Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Flea APT Targets Foreign Ministries with New Backdoor.Graphican

Date of Publication

June 22, 2023

Admiralty Code

A1

TA Number

TA2023275

Summary

First Appearance: 2004
Malware: Backdoor.Graphical
Targeted Countries: North, Central, and South America
Affected Platforms: Windows
Targeted Industries: Foreign Affairs, Government, Diplomatic, Finance, Political, Foreign
Actor Name: Flea (APT15, Playful Taurus, BackdoorDiplomacy, Vixen Panda, Ke3Chang, Playful Dragon, Bronze Palace, and NICKEL)
Attack: Flea APT group targeted foreign ministries with their new backdoor, Backdoor.Graphican, leveraging Microsoft Graph API and OneDrive for C&C communication.

Attack Regions

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2020-1472	Microsoft Netlogon Privilege Escalation Vulnerability	Microsoft Netlogon	✗	✓	✓

Attack Details

#1

The Flea advanced persistent threat group, has recently conducted a targeted attack campaign against foreign ministries. In this campaign, they utilized a newly developed backdoor called Backdoor.Graphican. The primary focus of their attacks was on foreign affairs ministries in the Americas, although they also targeted a government finance department, a corporation operating in Central and South America, and one victim in a European country.

#2

Flea is known for targeting government organizations, diplomatic missions, and non-governmental organizations (NGOs) in order to gather intelligence. Their attacks have been ongoing since at least 2004, and they have consistently evolved their tactics and techniques over time.

#3

The Backdoor.Graphican, which is an evolution of their previous backdoor called Ketrican, exploits the Microsoft Graph API and OneDrive for communication with its command-and-control (C&C) server. This technique involves connecting to OneDrive through the Microsoft Graph API to obtain an encrypted C&C server address from a specific folder.

#4

The malware then decodes the folder name and uses it as the C&C server. By leveraging this method, Flea can maintain control over compromised systems and execute commands remotely. In addition to Backdoor.Graphican, Flea employs a range of other tools in their attacks. These tools include EWSTEW, which extracts sent and received emails on infected Microsoft Exchange servers, as well as credential-dumping tools like Mimikatz, Pypykatz, and Safetykatz.

#5

They also utilize tools such as Lazagne, Quarks PwDump, SharpSecDump, K8Tools, EHole, and various web shells. Furthermore, Flea has been known to exploit vulnerabilities like CVE-2020-1472, which allows for privilege escalation.

Recommendations

Deploy and update advanced endpoint protection solutions, such as antivirus and anti-malware, to defend against Flea APT's Backdoor.Graphican and other malware. Enable real-time monitoring and automated response to swiftly identify and mitigate malicious activities.

Strengthen network defenses with firewalls, intrusion prevention systems, and secure web gateways to protect against Flea APT's attacks. Regularly patch and update network devices and applications to mitigate vulnerabilities exploited by the APT group.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	**TA0011** Command and Control	**TA0005** Defense Evasion	**TA0002** Execution
TA0007 Discovery	**TA0001** Initial Access	**TA0009** Collection	**TA0008** Lateral Movement
T1550 Use Alternate Authentication Material	**T1027** Obfuscated Files or Information	**T1204** User Execution	**T1140** Deobfuscate/Decode Files or Information
T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1083** File and Directory Discovery	**T1550.001** Application Access Token
T1059.001 PowerShell	**T1547.001** Registry Run Keys / Startup Folder	**T1547** Boot or Logon Autostart Execution	**T1082** System Information Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	172.104.244[.]187 50.116.3[.]164
Domains	www.beltsymd[.]org www.cyclophilit[.]com www.cyprus-villas[.]org www.perusmartcity[.]com www.verisims[.]com
SHA256	4b78b1a3c162023f0c14498541cb6ae143fb01d8b50d6aa13ac302a84553e2d5 a78cc475c1875186dcd1908b55c2eeaf1bcd59dedaff920f262f12a3a9e9bfa8 02e8ea9a58c13f216bdae478f9f007e20b45217742d0fbe47f66173f1b195ef5 617589fd7d1ea9a228886d2d17235aeb4a68fabd246d17427e50fb31a9a98bcd 858818cd739a439ac6795ff2a7c620d4d3f1e5c006913daf89026d3c2732c253 fd21a339bf3655fcf55fc8ee165bb386fc3c0b34e61a87eb1aff5d094b1f1476 177c4722d873b78b5b2b92b12ae2b4d3b9f76247e67afd18e56d4e0c0063eecf 8d2af0e2e755ffb2be1ea3eca41eebfcb6341fb440a1b6a02bfc965fe79ad56b f98bd4af4bc0e127ae37004c23c9d14aa4723943edb4622777da8c6dcf578286 865c18480da73c0c32a5ee5835c1cfd08fa770e5b10bc3fb6f8b7dce1f66cf48 d30ace69d406019c78907e4f796e99b9a0a51509b1f1c2e9b9380e534aaf5e30 bf4ed3b9a0339ef80a1af557d0f4e031fb4106a04b0f72c85f7f0ff0176ebb64 5600a7f57e79acdf711b106ee1c360fc898ed914e6d1af3c267067c158a41db6 f06692b482d39c432791acabb236f7d21895df6f76e0b83992552ab5f1b43c8d af4a10cbe8c773d6b1cfb34be2455eb023fb1b0d6f0225396920808fefb11523 548ce27996e9309e93bf0bd29c7871977530761b2c20fc7dc3e2c16c025eb7bc 9829c86fab4cbccb5168f98dcb076672dc6d069ddb693496b463ad704f31722e 18560596e61eae328e75f4696a3d620b95db929bc461e0b29955df06bc114051

