Suspected Russian Activity Targeting Government and Business Entities Around the Globe

mandiant.com/resources/russian-targeting-gov-business

Blog

Luke Jenkins, Sarah Hawley, Parnian Najafi, Doug Bienstock

Dec 06, 2021

16 mins read

Uncategorized Groups (UNC Groups)

Cloud

Threat Research

Malware

Russia

UPDATE (May 2022): We have merged UNC2452 with APT29. The UNC2452 activity described in this post is now attributed to APT29.

As the one-year anniversary of the discovery of the SolarWinds supply chain compromise passes, Mandiant remains committed to tracking one of the toughest actors we have encountered. These suspected Russian actors practice top-notch operational security and advanced tradecraft. However, they are fallible, and we continue to uncover their activity and learn from their mistakes. Ultimately, they remain an adaptable and evolving threat that must be closely studied by defenders seeking to stay one step ahead.

Summary

Mandiant continues to track multiple clusters of suspected Russian intrusion activity that have targeted business and government entities around the globe. Based on our assessment of these activities, we have identified two distinct clusters of activity, UNC3004 and UNC2652. We associate both groups with UNC2452 also referred to as Nobelium by Microsoft.

Some of the tactics Mandiant has recently observed include:

- Compromise of multiple technology solutions, services, and reseller companies since 2020.
- Use of credentials likely obtained from an info-stealer malware campaign by a third-party actor to gain initial access to organizations.
- Use of accounts with Application Impersonation privileges to harvest sensitive mail data since Q1 2021.
- Use of both residential IP proxy services and newly provisioned geo located infrastructure to communicate with compromised victims.
- Use of novel TTPs to bypass security restrictions within environments including, but not limited to the extraction of virtual machines to determine internal routing configurations.
- Use of a new bespoke downloader we call CEELOADER.
- Abuse of multi-factor authentication leveraging “push” notifications on smartphones

In most instances, post compromise activity included theft of data relevant to Russian interests. In some instances, the data theft appears to be obtained primarily to create new routes to access other victim environments. The threat actors continue to innovate and identify new techniques and tradecraft to maintain persistent access to victim environments, hinder detection, and confuse attribution efforts.

The following sections highlight intrusion activity from multiple incident response efforts that are currently tracked as multiple uncategorized clusters. Mandiant suspects the multiple clusters to be attributable to a common Russian threat. The information covers some of the

tactics, techniques, and procedures (TTPs) used by the threat actors for initial compromise, establishing a foothold, data collection, and lateral movement; how the threat actors provision infrastructure; and indicators of compromise. The information is being shared to raise awareness and allow organizations to better defend themselves.

Initial Compromise

Compromise of Cloud Services Providers

Mandiant has identified multiple instances where the threat actor compromised service providers and used the privileged access and credentials belonging to these providers to compromise downstream customers.

In at least one instance, the threat actor identified and compromised a local VPN account and made use of this VPN account to perform reconnaissance and gain further access to internal resources within the victim CSP's environment, which ultimately led to the compromise of internal domain accounts.

Access Obtained from Info-stealer Malware Campaign

Mandiant identified a campaign where the threat actors gained access to the target organization's Microsoft 365 environment using a stolen session token. Mandiant analyzed the workstations belonging to the end user and discovered that some systems had been infected with CRYPTBOT, an info-stealer malware, shortly before the stolen session token was generated. Mandiant observed that in some cases the user downloaded the malware after browsing to low reputation websites offering free, or "cracked", software.

Mandiant assesses with moderate confidence that the threat actor obtained the session token from the operators of the info-stealer malware. These tokens were used by the actor via public VPN providers to authenticate to the target's Microsoft 365 environment.

Abuse of Repeated MFA Push Notifications

Mandiant has also observed the threat actor executing multiple authentication attempts in short succession against accounts secured with multi-factor authentication (MFA). In these cases, the threat actor had a valid username and password combination. Many MFA providers allow for users to accept a phone app push notification or to receive a phone call and press a key as a second factor. The threat actor took advantage of this and issued multiple MFA requests to the end user's legitimate device until the user accepted the authentication, allowing the threat actor to eventually gain access to the account.

