LOGPOINT

EMERGING THREATS PROTECTION REPORT

Not Too Cozy: Cozy Bear

www.logpoint.com

FOREWORD

The Dukes, aka (amongst many aliases) APT29, Cozy Bear, or Nobelium, is a prominent cyber espionage group with a history spanning more than a decade. This group gained notoriety for its involvement in the intrusion of the Democratic National Committee during the lead-up to the 2016 U.S. presidential election. In 2019, they were linked to Operation Ghost, a large-scale espionage campaign targeting European foreign ministries. Additionally, in 2020, The Dukes made headlines for a supply-chain attack that exploited SolarWinds, leading to compromises in various sectors of the U.S. government and other critical institutions.

Swachchhanda Shrawan Poudel

Logpoint Security Research

Swachchhanda Shrawan Poudel is a cybersecurity enthusiast with a bachelor's degree in cybersecurity and certification as an ethical hacker. With an interest in both offensive and defensive security, he currently works as a Security Researcher at Logpoint, focusing on detection engineering, threat hunting, and remediation.

TABLE OF CONTENTS

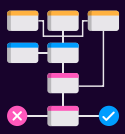
ABOUT LOGPOINT EMERGING THREATS PROTECTION

The cybersecurity threat landscape continuously changes while new risks and threats are discovered all the time. Not every organization has enough resources or the know-how to deal with evolving threats.

Emerging Threats Protection is a managed service provided by a Logpoint team of highly skilled security researchers who are experts in the field of threat intelligence and incident response. Our team keeps you informed on the latest threats and provides custom detection rules and tailor-made playbooks designed to help you investigate and mitigate emerging incidents.

**All new detection rules are available as part of Logpoint's latest release and through the Logpoint Help Center. Customized investigation and response playbooks are available to all Logpoint Emerging Threats Protection customers.

1. Research for emerging threats such as malware families, threat actors and vulnerabilities
2. Data retrieval e.g., malware samples, IOCs, and TTP



1. Analysis of the collected data and malware and, tracking of threat actors' activities
2. Creation and update analytics and playbooks
3. Writing of ETP report

1. Publishing of report

1. Continuous monitoring for other emerging threats to create next ETP report

Below is a rundown of the incident, potential threats, and how to detect any potential attacks and proactively defend using Logpoint Converged SIEM capabilities.

BACKGROUND

First, a public service announcement: The Dukes has many aliases, from this moment forward we will use them interchangeably through the blog and report. It should be noted, that they are the same. Aliases include: Group 100, COZY BEAR, The Dukes, Minidionis, SeaDuke, YTTRIUM, IRON HEMLOCK, Grizzly Steppe, G0016, ATK7, Cloaked Ursa, TA421, Blue Kitsune, ITG11, BlueBravo, and **Midnight Blizzard (NOBELIUM)**.

APT-29, also known as Cozy Bear, is the state-sponsored advanced persistent threat (APT), that is believed to be **associated with Russia's Foreign Intelligence Service (SVR)** which was initiated in 2008. The group gained significant notoriety for conducting sophisticated and cyber espionage activities against governments and non-governmental organizations, businesses, think tanks, and other high-profile targets.

They typically use spearphishing campaigns amongst many other techniques to gain initial access to target networks and then use a range of tools and techniques to move laterally within the network and exfiltrate sensitive data. The group is known for its ability to operate covertly and evade detection for extended periods.

In 2020, The **SolarWinds attack** (also known as the SolarWinds supply chain attack) occurred and is attributed to APT-29 - It's the most infamous supply chain attack to date.

Some notable attack characteristics and activities associated with APT-29 include:

