



APT27 : DECADE-OLD ACTIVE CHINESE THREAT GROUP



January 2023

Executive Summary



India Future Foundation (IFF) analyzed the APT27 cyber threat. This paper is a result of our findings. APT 27 is a Chinese threat group. This group is well-known for extensively using spear-phishing and watering hole attacks to target victims and organizations. APT 27, which has been active for over a decade now, uses a variety of malwares, exploits, and vulnerabilities to accomplish its espionage objectives. It continuously modifies its assault tactics and misdirection to stay undetected, while spying on victims. By incorporating ransomware in its assault efforts recently, the gang appears to have started working on a new type of espionage, in addition to financially driven attacks. The APT27 is also known under various other aliases. Some of the common ones are IronPanda, Lucky Mouse, LuckyMouse, Emissary Panda, Iron Tiger, ZipToken, Group 35, TEMP.Hippo, TG 3390, Bronze Union and Threat Group 3390.

APT27 employed the Zoho Manage Engine AdSelfService, Plus software authentication bypass vulnerability (CVE-2021-40539) from March 2021 until mid-September last year. A patch for (CVE-2021-40539) was released on Sept. 7, 2021. On October 25, they started to leverage the ServiceDesk vulnerability (whose vulnerability) (CVE-2021-44077). The attackers also made use of known Microsoft Exchange Server 2013, 2016, and 2019 proxy login vulnerabilities to deploy HYPERBRO (CVE-2021-26855, CVE 2021-26857, CVE-2021-26858, and CVE-2021-27065).

The APT27's attacks on American defence contractors are some of its most well-known operations. APT 27 started a campaign against several businesses, in the banking industry, and an attack on a data centre, in Central Asia, are two of APT27's other well-known operations. APT 27 is, in our opinion, is incredibly smart and inventive. The group's state-sponsored action has been aided by its history of financially driven targeting of the video gaming industry.

The APT27's arsenal of hacking tools includes threats that would enable them to conduct reconnaissance operations, gather private information from the infected host, or seize control of the compromised machine. APT27 has attacked various targets for several reasons, including obtaining information on cutting-edge technologies and spying on governments/civilian organizations and political dissidents.

FACTS TO KNOW ABOUT APT 27

Origin: 2009

Aliases (in order of): IronPanda, LuckyMouse, Emissary Panda, Iron Tiger, ZipToken, Group 35, TEMP.Hippo, TG 3390, Bronze Union, Threat Group 3390.

Targeted Sectors: Aerospace, Automotive Technology, Business Services, Electronics, Energy, Government, High Tech, Information Technology, Research, Travel.

Attack Vectors (path adopted to exploit vulnerabilities): Watering Holes, Spear Phishing, Remote Code Execution, Living off the Land Attack, Rootkit Attack, Supply Chain Attack, Unauthorized Access.

Targeted Countries: Eastern Asia, Middle East, North America, South America, South-East Asia, Western Asia.

Intent: Cyber Espionage, Data Theft, Ransom, Spear Phishing and Watering hole.

Malwares Used: ASPXSpy, FoundCore, Ghost, HyperBro, PlugX RAT, Sogu, Windows Credential Editor, ZxShell RAT.

Tools Used: China Chopper, gsecdump, HTTPBrowser, Impacket, ipconfig, Mimikatz, NBTscan, Net, OwaAuth, pwdump, ZxShell.

LATELY ACTIONS

Due to tensions in Taiwan, the ascribed Chinese APTs have recently started to operate. According to sources, APT27 has been continuously targeting Taiwan with cyberattacks. On 7th August 2022, National Taiwan University (NTU), in Taipei City, was the biggest target.

The website of the NTU displayed words in Chinese that suggested -- "There is only one China in the world." As reported by Taiwan news, it has been found that attacks had increased during the visit by the US House Speaker, Nancy Pelosi.

On 3rd August 2022 APT27 published a video on YouTube threatening to carry out a "Special cyber operation" against Taiwan. The hacking group also took responsibility for the series of anticipated online attacks on Taiwan.