Post Compromise Activity Via Cloud Solution Provider Compromise

Establish Foothold

In at least one case, the threat actor compromised a Microsoft Azure AD account within a Cloud Service Provider's (CSP) tenant. The account held a specific Azure AD role that allowed it to use the Admin on Behalf Of (AOBO) feature. With AOBO, users with a specific role in the CSP tenant have Azure Role Based Access Control (RBAC) Owner access to Azure subscriptions in their customer's tenants that were created through the reseller relationship. RBAC Owner access gives the role holder complete control over all resources within the Azure subscription. The threat actor leveraged the compromised csp's credentials and the AOBO feature to gain privileged access to Azure subscriptions used to host and manage downstream customer systems. The actor executed commands with NT AUTHORITY\SYSTEM privileges within Azure VMs using the Azure Run Command feature. The Azure Run Command feature allows a user to run PowerShell scripts within an Azure VM using the Azure Portal, REST API, or PowerShell without knowledge of Windows credentials that are valid on the VM itself.

Privilege Escalation

Mandiant found evidence that the threat actor used RDP to pivot between systems that had limited internet access. The threat actor accessed numerous devices using RDP and executed several native Windows commands. On one device, the threat actors made use of the Windows Task Manager to dump the process memory belonging to LSASS. The threat actor also obtained the Azure AD Connect configuration, the associated AD service account, and the key material used to encrypt the service account credentials. The Azure AD Connect account is used to replicate the on-premise instance of Active Directory into Azure AD. In addition to this, the threat actor obtained the Active Directory Federation Services (ADFS) signing certificate and key material. This allowed the threat actor to forge a SAML token which could be used to bypass 2FA and conditional access policies to access Microsoft 365. The actor stopped Sysmon and Splunk logging on these devices and cleared Windows Event Logs.

The threat actors leveraged compromised privileged accounts and used SMB, remote WMI, remote scheduled tasks registration, and PowerShell to execute commands within victim environments. The threat actor used the protocols mainly to perform reconnaissance (notably using the native command tasklist.exe to inspect remote systems), distribute BEACON around the network, as well as run native Windows commands for credential harvesting. In some cases, the actors passed in a specific Kerberos ticket during the WMIC execution using the /authority:Kerberos flag to authenticate as computer accounts. Computer accounts by design have local administrator rights over the computer for which they are named.

Lateral Movement Between CSP and Downstream Clients

CSPs have network filtering layers in place between their on-premises environment and downstream customer environments as an added security layer. Mandiant identified that the threat actor used the vSphere PowerCLI and custom PowerShell scripts configured to target

the vCenter Web endpoint to export the virtual disk image of a specific networking device and copy it off the service provider's infrastructure. To authenticate to vCenter the threat actor used a stolen session cookie for a Privileged Access Management (PAM) account. Mandiant believes the threat actor was able to analyze this virtual machine and identify devices within the CSP's network that were specifically allowed to communicate with targeted downstream customers.

Using this knowledge, the actor compromised the authorized source jump hosts that circumvented the network security restrictions of the service provider and downstream victim network. The actor compromised a customer administration account from one of the administration jump hosts used for customer administration within the CSP's environment. The CSP would connect via these jump hosts using dedicated customer admin accounts to interact with a downstream customer's infrastructure. The actor then performed lateral movement through RDP and the stolen target credentials towards the victim customer network.

In another case, the threat actor used Azure's built-in Run Command feature to execute commands on numerous downstream devices. The threat actor used native Windows tools to perform initial reconnaissance, credential theft and deploy Cobalt Strike BEACON to devices via PowerShell.

The actor then used this BEACON implant to persistently install CEELOADER as a Scheduled Task that ran on login as SYSTEM on specific systems. CEELOADER is downloader that decrypts a shellcode payload to execute in memory on the victim device.