1. **Russian Origin:**
   - APT-29 is widely believed to be backed up by the Russian government with links to the Russian intelligence agency, the Federal Security Service (FSB).
2. **Cyber Espionage**
   - APT-29 is widely known for its cyber espionage, stealing sensitive information and intelligence from its targets. It often deploys sophisticated persistence techniques to stay vigilant persistence in the target machine.
3. **High-Profile Targets**
   - Government/Non-government agencies think tanks, and organizations commonly involved in geopolitically sensitive issues are common targets of APT-29. According to **Mandiant**, APT-29 is concentrating its efforts on Ukraine, particularly against foreign embassies. This is intriguing since they are attempting to deceive nations that are normally supportive of Russia. They appear to be doing this to assist Russia's intelligence service (SVR) in gathering information at the present critical phase of the war in Ukraine.
4. **Advanced Techniques and Toolset**
   - This gang is well-known for using sophisticated strategies and tools to infiltrate its targets, including zero-day vulnerabilities and custom malware.
5. **Cozy Bear vs. Fancy Bear**
   - It is critical to distinguish between APT-29 (Cozy Bear) and APT-28 (Fancy Bear), two distinct Russian APT organizations. While both are thought to be state-sponsored, their tactics, techniques, and targets differ.
6. **Ongoing Threat**
   - APT-29 is still a notorious and persistent threat in the cybersecurity world. Organizations and governments throughout the world should continue to be cautious in their defense against cyberattacks.

CYBERATTACKS ASSOCIATED WITH APT-29

In early 2013, a sophisticated strain of malware known as '**Miniduke**' emerged - it was attributed to APT-29 (CozyDuke). This malware was notably deployed against prominent targets, including NATO and various European government agencies. **Operation Ghost** was an APT-29 campaign that began in 2013 and involved activities targeting European foreign ministries as well as the embassy of an EU country in Washington, D.C. APT-29 deployed new malware families and used web services, steganography, and unique C2 infrastructure for each victim during Operation Ghost.

According to the **f-secure lab's** report in 2015, throughout its initiation from 2008 to 2015, APT-29 (CozyDuke) continuously improved and expanded its arsenal of malware toolsets. These diverse malware families included MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. More details of the APT-29's activities between 2008 and 2015 are detailed in the **f-secure lab's whitepaper**. The years that followed showed a flurry of activity.

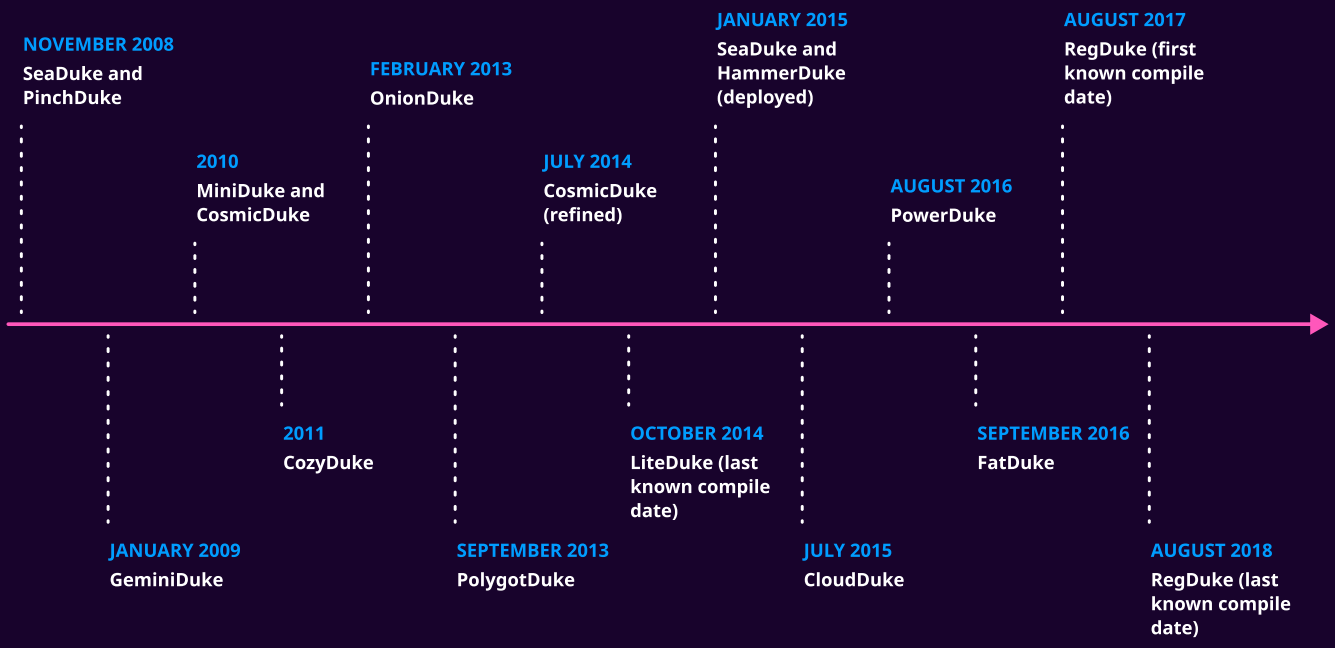
- In **2016**, Crowdstrike was contacted to investigate a suspected **breach at the Democratic National Committee (DNC)**. Following the comprehensive investigation, it was concluded that APT-29 and another Russian APT group called APT28 (Fancy Bear) had been in their networks since 2015 persisting and stealing their data and information.