Over 200,000 Taiwanese-connected gadgets, according to the hacker gang, are under the control of the APT27 group. Taiwan could compromise its national security if APT27 continues to escalate the situation by leaking official data and declaring "Taiwanese equipment zero-day" attacks.



HOPPING ATTACK METHODS

APT27 can use a wide range of instruments and strategies for its cyberespionage missions. Between 2015 and 2017, the threat organization used watering hole assaults through approximately 100 hacked legitimate websites to breach networks of its victims. The gang's cyberespionage operations persisted, and so did its tactics evolve, this despite public revelations of its operations in 2017.

The gang tried a living-off-the-land attack in February 2019 to obtain knowledge about cutting-edge weaponry and to spy on dissidents and other civilian organizations.

In March 2020, the APT group abused the COVID-19 pandemic fear to lure people by sending thematic email campaigns or thematic IMs with phishing/malware links. In April 2020, it carried out cross-platform attacks on back-end servers to steal business data.



MALWARE USED AND VULNERABILITIES EXPLOITED

A honeypot computer found in 2011 that Microsoft products had vulnerabilities in which APT27 had dumped the Gh0st RAT. The gang was found to be utilizing several PlugX malware variants, in 2013. The same year, the team used a web shell called China Chopper to attack Middle Eastern Government's SharePoint servers. Researchers detected an HTTP Browser malware version, in June 2016, and connected it to the APT27 group. It was directed at a European consumer drone business.

Using two variations of the Mimikatz password-scraping tool, the organization initiated the PZChao assault campaign, in February 2018, gathering credentials and uploading them to the C2 server. With the help of malware Zombie Boy, which exploited several security flaws to infiltrate target networks, such as CVE-2017-9073, CVE-2017-0143, and CVE-2017-0146, the threat actors tried their hand at crypto mining assaults. A malicious NDIS Proxy driver with a certificate from a Chinese IT business was used in an attack, in September 2018, that resulted in the discovery of many infections from a previously unknown trojans.

APT27 used the most recent version of ZxShell RAT to attack Windows 10, in January 2020.



The attackers used an outdated Google Updater executable open to DLL side-loading, in January 2021, to distribute Clambling and PlugX. They also misused CVE-2017-0213 to get elevated privileges. Other tools, such as ASPXSpy web shell, post-exploitation tool bitsadmin, HyperBro backdoor, BitLocker, MimiKatz, and a crypto miner, were used to find it. The gang used CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, and CVE-2021-26855 (ProxyLogon) vulnerabilities affecting Microsoft Exchange servers, in March 2021, to exploit several flaws. The organization added an improved SysUpdate malware strain to their toolset, in April 2021. Researchers claimed, in September, that APT27 was responsible for an attack campaign that used the CVE-2021-40539 vulnerability in ADSelfService Plus, a ManageEngine product, from Zoho. The Chinese group was targeted by a similar assault using a recently discovered vulnerability (CVE-2021-44077) in Zoho's ManageEngine ServiceDesk Plus.

Security analysts have also found APT27 using the HyperBro RAT, to backdoor targets, in Germany, in January 2022. Meanwhile, experts believe the APT27 group was responsible for the fileless and socketless backdoor malware known as SockDetour, deployed against American defence contractors, in February 2022.



ATTACK HISTORY

When APT27 stole trillions of bytes of sensitive data from the U.S. Government and its military defence contractors, intelligence agencies, and FBI-based partners, in September 2015, it gained widespread attention. In the next month, a Korplug RAT version (also known as PlugX) targeting Vietnamese institutions and doxing 400,000 Vietnam Airlines employees was discovered. In June of 2018, the group undertook an espionage operation by covertly inserting malware into the websites of the Mongolian Government. The group stole private data from their devices using malware for Windows and Android.

From 2021 onwards, the group entered the scene of financially driven cybercrime and started utilizing ransomware, in their assaults. According to reports, it affected the servers of many well-known gaming firms across the globe. Researchers discovered the assaults, in April 2021. They targeted military and governmental institutions, in Vietnam. The following month, the threat group compromised government entities by installing web shells on SharePoint systems. Later in December 2021, the HyperBro backdoor, Korplug RAT, and Tmanger were transmitted through the chat programme Able Desktop, utilized by 430 government agencies, in Mongolia. APT27 impacted nine firms, including those in the technology, energy, healthcare, and defence industries, during its attack on the Zoho platform.

