Graphican: Flea Uses New Backdoor in Attacks Targeting Foreign Ministries

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15

Threat Hunter TeamSymantec

The Flea (aka APT15, Nickel) advanced persistent threat (APT) group continued to focus on foreign ministries in a recent attack campaign that ran from late 2022 into early 2023 in which it leveraged a new backdoor called Backdoor.Graphican.

This campaign was primarily focused on foreign affairs ministries in the Americas, although the group also targeted a government finance department in a country in the Americas and a corporation that sells products in Central and South America. There was also one victim based in a European country, which was something of an outlier. This victim had also previously suffered a seemingly unrelated ransomware attack in July 2022. However, the primary focus of the campaign observed by the Threat Hunter Team at Symantec, part of Broadcom, does appear to be on ministries of foreign affairs in the Americas.

Flea has a track record of honing in on government targets, diplomatic missions, and embassies, likely for intelligence-gathering purposes.

Tools

Flea used a large number of tools in this campaign. As well as the new Graphican backdoor, the attackers leveraged a variety of living-off-the-land tools, as well as tools that have been previously linked to Flea. We will detail these tools in this section.

Backdoor.Graphican

Graphican is an evolution of the known Flea backdoor Ketrican, which itself was based on a previous malware — BS2005 — also used by Flea. Graphican has the same basic functionality as Ketrican, with the difference between them being Graphican's use of the Microsoft Graph API and OneDrive to obtain its command-and-control (C&C) infrastructure.

This technique was used in a similar way by the Russian state-sponsored APT group Swallowtail (aka APT28, Fancy Bear, Sofacy, Strontium) in a campaign in 2022 in which it delivered the Graphite malware. In that campaign, the Graphite malware used the Microsoft Graph API and OneDrive as a C&C server.

The observed Graphican samples did not have a hardcoded C&C server, rather they connected to OneDrive via the Microsoft Graph API to get the encrypted C&C server address from a child folder inside the "Person" folder. The malware then decoded the folder name and used it as a C&C server for the malware. All instances of this variant used the same parameters to authenticate to the Microsoft Graph API. We can assume they all have the same C&C, which can be dynamically changed by the threat actors.

Once on a machine, Graphican does the following:

- Disables the Internet Explorer 10 first run wizard and welcome page via registry keys
- Checks if the iexplore.exe process is running
- Creates a global IWebBrowser2 COM object to access the internet
- Authenticates to the Microsoft Graph API to get a valid access token and a refresh_token
- Using the Graph API it enumerates the child files and folders inside the "Person" folder in OneDrive
- Obtains the name of the first folder and decrypts it to use it as a C&C server
- Generates a Bot ID based on the hostname, local IP, Windows version, the system default language identifier, and the process bitness (32-bit or 64-bit) of the compromised machine

- Registers the bot into the C&C with the format string "f$$$%s&&&%s&&&%s&&&%d&&&%ld&&&%s" or "f@@@%s###%s###%s###%d###%ld###%s" filled with the previously collected information from the victim's computer
- Polls C&C server for new commands to execute

Commands that can be executed by Graphican include:

- 'C' — Creates an interactive command line that is controlled from the C&C server
- 'U' — Creates a file on the remote computer
- 'D' — Downloads a file from the remote computer to the C&C server
- 'N' — Creates a new process with a hidden window
- 'P' — Creates a new PowerShell process with a hidden window and saves the results in a temporary file in the TEMP folder and sends the results to the C&C server

During the course of this campaign, we also observed an updated version of Ketrican, which had a hardcoded C&C server and only implemented the 'C', 'U', and 'D' commands. We also saw an older version of Ketrican (compiled in 2020) that implemented only the 'N' and 'P' commands. This demonstrates that the group is actively developing and adapting Ketrican to suit its objectives.

Other Tools

Other tools leveraged by Flea in this recent activity include:

- **EWSTEW** — This is a known Flea backdoor that is used to extract sent and received emails on infected Microsoft Exchange servers. We saw new variants of this tool being used in this campaign.
- **Mimikatz, Pypykatz, Safetykatz** — Mimikatz is a publicly available credential-dumping tool. It allows a local attacker to dump secrets from memory by exploiting Windows single sign-on functionality. Pupykatz and Safetykatz are Mimikatz variants with the same functionality.
- **Lazagne** — A publicly available, open-source tool designed to retrieve passwords from multiple applications.
- **Quarks PwDump** —Quarks PwDump is an open-source tool that can dump various types of Windows credentials: local accounts, domain accounts, and cached domain credentials. It was reported as being used in a campaign that Kaspersky called IceFog all the way back in 2013.
- **SharpSecDump** — The .Net port of the remote SAM and LSA Secrets dumping functionality of Impacket's secretsdump.py.

- **K8Tools** - This is a publicly available toolset with a wide variety of capabilities, including privilege escalation, password cracking, a scanning tool, and vulnerability utilization. It also contains exploits for numerous known vulnerabilities in various systems.
- **EHole** —A publicly available tool that can help attackers identify vulnerable systems.
- **Web shells** —The attackers use a number of publicly available web shells, including AntSword, Behinder, China Chopper, and Godzilla. Web shells provide a backdoor onto victim machines. Some of these web shells, such as China Chopper and Behinder, are associated with Chinese threat actors.
- **Exploit of CVE-2020-1472** — This is an elevation of privilege vulnerability that exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploits the vulnerability could run a specially crafted application on a device on the network. A patch has been available for this vulnerability since the first quarter of 2021.

Flea Background

Flea has been in operation since at least 2004. Over that time its tactics, techniques, and procedures (TTPs), as well as its targeting, have changed and developed. In recent years, the group has primarily focused on attacks against government organizations, diplomatic entities, and non-governmental organizations (NGOs) for the purposes of intelligence gathering. North and South America does appear to have become more of a focus for the group in recent times, which aligns with the targeting we saw in this campaign. The goal of the group does seem to be to gain persistent access to the networks of victims of interest for the purposes of intelligence gathering. Its targets in this campaign, of ministries of foreign affairs, also point to a likely geo-political motive behind the campaign.

Flea traditionally used email as an initial infection vector, but there have also been reports of it exploiting public-facing applications, as well as using VPNs, to gain initial access to victim networks.

Microsoft seized domains belonging to Flea in December 2021. The company seized 42 domains that it said were used in operations that targeted organizations in the U.S. and 28 other countries for intelligence-gathering purposes. Flea was also linked in a November 2022 report by Lookout to a long-running campaign targeting Uyghur-language websites and social media in China.

Flea is believed to be a large and well-resourced group, and it appears that exposure of its activity, and even takedowns such as that detailed by Microsoft, have failed to have a significant impact when it comes to stopping the group's activity.

New Backdoor and Notable Technique

The use of a new backdoor by Flea shows that this group, despite its long years of operation, continues to actively develop new tools. The group has developed multiple custom tools over the years. The similarities in functionality between Graphican and the known Ketrican backdoor may indicate that the group is not very concerned about having activity attributed to it.

The most noteworthy thing about Graphican itself is the abuse of the Microsoft Graph API and OneDrive to obtain its C&C server. The fact that a similar technique was used by Swallowtail, an unconnected APT group operating out of a different region, is also worth noting. Once a technique is used by one threat actor, we often see other groups follow suit, so it will be interesting to see if this technique is something we see being adopted more widely by other APT groups and cyber criminals.

Flea's targets — foreign ministries — are also interesting; though they do align with the targets the group has directed its activity at in the past. It appears the Flea's interests remain similar to what they have been in recent years, even as its tools and techniques continue to evolve.

Protection

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.