KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Chinese APT targets Industrial and Public Enterprises

Tracker ID: TN0817 **Date:** 17/Aug/22 **Category:** Threat Actor **Industry:** All **Region**: Asia, Europe

Background

A new Windows malware was leveraged in a widespread series of attacks to backdoor government organizations and enterprises. The campaign is linked to the Chinese APT organization TA428, which is known for targeting businesses in Asia and Eastern Europe and focusing on information theft and espionage. Threat actors were able to successfully infiltrate the networks of multiple targets and seize control of their entire IT infrastructure by exploiting systems used to administer security solutions. According to the evidence acquired throughout the investigation, the aim of this series of attacks was cyberespionage.

The attackers gain access to the enterprise network by using customized phishing emails for each organization. Some of these emails contain information that is specific to the company under assault and is not available to the broader public. This could imply that the attackers planned ahead of time (they may have obtained the information from earlier attacks on the same organization or its employees, or other organizations or individuals associated with the victim organization).

The Microsoft Word attachments in the phishing emails contain malicious code that exploits the CVE-2017-11882 vulnerability. Without further user interaction, the vulnerability allows an attacker to execute arbitrary code (in the attacks examined, the core module of the PortDoor malware). In the most recent series of attacks, the attackers used six unique backdoors at the same time, most likely to establish backup communication channels with infected PCs in case one of the malicious applications was identified and deleted by security software. Backdoors provide complete capabilities for administering infected computers and acquiring private data.

The Ladon hacking utility is the main lateral movement tool. It has password theft, network scanning, and vulnerability search and exploitation capabilities. The attackers also make extensive use of the common tools included in the Windows operating system. The last phase of the attack entails taking over the domain controller and managing every workstation and server in the organization. Following the acquisition of domain administrator access, the attackers search for and exfiltrate documents and other files containing sensitive data from the targeted organization to servers in other countries, which are also employed as C&C servers.

The attackers compressed the stolen data into password-protected and encrypted ZIP archives. After retrieving the collected data, the C&C servers sent the acquired archives to a stage two server in China. The attackers heavily used process hollowing and DLL hijacking tactics to prevent security tools from detecting the infection. According to the evidence gathered, the attacks are very likely the work of a Chinese-speaking organization. Given that this is not the first strike in the campaign and that they have had some success, the attackers may carry out similar strikes in the future. To successfully defend against such attacks, commercial and public institutions need have substantial precautions.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Chinese APT targets Industrial and Public Enterprises

Tracker ID: TN0817 **Date:** 17/August/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Europe

MITRE ATT&CK Tactics

Reconnaissance, Initial Access, Execution, Defense Evasion, Lateral Movement, Command and Control and Exfiltration.

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. Validate the IOCs attached and implement the detection & prevention accordingly.
- Ensure patches are applied for CVE-2017-11882, aka "Microsoft Office Memory Corruption Vulnerability."
- Make certain that security software with support for centralized security policy management is installed on all servers and workstations and keep the antivirus databases and program modules of your security solutions up-to-date.
- Check that all security software components are enabled on all systems and that a policy is in place requiring the administrator password to be entered in the event of attempts to disable protection.
- Check that the Active Directory policy includes restrictions on user attempts to log in to systems. Users should be only allowed to log in to those systems which they need to access to perform their job responsibilities.
- Restrict network connections, including VPN, to the systems on the OT network; block connections on all those ports the use of which is not required by the industrial process.
- Limit trust relationships between the organization’s domains and minimize the number of users with domain administrator privileges.
- Train employees to securely work with internet resources and corporate communication channels such as email. Focus on identifying phishing emails and on secure practices related to working with Microsoft Office documents.
- Avoid opening untrusted links and email attachments without first verifying their authenticity. Check the sender's email address to confirm its legitimacy.
- Use accounts with local administrator and domain administrator privileges only when necessary to perform the job.
- Restrict the ability of programs to gain SeDebugPrivilege privileges wherever possible.
- Enforce a password policy that has password complexity requirements and requires passwords to be changed regularly.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Chinese APT targets Industrial and Public Enterprises

Tracker ID: TN0817 **Date:** 17/August/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Europe

