APT29

attack.mitre.org/groups/G0016

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).[1][2] They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.[3][4][5][6]

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes.[7][8] Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.[9][10][11][12][13]

ID: G0016

ⓘ

Associated Groups: IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke

Contributors: Daniyal Naeem, BT Security; Matt Brenton, Zurich Insurance Group; Katie Nickels, Red Canary

Version: 3.0

Created: 31 May 2017

Last Modified: 14 April 2022

Version Permalink
Live Version

Associated Group Descriptions

Name	Description
IRON RITUAL	[14]
IRON HEMLOCK	[15]
NobleBaron	[16]
Dark Halo	[12]
StellarParticle	[11][17]
NOBELIUM	[10][18][19][20]
UNC2452	[9]
YTTRIUM	[21]
The Dukes	[3][22][23][13]
Cozy Bear	[5][22][23][13][17]
CozyDuke	[5]

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has bypassed UAC.[24]
Enterprise	T1087	Account Discovery	APT29 obtained a list of users and their roles from an Exchange server using `Get-ManagementRoleAssignment`.[12]	
		.002	Domain Account	APT29 has used PowerShell to discover domain accounts b `ADUser` and `Get-DGroupMember`.[17][14]
		.004	Cloud Account	APT29 has conducted enumeration of Azure AD accounts.[2
Enterprise	T1098	.001	Account Manipulation: Additional Cloud Credentials	APT29 has added credentials to OAuth Applications and Se [17]
		.002	Account Manipulation: Additional Email Delegate Permissions	APT29 added their own devices as allowed IDs for active sy `CASMailbox`, allowing it to obtain copies of victim mailboxes additional permissions (such as Mail.Read and Mail.ReadW compromised Application or Service Principals.[12][26][25]
		.003	Account Manipulation: Additional Cloud Roles	APT29 has granted `company administrator` privileges to service principal.[17]
		.005	Account Manipulation: Device Registration	APT29 registered devices in order to enable mailbox syncin `CASMailbox` command.[12]
Enterprise	T1583	.001	Acquire Infrastructure: Domains	APT29 has acquired C2 domains, sometimes through resell
		.006	Acquire Infrastructure: Web Services	APT29 has registered algorithmically generated Twitter han for C2 by malware, such as HAMMERTOSS.[28][18]
Enterprise	T1595	.002	Active Scanning: Vulnerability Scanning	APT29 has conducted widespread scanning of target enviro vulnerabilities for exploit.[13]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	APT29 has used HTTP for C2 and data exfiltration.[12]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	APT29 used 7-Zip to compress stolen emails into password archives prior to exfiltration.[12][29][17]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT29 added Registry Run keys to establish persistence.[24
		.009	Boot or Logon Autostart Execution: Shortcut Modification	APT29 drops a Windows shortcut file for execution.[30]
Enterprise	T1110	.003	Brute Force: Password Spraying	APT29 has conducted brute force password spray attacks.[2
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	APT29 has used encoded PowerShell scripts uploaded to C installations to download and install SeaDuke. APT29 also u create new tasks on remote machines, identify configuration defenses, exfiltrate data, and to execute other commands.[1 [19]
		.003	Command and Scripting Interpreter: Windows Command Shell	APT29 used `cmd.exe` to execute commands on remote ma
		.005	Command and Scripting Interpreter: Visual Basic	APT29 has written malware variants in Visual Basic.[13]
		.006	Command and Scripting Interpreter: Python	APT29 has developed malware variants written in Python.[2

