AL2021_57 NICKEL Targeting Government Organizations (23rd December 2021)

Description

NICKEL, a China-based threat actor has been observed targeting governments, diplomatic entities, and non-governmental organizations (NGOs) across Central and South America, the Caribbean, Europe, and North America. Microsoft Threat Intelligence Center (MSTIC) has been tracking NICKEL and observed some common activity with other actors known in the security community as APT15, APT25, and KeChang. On December 6th, 2021, the Microsoft Digital Crimes Unit (DCU) announced the successful seizure of a set of NICKEL-operated websites and disruption of their ongoing attacks targeting organizations in 29 countries, following a court order from the U.S. District Court for the Eastern District of Virginia granting Microsoft the authority to seize these sites.

Summary

NICKEL actors were observed by MSTIC exploiting vulnerabilities in unpatched systems to compromise remote access services and appliances. Once intrusion was successful, they used credential dumpers or stealers to obtain credentials, which they used to gain access to victim accounts. The threat actors created and deployed custom malware that allowed them to maintain access and control on victim networks over extended periods of time. MSTIC has also observed NICKEL perform frequent and scheduled data collection and exfiltration from victim networks.

How it works

NICKEL successfully compromises networks using attacks on internet-facing web applications running on unpatched Microsoft Exchange and SharePoint. They also attack remote access infrastructure, such as unpatched VPN appliances.

After gaining an initial foothold the threat actors carried out regular surveillance on the network, working to gain access to additional accounts or systems with higher valued data. NICKEL typically deployed a keylogger to capture credentials from users on compromised systems. NICKEL was observed using Mimikatz, an older authentication method that allows the attacker access to credentials in clear text

known as WDigest, NTDSDump, and other password dumping tools to gather credentials on a targeted system and from target browsers.

Another attack method used by NICKEL is deploying malware for command and control (C2). MSTIC has tracked several malware families used by NICKEL as Neoichor, Leeson, NumbIdea, NullItch, and Rokum. The malware is dropped into existing software paths to make the malware appear to be files used by installed applications. Some example of these paths are:

- C:\Program Files\Realtek\Audio\HDA\AERTSr.exe
- C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitRdr64.exe
- C:\Program Files (x86)\Adobe\Flash Player\AddIns\airappinstaller\airappinstall.exe
- C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd64.exe

The Leeson, Neoichor, and NumbIdea malware families typically use the Internet Explorer (IE) COM interface to connect and receive commands from hardcoded C2 servers. Due to their reliance on IE, these malware families intentionally configure the browser settings by modifying the following registry entries:

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
Start Page = “about:blank”
DisableFirstRunCustomize = 1
RunOnceComplete = 1
RunOnceHasShown = 1
Check_Associations = 1

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery]
AutoRecover = 0

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Privacy]
ClearBrowsingHistoryOnExit = 1

[HKEY_CURRENT_USER\Software\Microsoft\Internet Connection Wizard]
Completed = 1

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap]
IEHarden = 0

When connecting to the C2 servers, the URL requests follow these formats:

http[:]//<C2>?id=<5-digit-rand><system-specific-string>
http[:]//<C2>?setssion==<rand><GetTickCount>

http[:]//<C2>?newfrs%dsetssion=<rand><GetTickCount>
http[:]//<C2>/index.htm?content=<base64-system-specifc-string>&id=<num>

A typical response from the C2 server is a legitimate-looking webpage containing the string "!DOCTYPE html", which the malware checks. The malware then locates a Base64-encoded blob, which it decodes and proceeds to load as a shellcode.

For the Neoichor family, the malware checks for internet connectivity by contacting bing.com with the request format bing.com?id=<GetTickCount> and drops files as ~atemp and ~btemp containing error codes and debug resources.

The backdoors implanted collect system information such as IP address, OS version, system language ID, computer name and signed in username. The basic functionalities of these backdoors are to launch a process, upload a file, download a file and execute shellcode in memory.

Remediation

The following guidance can help mitigate the techniques and threat activity described in this blog:

- Block legacy authentication protocols in Azure Active Directory – especially Exchange Web Services (EWS). You can follow the following link for instructions on implementing this https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication
- Enable multi-factor authentication to mitigate compromised credentials.
- For Office 365 users, see multi-factor authentication support.
- For Consumer and Personal email accounts, see how to use two-step verification.
- Use passwordless solutions like Microsoft Authenticator to secure accounts.
- Review and enforce recommended Exchange Online access policies. Use the following link for more information on these policies: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/secure-email-recommended-policies?view=o365-worldwide
- Block ActiveSync clients from bypassing Conditional Access policies.
- Block all incoming traffic from anonymizing services, where possible.
- Turn on the following attack surface reduction rule to block or audit activity associated with this threat:
  Block credential stealing from the Windows local security authority subsystem (lsass.exe)

References

- Microsoft Security. (6th December 2021). NICKEL targeting government organizations across Latin America and Europe. Retrieved from Microsoft: https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/

- Miller, Maggie. (6th December 2021). Microsoft disrupts Chinese hacking group targeting organizations in dozens of countries. Retrieved from The Hill: https://thehill.com/policy/technology/584520-microsoft-disrupts-chinese-hacking-group-targeting-organizations-in-dozens?rl=1