German domestic intelligence services warned about ongoing assaults planned by APT27, in January 2022. The organization may be a component of a bigger TiltedTemple attack that infiltrated the networks of at least one American defence firm.

TARGETED ENTITIES

Asia, America, the Middle East, and Europe are just a few places the group has targeted globally. The targeted industries have always seemed to be interested in business services, high tech, energy, aerospace, travel, automotive, and electronics. Amper SA, Microsoft, Able Desktop, Mongolian Government agencies, Turkish agencies, and German business groups are some of their notable targets.

MITIGATION

Given the frequency with which APT27 uses email as a method of attack and the gravity of its dangers, corporations are advised to train their staff members periodically, in this regard. They need to use routine programme and operating system upgrades to patch any known vulnerabilities as a defence against web shells. Implement a least-rights policy on the webserver to minimize the misuse of illegal access and limit an attacker's ability to escalate privileges or pivot laterally. Since APT27 carries out ransomware attacks, it is advised to often back up important data and use effective anti-ransomware programmes for increased security. Additionally, operationalizing threat intelligence across security processes utilizing cutting-edge threat intelligence systems is the best method to combat an attack vector that is constantly developing.

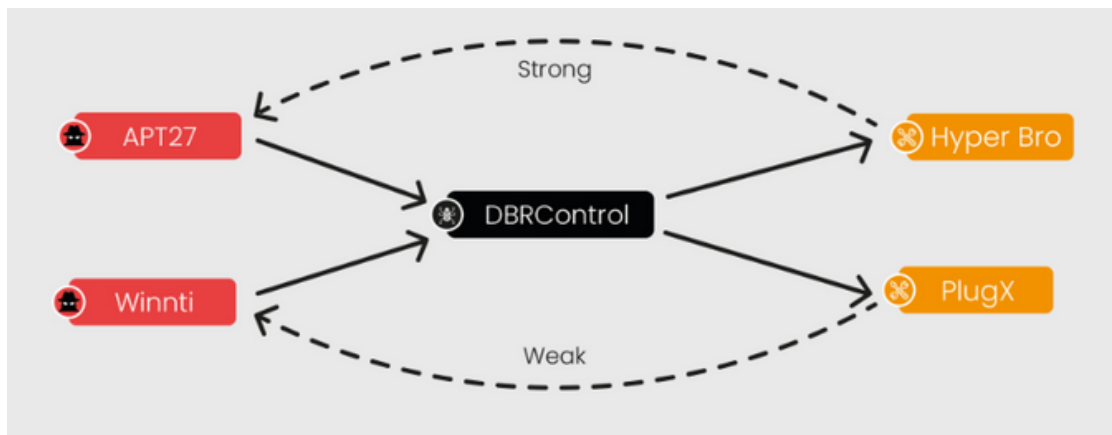
INFECTION CHAIN

As previously revealed, a third-party compromise allowed the threat actors to access the company's systems. Additionally, an ASPXSpy web shell was set up to aid lateral movement. The Google Updater programme loading the PlugX and Clambling samples into memory was susceptible to DLL Side-Loading. A genuine executable, a malicious DLL, and a binary file containing shellcode that oversaw separating the payload from itself and executing it in memory were all present for each of the two samples. While both DLLs were titled goopdate.dll and both samples utilized the signed Google Updater, the PlugX binary file had the name license.rtf, and the Clambling binary file had the name English.rtf.

Researchers also found a generic Mimikatz sample that the attackers had not altered before distributing it, on the infected system.

In addition, researchers discovered malware that used the publicly accessible source code CVE-2017-0213 to escalate privileges. This is consistent with the TrendMicro report, which makes note of the use of the same attack. In the past, APT27 has been known to escalate privileges using this attack. In one case, a CryptoMiner was dumped onto the system. This demonstrates that APT27 has historically been motivated by money, while launching attacks.

