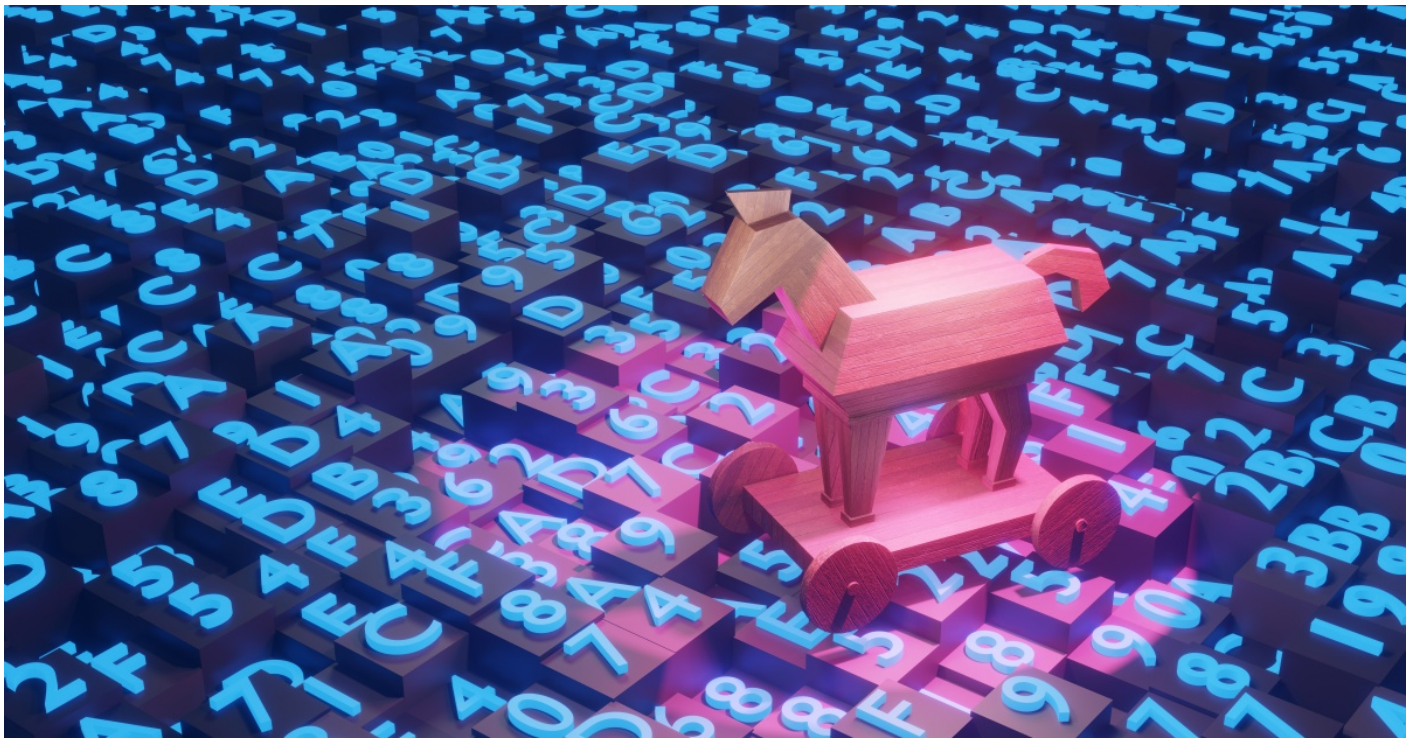
Graphican: Flea Uses New Backdoor in Attacks Targeting Foreign Ministries



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.

SHA256 file hashes
4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5 Backdoor.Graphican
a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8 Backdoor.Graphican
02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5 Backdoor.Graphican
617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd Backdoor.Ketrican
858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253 Backdoor.Ketrican
fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5d094b1f1476 Backdoor.Ketrican
177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e56d4e0c0063eecf Backdoor.Ketrican
8d2af0e2e755ffb2be1ea3eca41eebfcb6341fb440a1b6a02bfc965fe79ad56b Backdoor.Ketrican
f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777da8c6dcf578286 Backdoor.Ketrican
865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b7dce1f66cf48 Backdoor.Ketrican
d30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9380e534aaf5e30 Backdoor.Ketrican
bf4ed3b9a0339ef80a1af557d0f4e031fb4106a04b0f72c85f7f0ff0176ebb64 EWSTEW
5600a7f57e79acdf711b106ee1c360fc898ed914e6d1af3c267067c158a41db6 EWSTEW
f06692b482d39c432791acabb236f7d21895df6f76e0b83992552ab5f1b43c8d EWSTEW
af4a10cbe8c773d6b1cfb34be2455eb023fb1b0d6f0225396920808fefb11523 EWSTEW