Data Collection

Mandiant identified multiple attempts by the threat actor to dump the Active Directory database (ntds.dit) using the built-in ntdsutil.exe command. There was also evidence that the threat actor used Sysinternals ProcDump to dump the process memory of the LSASS process. In addition to this, Mandiant discovered that the threat actor had stolen the AD FS token signing certificate and the DKM key material. This would allow the threat actor to perform Golden SAML attacks and authenticate as any user into federated environments that used AD FS for authentication, such as Microsoft 365.

The threat actors performed data theft through several PowerShell commands, uploading several sequential archive files ending with the .7z extension. The threat actor uploaded these files to a webserver they presumably controlled.

Mandiant identified binaries that were configured to upload data to the Mega cloud storage provider. The threat actor deployed the tool in the %TEMP%\d folder as mt.exe and mtt.exe. Owing to several mistakes made by the threat actor, Mandiant was able to identify that the

execution of the renamed tool failed. Upon investigation, it appears that the Megatools binary used by the threat actors fails to execute if renamed. Due to this it is unclear whether the actor was able to successfully exfiltrate data to Mega using this method.

Mandiant also observed the threat actor access a victim's on-premises SharePoint server looking for sensitive technical documentation and credentials. The threat actor then used the gathered credentials to move laterally around the network.

Application Impersonation

Microsoft Exchange and Exchange Online provide an impersonation role (titled ApplicationImpersonation) that grants an account the ability to access another account's mailbox and "act as" that mailbox owner. Mandiant identified that the threat actor was able to authenticate to an existing account that was previously granted the ApplicationImpersonation role; it is unclear how the actor obtained this initial access.

Through this account, Mandiant witnessed the threat actor use impersonation to access multiple mailboxes belonging to users within the victim organization. The threat actor also created a new account within the Microsoft 365 environment which Mandiant deems was for backup access in the event of detection.

Threat Actor Infrastructure

Residential Internet Access

In some campaigns, Mandiant identified that the threat actor was using residential IP address ranges to authenticate to victim environments. Mandiant believes that this access was obtained through residential and mobile IP address proxy providers. The providers proxy traffic through actual mobile devices such as phones and tablets by legitimately bundling a proxy application in return for free applications and/or services.

The actor used these services to access mailboxes in victim Microsoft 365 tenants. By doing so, the source logon IP address belongs to a major Internet Service Provider that serves customers in the same country as the victim environment. These tactics showcase the complexity of the attacker's operations and is rarely seen executed by other threat actors. Accomplishing this can make it very difficult for investigators to differentiate between normal user activity and the threat actor's activity.

Geo-located Azure Infrastructure

In another campaign, the threat actor provisioned a system within Microsoft Azure that was within close proximity to a legitimate Azure-hosted system belonging to the CSP that they used to access their customer's environment. This allowed the actor to establish geo-proximity with the victims which resulted in the recorded source IP address for the activity originating from within legitimate Azure IP ranges. Similar to the technique of using

residential IP addresses, using Azure infrastructure within close proximity to victim networks makes it difficult for investigators to differentiate between normal user activity and the threat actor's activity.

Compromised WordPress Sites Hosting Second Stage Payloads

In several campaigns by the actor, Mandiant and our partners identified that the actor was hosting second stage payloads as encrypted blobs on legitimate websites running WordPress. Mandiant observed at least two separate malware families attributed to the threat actor hosted on compromised WordPress sites.

TOR, VPS and VPN Providers

In multiple campaigns by the threat actor, Mandiant witnessed the actor use a mixture of TOR, Virtual Private Servers (VPS) and public Virtual Private Networks (VPN) to access victim environments. In a particular campaign, Mandiant identified that the threat actor performed initial reconnaissance via a VPS provider located in the same region as the victim. Mandiant believes a misconfiguration by the threat actor meant that the VPN services running on the VPS stopped functioning after 8 hours. Mandiant was then able to identify numerous TOR exit nodes that the threat actor used based on new authentication events.