LINKS BETWEEN APT27 AND WINNTI



Source: Global Threat Centre

LINKS WITH THREAT ACTORS

According to the TrendMicro analysis, two potential organizations are connected to the DRBControl effort—Winnti and APT27. Due to the use of the HyperBro backdoor in one of the events, APT27 was connected to the campaign. Instead of being a widely used utility like PlugX, HyperBro is often considered specific to APT27. This may mean that APT27 is behind the effort, or they're starting to share tools with other cybercriminal organizations.

Based on comparable mutexes and the attackers' post-exploitation instructions, Winnti had a considerably stronger connection to the campaign. One of the post-exploitation instructions made a bitsadmin call to a Winnti infrastructure-related IP address. Another Windows utility that enables file transfers and may be used to download distant files is bitsadmin. APT27 frequently targets government organizations, the defence industry, and other sectors, Winnti, in comparison, is known to target firms into computer games. Thus, the crossover from that to gambling enterprises is not too far-fetched to assume.

Our study revealed parallels between our Clambling sample and previous, verified APT27 implants, particularly the use of DLL Side-Loading with the primary payload stored in a separate file and the strategy of utilizing the number of arguments to execute various functions. Unfortunately, this was insufficient to support the theory that APT27 was responsible for this campaign. Since we lacked samples like HyperBro, we focused instead on the likelihood of a Winnti connection.

We found a report by Command54 about an incident that happened, in 2011. APT27 targeted the South Korean tech business SK Communications after looking for code commonality. The incident, which resulted from the seizure of an ESTSoft5 server owned by a third party, entailed the theft of up to 35 million records' worth of personal information.

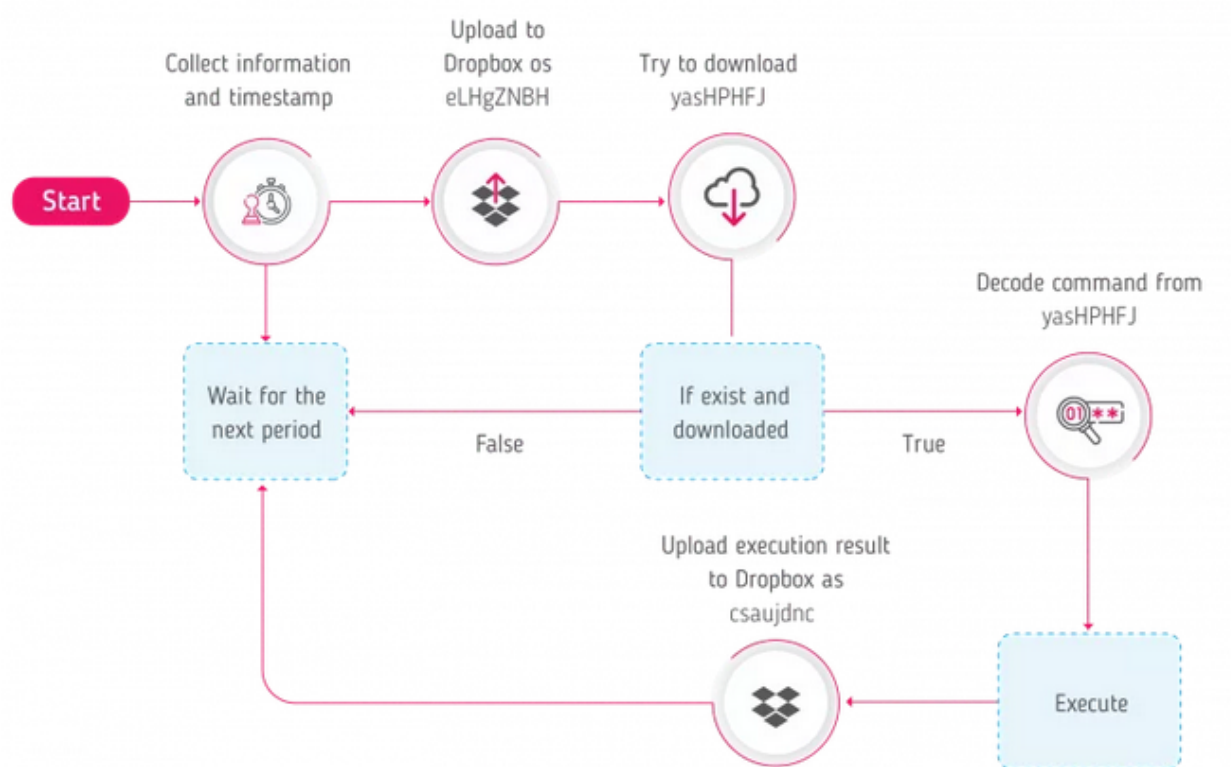
The server in issue offered ESTSoft's archive software automatic updates. When hackers took it over, it provided an upgrade to SK Communications systems, allowing a hacker to do DLL Side-Loading via the trusted archive software. Interestingly, one of TrendMicro's Clambling infections involves a modified version of HaoZip, a Chinese competitor to WinRAR and WinZip.