Domain	ID	Name	Use	
Enterprise	T1586	.002	Compromise Accounts: Email Accounts	APT29 has compromised email accounts to further enable p campaigns.[34]
Enterprise	T1584	.001	Compromise Infrastructure: Domains	APT29 has compromised domains to use for C2.[10]
Enterprise	T1136	.003	Create Account: Cloud Account	APT29 can create new users through Azure AD.[25]
Enterprise	T1555	Credentials from Password Stores	APT29 used account credentials they obtained to attempt access to Group Managed Service Account (gMSA) passwords.[29]	
		.003	Credentials from Web Browsers	APT29 has stolen user's saved passwords from Chrome.[17]
Enterprise	T1213	Data from Information Repositories	APT29 has accessed victims' internal knowledge repositories (wikis) to view sensitive corporate information on products, services, and internal business operations.[17]	
		.003	Code Repositories	APT29 has downloaded source code from code repositories
Enterprise	T1005	Data from Local System	APT29 has extracted files from compromised networks.[12]	
Enterprise	T1001	.002	Data Obfuscation: Steganography	APT29 has used steganography to hide C2 communications
Enterprise	T1074	.002	Data Staged: Remote Data Staging	APT29 staged data and files in password-protected archives OWA server.[12]
Enterprise	T1140	Deobfuscate/Decode Files or Information	APT29 used 7-Zip to decode its Raindrop malware.[36]	
Enterprise	T1587	.001	Develop Capabilities: Malware	APT29 has leveraged numerous pieces of malware that app to APT29 and were likely developed for or by the group.[9][11
		.003	Develop Capabilities: Digital Certificates	APT29 has created self-signed digital certificates to enable authentication for malware.[37][38]
Enterprise	T1484	.002	Domain Policy Modification: Domain Trust Modification	APT29 changed domain federation trust settings using Azur administrative permissions to configure the domain to accep tokens signed by their own SAML signing certificate.[39][14]
Enterprise	T1482	Domain Trust Discovery	APT29 used the `Get-AcceptedDomain` PowerShell cmdlet to enumerate accepted domains through an Exchange Management Shell.[12] They also used AdFind to enumerate domains and to discover trust between federated domains.[29][12]	
Enterprise	T1568	Dynamic Resolution	APT29 used dynamic DNS resolution to construct and resolve to randomly-generated subdomains for C2.[12]	
Enterprise	T1114	.002	Email Collection: Remote Email Collection	APT29 collected emails from specific individuals, such as ex staff, using `New-MailboxExportRequest` followed by `Get-MailboxExportRequest`.[12][13]

Domain	ID	Name	Use	
Enterprise	T1573	Encrypted Channel	APT29 has used multiple layers of encryption within malware to protect C2 communication.[15]	
Enterprise	T1546	.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	APT29 has used WMI event subscriptions for persistence.[2
		.008	Event Triggered Execution: Accessibility Features	APT29 used sticky-keys to obtain unauthenticated, privilege
Enterprise	T1048	.002	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	APT29 has exfiltrated collected data over a simple HTTPS r password-protected archive staged on a victim's OWA serve
Enterprise	T1190	Exploit Public-Facing Application	APT29 has exploited CVE-2019-19781 for Citrix, CVE-2019-11510 for Pulse Secure VPNs, CVE-2018-13379 for FortiGate VPNs, and CVE-2019-9670 in Zimbra software to gain access. They have also exploited CVE-2020-0688 against the Microsoft Exchange Control Panel to regain access to a network.[29][12][19]	
Enterprise	T1203	Exploitation for Client Execution	APT29 has used multiple software exploits for common client software, like Microsoft Word, Exchange, and Adobe Reader, to gain code execution.[3][13][18]	
Enterprise	T1068	Exploitation for Privilege Escalation	APT29 has exploited CVE-2021-36934 to escalate privileges on a compromised host.[33]	
Enterprise	T1133	External Remote Services	APT29 has used compromised identities to access networks via SSH, VPNs, and other remote access tools.[10][23][17]	
Enterprise	T1083	File and Directory Discovery	APT29 obtained information about the configured Exchange virtual directory using `Get-WebServicesVirtualDirectory`.[12]	
Enterprise	T1606	.001	Forge Web Credentials: Web Cookies	APT29 has bypassed MFA set on OWA accounts by genera from a previously stolen secret key.[12]
		.002	Forge Web Credentials: SAML Tokens	APT29 created tokens using compromised SAML signing ce
Enterprise	T1589	.001	Gather Victim Identity Information: Credentials	APT29 has conducted credential theft operations to obtain c used for access to victim environments.[17]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	APT29 used the service control manager on a remote syste services associated with security monitoring products.[29]
		.002	Impair Defenses: Disable Windows Event Logging	APT29 used `AUDITPOL` to prevent the collection of audit lo
		.004	Impair Defenses: Disable or Modify System Firewall	APT29 used `netsh` to configure firewall rules that limited c outbound packets.[29]

