Hive Pro

THREAT ADVISORY

APT27 group uses the HyperBro remote access trojan to inject backdoors into victim's network

TA2022022

Threat Level RED

Publish Date – Feb 1, 2022

The German Federal Office for the Protection of the Constitution has warned of ongoing attacks coordinated by the Chinese cyber attack group APT27 (also known as TG-3390, Emissary Panda, BRONZE UNION, Iron Tiger and LuckyMouse).

The malicious campaign targets German commercial organizations where the attackers use the HyperBro remote access trojan to inject backdoors into the victims' network. HyperBro allows hackers to persist on victim networks by acting as an in-memory backdoor with remote administration capabilities. The threat group's goal is to steal sensitive information as well as attempt to target their victims' customers in supply chain attacks.

APT27 has been exploiting vulnerabilities in Zoho Manage Engine AdSelf Service Plus software (CVE-2021-40539) since March 2021 until mid-September last year, and from October 25 they began to exploit the vulnerability in ServiceDesk (CVE-2021-44077). The attackers were also exploiting known vulnerabilities in Microsoft Exchange Server 2013, 2016 and 2019 proxy logon vulnerabilities(CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065) used to deliver HYPERBRO.

As per the available information, during the campaign, the group successfully compromised at least nine organizations from critical sectors around the world, including defense, healthcare, energy, technology and education.

The Techniques used by the APT27 using HyperBro includes:
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

Actor Details

Name	Origin	Target Locations	Target sectors
APT 27	China	Australia, Canada, China, Hong Kong, India, Iran, Israel, Japan, France Middle East, Philippines, Russia, South Korea, Taiwan, Thailand, Tibet, UK, USA and Germany	Retail, Defense, Education, Healthcare, Embassies, Government, Technology, Telecommunications and Think Tanks

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:manageengine_adselfservice_plus:5.8:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:6.0:*:*:*:*:*:*:*, cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:6.1:*:*:*:*:*:*:*	Zoho ManageEngine ADSelfService Plus REST API improper authentication	CWE-287
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:2019_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

Patch Link

https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26857
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26858
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-27065

References

https://www.bleepingcomputer.com/news/security/german-govt-warns-of-apt27-hackers-backdooring-business-networks/
https://www.bleepingcomputer.com/news/security/hackers-use-in-house-zoho-servicedesk-exploit-to-drop-webshells/