548ce27996e9309e93bf0bd29c7871977530761b2c20fc7dc3e2c16c025eb7bc EWSTEW
9829c86fab4cbccb5168f98dcb076672dc6d069ddb693496b463ad704f31722e EWSTEW
18560596e61eae328e75f4696a3d620b95db929bc461e0b29955df06bc114051 Mimikatz
f6f57fc82399ef3759dcbc16b7a25343dea0b539332dacdf0ed289cc82e900db Mimikatz
df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f Mimikatz
c559eb7e2068e39bd26167dd4dca3eea48e51ad0b2c7631f2ed6ffcba01fb819 Pypykatz
7d93862c021d56b4920cab5e6cb30a2d5fb21478e7158f104e520cc739a1678d Pypykatz
17a63ccd749def0417981c42b0765f7d56e6be3092a1f282b81619ca819f82ef Pypykatz
b42f9571d486a8aef5b36d72c1c8fff83f29cac2f9c61aece3ad70537d49b222 Safetykatz
bff65d615d1003bd22f17493efd65eb9ffbfe9a63668deebe09879982e5c6aa8 CVE-2020-1472
ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56 Lazagne
e7a6997e32ca09e78682fc9152455edaa1f9ea674ec51aecd7707b1bbda37c2f Pwdump
07fc745c29db1e2db61089d8d46299078794d7127120d04c07e0a1ea6933a6df Pwdump
42379bb392751f6a94d08168835b67986c820490a6867c28a324a807c49eda3b Pwdump
a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86 Pwdump
e25cc57793f0226ff31568be1fce1e279d35746016fc086a6f67734d26e305a0 Pwdump
617af8e063979fe9ca43479f199cb17c7abeab7bfe904a2baf65708df8461f6d Pwdump
dc2423e21752f431ce3ad010ce41f56914e414f5a88fd3169e78d4cc08082f7b Pwdump
f653e93adf00cf2145d4bfa00153ae86905fe2c2d3c1f63e8f579e43b7069d51 Pwdump
65436d5646c2dbb61607ed466132302f8c87dab82251f9e3f20443d5370b7806 Hadmad
44c1c5c92771c0384182f72e9866d5fed4fda896d90c931fe8de363ed81106cf Hadmad
7fa350350fc1735a9b6f162923df8d960daffb73d6f5470df3c3317ae237a4e6 AntswordLoader
9a94483a4563228cb698173c1991c7cf90726c2c126a3ce74c66ba226040f760 BehinderWebshell
f4575af8f42a1830519895a294c98009ffbb44b20baa170a6b5e4a71fd9ba663 BehinderWebshell
2da9a09a14c52e3f3d8468af24607602cca13bc579af958be9e918d736418660 JSPWebshell
d21797e95b0003d5f1b41a155cced54a45cd22eec3f997e867c11f6173ee7337 PHPWebshell
31529b8b86d4b6a99d8f3b5f4b1f1b67f3c713c11b83b71d8df7d963275c5203 China Chopper
7d3f6188bfdde612acb17487da1b0b1aaaeb422adc9e13fd7eb61044bac7ae08 Sharpsecdump
2b60e49e85b21a439855b5cb43cf799c1fb3cc0860076d52e41d48d88487e6d8 Sharpsecdump
819d0b70a905ae5f8bef6c47423964359c2a90a168414f5350328f568e1c7301 K8Tools
7aa10e5c59775bfde81d27e63dfca26a1ec38065ddc87fe971c30d2b2b72d978 EHole

Network Indicators

172.104.244[.]187
50.116.3[.]164
www.beltsymd[.]org
www.cyclophilit[.]com
www.cyprus-villas[.]org
www.perusmartcity[.]com
www.verisims[.]com