NICKEL targeting government organizations across Latin America and Europe

microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/

December 6, 2021

The Microsoft Threat Intelligence Center (MSTIC) has observed NICKEL, a China-based threat actor, targeting governments, diplomatic entities, and non-governmental organizations (NGOs) across Central and South America, the Caribbean, Europe, and North America. MSTIC has been tracking NICKEL since 2016 and observed some common activity with other actors known in the security community as APT15, APT25, and KeChang. Today, 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.

MSTIC has tracked the current NICKEL operations, including attacks against government organizations, diplomatic entities, and NGOs, since September 2019. During this time, NICKEL activity has been observed across several countries, with a large amount of activity targeting Central and South American governments. Notably, NICKEL has achieved long-term access to several targets, allowing NICKEL to conduct activities such as regularly scheduled exfiltration of data. As China's influence around the world continues to grow and the nation establishes bilateral relations with more countries and extends partnerships in support of China's Belt and Road Initiative, we assess that China-based threat actors will continue to target customers in government, diplomatic, and NGO sectors to gain new insights, likely in pursuit of economic espionage or traditional intelligence collection objectives. Portions of the NICKEL activity we are highlighting have also been blogged about by our colleagues at ESET.

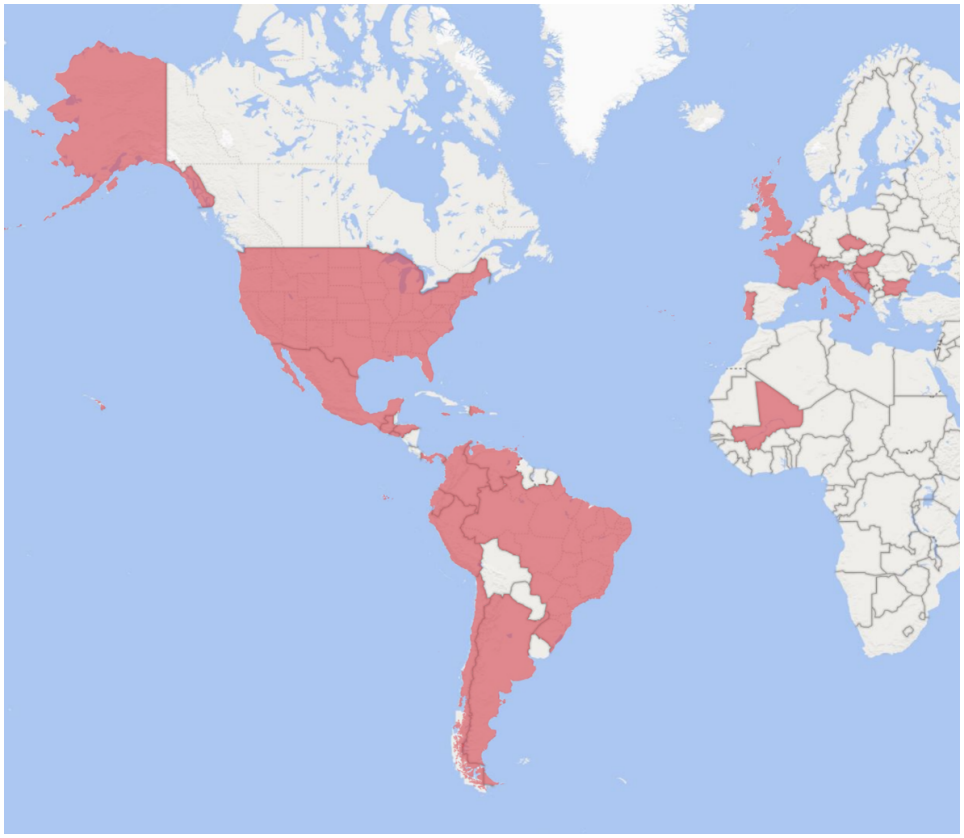

Figure 1: NICKEL targeted countries: *Argentina, Barbados, Bosnia and Herzegovina, Brazil, Bulgaria, Chile, Colombia, Croatia, Czech Republic, Dominican Republic, Ecuador, El Salvador, France, Guatemala, Honduras, Hungary, Italy, Jamaica, Mali, Mexico, Montenegro, Panama, Peru, Portugal, Switzerland, Trinidad and Tobago, United Kingdom, United States of America, Venezuela*

As with any observed nation-state actor activity, Microsoft continues to notify customers that have been targeted or compromised, providing them with the information they need to help secure their organizations. To reduce the potential impact of this NICKEL activity, Microsoft encourages our customers to immediately review the activity and guidance below, then implement risk mitigations, harden environments, and investigate suspicious behaviors that match the tactics described in this blog. MSTIC will continue to observe, monitor, and notify affected customers and partners, when possible, through our nation-state notification process.