Domain	ID	Name	Use
Enterprise	T1070	Indicator Removal on Host	APT29 removed evidence of email export requests using `Remove-MailboxExportRequest`.[12] They temporarily replaced legitimate utilities with their own, executed their payload, and then restored the original file.[9]
	.004	File Deletion	APT29 routinely removed their tools, including custom back remote access was achieved. APT29 has also used SDelete artifacts from victims.[9][24]
	.006	Timestomp	APT29 modified timestamps of backdoors to match legitima
Enterprise	T1105	Ingress Tool Transfer	APT29 has downloaded additional tools, such as TEARDROP malware and Cobalt Strike, to a compromised host following initial access.[9]
Enterprise	T1036	Masquerading	APT29 has set the hostnames of its C2 infrastructure to match legitimate hostnames in the victim environment. They have also used IP addresses originating from the same country as the victim for their VPN infrastructure.[9]
	.004	Masquerade Task or Service	APT29 named tasks `\Microsoft\Windows\SoftwareProtectionPlatform\Ev` in order to appear legitimate.[12]
	.005	Match Legitimate Name or Location	APT29 renamed software and DLL's with legitimate names t
Enterprise	T1621	Multi-Factor Authentication Request Generation	APT29 has used repeated MFA requests to gain access to victim accounts.[41]
Enterprise	T1095	Non-Application Layer Protocol	APT29 has used TCP for C2 communications.[30]
Enterprise	T1027	Obfuscated Files or Information	APT29 has used encoded PowerShell commands.[30]
	.001	Binary Padding	APT29 has used large file sizes to avoid detection.[16]
	.002	Software Packing	APT29 used UPX to pack files.[24]
	.006	HTML Smuggling	APT29 has embedded an ISO file within an HTML attachme JavaScript code to initiate malware execution.[33]
Enterprise	T1588	.002	Obtain Capabilities: Tool	APT29 has obtained and used a variety of tools including M Tor, meek, and Cobalt Strike.[24][3][30]
Enterprise	T1003	.006	OS Credential Dumping: DCSync	APT29 leveraged privileged accounts to replicate directory s domain controllers.[39][29][17]
Enterprise	T1069	Permission Groups Discovery	APT29 used the `Get-ManagementRoleAssignment` PowerShell cmdlet to enumerate Exchange management role assignments through an Exchange Management Shell.[12]

Domain	ID	Name	Use	
		.002	Domain Groups	APT29 has used AdFind to enumerate domain groups.[17]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	APT29 has used spearphishing emails with an attachment t exploits to initial victims.[3][30][22][18][33][15]
		.002	Phishing: Spearphishing Link	APT29 has used spearphishing with a link to trick victims int to a zip file containing malicious files.[24][18][42]
		.003	Phishing: Spearphishing via Service	APT29 has used the legitimate mailing service Constant Co phishing e-mails.[13]
Enterprise	T1057	Process Discovery	APT29 has used multiple command-line utilities to enumerate running processes.[12][29][17]	
Enterprise	T1090	.001	Proxy: Internal Proxy	APT29 has used SSH port forwarding capabilities on public- and configured at least one instance of Cobalt Strike to use over SMB during the 2020 SolarWinds intrusion.[36][17]
		.003	Proxy: Multi-hop Proxy	A backdoor used by APT29 created a Tor hidden service to the Tor client to local ports 3389 (RDP), 139 (Netbios), and 4 enabling full remote access from outside the network and ha [24][42]
		.004	Proxy: Domain Fronting	APT29 has used the meek domain fronting plugin for Tor to destination of C2 traffic.[24]
Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	APT29 has used RDP sessions from public-facing systems [17]
		.002	Remote Services: SMB/Windows Admin Shares	APT29 has used administrative accounts to connect over SI users.[17]
		.006	Remote Services: Windows Remote Management	APT29 has used WinRM via PowerShell to execute comma on remote hosts.[36]
Enterprise	T1018	Remote System Discovery	APT29 has used AdFind to enumerate remote systems.[29]	
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT29 used `scheduler` and `schtasks` to create new tas hosts as part of lateral movement.[12] They have manipulate by updating an existing legitimate task to execute their tools the scheduled task to its original configuration.[9] APT29 also scheduled task to maintain SUNSPOT persistence when the during the 2020 SolarWinds intrusion.[11] They previously us hijacked scheduled tasks to also establish persistence.[24]
Enterprise	T1505	.003	Server Software Component: Web Shell	APT29 has installed web shells on exploited Microsoft Excha
Enterprise	T1558	.003	Steal or Forge Kerberos Tickets: Kerberoasting	APT29 obtained Ticket Granting Service (TGS) tickets for A Service Principle Names to crack offline.[29]
Enterprise	T1539	Steal Web Session Cookie	APT29 has stolen Chrome browser cookies by copying the Chrome profile directories of targeted users.[17]	
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	APT29 was able to get SUNBURST signed by SolarWinds c certificates by injecting the malware into the SolarWinds Ori lifecycle.[9]