- In **April 2017**, Mandiant released a study on the toolset used by APT-29 which is a stealthy backdoor, called POSHSPY. It operates stealthily, leveraging built-in Windows features like PowerShell and Windows Management Instrumentation (WMI). The backdoor employs legitimate system processes, making malicious code execution visible only through enhanced logging or memory analysis. Its infrequent network activity, traffic obfuscation, robust encryption, and use of local, legitimate websites for command and control (C2) enhance its covert nature. Mandiant further adds that they identified POSHSPY in several other environments compromised by APT-29 over the past two years.
- In late **2018**, there was a large phishing campaign against multiple organizations spanning “military agencies, law enforcement, defense contractors, media companies and pharmaceutical companies. Some of the common techniques from past campaigns of CozyBear were seen in those campaigns. The attack leveraged a malicious Windows shortcut (a .lnk file) that has similarities to a malicious shortcut used by the Dukes in 2016.
- In **June 2019**, ESET published a report on "Operation Ghost," an espionage campaign attributed to APT-29. This campaign was believed to have commenced in 2013, particularly targeting ministries of foreign affairs in Europe and the Washington, D.C. embassy of a European Union country. According to MITRE ATT&CK®, During Operation Ghost, APT-29 used new families of malware and leveraged web services, steganography, and unique C2 infrastructure for each victim.
- Custom Powershell malware was used in the 2019 APT-29 operations. It was thought that there may even be PowerShell-based utilities dedicated to each attack. It was also suspected that steganography had been extensively used to mask the malware payloads.
- In **2020**, a significant cyber attack commonly known as SolarWinds Attacks, thought to have been carried out by an APT-29 infiltrated thousands of institutions worldwide, including multiple elements of the US federal government, resulting in a series of data breaches. With 18,000 firms globally downloading trojanized versions of the IT management platform SolarWinds Orion, the SolarWinds campaign is recognized as one of the most sophisticated supply-chain attacks to date.
- In **2021**, both MSTIC and CERTFR reported on APT-29's ongoing cyber threats. MSTIC identified APT-29's use of malware families like EnvyScout, BoomBox, NativeZone, and VaporRage in email attacks aimed at government and diplomatic entities since February 2021. Around the same timeframe, in December 2021, CERTFR disclosed that French organizations had faced phishing attacks since the same timeframe, with tactics resembling the SolarWinds supply chain attack, highlighting APT-29's persistent and adaptable threat landscape.
- Beginning in **mid-January 2022**, Mandiant discovered and reacted to an APT-29 phishing attempt targeting a diplomatic organization. During the investigation, Mandiant discovered BEATDROP and BOOMMIC downloaders being used in the campaigns. Mandiant uncovered APT-29 targeting several other diplomatic and government organizations through a series of phishing waves shortly after this campaign was identified.

Recently this year Mandiant released another article in September, mentioning the new phishing campaigns run by APT-29 targeting particularly against foreign embassies situated in Ukraine. In the article, it has been stated As Kyiv initiated its counteroffensive in the first half of 2023, APT-29's speed of activities and attention on Ukraine grew, highlighting the SVR's major involvement in gathering intelligence regarding the present crucial phase of the war.

MALWARE TIMELINE

Here's a mapping of APT-29's malware families with the years they were first known to have appeared based on this blog.



It's important to note that APT-29 continued to evolve and develop new malware families over the years, even when some of their older malware became publicly exposed. They did not retire malware wholesale but instead adapted and refined their tools to avoid detection while continuing their operations.