Observed activity

MSTIC has observed NICKEL actors using exploits against unpatched systems to compromise remote access services and appliances. Upon successful intrusion, they have used credential dumpers or stealers to obtain legitimate credentials, which they used to gain access to victim accounts. NICKEL actors created and deployed custom malware that allowed them to maintain persistence on victim networks over extended periods of time. MSTIC has also observed NICKEL perform frequent and scheduled data collection and exfiltration from victim networks.

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, as referenced in the FireEye April 2021 blog detailing a 0-day vulnerability in Pulse Secure VPN that has since been patched.

After gaining an initial foothold on a compromised system, the NICKEL actors routinely performed reconnaissance on the network, working to gain access to additional accounts or higher-value systems. NICKEL typically deployed a keylogger to capture credentials from users on compromised systems. We've observed NICKEL using Mimikatz, WDigest (an older authentication method that allows the attacker access to credentials in clear text), NTDSDump, and other password dumping tools to gather credentials on a targeted system and from target browsers.

Deploying malware for command and control
MSTIC tracks multiple malware families used by NICKEL for command and control as Neoichor, Leeson, NumbIdea, NullItch, and Rokum.

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 NICKEL implants are backdoors capable of collecting system information, such as:

- IP address
- OS version
- System language ID
- Computer name
- Signed-in username

They implement basic backdoor functionalities, including:

- Launching a process
- Uploading a file
- Downloading a file
- Executing a shellcode in memory

MSTIC has observed NICKEL drop their malware into existing installed software paths. They did this to make their malware appear to be files used for an installed application. The following are example paths:

- 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

Using compromised credentials for routine email collection

NICKEL used compromised credentials to sign into victims' Microsoft 365 accounts through normal sign-ins with a browser and the legacy Exchange Web Services (EWS) protocol to review and collect victim emails. MSTIC has observed successful NICKEL sign-ins to compromised accounts through commercial VPN providers as well as from actor-controlled infrastructure. The activity graphed below shows NICKEL sign-in activity happening most frequently on Monday through Friday from 12:00 AM UTC (8:00 AM China Standard time) through 09:00 AM UTC (5:00 PM China Standard Time). There are also possible indications of a shift-based scheduling model based on the observed limited set of activity during a typical weekend.

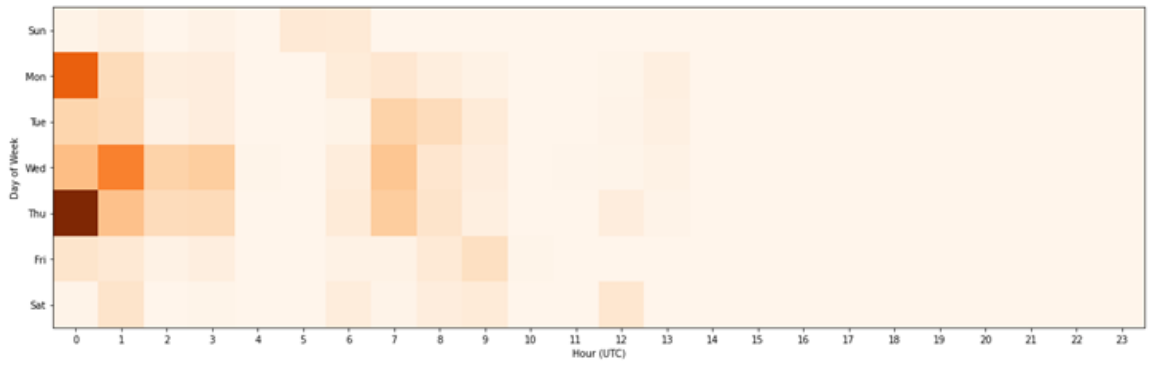

Figure 2: Heatmap of observed NICKEL login activity by day of week and hour (UTC time)

Evidence of routine host data collection

In several observed cases, NICKEL was seen performing regular data collection for exfiltration purposes. Their activity included looking in directories of interest for new files added since the last time they collected data. In the example below, NICKEL was collecting data that had been created or modified multiple times over a one-month period. For instance, on October 22, NICKEL looked for files that had been created since October 19 in multiple folders. Previously, on October 20 they had done the same thing looking for files that were modified or created since October 13.