Domain	ID	Name	Use	
		.005	Subvert Trust Controls: Mark-of-the-Web Bypass	APT29 has embedded ISO images and VHDX files in HTML the-Web.[33]
Enterprise	T1195	.002	Supply Chain Compromise: Compromise Software Supply Chain	APT29 gained initial network access to some victims via a tr SolarWinds Orion software.[9][13][14][25]
Enterprise	T1218	.005	System Binary Proxy Execution: Mshta	APT29 has use `mshta` to execute malicious scripts on a co [26]
		.011	System Binary Proxy Execution: Rundll32	APT29 has used `Rundll32.exe` to execute payloads.[26][2
Enterprise	T1082	System Information Discovery	APT29 used `fsutil` to check available free space before executing actions that might create large files on disk.[29]	
Enterprise	T1016	.001	System Network Configuration Discovery: Internet Connection Discovery	APT29 has used GoldFinder to perform HTTP GET requests connectivity and identify HTTP proxy servers and other redir HTTP request travels through.[10]
Enterprise	T1199	Trusted Relationship	APT29 has gained access through compromised accounts at cloud solution partners, and used compromised certificates issued by Mimecast to authenticate to Mimecast customer systems.[13][17] [26]	
Enterprise	T1552	.004	Unsecured Credentials: Private Keys	APT29 obtained PKI keys, certificate files and the private en an Active Directory Federation Services (AD FS) container t corresponding SAML signing certificates.[39][13]
Enterprise	T1550	Use Alternate Authentication Material	APT29 used forged SAML tokens that allowed the actors to impersonate users and bypass MFA, enabling APT29 to access enterprise cloud applications and services.[39] [14]	
		.001	Application Access Token	APT29 has used compromised service principals to make cl Office 365 environment.[17]
		.003	Pass the Ticket	APT29 used Kerberos ticket attacks for lateral movement.[24
		.004	Web Session Cookie	APT29 used stolen cookies to access cloud resources, and `sid` cookie to bypass MFA set on an email account.[12][17]
Enterprise	T1204	.001	User Execution: Malicious Link	APT29 has used various forms of spearphishing attempting click on a malicous link.[30][22][18][42]
		.002	User Execution: Malicious File	APT29 has used various forms of spearphishing attempting open attachments, including, but not limited to, malicious Mi documents, .pdf, and .lnk files. [3] [30][22][33][15]
Enterprise	T1078	Valid Accounts	APT29 used different compromised credentials for remote access and to move laterally.[9][10][13]	
		.002	Domain Accounts	APT29 has used valid accounts, including administrator acc facilitate lateral movement on compromised networks.[22][23]
		.003	Local Accounts	APT29 has used compromised local accounts to access vict

Domain	ID	Name	Use	
		.004	Cloud Accounts	APT29 has used a compromised O365 administrator accou Service Principal.[17]
Enterprise	T1102	.002	Web Service: Bidirectional Communication	APT29 has used social media platforms to hide communicat servers.[22]
Enterprise	T1047	Windows Management Instrumentation	APT29 used WMI to steal credentials and execute backdoors at a future time.[24] They have also used WMI for the remote execution of files for lateral movement.[39][29]	

Software

ID	Name	References	Techniques
S0677	AADInternals	[25]	Account Discovery: Cloud Account, Account Manipulation: Device Registration, Cloud Service Discovery, Command and Scripting Interpreter: PowerShell, Create Account: Cloud Account, Domain Policy Modification, Forge Web Credentials: SAML Tokens, Gather Victim Identity Information: Email Addresses, Gather Victim Network Information: Domain Properties, Modify Registry, OS Credential Dumping: LSA Secrets, Permission Groups Discovery: Cloud Groups, Phishing: Spearphishing Link, Phishing for Information: Spearphishing Link, Steal Application Access Token, Steal or Forge Kerberos Tickets: Silver Ticket, Unsecured Credentials: Credentials In Files, Unsecured Credentials: Private Keys
S0552	AdFind	[31][17][33]	Account Discovery: Domain Account, Domain Trust Discovery, Permission Groups Discovery: Domain Groups, Remote System Discovery, System Network Configuration Discovery
S0521	BloodHound	[33]	Account Discovery: Domain Account, Account Discovery: Local Account, Archive Collected Data, Command and Scripting Interpreter: PowerShell, Domain Trust Discovery, Group Policy Discovery, Native API, Password Policy Discovery, Permission Groups Discovery: Local Groups, Permission Groups Discovery: Domain Groups, Remote System Discovery, System Owner/User Discovery
S0635	BoomBox	[19]	Account Discovery: Domain Account, Account Discovery: Email Account, Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Deobfuscate/Decode Files or Information, Execution Guardrails, Exfiltration Over Web Service: Exfiltration to Cloud Storage, File and Directory Discovery, Ingress Tool Transfer, Masquerading, Obfuscated Files or Information, System Binary Proxy Execution: Rundll32, System Information Discovery, System Owner/User Discovery, User Execution: Malicious File, Web Service
S0054	CloudDuke	[3]	Application Layer Protocol: Web Protocols, Ingress Tool Transfer, Web Service: Bidirectional Communication