TYPE	VALUE
SHA256	f6f57fc82399ef3759dcbc16b7a25343dea0b539332dacdf0ed289cc82e900db df6a740b0589dbd058227d3fcab1f1a847b4aa73feab9a2c157af31d95e0356f c559eb7e2068e39bd26167dd4dca3eea48e51ad0b2c7631f2ed6ffcba01fb819 7d93862c021d56b4920cab5e6cb30a2d5fb21478e7158f104e520cc739a1678d 17a63ccd749def0417981c42b0765f7d56e6be3092a1f282b81619ca819f82ef b42f9571d486a8aef5b36d72c1c8fff83f29cac2f9c61aece3ad70537d49b222 bff65d615d1003bd22f17493efd65eb9ffbfe9a63668deebe09879982e5c6aa8 ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56 e7a6997e32ca09e78682fc9152455edaa1f9ea674ec51aecd7707b1bbda37c2f 07fc745c29db1e2db61089d8d46299078794d7127120d04c07e0a1ea6933a6df 42379bb392751f6a94d08168835b67986c820490a6867c28a324a807c49eda3b a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86 e25cc57793f0226ff31568be1fce1e279d35746016fc086a6f67734d26e305a0 617af8e063979fe9ca43479f199cb17c7abeab7bfe904a2baf65708df8461f6d dc2423e21752f431ce3ad010ce41f56914e414f5a88fd3169e78d4cc08082f7b f653e93adf00cf2145d4bfa00153ae86905fe2c2d3c1f63e8f579e43b7069d51 65436d5646c2dbb61607ed466132302f8c87dab82251f9e3f20443d5370b7806 44c1c5c92771c0384182f72e9866d5fed4fda896d90c931fe8de363ed81106cf 7fa350350fc1735a9b6f162923df8d960daffb73d6f5470df3c3317ae237a4e6 9a94483a4563228cb698173c1991c7cf90726c2c126a3ce74c66ba226040f760 f4575af8f42a1830519895a294c98009ffbb44b20baa170a6b5e4a71fd9ba663 2da9a09a14c52e3f3d8468af24607602cca13bc579af958be9e918d736418660 d21797e95b0003d5f1b41a155cced54a45cd22eec3f997e867c11f6173ee7337 31529b8b86d4b6a99d8f3b5f4b1f1b67f3c713c11b83b71d8df7d963275c5203 7d3f6188bfdde612acb17487da1b0b1aaaeb422adc9e13fd7eb61044bac7ae08

TYPE	VALUE
SHA256	2b60e49e85b21a439855b5cb43cf799c1fb3cc0860076d52e41d48d88487e6d8 819d0b70a905ae5f8bef6c47423964359c2a90a168414f5350328f568e1c7301 7aa10e5c59775bfde81d27e63dfca26a1ec38065ddc87fe971c30d2b2b72d978

Patch Details

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

References

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

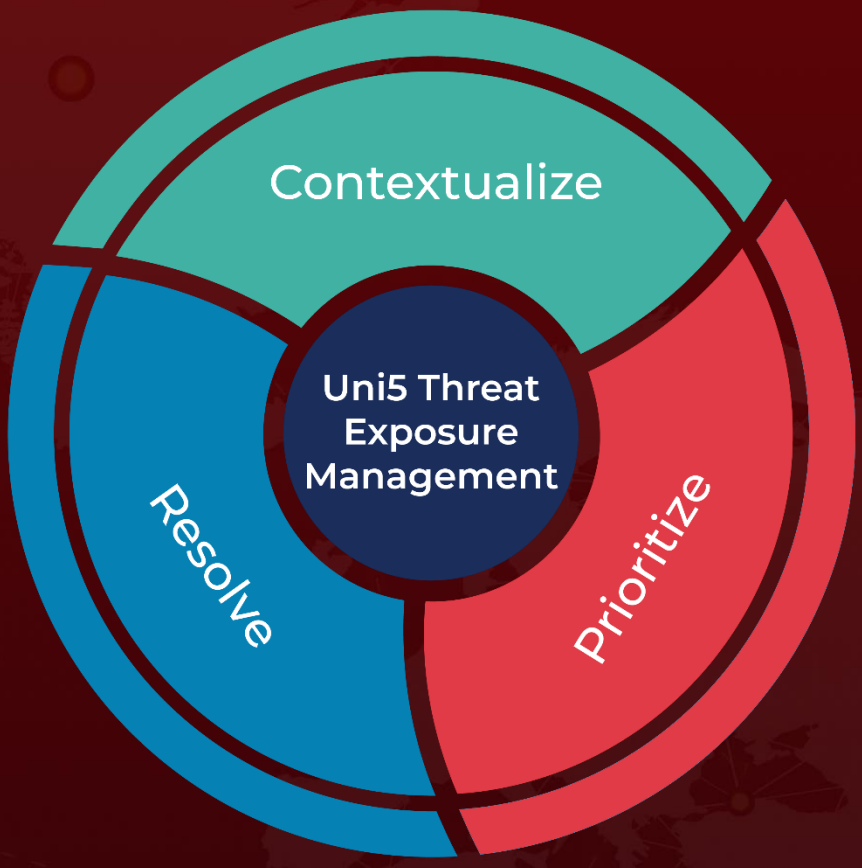
https://www.hivepro.com/apt15-enhanced-its-arsenal-with-an-updated-variant-of-the-turian-backdoor/

https://www.hivepro.com/backdoordiplomacy-targets-the-telecom-industry-in-the-middle-east/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 22, 2023 • 8:30 AM

More at www.hivepro.com