Here are recent examples of NICKEL's routine data collection:

```
Process creation time           Process command line
 2021-10-13T00:42:33.821699Z     xcopy  /D:09-29-2021 /S/Y/C c:\users\[REDACTED]\Desktop c:\windows\temp\wmi\
 2021-10-13T00:42:33.8671327Z    xcopy  /D:09-29-2021 /S/Y/C c:\users\[REDACTED]\Downloads c:\windows\temp\wmi\
 2021-10-13T00:42:33.9199098Z    xcopy  /D:09-29-2021 /S/Y/C c:\users\[REDACTED]\Documents c:\windows\temp\wmi\
 2021-10-20T00:20:10.1822999Z    xcopy  /D:10-13-2021 /S/Y/C c:\users\[REDACTED]\Desktop c:\windows\temp\wmi\
 2021-10-20T00:20:10.2169051Z    xcopy  /D:10-13-2021 /S/Y/C c:\users\[REDACTED]\Downloads c:\windows\temp\wmi\
 2021-10-20T00:20:10.2437751Z    xcopy  /D:10-13-2021 /S/Y/C c:\users\[REDACTED]\Documents c:\windows\temp\wmi\
 2021-10-22T02:37:15.0410154Z    xcopy  /D:10-19-2021 /S/Y/C c:\users\[REDACTED]\Desktop c:\windows\temp\wmi\
 2021-10-22T02:37:15.0733287Z    xcopy  /D:10-19-2021 /S/Y/C c:\users\[REDACTED]\Downloads c:\windows\temp\wmi\
 2021-10-22T02:37:15.1113048Z    xcopy  /D:10-19-2021 /S/Y/C c:\users\[REDACTED]\Documents c:\windows\temp\wmi\
 2021-10-26T03:02:27.6976047Z    xcopy  /D:10-21-2021 /S/Y/C c:\users\[REDACTED]\Desktop c:\windows\temp\wmi\
 2021-10-26T03:02:27.730238Z     xcopy  /D:10-21-2021 /S/Y/C c:\users\[REDACTED]\Downloads c:\windows\temp\wmi\
 2021-10-26T03:02:27.7609891Z    xcopy  /D:10-21-2021 /S/Y/C c:\users\[REDACTED]\Documents c:\windows\temp\wmi\
```

After collecting the data in a central directory, the attackers then used either a renamed *rar.exe* or *7z.exe* to archive the files. NICKEL also frequently used keyboard walks as a password for their archived data collections. The following are examples of RAR archiving for exfiltration:

```
wp.exe a -v500 -p4rfvbgt56yhn %temp%\b.rar

wp.exe a -v1000 -p5tgbnhy67ujm %temp%\p.rar
```

Here is an example of 7zip archiving for exfiltration:

```
"7z.exe"  a -p1qazxsw23edc -t7z -y C:\windows\temp\wmi.7z c:\windows\temp\wmi\
```

Microsoft will continue to monitor NICKEL activity and implement product protections for our customers. The IOCs, current detections, and advanced protections in place across our security products are detailed below.