ID	Name	References	Techniques
S0154	Cobalt Strike	[30][9][13][18][19][16][33][14][42]	Abuse Elevation Control Mechanism: Sudo and Sudo Caching, Abuse Elevation Control Mechanism: Bypass User Account Control, Access Token Manipulation: Token Impersonation/Theft, Access Token Manipulation: Make and Impersonate Token, Access Token Manipulation: Parent PID Spoofing, Account Discovery: Domain Account, Application Layer Protocol: Web Protocols, Application Layer Protocol: DNS, Application Layer Protocol, BITS Jobs, Browser Session Hijacking, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: JavaScript, Command and Scripting Interpreter: Windows Command Shell, Command and Scripting Interpreter: Python, Command and Scripting Interpreter: Visual Basic, Commonly Used Port, Create or Modify System Process: Windows Service, Data Encoding: Standard Encoding, Data from Local System, Data Obfuscation: Protocol Impersonation, Data Transfer Size Limits, Deobfuscate/Decode Files or Information, Encrypted Channel: Asymmetric Cryptography, Encrypted Channel: Symmetric Cryptography, Exploitation for Client Execution, Exploitation for Privilege Escalation, File and Directory Discovery, Hide Artifacts: Process Argument Spoofing, Impair Defenses: Disable or Modify Tools, Indicator Removal on Host: Timestomp, Ingress Tool Transfer, Input Capture: Keylogging, Modify Registry, Multiband Communication, Native API, Network Service Discovery, Network Share Discovery, Non-Application Layer Protocol, Obfuscated Files or Information, Obfuscated Files or Information: Indicator Removal from Tools, Office Application Startup: Office Template Macros, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Security Account Manager, Permission Groups Discovery: Domain Groups, Permission Groups Discovery: Local Groups, Process Discovery, Process Injection: Process Hollowing, Process Injection: Dynamic-link Library Injection, Process Injection, Protocol Tunneling, Proxy: Internal Proxy, Proxy: Domain Fronting, Query Registry, Reflective Code Loading, Remote Services: Remote Desktop Protocol, Remote Services: Distributed Component Object Model, Remote Services: Windows Remote Management, Remote Services: SSH, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, Scheduled Transfer, Screen Capture, Software Discovery, Subvert Trust Controls: Code Signing, System Binary Proxy Execution: Rundll32, System Network Configuration Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, Use Alternate Authentication Material: Pass the Hash, Valid Accounts: Domain Accounts, Valid Accounts: Local Accounts, Windows Management Instrumentation
S0050	CosmicDuke	[3][15]	Application Layer Protocol: Web Protocols, Automated Exfiltration, Clipboard Data, Create or Modify System Process: Windows Service, Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores, Data from Local System, Data from Network Shared Drive, Data from Removable Media, Email Collection: Local Email Collection, Encrypted Channel: Symmetric Cryptography, Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol, Exploitation for Privilege Escalation, File and Directory Discovery, Input Capture: Keylogging, OS Credential Dumping: Security Account Manager, OS Credential Dumping: LSA Secrets, Scheduled Task/Job: Scheduled Task, Screen Capture
S0046	CozyCar	[3][15]	Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Masquerading: Rename System Utilities, Obfuscated Files or Information, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Security Account Manager, Scheduled Task/Job: Scheduled Task, Software Discovery: Security Software Discovery, System Binary Proxy Execution: Rundll32, System Information Discovery, Virtualization/Sandbox Evasion, Web Service: Bidirectional Communication
S0634	EnvyScout	[19]	Command and Scripting Interpreter: JavaScript, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, Deobfuscate/Decode Files or Information, Execution Guardrails, Forced Authentication, Hide Artifacts: Hidden Files and Directories, Masquerading, Obfuscated Files or Information, Obfuscated Files or Information: HTML Smuggling, Phishing: Spearphishing Attachment, System Binary Proxy Execution: Rundll32, System Information Discovery, User Execution: Malicious File
S0512	FatDuke	[22][15]	Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: PowerShell, Data from Local System, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Fallback Channels, File and Directory Discovery, Indicator Removal on Host: File Deletion, Masquerading, Native API, Obfuscated Files or Information: Binary Padding, Obfuscated Files or Information, Obfuscated Files or Information: Software Packing, Process Discovery, Proxy: Internal Proxy, Query Registry, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration Discovery, Virtualization/Sandbox Evasion: Time Based Evasion