Operational Security and Planning

Mandiant identified attempts to compromise multiple accounts within an environment and kept use of each account separated by function. This reduced the likelihood that detecting one activity could expose the entire scope of the intrusion. Mandiant found evidence that the actor compromised multiple accounts and used one for the sole purpose of reconnaissance, while the others were reserved for lateral movement within the organization. Mandiant previously observed this threat actor using strict operational security to use specific accounts and systems in victim environments for activities that are often higher risk, such as data theft and large-scale reconnaissance.

Once within an environment, the threat actor was able to quickly pivot to on-premises servers and crawl these servers for technical documentation and credentials. From this documentation, the actor was able to identify a route to gain access to their ultimate target's network. This reconnaissance shows that the threat actor had a clear end goal in mind and were able to identify and exploit an opportunity to obtain required intelligence to further their goals.

Mandiant also observed efforts to avoid detection by circumventing or deleting system logging within the victim's environment. Namely, Mandiant identified the threat actor disabling SysInternals Sysmon and Splunk Forwarders on victim machines that they accessed via Microsoft Remote Desktop in addition to clearing Windows Event Logs.

Malware Descriptions

Cobalt Strike BEACON: Backdoor written in C/C++ that is part of the Cobalt Strike framework. Supported backdoor commands include shell command execution, file transfer, file execution, and file management. BEACON can also capture keystrokes and screenshots as well as act as a proxy server. BEACON may also be tasked with harvesting system credentials, port scanning, and enumerating systems on a network. BEACON communicates with a command and control (C2) server via HTTP(S) or DNS.

CEELOADER: Downloader written in C programing language. It supports shellcode payloads that are executed in memory. An obfuscation tool has been used to hide the code in CEELOADER in between large blocks of junk code with meaningless calls to the Windows API. The meaningful calls to the Windows API are hidden within obfuscated wrapper functions that decrypt the name of the API and dynamically resolve it before calling. CEELOADER communicates via HTTP and the C2 response is decrypted using AES-256 in CBC mode. Additionally, the HTTP request contains a statically defined id that may vary from sample to sample. CEELOADER does not contain a persistence mechanism.

Attribution

Mandiant assesses that some of this activity is UNC2652, a cluster of activity observed targeting diplomatic entities with phishing emails containing HTML attachments with malicious JavaScript, ultimately dropping a BEACON launcher.

Mandiant also assesses that some of this activity is UNC3004, a cluster of activity observed targeting both government and business entities through gaining access to Cloud Solution Providers/Managed Service Providers to gain access to downstream customers.

Microsoft has previously reported on both UNC2652 and UNC3004 activity and links it to UNC2452, the group behind the SolarWinds compromise, under the name “Nobelium”. While it is plausible that they are the same group, currently, Mandiant does not have enough evidence to make this determination with high confidence.

Outlook and Implications

This intrusion activity reflects a well-resourced threat actor set operating with a high level of concern for operational security. The abuse of a third party, in this case a CSP, can facilitate access to a wide scope of potential victims through a single compromise. Though Mandiant cannot currently attribute this activity with higher confidence, the operational security associated with this intrusion and exploitation of a third party is consistent with the tactics employed by the actors behind the SolarWinds compromise and highlights the effectiveness of leveraging third parties and trusted vendor relationships to carry out nefarious operations.

Acknowledgements

Hundreds of consultants, analysts and reverse engineers have been working together to understand and track these security incidents over the past year. This larger group has built a baseline of knowledge that enables us to continue tracking this actor. We would like to specifically thank Luis Rocha, Marius Fodoreanu, Mitchell Clarke, Manfred Erjak, Josh Madeley, Ashraf Abdalhalim and Juraj Sucik from Mandiant Consulting and Wojciech Ledzion, Gabriella Roncone, Jonathan Leathery and Ben Read from Mandiant Intelligence for their assistance in writing and reviewing this blog post.