Recommended defenses

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)
- 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.
  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)

Indicators of compromise (IOCs)

Type	Indicator
SHA-256	02daf4544bcefb2de865d0b45fc406bee3630704be26a9d6da25c9abe906e7d2
SHA-256	0a45ec3da31838aa7f56e4cbe70d5b3b3809029f9159ff0235837e5b7a4cb34c
SHA-256	0d7965489810446ca7acc7a2160795b22e452a164261313c634a6529a0090a0c
SHA-256	10bb4e056fd19f2debe61d8fc5665434f56064a93ca0ec0bef946a4c3e098b95
SHA-256	12d914f24fe5501e09f5edf503820cc5fe8b763827a1c6d44cdb705e48651b21
SHA-256	1899f761123fedfeba0fee6a11f830a29cd3653bcdcf70380b72a05b921b4b49
SHA-256	22e68e366dd3323e5bb68161b0938da8e1331e4f1c1819c8e84a97e704d93844
SHA-256	259783405ec2cb37fdd8fd16304328edbb6a0703bc3d551eba252d9b450554ef
SHA-256	26debed09b1bbf24545e3b4501b799b66a0146d4020f882776465b5071e91822
SHA-256	35c5f22bb11f7dd7a2bb03808e0337cb7f9c0d96047b94c8afdab63efc0b9bb2
SHA-256	3ae2d9ffa4e53519e62cc0a75696f9023f9cce09b0a917f25699b48d0f7c4838
SHA-256	3bac2e459c69fcef8c1c93c18e5f4f3e3102d8d0f54a63e0650072aeb2a5fa65
SHA-256	3c0bf69f6faf85523d9e60d13218e77122b2adb0136ffebbad0f39f3e3eed4e6
SHA-256	3dc0001a11d54925d2591aec4ea296e64f1d4fdf17ff3343ddeea82e9bd5e4f1
SHA-256	3fd73af89e94af180b1fbf442bbfb7d7a6c4cf9043abd22ac0aa2f8149bafc90
SHA-256	6854df6aa0af46f7c77667c450796d5658b3058219158456e869ebd39a47d54b
SHA-256	6b79b807a66c786bd2e57d1c761fc7e69dd9f790ffab7ce74086c4115c9305ce
SHA-256	7944a86fbef6238d2a55c14c660c3a3d361c172f6b8fa490686cc8889b7a51a0
SHA-256	926904f7c0da13a6b8689c36dab9d20b3a2e6d32f212fca9e5f8cf2c6055333c
SHA-256	95e98c811ea9d212673d0e84046d6da94cbd913428427519580027859359 4b5a
SHA-256	a142625512e5372a1728595be19dbee23eea50524b4827cb64ed5aaeaaa0270b
SHA-256	afe5e9145882e0b98a795468a4c0352f5b1ddb7b4a534783c9e8fc366914cf6a
SHA-256	b9027bad09a9f5c917cf0f811610438e46e42e5e984a8984b6d69206ceb74124
SHA-256	c132d59a3bf0099e0f9f5667daf7b65dba66780f4addd88f04eecae47d5d99fa
SHA-256	c9a5765561f52bbe34382ce06f4431f7ac65bafe786db5de89c29748cf371dda
SHA-256	ce0408f92635e42aadc99da3cc1cbc0044e63441129c597e7aa1d76bf2700c94
SHA-256	ce47bacc872516f91263f5e59441c54f14e9856cf213ca3128470217655fc5e6
SHA-256	d0fe4562970676e30a4be8cb4923dc9bfd1fca8178e8e7fea0f3f02e0c7435ce
SHA-256	d5b36648dc9828e69242b57aca91a0bb73296292bf987720c73fcd3d2becbae6
SHA-256	e72d142a2bc49572e2d99ed15827fc27c67fc0999e90d4bf1352b075f86a83ba
Domain name	beesweiserdog[.]com

Domain name	bluehostfit[.]com
Domain name	business-toys[.]com
Domain name	cleanskycloud[.]com
Domain name	cumberbat[.]com
Domain name	czreadsecurity[.]com
Domain name	dgtresorgouv[.]com
Domain name	dimediamikedask[.]com
Domain name	diresitioscon[.]com
Domain name	elcolectador[.]com
Domain name	elperuanos[.]org
Domain name	eprotectioneu[.]com
Domain name	fheacor[.]com
Domain name	followthewaterdata[.]com
Domain name	francevrteepress[.]com
Domain name	futtuhy[.]com
Domain name	gardienweb[.]com
Domain name	heimflugaustr[.]com
Domain name	ivpsers[.]com
Domain name	jkeducation[.]org
Domain name	micrlmb[.]com
Domain name	muthesck[.]com
Domain name	netscalertech[.]com
Domain name	newgoldbalmap[.]com
Domain name	news-laestrella[.]com
Domain name	noticialif[.]com
Domain name	opentanzanfoundation[.]com
Domain name	optonlinepress[.]com
Domain name	palazzochigi[.]com
Domain name	pandemicacre[.]com
Domain name	papa-ser[.]com
Domain name	pekematclouds[.]com
Domain name	pipcake[.]com
Domain name	popularservicenter[.]com