APT27 TURNS TO RANSOMWARE – CASE STUDY OF A GAMING INDUSTRY

The Intelligence Team (which intelligence team) examined malware samples containing ransomware and server encryption from major gaming corporations worldwide, in December 2020. The group named this variation Clambling because it mimics the DRBControl version linked to APT27. The DRBControl backdoor's use of Dropbox as a Command and Control (C2) server is an intriguing feature. Although the Clambling version and DRBControl are similar, DRBControl does not support Dropbox. The researchers also uncovered the ASPXSpy web shell, a sample of PlugX, and Mimikatz, in addition to the backdoor that was found. The virus encrypted the core servers using BitLocker, a local disc encryption technology included in Windows.

HOW THREAT ACTORS ENTERED THE SYSTEM

As is typical of cyberattacks in the gaming sector and elsewhere, the threat actors got into the system through a third-party compromise. The RAM loaded with the PlugX and Clambling samples using the Google Updater application. A legal executable, a malicious DLL, and a binary file contain a shellcode that is intended to extract the payload and run it in the memory of each sample. The Google Updater with the DLL name goopdate.dll was signed and utilized in both the PlugX and Clambling examples. The Clambling binary file was English.rtf, whereas the PlugX binary file's name was license.rtf. Additionally found was the binary that used CVE-2017-0213 to escalate privileges. APT27 has traditionally used this vulnerability to increase its privileges.



Clambling Infection - Cyberattacks in the Gaming Industry

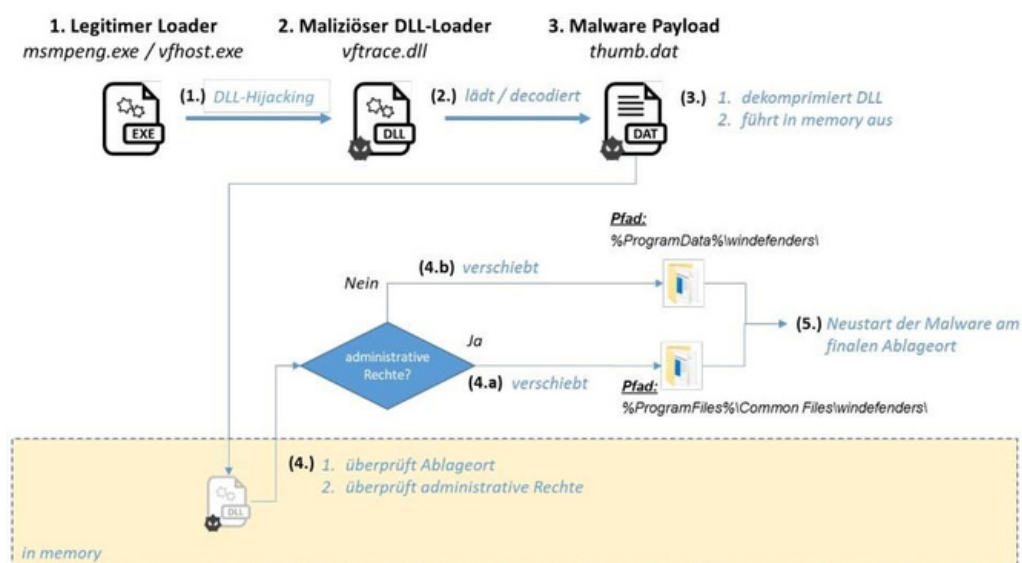
Source: x-phy.com

APT27 GROUP USES THE HYPERBRO REMOTE ACCESS TROJAN TO INJECT BACKDOORS INTO THE BUSINESS/VICTIM'S NETWORK

The malicious campaign targets German business enterprises, and the attackers implant backdoors into the victims networks using the HyperBro remote access trojan. Because it functions as an in-memory backdoor with remote administration capabilities, HyperBro enables hackers to stay on the target networks. The threat organization aims to steal private information and makes supply chain assaults against the consumers of its victims.

