Online
- The Resurgence of Russian Threat Actor, NOBELIUM (avertium.com)
- New tricks of APT29 – update on the CERT.PL report (lab52.io)
- New invitation from APT29 to use CCleaner - AlienVault - Open Threat Exchange
- MagicWeb: NOBELIUM’s post-compromise trick to authenticate as anyone | Microsoft Security Blog
- Microsoft Uncovers New Post-Compromise Malware Used by Nobelium Hackers (thehackernews.com)
- APT29 Exploited a Windows Feature to Compromise European Diplomatic Entity Network (thehackernews.com)
- New invitation from APT29 to use CCleaner (lab52.io)
- Russian hackers lured diplomats in Ukraine with cheap BMW ad | Reuters
- They See Me Roaming: Following APT29 by Taking a Deeper Look at Windows Credential Roaming | Mandiant
- BlueBravo Uses Ambassador Lure to Deploy GraphicalNeutrino Malware (recordedfuture.com)
- Espionage campaign linked to Russian intelligence services - Baza wiedzy - Portal Gov.pl (www.gov.pl)

- Russia-Linked APT29 Uses New Malware in Embassy Attacks - SecurityWeek
- APT29 intensifies credential-stealing attacks | SC Media (scmagazine.com)
- Diplomats Beware: Cloaked Ursa Phishing With a Twist (paloaltonetworks.com)

APPENDIX II: Disclaimer

This document and its contents do not constitute, and are not a substitute for, legal advice. The outcome of a Security Risk Assessment should be utilized to ensure that diligent measures are taken to lower the risk of potential weaknesses be exploited to compromise data.

Although the Services and this report may provide data that Client can use in its compliance efforts, Client (not Avertium) is ultimately responsible for assessing and meeting Client's own compliance responsibilities. This report does not constitute a guarantee or assurance of Client's compliance with any law, regulation or standard.