Domain name	projectsyndic[.]com
Domain name	qsadtv[.]com
Domain name	sankreal[.]com
Domain name	scielope[.]com
Domain name	seoamdcopywriting[.]com
Domain name	slidenshare[.]com
Domain name	somoswake[.]com
Domain name	squarespacenow[.]com
Domain name	subapostilla[.]com
Domain name	suzukicycles[.]net
Domain name	tatanotakeeps[.]com
Domain name	tijuanazxc[.]com
Domain name	transactioninfo[.]net
Domain name	eurolabspro[.]com
Domain name	adelluminate[.]com
Domain name	headhunterblue[.]com
Domain name	primenuesty[.]com

Detections

Microsoft 365 Defender

Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- Backdoor:Win32/Leeson
- Trojan:Win32/Kechang
- Backdoor:Win32/Nightimp!dha
- Trojan:Win32/Rokum
- TrojanSpy:Win32/KeyLogger

Endpoint detection and response (EDR)

Alerts with the following titles in the security center can indicate NICKEL threat activity on your network:

- NICKEL activity group
- Malware associated with NICKEL activity group
- Communication with NICKEL infrastructure

The following alerts may also indicate threat activity associated with NICKEL but may also be triggered by unrelated threat activity:

- Mimikatz credential theft tool
- Suspected credential theft activity

- Malicious credential theft tool execution detected
- Sensitive credential memory read
- Password hashes dumped from LSASS memory
- Suspicious credential dump from NTDS.dit
- Compression of sensitive data
- Staging of sensitive data
- Suspicious process transferring data to external network
- Possible data exfiltration through multiple egress points

Microsoft 365 Defender correlates related alerts into consolidated incidents to help customers determine with confidence if observed alerts are related to this activity. We also published a threat analytics report on the NICKEL activity described in this blog. Microsoft 365 Defender can use the threat analytics report to get technical information, as well as view, investigate, and respond to incidents and alerts that include any detections of related NICKEL activity.

Advanced hunting queries

Microsoft Sentinel

The indicators of compromise (IoCs) included in this blog post can be used by Microsoft Sentinel customers for detection purposes using the queries detailed below.

Match known NICKEL domains and hashes

The following query matches domain name, hash IOCs and Microsoft 365 Defender signatures related to the NICKEL activity group with CommonSecurityLog, DnsEvents, VMConnection and SecurityEvents dataTypes.

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/NICKELIOCsNov2021.yaml

Identify NICKEL registry modifications patterns

The following query identifies instances where NICKEL malware intentionally configures the browser settings for its use by modifying registry entries.

https://github.com/azure/azure-sentinel/blob/master/Hunting%20Queries/MultipleDataSources/NickelRegIOCPatterns.yaml

Hunt for NICKEL Command Line Activity November 2021

The below query looks for process command line activity related to data collection and staging observed being used by NICKEL. It hunts for use of tools such as *xcopy* and renamed archiving tools used for data collection and staging on the hosts with signatures observed in NICKEL activity.

https://github.com/azure/azure-sentinel/blob/master/Hunting%20Queries/MultipleDataSources/NICKELCommandLineActivity-Nov2021.yaml

Microsoft 365 Defender

Surface WDigest authentication changes

Use this query to look for alerts related to enabling WDigest Authentication, which allows attackers to dump credentials in clear text. Run query

```
AlertInfo
| where Title == "WDigest configuration change"
| join AlertEvidence on AlertId
```

Surface discovery activity

Use this query to surface potential NICKEL discovery activity. Run query

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "rundll32.exe" and InitiatingProcessCommandLine has ",start"
| where ProcessCommandLine has_any("cmd",
"netstat", "tasklist", "dir", "del", "net use", "ipconfig", "systeminfo", "xcopy", "mkdir", ".bat")
```