From March 2021 until mid-September 2021, APT27 used vulnerabilities in the Zoho Manage Engine AdSelf Service Plus software (CVE-2021-40539). Starting 25 October 2022, they began to exploit the ServiceDesk vulnerability (CVE-2021-44077). To deploy HYPERBRO, the attackers also used known vulnerabilities in Microsoft Exchange Server 2013, 2016, and 2019 proxy login vulnerabilities (CVE-2021-26855, CVE 2021-26857, CVE-2021-26858, and CVE-2021-27065).

HyperBro operates as an in-memory backdoor with remote administration capabilities, assisting threat actors to permanently stay on their victims networks.



Source: Bleepingcomputer.com

HyperBro infection chain (BfV)

Techniques used by the APT27 using HyperBro include the following:

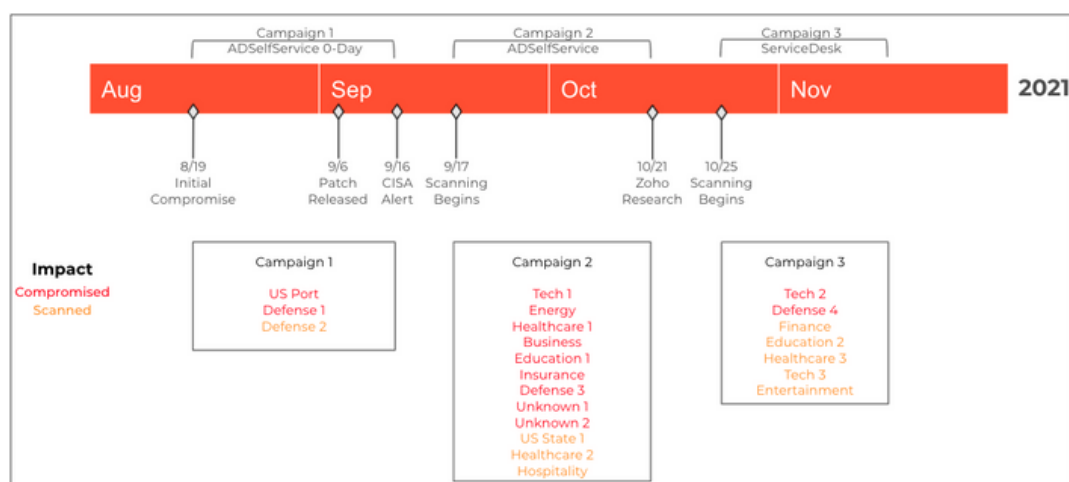
- T1071.001: Application Layer Protocol: Web Protocols
- T1574.002: Hijack Execution Flow: DLL Side-Loading
- T1070.004: Indicator Removal on Host: File Deletion
- T1105: Ingress Tool Transfer
- T1106: Native API
- T1055: Process Injection
- T1113: Screen Capture
- T1007: System Service Discovery
- T1569.002: System Services: Service Execution

BREACHING NETWORKS VIA ZOHOO AND EXCHANGE SERVERS

According to the German intelligence agency, the Zoho AdSelfService Plus product, an enterprise password management solution for Active Directory and cloud apps, contains vulnerabilities that APT27 has been using since March 2021.

This finding is consistent with earlier claims that several efforts targeting Zoho ManageEngine installations, in 2021, were orchestrated by nation-state hackers using techniques and equipment akin to those used by APT27.

Up until mid-September of 2021, they employed an ADSelfService zero-day attack. Then, they shifted to an n-day AdSelfService exploit, and starting 25 October, they began using a ServiceDesk issue.