ANALYSIS OF APT-29'S ACTIVITY

Examining APT-29's past operations indicates their incredible capacity to constantly improve and produce new malware tools, all while remaining adept at being both visible and hidden in the cybersecurity scene. From 2008 until 2023, APT-29 seldom exhibited a readiness to retire an entire malware family, even when their operations were well known in the media. This implies that, at least in this case, APT-29 was not willing to discontinue activities or abandon its tools in the face of heightened scrutiny. This case demonstrates the tenacity of certain APT organizations in avoiding detection and continuing their actions.

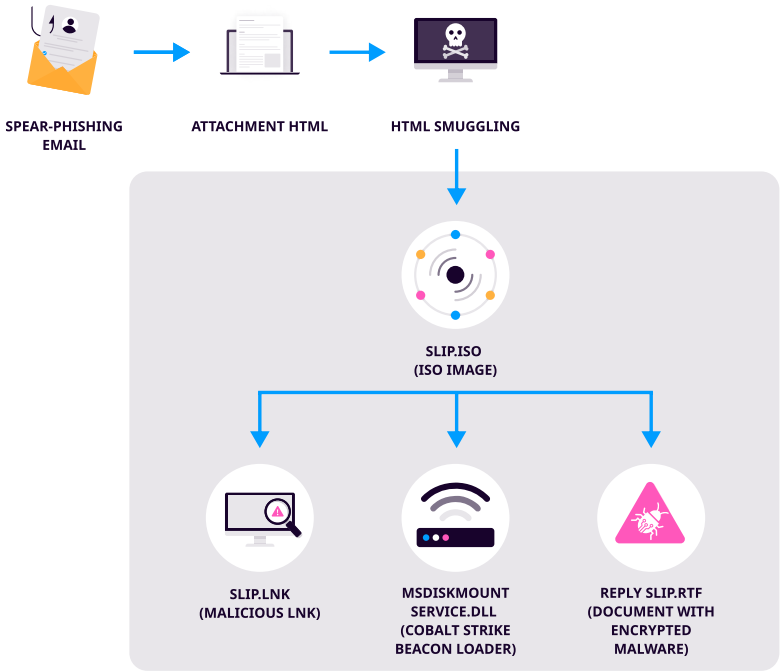
RECENT EVOLUTION OF APT-29 MALWARE DELIVERY TECHNIQUES

Since 2021, both MSTIC and Mandiant have been actively monitoring APT-29's activities, revealing distinctive malware delivery techniques. The phishing emails sent by APT-29 masqueraded as administrative notices related to various embassies. While phishing emails remain a common element across most of their campaigns, the intricacies of how the malware is deployed exhibit variations and commonalities. In this analysis, we will delve into the specifics of each malware delivery technique employed by APT-29, highlighting both the similarities and differences between them.

Over the years, APT-29's techniques have displayed remarkable consistency, with only occasional adjustments. What's particularly intriguing is their ability to consistently execute successful campaigns using these seemingly unaltered techniques without significant concerns or setbacks. This resilience and effectiveness in their operations highlight the sophistication and adaptability of APT-29 as a threat actor.

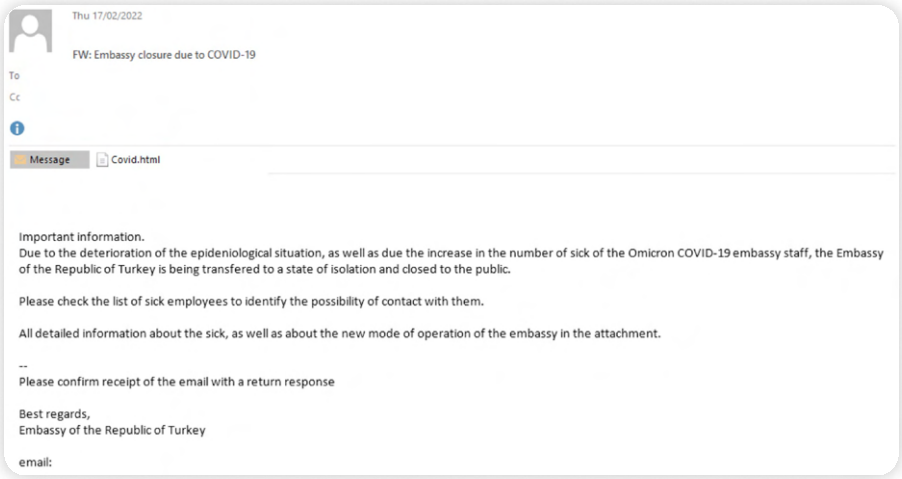
NOBELIUM's HTML Smuggling Spear-Phishing Attack: Malware Deployment