ID	Name	References	Techniques
S0661	FoggyWeb	[43]	Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Library, Archive Collected Data: Archive via Custom Method, Data from Local System, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Exfiltration Over C2 Channel, File and Directory Discovery, Hijack Execution Flow: DLL Search Order Hijacking, Ingress Tool Transfer, Masquerading, Masquerading: Match Legitimate Name or Location, Native API, Network Sniffing, Obfuscated Files or Information, Obfuscated Files or Information: Compile After Delivery, Process Discovery, Reflective Code Loading, Shared Modules, Unsecured Credentials: Private Keys, Use Alternate Authentication Material
S0049	GeminiDuke	[3]	Account Discovery: Local Account, Application Layer Protocol: Web Protocols, File and Directory Discovery, Process Discovery, System Network Configuration Discovery, System Service Discovery
S0597	GoldFinder	[10][13][19][14]	Application Layer Protocol: Web Protocols, Automated Collection, System Network Configuration Discovery: Internet Connection Discovery
S0588	GoldMax	[10][13][18][19][14]	Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: Windows Command Shell, Data Obfuscation: Junk Data, Deobfuscate/Decode Files or Information, Encrypted Channel: Asymmetric Cryptography, Exfiltration Over C2 Channel, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Masquerading: Masquerade Task or Service, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information, Scheduled Task/Job: Scheduled Task, Scheduled Task/Job: Cron, System Network Configuration Discovery, System Time Discovery, Virtualization/Sandbox Evasion: System Checks, Virtualization/Sandbox Evasion: Time Based Evasion
S0037	HAMMERTOSS	[3][15]	Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: PowerShell, Data Obfuscation: Steganography, Encrypted Channel: Symmetric Cryptography, Exfiltration Over Web Service: Exfiltration to Cloud Storage, Hide Artifacts: Hidden Window, Web Service: One-Way Communication
S0100	ipconfig	[44]	System Network Configuration Discovery
S0513	LiteDuke	[22][15]	Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Deobfuscate/Decode Files or Information, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information: Steganography, Query Registry, Software Discovery: Security Software Discovery, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, Virtualization/Sandbox Evasion: Time Based Evasion
S0175	meek	[24]	Proxy: Domain Fronting
S0002	Mimikatz	[3][39][17]	Access Token Manipulation: SID-History Injection, Account Manipulation, Boot or Logon Autostart Execution: Security Support Provider, Credentials from Password Stores: Windows Credential Manager, Credentials from Password Stores, Credentials from Password Stores: Credentials from Web Browsers, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Security Account Manager, OS Credential Dumping: DCSync, OS Credential Dumping: LSA Secrets, Rogue Domain Controller, Steal or Forge Kerberos Tickets: Golden Ticket, Steal or Forge Kerberos Tickets: Silver Ticket, Unsecured Credentials: Private Keys, Use Alternate Authentication Material: Pass the Ticket, Use Alternate Authentication Material: Pass the Hash
S0051	MiniDuke	[3][22][15]	Application Layer Protocol: Web Protocols, Dynamic Resolution: Domain Generation Algorithms, Fallback Channels, File and Directory Discovery, Ingress Tool Transfer, Obfuscated Files or Information, Proxy: Internal Proxy, System Information Discovery, Web Service: Dead Drop Resolver
S0637	NativeZone	[16]	Deobfuscate/Decode Files or Information, Execution Guardrails, Masquerading, System Binary Proxy Execution: Rundll32, User Execution: Malicious File, Virtualization/Sandbox Evasion: System Checks
S0039	Net	[44]	Account Discovery: Domain Account, Account Discovery: Local Account, Create Account: Local Account, Create Account: Domain Account, Indicator Removal on Host: Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery: Domain Groups, Permission Groups Discovery: Local Groups, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, System Time Discovery
S0052	OnionDuke	[3][22][15]	Application Layer Protocol: Web Protocols, Deobfuscate/Decode Files or Information, Endpoint Denial of Service, OS Credential Dumping, Web Service: One-Way Communication

