KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | China-backed threat group Winnti breaches multiple firms

Tracker ID: TN0909 **Date:** 02/Sep/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Europe, N. America

Background

Last year, at least 80 businesses were targeted by Winnti, also known as "APT41" or "Wicked Spider," a Chinese hacker group that managed to breach the networks of at least thirteen of those targets. This threat actor targeted hotels and software development firms in the United States, an Indian aviation corporation, a Taiwanese government, a manufacturing and media group, and even Chinese software suppliers. To enhance their efforts, they also hacked Thai military portals, academic websites in the United Kingdom, Ireland, and Hong Kong, as well as various government websites in India.

Winnti employed a variety of techniques, including phishing, watering holes, supply chain attacks, and SQL injection-based attacks. Acunetix, Nmap, SQLmap, OneForAll, subdomain3, subDomainsBrute, Sublist3r, and the "venerable" Cobalt Strike were used by threat actors to discover vulnerabilities in targeted networks or spread laterally within them. To evade malware detection, one of its unique tactics for delivering the Cobalt Strike beacons was to disguise the payload on the host. The payload is divided into 775 character chunks by the hackers, who then base64-encode them before echoing the fragments to a text file called dns.txt.

In some cases, the attackers increased the chunk size to 1,024 characters to reduce the number of iterations, while in others, it took 154 repeats of this process to write the payload to a file. Certutil LOLBin is also used by the threat actor to reassemble and run the Cobalt Strike executable. Another unique technique for distributing Cobalt Strike is Winnti's usage of listeners with over 106 bespoke SSL certificates to mimic Microsoft, Facebook, and Cloudflare. These certificates ensure that only connections from the phony beacons are acknowledged by the C2 servers' listeners, keeping curious hackers and researchers at distant.

Researchers were able to roughly determine the location of the hackers based on their working hours, which typically adhered to a defined pattern after watching the threat group's operations for so long. The staff begins working at 9:00 AM and finishes around 7:00 PM in the UTC+8 time zone. The hacker group is now well-positioned to perform real-time operations against targets in China, Malaysia, Singapore, Russia, Australia, and Malaysia. Notably, Winnti worked extremely few hours on weekends, while there was modest activity on Sundays, probably to accomplish chores that understaffed IT employees are unlikely to notice.

The highly sophisticated Chinese threat group continues to conduct cyber-espionage unnoticed. In January 2022, Winnti deployed "MoonBounce," a sophisticated UEFI firmware implant, against well-known companies. In March 2022, they leveraged Cisco and Citrix's vulnerabilities to get into government networks in six U.S. states. After mapping a previously unknown operation that had been ongoing since at least 2019, a large portion of Winnti's arsenal and TTPs (techniques, tactics, and procedures) were uncovered in May 2022.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | China-backed threat group Winnti breaches multiple firms

Tracker ID: TN0909 **Date:** 02/Sep/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Europe, N. America

MITRE ATT&CK Tactics

Reconnaissance, Initial Access, Execution, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration

Indicators of Compromise

Please refer to the attached sheet for IOCs.

Recommendations

- Validate the IOCs attached and implement the detection & prevention accordingly. Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Keep systems and products updated and patched as soon as possible after the patches are released.
- Avoid opening untrusted links and email attachments without first verifying their authenticity. Check the sender's email address to confirm its legitimacy.
- Implement network segmentation to limit or block lateral movement. Follow multilayered defense solutions and active monitoring to detect and thwart threats.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically.

References

- Nikita Rostovtsev, APT41 World Tour 2021 on a tight schedule, Group-IB, 18th August 2022, External Link (blog.group-ib.com).
- Ravie Lakshmanan, China-backed APT41 Hackers Targeted 13 Organisations Worldwide Last Year, The Hacker News, 18th August 2022, External Link (thehackernews.com).
- Bill Toulas, Winnti hackers split Cobalt Strike into 154 pieces to evade detection, Bleeping Computer, 18th August 2022, External Link(www.bleepingcomputer.com).

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

KPMG in India Cyber Response Hotline : +91 9176 471 471

PMG CTI.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | China-backed threat group Winnti breaches multiple firms

Tracker ID: TN0909 **Date:** 02/Sep/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Europe, N. America

*

IP	Domain
45.142.214[.]242	columm[.]tk
45.153.231[.]31	mute-pond-371d.zalocdn[.]workers.dev
45.144.31[.]31	socialpt2021[.]club
45.142.214[.]56	gentle-voice-65e3.bsnl[.]workers.dev
45.140.146[.]169	newimages.socialpt2021[.]tk
45.142.212[.]47	updata.microsoft-api[.]workers.dev
185.250.150[.]22	cs16.dns04[.]com
185.118.166[.]66	delaylink[.]tk
	javaupdate.biguserup[.]workers.dev