In their **2021 report**, MSTIC detailed the next phase of NOBELIUM's campaign, wherein they observed attempts to compromise systems through a spear-phishing email containing an HTML file attachment (HTML Smuggling). Once this HTML file was opened by the targeted user, an embedded JavaScript initiated the download of an ISO file on the disk hosted on the Google Firebase platform and urged the recipient to open it. This ISO file was then mounted akin to an external or network drive. Subsequently, a shortcut file (LNK) was triggered to execute an associated DLL, ultimately leading to the execution of Cobalt Strike Beacon on the compromised system.



HTML smuggling Infection Chain (Source: **Microsoft**)

In April 2022, Mandiant's report also highlighted the same kind of initial delivery approach of payloads, which is the adoption of HTML Smuggling techniques by APT-29 for malware delivery. The HTML file attachments sent through such spear-phishing technique by APT-29 have been alternatively called ROOTSAW or **EnvyScout**. It can be best described as the primary dropper capable of de-obfuscating and writing a malicious second-stage payload i.e., ISO/ zip file to disk.



APT-29 Phishing Lure Example, using an attached file Covid.html (Source:**Mandiant**)

A Windows shortcut (LNK) file and a malicious DLL are included in the ISO/image file. If the user double-clicks the LNK file, the "Target" command will run normally. This method tricks the victim into opening the LNK file, launching the malicious DLL unintentionally.

The consistent use of LNK files, which showed considerable similarities to those found in 2021 operations, was a key component of the APT-29 campaign. These similarities included specific features like the usage of a specific icon location, as well as matching machine IDs and MAC addresses.

APT-29's Use of Compromised Web Services for Malware Distribution

According to a recent **Mandiant** report in September 2023, another notable discovery is that ROOTSAW's major position in APT-29 activities has resulted in substantial modifications in its malware supply chain. This research emphasizes the shift away from utilizing HTML attachments (HTML Smuggling) as the first infection vector and toward putting first-stage payloads on compromised web services such as WordPress sites. This strategic decision to server-side hosting has most certainly given APT-29 better control over how they deliver their malware and be more selective in revealing their advanced capabilities in the later stages of their attacks.

Additionally, the **report** notes that APT-29 has implemented various filters within its initial malware payloads. These filters serve two purposes: they assist in preventing malware discovery in environments that were not intended to be hacked, and they guarantee that staged malware is removed from compromised systems soon after it has fulfilled its purpose. What's more, these methods have proven effective in keeping their malware out of public malware libraries and other standard security research tools. This allows APT-29 to avoid detection and keep its newer malware variants active for extended periods.

APT-29 combination of techniques for Malware distribution

Even though the aforementioned two ways have been common in multiple campaigns, Mandiant reports threat actors have employed various methods to deliver their payloads. The techniques involve either combining additional steps with the ones previously mentioned or through entirely new approachescombining other steps in between with these or completely new ways.

- Directly delivering the malicious attachment containing the ROOTSAW to the victim
- Hosting the ROOTSAW on a compromised website, and enticing the victim via mail to click and download the ROOTSAW
- Sending a deceptive attached document through the mail, that contains a link to a compromised website where ROOTSAW or other first-stage payloads are hosted
- Sending a luring document through the mail, that contains a link to a compromised website where direct second stage payload in the above steps i.e. (ISO/ZIP) files are hosted
- Hosting the primary malicious (ISO/ZIP) on a compromised website, and luring the victim through mail to download and execute the malware

NOTE: ROOTSAW is the malicious HTML document (first-stage payload), in which embedded javascript works to de-obfuscate the obfuscated content of the payload and directs the download of the second-stage payload, which is the actual malware in the form of ZIP or ISO files.