References

- Sergiu Gatlan, Chinese hackers use new Windows malware to backdoor govt, defense orgs, Bleeping Computer, 08th August 2022, External Link (bleepingcomputer.com).
- Targeted attack on industrial enterprises and public institutions, Kaspersky, 08th August 2022, External Link (ics-cert.kaspersky.com)
- AJ Vicens, Researchers uncover sophisticated global Chinese hacking operation, CyberScoop, 08th August 2022, External Link (cyberscoop.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 9176 471 471

Hash MD5	IP	Domain
0A2E7C01B847D3B1C6EEBE6AF63DC140	45.151.180[.]178	www1.nppnavigator[.]net
0A945587E0E11A89D72B4C0B45A4F77E	160.202.162[.]122	www3.vpkimplus[.]com
10818F47AA4DC2B39A7B5EEF652F3C68	192.248.182[.]121	custom.songuulcomiss[.]com
1157132504BE3BF556A80DB8A2FF9395	54.36.189[.]105	tech.songuulcomiss[.]com
11955356232DCF6834515BF111BB5138	5.180.174[.]10	video.nicblainfo[.]net
11BA5665EC1DBA660401AFDE64C2B125	45.63.27[.]162	doc.redstrpela[.]net
17FA7898D040FA647AFA4467921A66CF		fax.internnetionfax[.]com
180EE3E469BFCFC079E1A46D16440467		www2.defensysminck[.]net
1EA58FF469F5EE0FDCF5B30FC19E4CB8		info.ntcprotek[.]com
216D9F82BA2B9289E68F9778E1E40AC9		www1.dotomater[.]club
29B62694DC9F720BD09438F37B7B358A		www2.sdelanasnou[.]com
3953EB8F7825E756515BE79EF45655B0		server.dotomater[.]club

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Chinese APT targets Industrial and Public Enterprises

Tracker ID: TN0817 **Date:** 17/August/2022 **Category:** Threat Actor **Industry:** All **Region**: Asia, Europe

Hash MD5		
3A13B99B2567190AB87E8AB745761017	7FE40325F0CEF8A32E69A6087EBC7157	EBCFFECE1B1AF517743D3DFFDE72CB43
40EB08F151859C1FE4DC8E6BC466B06F	84DF335EBC10633DA1524C7DBB836994	F01A9A2D1E31332ED36C1A4D2839F412
413FA4AD3AFE00B34102C520A91F031C	94AF1B400FDBDEBD8EDA337474C07479	FB2B4C9CA6A7871A98C6E2405E27A21F
4866622D249F3EA114495A4A249F3064	AA7231904A125273F5E5EE55A1441BA4	FF6D8578BE65A31F3624B62E07BEF795
4AD1AD14044BD2C5A5C5E7E7DD954B23	AB26F4C877A7357CABF95FB5033A5BEF	6860189B79FF35199F99171548F5CD65
4D42C314FF4341F2D1315D7810BD4E15	AB55A08ED77736CE6D26874187169BC9	9EC56A18333D4D4E4D3C361D487C05BD
51367DC409A7A7E5521C2F700C56A452	AE11F7218E919DF5B8A9A2C0DC247F56	E5B6571E1512D3896F8C2367DDC5A02D
51BEFD74AC3B8943DA58C841017A57A8	B2C9F5CAE72AF5A50940D55BB5B92E98	7CB0D8CFFE48DF7B531B6BEDE8137199
56AF3279253E4A60BD080DD6A5CA7BA8	C6D6CFFD56638A68A0DE11035B9C9097	86BB8FA0D00FD94F15AE1BD001037C6C
5EA338D71D2A49E7B3259BC52F424303	CBECDFA1D0708D60500864A2A9DE4992	9F5BBA1ACEF3CCBBDC789F8813B99067
5EB42E1BA99FACE02CE50EA1AAF72AB5	CCC9482A7BEE777BBB08172DCCDAB8AA	4EA2B943A1D9539E42C5BDBA3D3CA7A0
6038583B155F73FAF1B5EF8135154278	D394F005416A20505C597ECF7882450F	5934B7E24D03E92B3DBACBE49F6E677C