Also special thanks to the Microsoft DART and MSTIC teams for their ongoing collaboration.

Remediation

Mandiant recommends that organizations review and implement the changes suggested in the following Mandiant white paper which was recently updated to include advice around the Application Impersonation role and trust relationships with Cloud Service Providers and their customers.

Technical Highlights to Aid Investigations or Hunting

Recent Staging Directories:

- %PROGRAMFILES%\Microsoft SQL Server\ms
- %WINDIR%\Temp
- %WINDIR%\Temp\d

Recent Staging Names:

- d.7z
- vcredist.ps1
- fc.r
- out
- d.ps1
- d.z
- megatools.exe
- mt.exe
- mtt.exe
- ntds.dit
- handle64.exe
- movefile.exe
- diagview.dll
- diag.ps1
- diag.bat

Recent Scheduled Task Names:

- Microsoft Diagnostics
- Microsoft Azure Diagnostics
- Google Chrome Update

Recent Administrative or Utility Tools:

- Azure Run Command
- Sysinternals Handle
- Sysinternals MoveFile
- ntdsutil
- netstat
- net
- tasklist
- RAR / 7zip
- AADInternals
- vSphere PowerCLI
- Sysinternals Procdump
- Windows Task Manager

Indicators of Compromise

Hashes for Known Activity:

- diag.ps1 (MD5: 1d3e2742e922641b7063db8cafed6531)
  BEACON.SMB malware connecting to \\.\pipe\chrome.5687.8051.183894933787788877a1
- vcredist.ps1 (MD5: 273ce653c457c9220ce53d0dfd3c60f1)
  BEACON malware connecting via HTTPS to nordicmademedia[.]com
- logo.png (MD5: 3304036ac3bbf6cb2205e30226c89a1a)
  - Hosted on http://23.106.123[.]15/logo.png
  - BEACON malware connected via HTTPS to stonecrestnews.com
- LocalData.dll (MD5: 3633203d9a93fecfa9d4d9c06fc7fe36)
  CEELOADER malware that obtains a payload from http://theandersonco[.]com/wp_info.php
- Unknown (MD5: e5aacf3103af27f9aaafa0a74b296d50)
  BEACON malware connecting via HTTPS to nordicmademedia[.]com
- DiagView.dll (MD5: f3962456f7fc8d10644bf051ddb7c7ef)
  CEELOADER malware that obtains a payload from http://tomasubiera[.]com/wp_getcontent.php

IP Addresses Used for Authenticating Through Public VPN Providers:

Note: Mandiant have removed anonymized addresses from this list, the remaining addresses are from legitimate hosting providers.

- 20.52.144[.]179
- 20.52.156[.]76
- 20.52.47[.]99
- 51.140.220[.]157
- 51.104.51[.]92
- 176.67.86[.]130
- 176.67.86[.]52

IP Addresses Used for Authenticating From the Mobile Proxy Providers:

- 216.155.158[.]133
- 63.75.244[.]119
- 63.162.179[.]166
- 63.162.179[.]94
- 63.75.245[.]144
- 63.75.245[.]239
- 63.75.247[.]114

IP Addresses Used for Command and Control:

- 91.234.254[.]144
- 23.106.123[.]15

URL Addresses Used for Command and Control:

- nordicmademedia[.]com
- stonecrestnews[.]com

URL Addresses of Compromised WordPress Sites Hosting CEELOADER Payloads:

Note: Mandiant believes the actor hosted a malicious payload on the following domains.