MALWARE DELIVERY ANALYSIS HINDSIGHT

The common thread among the previously mentioned delivery methods was the use of malicious disk images (specifically, .iso files). APT-29 consistently relied on ISO files as their chosen vehicle for malware deployment, capitalizing on a key vulnerability in Windows systems. ISO files can bypass the **Mark-of-the-Web (MotW)** feature of Windows. Windows uses the MotW to indicate that a file originated from the Internet, which allows Microsoft Defender SmartScreen to perform additional inspection of the content. When high-risk extensions are deployed, MotW assists in informing the user with an additional prompt. APT-29 chose ISO files for malware distribution because they took advantage of a unique Windows feature. Windows does not use the "Mark-of-the-Web" capability to identify ISO files and their contents as coming from the internet, which usually results in additional security precautions such as improved antivirus scans. The lack of Mark-of-the-Web categorization effectively allowed ISO files to bypass Windows' SmartScreen function, allowing APT-29 to launch its malware without prompting the user for consent. APT-29 wanted to increase the success rate of their malicious payloads reaching their intended targets without raising suspicion or hitting extra security hurdles by leveraging this Windows feature.

STRENGTHENING SECURITY MEASURES IN LIGHT OF MARK OF THE WEB (MOTW) WEAKNESS

Now that we have insight into the constraints of Mark of the Web (MOTW) and the appeal of .iso files for threat actors, we are well-equipped to establish both protective measures and enhance awareness.

Mitigations

MITRE ATT&CK suggests two mitigation strategies to address the vulnerabilities associated with the Mark of the Web (MOTW).

Disable or Remove Feature or Program

MITRE ATT&CK recommends considering the disabling of auto-mounting for disk image files, such as .iso, .img, .vhd, and .vhdx. It can be achieved in multiple ways as you like which are described below.

a. Modify Registry values associated with Windows Explorer file associations

Disabling auto-mounting for disk image files can be done by making adjustments to the Registry values associated with Windows Explorer file associations. By doing so, you can effectively disable the automatic Explorer "Mount and Burn" dialog that appears for these specific file extensions. By navigating to `HKEY_CLASSES_ROOT`, followed by `Windows.ISO.File` and `Windows.VHD.File`, and deleting the 'mount' subkey within the 'shell' subkey, you can effectively disable the 'Mount' option for .ISO and .VHD files. `reg.exe` utility can also be used to modify these registry values as below.

To remove 'Mount' for .ISO files:

```
reg.exe delete HKEY_CLASSES_ROOT\Windows.ISO.File\shell\mount
```

To remove 'Mount' for .VHD files:

```
reg.exe delete HKEY_CLASSES_ROOT\Windows.VHD.File\shell\mount
```

b. Modify the NoAutoMount registry value

To effectively stop the auto-mounting of drives, one approach is to modify the Windows Registry using the `reg.exe` command. By setting `NoAutoMount` to 1, automatic mounting of new drives can be disabled, allowing for a degree of flexibility in managing these drives. One implementation of doing this through reg.exe is given below.

```
reg.exe add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mountmgr" /v NoAutoMount /t REG_DWORD /d 1 /f
```

While implementing this change, it's important to understand that this action will not deactivate the core mount functionality itself. Your system will remain fully functional while mitigating potential risks associated with the automatic mounting of these types of files. Organizations can use any of the ways to change these registry values while changing it through GPO is more manageable and scalable.

EXECUTION PREVENTION

MITRE ATT&CK also recommends blocking container file types at web and/or email gateways and unregistering container file extensions in Windows File Explorer.

a. Blocking Container File Types at Web and/or Email Gateways:

Configuring web and email gateways to restrict specific types of container files, such as.iso files, from being sent or received, is part of this strategy. Organizations can limit the danger of harmful container files reaching endpoints by restricting these file types at the network level.

b. Unregistering Container File Extensions in Windows File Explorer:

Windows File Explorer is the operating system's default file management application. Disable Windows Explorer file associations for Disc Image Mount (ISO, IMG, VHD, VHDX). Unregistering container file extensions involves deleting the associated file handlers for certain file types from Windows File Explorer. It entails removing the default behavior of automatically mounting and running certain container files, such as .iso files when they are accessed in the context of minimizing MOTW gaps. This is accomplished by deleting the registry entries that permit the automatic execution of certain files.