Source: Bleepingcomputer.com

Zoho ManageEngine campaigns

According to experts at Palo Alto Networks, they effectively breached at least nine companies in crucial global industries. This included industries in sectors like defence, healthcare, energy, technology, and education.

Due to these efforts, the FBI and CISA jointly released warnings (1, 2) alerting the public of APT actors using ManageEngine weaknesses to inject web shells into the networks of compromised critical infrastructure organizations.

Early in March 2021, critical ProxyLogon issues were exploited by APT27 and other Chinese-backed hacker organizations, enabled them to seize control of unpatched Microsoft Exchange servers worldwide and steal their data.

The massive Microsoft Exchange hacking effort from the previous year was publicly attributed to China by the US and its allies (the European Union, the United Kingdom, and NATO) in June 2021.



VULNERABILITY DETAILS

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus up to 6.1:6113	cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:4.5:*****, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.0:*****, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.1:*****, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.2:*****, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.3:*****, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.4:*****, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.5:*****, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.6:*****, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:5.7:*****, cpe:2.3:a:zohocorp:manage	Zoho ManageEngine ADSelfService Plus REST API improper authentication	CWE - 287

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
		engine_adself service_plus:5.8.*: ***** *****, cpe:2.3:a:zohocorp :manageengine_ adself service_plus:6.0.*: ***** *****, cpe:2.3:a:zohocorp :manageengine_ adself service_plus:6.1.*: ***** *****		
CVE-2021-26855	Microsoft Exchange Server 2013, Microsoft Exchange Server 2016, Microsoft Exchange Server 2019	cpe:2.3:a:microsoft :exchange_server: 2013 _cu23:*****, cpe:2.3:a:microsoft :exchange_server: 2016 _cu18:*****, cpe:2.3:a:microsoft :exchange_server: 2016 _cu19:*****, cpe:2.3:a:microsoft :exchange_server: 2019 _cu7:*****, cpe:2.3:a:microsoft :exchange_server: 20 19_cu8:*****	SSRF vulnerability in Microsoft Exchange Server	CWE-918
CVE-2021-26857			An insecure deserialization vulnerability in Microsoft Exchange	CWE-20
CVE-2021-26858			An arbitrary file write vulnerabilities in Microsoft Exchange	CWE-20
CVE-2021-27065			An arbitrary file write vulnerabilities in Microsoft Exchange	CWE-20

INDICATORS OF COMPROMISE (IOCS)

Type	Value
SHA-256	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78, a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
Mutex	80A85553-1E05-4323-B4F9-43A4396A4507
File Path	%ProgramFiles%\Common Files\windefenders\ %ProgramFiles%\Common Files\windefenders\config.ini, %ProgramFiles%\Common Files\windefenders\msmpeng.exe, %ProgramFiles%\Common Files\windefenders\thumb.dat, %ProgramFiles%\Common Files\windefenders\vftrace.dll, %ProgramData%\windefenders\ %ProgramData%\windefenders\config.ini, %ProgramData%\windefenders\msmpeng.exe, %ProgramData%\windefenders\thumb.dat, %ProgramData%\windefenders\vftrace.dll,
IP	104.168.236.46, 103.79.77.200, 87.98.190.184
File Name	%TEMP%\clip.log, %TEMP%\key.log

CONCLUSION

APT27 threat organization is suspected of having ties with the Chinese Government and is in China. They are suspected to be funded by the state. Input capture, remote file copying, and external remote services are a few methods to target them. They used the following exploits to get a foothold inside the companies: CVE-2021-40539, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, & CVE-2021-27065. At the end of January 2022, the last activity by the APT27 group (aka LuckyMouse) targeted German commercial companies.

To stay in the game, the group regularly updates their tools, tactics, and procedures (TTPs). Researchers believe that the group will keep attacking and devising new and improved strategies. To prevent future harm to their business, firms should remain vigilant and actively watch out for this threat group.



Freedom of Expression, Trust and Safety on the Internet

🌐 www.indiafuturefoundation.com

☎ +91-1244045954, +91-9312580816

📍 Building no. 2731 EP, Sector 57,
Golf Course Ext. Road, Gurugram, Haryana, India – 122003