



KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Cranefly Employs Novel Tools & Techniques to Target IIS Servers



Tracker ID: TN1105

Date: 16/Nov/2022

Category: Vulnerability

Industry: All

Region: All

Background

A new trojan known as "Danfuan" has been discovered, targeting employees involved in business transactions. The dropper "Trojan.Geppei" is used to drop another backdoor called "Trojan.Danfuan" and some other tools using a new method for reading commands from Internet Information Services (IIS) logs. According to the preliminary investigation, the activity is linked to the hacking groups "Cranefly" and "UNC3524."

UNC3524 is a suspected cyber espionage group that first surfaced in May 2022 as a result of its concentration on bulk email collection from targets involved in mergers and acquisitions and other financial activities. It is regarded as having a high level of operational security, a low malware footprint, adept evasive skills, and a massive Internet of Things (IoT) device botnet at its disposal. It partially overlaps with numerous Russian-based espionage actors (APT28 and APT29). The group's main malware strain is "QUIETEXIT," a backdoor planted on network appliances such as load balancers and wireless access point controllers that do not enable antivirus or endpoint detection, which allows the attacker to go undiscovered for an extended period.

Cranefly's arsenal of specialized cyber weapons has been bolstered by "Geppei" and "Danfuan," with Geppei acting as a dropper that reads commands from IIS logs. The attacker sends commands to a compromised web server by disguising them as web access requests. IIS logs them as normal but Trojan.Geppei can read them as commands. The commands issued by Geppei contain a malicious "encoded.ashx" file. These files act as backdoors and are saved to a folder determined by the command option. It also includes "reGeorg," a web shell utilized by other actors such as APT28, DeftTorero, and Worok, as well as "Danfuan," designed to execute the incoming C# code.

The strings Wrde, Exco, and Cll0 are not commonly found in IIS log files. Geppei appears to employ these strings for malicious HTTP request parsing; the existence of these strings leads the dropper to do activity on a machine. The attacker sends these commands using a dummy URL or even a non-existent URL because IIS reports 404s in the same log file by default.

Despite spending 18 months on compromised networks, the threat actor wasn't exfiltrating the data from victim machines. Based on the deployment of a novel approach and proprietary tools, as well as the precautions taken to conceal evidence of this activity on victim machines, Cranefly appears to be a skilled threat actor. The tools used and the procedures taken to conceal this conduct indicate that intelligence gathering is the group's primary objective.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMGjosh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia





KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Cranefly Employs Novel Tools & Techniques to Target IIS Servers



Tracker ID: TN1105

Date: 16/Nov/2022

Category: Malware

Industry: All

Region: All

MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion, Command and control, and Collection.

Indicators of Compromise

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Continuously monitor IIS logs for suspicious or anomalous activities, including log deletion. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Lookout for malicious ".ashx" files in the directory, generally saved as "C:\\inetpub\\wwwroot\\test\\backdoor.ashx".
- Identify network devices that don't support monitoring tools, harden them, and limit or prohibit egress traffic from such devices.
- It is advised to constantly monitor the services and critical assets that are exposed to the Internet.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Threat Hunter Team, Cranefly: Threat Actor Uses Previously Unseen Techniques and Tools in Stealthy Campaign, Symantec, 28th October 2022, External Link (symantec-enterprise-blogs.security.com).
- Nathan Eddy, Cranefly Cyberspy Group Spawns Unique ISS Technique, Dark Reading, 28th October 2022, External Link (www.darkreading.com).
- Ravie Lakshmanan, Researchers Uncover Stealthy Techniques Used by Cranefly Espionage Hackers, The Hacker News, 28th October 2022, External Link (thehackernews.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMGjosh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia





KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Cranefly Employs Novel Tools & Techniques to Target IIS Servers



Tracker ID: TN1105

Date: 16/Nov/2022

Category: Malware

Industry: All

Region: All

*

SHA-256 Hash
12eaac1b8dc29ba29287e7e30c893017f82c6fadb73dbc8ef2fa6f5bd5d9d84e
981b28d7521c5b02f026cb1ba5289d61ae2c1bb31e8b256db21b5dcfb8837475
6dcfa79948cf90b10b05b59237cf46adb09b2ce53bc2c0d38fce875eccd3a7e1
0af8bf1fa14fe492de1cc870ac0e01fc8b2f6411de922712a206b905a10ee379
7d5018d823939a181a84e7449d1c50ac3eb94abf3585a2154693ef5180877b95
b5a4804cf7717fda1f01f23c1c2fe99fe9473b03f0247bcc6190f17d26856844
1975bea7ca167d84003b601f0dfb95c4b31a174ce5af0b19e563cb33cba22ffa
56243c851b13218d3031ca7e5af8f2b891e139cbd6d7e3f40508e857802a1077
0b8d024ec29619ff499e4b5024ff14451731a4e3155636a02ef5db2df0e0f0dd
0b168638224589937768eb15c9ebbe795d6539d1fbe744a8f065fedd569bfc5e

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMGjosh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