DETECTION

Initial Access

If totally blocking these files isn't a possibility, and you come across a disk image via email, a site download, or another method such as HTML smuggling, it's critical to examine the file's intended function and format. Consider a popular phishing approach in which an "invoice" is attached to an email. In such cases, detection engineers should be wary of uncommon file formats such as ISO images since there is usually no logical justification for an invoice document to be delivered in the form of a disk image.

Analysts can look at Sysmon Event ID 11 (file creation) events in the Downloads or temp folder to check if the file extension ends with image format files such as .iso, .vhd, .vhdx, etc.

```
label=File label=Create
event_id=11
(path="*Users*" path="*Downloads*") OR (path="*Appdata*")
file IN ["*.iso", "*.vhd", "*.vhdx"]
```

This query can generate false positive results if the user downloads legitimate image files in their system.

You can also use this awesome **sigma rule** by Florian which detects the creation of a recent element file that points to an .ISO, .IMG, .VHD or .VHDX file. This query also needs Sysmon Event ID 11 events ingested in Logpoint.

```
label=File label=Create
event_id=11
file IN ["*.iso.lnk", "*.img.lnk", "*.vhd.lnk*", "*.vhdx.lnk*"]
path="*\Microsoft\Windows\Recent\*"
```

This query can generate false positive results if the user mounts an image file for legitimate reasons.

PERSISTENCE

Unlike the Ransomware or malware families, which typically engage in a lot of overt activities such as system enumeration, file encryption, data exfiltration, and other conspicuous actions. Generally, these activities are visible to users and they create enough telemetry in the SIEM for an analyst to detect and take necessary preventive measures. But State Sponsored Threat Actors like APT-29 have distinct objectives that are not financially driven, indifferent from ransomware or malware. With APT-29 it has been observed their main motive is to gain intelligence or sensitive information from international diplomats, embassies, think tanks, and government/non-governmental bodies that are directly or indirectly involved with geopolitical matters. To accomplish this, APT-29 employs a strategic approach that prioritizes stealthy persistence within a victim's system, allowing them to clandestinely maintain access for extended periods while surreptitiously exfiltrating confidential and sensitive data. This clandestine approach significantly limits the availability of telemetry that could trigger alerts in a Security Information and Event Management (SIEM) system, making it exceptionally challenging for analysts to detect compromised machines.

In such cases, the only viable option for analysts is to proactively hunt for signs of known persistence techniques that might have been employed by APT-29. This proactive hunting approach becomes essential in the absence of overt and suspicious behavior that typically triggers detection mechanisms.

One method for being persistent in the system is to include a script in the startup folder that runs when the computer boots. It is also usual for Threat Actors to place their malicious payload in the starting folder. Even though it is common, there are still different ways of persistence. We currently have analytics at Logpoint to identify numerous techniques for different tactics. Some of the notable ones that could be used in this scenario, particularly about persistence are as below:

- **LP_Suspicious Execution of Gpscript Detected**
- **LP_Autorun Keys Modification Detected**
- **LP_Narrators Feedback-Hub Persistence Detected**
- **LP_New RUN Key Pointing to Suspicious Folder Detected**
- **LP_Suspicious RUN Key from Download Detected**
- **LP_Malicious Image Loaded Via Excel**
- **LP_Direct Autorun Keys Modification Detected**
- **LP_Suspicious Netsh DLL Persistence Detected**
- **LP_Suspicious Service Path Modification Detected**
- **LP_New Service Creation**

This is by no means an exhaustive list of alerts for identifying persistence techniques. Our robust arsenal of analytics includes a wide array of detection mechanisms tailored to identify various types of malicious techniques. Furthermore, we are committed to continuously improving our defensive capabilities by providing new detection analytics geared to counter-developing approaches and strategies. This proactive strategy guarantees that our defenses stay adaptive and resilient in the ever-changing cyber threat scenario.