- tomasubiera[.]com
- theandersonco[.]com

MITRE ATT&CK Techniques Observed

ATT&CK Tactic Category	Techniques

Resource Development	• Acquire Infrastructure (T1583) Virtual Private Server (T1583.003) • Compromise Infrastructure (T1584) • Stage Capabilities (T1608) Link Target (T1608.005) • Obtain Capabilities (T1588) Digital Certificates (T1588.004)
Initial Access	• Phishing (T1566) ◦ Spearphishing Attachment (T1566.001) ◦ Spearphishing Link (T1566.002) • External Remote Services (T1133) • Valid Accounts (T1078) • Trusted Relationship (T1199)
Execution	• User Execution (T1204) ◦ Malicious Link (T1204.001) ◦ Malicious File (T1204.002) • Command and Scripting Interpreter (T1059) ◦ PowerShell (T1059.001) ◦ Windows Command Shell (T1059.003) ◦ JavaScript (T1059.007) • Scheduled Task/Job (T1053) Scheduled task (T1053.005) • Windows Management Instrumentation (T1047)
Persistence	• Boot or Logon Autostart Execution (T1547) ◦ Registry Run Keys / Startup Folder (T1547.001) ◦ Shortcut Modification (T1547.009) • Scheduled Task/Job (T1053) Scheduled task (T1053.005) • External Remote Services (T1133) • Valid Accounts (T1078)
Privilege Escalation	• Process Injection (T1055) • Access Token Manipulation (T1134) Token Impersonation/Theft (T1134.001) • Boot or Logon Autostart Execution (T1547) Shortcut Modification (T1547.009) • Valid Accounts (T1078) • Scheduled Task (T1053) Scheduled task (T1053.005)

Defence Evasion	• Process Injection (T1055)
	• Access Token manipulation (T1145)
	• Indicator Removal on Host (T1070)
	• Hide Artifacts (T1564)
	  Hidden window (T1564.003)
	• Indicator Removal on Host (T1070)
	  ◦ Clear Windows Event Logs (T1070.001)
	  ◦ File Deletion (T1070.004)
	  ◦ Timestomp (T1070.006)
	• Obfuscated Files or information (T1027)
	  Indicator Removal from Tools (T1027.005)
	• Virtualization/Sandbox Evasion (T1497)
	  System Checks (T1497.004)
	• Modify Registry (T1112)
	• Deobfuscate/Decode Files or Information (T1140)
	• Reflective Code Loading (T1620)
	• Valid Accounts (T1078)

Credential Access	OS Credential Dumping (T1003)
	  ◦ NTDS (T1003.003)
	  ◦ Keylogging (T1003.001)

Discovery	• System Information Discovery (T1082)
	• File and Directory Discovery (T1083)
	• Account Discovery (T1087)
	  ◦ Local Account (T1087.001)
	  ◦ Domain Account (T1087.002)
	• System Network Configuration Discovery (T1016)
	• Virtualization/Sandbox Evasion (T1497)
	  System Checks (T1497.001)
	• System Owner/User Discovery (T1033)
	• System network Connections Discovery (T1049)
	• Network Service Scanning (T1046)
	• Process Discovery (T1057)
	• System Service Discovery (T1007)
	• Permission Groups Discovery (T1069)
	• Software Discovery (T1518)
	• Query Registry (T1012)

Lateral Movement	Remote Services (T1021)
	  ◦ Remote Desktop Protocol (T1021.001)
	  ◦ SSH (T1021.004)

Collection	• Archive Collected Data (T1560)
	  Archive via Utility (T1560.001)
	• Data from Information Repositories (T1213)
	  Sharepoint (T1213.002)
	• Input Capture (T1056)
	  Keylogging (T1056.001)

Command and Control	• Web Service (T1102)
	• Application Layer Protocol (T1071)
	  ◦ Web Protocols (T1071.001)
	  ◦ DNS (T1071.004)
	• Encrypted Channel (T1573)
	  Asymmetric Cryptography (T1573.002)
	• Non-Application layer Protocol (T1095)
	• Non-Standard Port (T1571)
	• Ingress Tool Transfer (T1105)

Exfiltration	Data Transfer Size Limits (T1030)
Impact	Service Stop (T1489)
Discovery	System Network Configuration Discovery (T1016)