ID	Name	References	Techniques
S0048	PinchDuke	[3]	Application Layer Protocol: Web Protocols, Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores, Data from Local System, File and Directory Discovery, OS Credential Dumping, System Information Discovery
S0518	PolyglotDuke	[22][15]	Application Layer Protocol: Web Protocols, Deobfuscate/Decode Files or Information, Ingress Tool Transfer, Modify Registry, Native API, Obfuscated Files or Information, Obfuscated Files or Information: Steganography, System Binary Proxy Execution: Rundll32, Web Service: Dead Drop Resolver
S0150	POSHSPY	[45]	Command and Scripting Interpreter: PowerShell, Data Transfer Size Limits, Dynamic Resolution: Domain Generation Algorithms, Encrypted Channel: Asymmetric Cryptography, Event Triggered Execution: Windows Management Instrumentation Event Subscription, Indicator Removal on Host: Timestomp, Ingress Tool Transfer, Obfuscated Files or Information
S0139	PowerDuke	[46]	Application Window Discovery, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Commonly Used Port, Data Destruction, File and Directory Discovery, Hide Artifacts: NTFS File Attributes, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Obfuscated Files or Information: Steganography, Process Discovery, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Time Discovery
S0029	PsExec	[3][22]	Create Account: Domain Account, Create or Modify System Process: Windows Service, Lateral Tool Transfer, Remote Services: SMB/Windows Admin Shares, System Services: Service Execution
S0565	Raindrop	[36][19][14]	Deobfuscate/Decode Files or Information, Masquerading, Masquerading: Match Legitimate Name or Location, Obfuscated Files or Information, Obfuscated Files or Information: Steganography, Obfuscated Files or Information: Software Packing, Virtualization/Sandbox Evasion: Time Based Evasion
S0511	RegDuke	[22][15]	Command and Scripting Interpreter: PowerShell, Deobfuscate/Decode Files or Information, Event Triggered Execution: Windows Management Instrumentation Event Subscription, Ingress Tool Transfer, Modify Registry, Obfuscated Files or Information, Obfuscated Files or Information: Steganography, Web Service: Bidirectional Communication
S0684	ROADTools	[25]	Account Discovery: Cloud Account, Automated Collection, Cloud Service Discovery, Permission Groups Discovery: Cloud Groups, Remote System Discovery, Valid Accounts: Cloud Accounts
S0195	SDelete	[24]	Data Destruction, Indicator Removal on Host: File Deletion
S0053	SeaDuke	[3][15]	Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Library, Boot or Logon Autostart Execution: Shortcut Modification, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Data Encoding: Standard Encoding, Email Collection: Remote Email Collection, Encrypted Channel: Symmetric Cryptography, Event Triggered Execution: Windows Management Instrumentation Event Subscription, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Obfuscated Files or Information: Software Packing, Use Alternate Authentication Material: Pass the Ticket, Valid Accounts
S0589	Sibot	[10][13][19][14]	Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: Visual Basic, Deobfuscate/Decode Files or Information, Indicator Removal on Host: File Deletion, Indicator Removal on Host, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Modify Registry, Obfuscated Files or Information, Query Registry, Scheduled Task/Job: Scheduled Task, System Binary Proxy Execution: Mshta, System Binary Proxy Execution: Rundll32, System Network Configuration Discovery, System Network Connections Discovery, Web Service, Windows Management Instrumentation
S0633	Sliver	[13][15]	Access Token Manipulation, Application Layer Protocol: Web Protocols, Application Layer Protocol: DNS, Data Encoding: Standard Encoding, Data Obfuscation: Steganography, Encrypted Channel: Symmetric Cryptography, Encrypted Channel: Asymmetric Cryptography, Exfiltration Over C2 Channel, File and Directory Discovery, Ingress Tool Transfer, Obfuscated Files or Information, Process Injection, Screen Capture, System Network Configuration Discovery, System Network Connections Discovery