CONCLUSION

In a nutshell, APT-29 is a highly sophisticated advanced persistent threat, posing a severe threat to governments and diplomatic entities globally. The current assaults have been targeted against these organizations in order to collect political intelligence and there are no such indications that these activities will slow down. We have observed continuous efforts from APT-29 modifying their methods in their initial access of its malware delivery chain like anti-analysis components, etc. But what has been consistent is the high-level way of their malware delivery, using HTML smuggling and malicious ISO images.

Converged SIEM, Logpoint's security operations platform, includes several comprehensive tools and features for detecting, analyzing, and mitigating the effect of APT-29's operations. It allows security teams to automate important incident response procedures, capture vital logs and data, and accelerate malware detection, and removal operations with features such as native endpoint solution AgentX and SOAR with pre-configured playbooks. In an ever-changing threat landscape, Logpoint provides enterprises with the tools and functionality they need to manage risks, strengthen defenses, and guard against the operations of APT groups like APT-29.

RECOMMENDATION

Employee Training and Awareness:

- Social engineering, Phishing in particular is the common and effective initial vector of any successful breach or attack. Organizations should provide regular training to employees on how to recognize and respond to social engineering attacks like phishing mail, including simulated exercises that replicate real-world scenarios making them aware of the latest trends and tactics of Threat Actors. Also, encourage a culture of reporting potential phishing attempts to the IT or security team.

Implement Web Filtering and Email Security:

- Utilize web filtering tools to block access to malicious websites and implement robust email security measures, including anti-phishing and anti-malware solutions. Use strong email filtering technology to detect and prevent phishing emails from reaching employees' inboxes. By evaluating email content, attachments, and sender reputation, these filters may identify and quarantine potentially harmful emails.

Multi-Factor Authentication (MFA):

- Make multi-factor authentication mandatory for accessing important accounts and systems. MFA provides an extra layer of security by asking users to give a second form of verification in addition to their password (e.g., a one-time code texted to their mobile device).

Regular Security Patching and Updates:

- Ensure that all software, operating systems, and security apps have the most recent patches and upgrades. To initiate phishing attacks, cybercriminals frequently exploit known weaknesses in obsolete software. Regular upgrades assist in mitigating these vulnerabilities and improving overall cybersecurity posture.In the case where patching is not available or is not feasible to patch the vulnerability, mitigations provided by vendors should be applied. Also in other cases where many security issues need to be fixed, prioritize the issues based on severity and patch or apply mitigation accordingly.

Threat Intelligence:

- Keep up to date on the most recent APT groups, their tactics, methods, and procedures (TTPs), and their targets. To proactively prepare for prospective risks, subscribe to threat intelligence services and disseminate important information within your firm.

Network Segmentation:

- Implement network segmentation to separate critical assets from less critical ones. This reduces the potential impact if an APT gains access to your network.

Access Controls:

- Enforce strict access controls based on the principle of least privilege (PoLP). Limit user and system access to only the resources they require for their roles.

Apply Robust Security Solutions

- Proper logging, asset visibility, and system monitoring are essential components of a robust cybersecurity strategy. These measures provide an overview of the network and help to detect anomalies that may indicate a security threat. It is important to monitor and audit the network regularly to keep track of user activity and network traffic and identify any unusual behavior. It is also crucial to ensure that logs are being collected from every system to ensure comprehensive coverage. Logpoint Converged SIEM Platform can be used for centralized logging and visibility that comes up with the native capability of SIEM, SOAR, UEBA, and AgentX.Additionally, it is recommended to have an adequate log retention policy in place to ensure that log data is available for analysis in the event of an incident. For better visibility, it is recommended to have a log retention time of at least 6 months, but it may be necessary to retain logs for longer periods depending on regulatory or compliance requirements. In some cases, it may not be feasible to store logs for such mentioned time.

Audit Privilege Accounts

- Auditing privileged accounts and their actions regularly is vital because these accounts have elevated access and permissions that might allow bad actors unauthorized access to sensitive data or key systems. Without effective monitoring, privileged accounts can be exploited, resulting in data breaches, system outages, and other security events. Auditing privilege accounts may also give useful insights into how these accounts are utilized, helping to make educated decisions regarding access control, resource allocation, and risk management.

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**