ID	Name	References	Techniques
S0516	SoreFang	[23][44]	Account Discovery: Local Account, Account Discovery: Domain Account, Application Layer Protocol: Web Protocols, Deobfuscate/Decode Files or Information, Exploit Public-Facing Application, File and Directory Discovery, Ingress Tool Transfer, Obfuscated Files or Information, Permission Groups Discovery: Domain Groups, Process Discovery, Scheduled Task/Job: Scheduled Task, System Information Discovery, System Network Configuration Discovery
S0559	SUNBURST	[9][18][14]	Application Layer Protocol: Web Protocols, Application Layer Protocol: DNS, Command and Scripting Interpreter: Visual Basic, Data Encoding: Standard Encoding, Data from Local System, Data Obfuscation: Junk Data, Data Obfuscation: Steganography, Data Obfuscation: Protocol Impersonation, Dynamic Resolution, Encrypted Channel: Symmetric Cryptography, Event Triggered Execution: Image File Execution Options Injection, File and Directory Discovery, Impair Defenses: Disable or Modify Tools, Indicator Removal on Host, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Modify Registry, Obfuscated Files or Information: Indicator Removal from Tools, Obfuscated Files or Information, Process Discovery, Query Registry, Software Discovery: Security Software Discovery, Subvert Trust Controls: Code Signing, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Service Discovery, Virtualization/Sandbox Evasion: Time Based Evasion, Virtualization/Sandbox Evasion: System Checks, Windows Management Instrumentation
S0562	SUNSPOT	[11][19]	Access Token Manipulation, Data Manipulation: Stored Data Manipulation, Deobfuscate/Decode Files or Information, Execution Guardrails, File and Directory Discovery, Indicator Removal on Host: File Deletion, Masquerading: Match Legitimate Name or Location, Native API, Obfuscated Files or Information, Process Discovery, Supply Chain Compromise: Compromise Software Supply Chain
S0096	Systeminfo	[44]	System Information Discovery
S0057	Tasklist	[44]	Process Discovery, Software Discovery: Security Software Discovery, System Service Discovery
S0560	TEARDROP	[9][18][19][14]	Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, Masquerading: Match Legitimate Name or Location, Modify Registry, Obfuscated Files or Information, Query Registry
S0183	Tor	[24]	Encrypted Channel: Asymmetric Cryptography, Proxy: Multi-hop Proxy
S0682	TrailBlazer	[17]	Application Layer Protocol: Web Protocols, Data Obfuscation: Junk Data, Data Obfuscation, Event Triggered Execution: Windows Management Instrumentation Event Subscription, Masquerading
S0636	VaporRage	[19]	Application Layer Protocol: Web Protocols, Deobfuscate/Decode Files or Information, Execution Guardrails, Ingress Tool Transfer
S0515	WellMail	[47][23][13]	Archive Collected Data, Data from Local System, Deobfuscate/Decode Files or Information, Encrypted Channel: Asymmetric Cryptography, Ingress Tool Transfer, Non-Application Layer Protocol, Non-Standard Port, System Network Configuration Discovery, System Owner/User Discovery
S0514	WellMess	[37][38][48][23][13]	Application Layer Protocol: DNS, Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Data Encoding: Standard Encoding, Data from Local System, Data Obfuscation: Junk Data, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Encrypted Channel: Asymmetric Cryptography, Ingress Tool Transfer, Permission Groups Discovery: Domain Groups, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery

References

White House. (2021, April 15). Imposing Costs for Harmful Foreign Activities by the Russian Government. Retrieved April 16, 2021. UK Gov. (2021, April 15). UK and US expose global campaign of malign activity by Russian intelligence services . Retrieved April 16, 2021. F-Secure Labs. (2015, September 17). The Dukes: 7 years of Russian cyberespionage. Retrieved December 10, 2015. Department of Homeland Security and Federal Bureau of Investigation. (2016, December 29). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Retrieved January 11, 2017. Alperovitch, D.. (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee. Retrieved August 3, 2016. UK Gov. (2021, April 15). UK exposes Russian involvement in SolarWinds cyber compromise . Retrieved April 16, 2021. NSA, FBI, DHS. (2021, April 15). Russian SVR Targets U.S. and Allied Networks. Retrieved April 16, 2021. UK NCSC. (2021, April 15). UK and US call out Russia for SolarWinds compromise. Retrieved April 16, 2021. FireEye. (2020, December 13). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. Retrieved January 4, 2021. Nafisi, R., Lelli, A. (2021, March 4).

GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's layered persistence. Retrieved March 8, 2021. CrowdStrike Intelligence Team. (2021, January 11). SUNSPOT: An Implant in the Build Process. Retrieved January 11, 2021. Cash, D. et al. (2020, December 14). Dark Halo Leverages SolarWinds Compromise to Breach Organizations. Retrieved December 29, 2020. NCSC, CISA, FBI, NSA. (2021, May 7). Further TTPs associated with SVR cyber actors. Retrieved July 29, 2021. Secureworks CTU. (n.d.). IRON RITUAL. Retrieved February 24, 2022. Secureworks CTU. (n.d.). IRON HEMLOCK. Retrieved February 22, 2022. Guerrero-Saade, J. (2021, June 1). NobleBaron | New Poisoned Installers Could Be Used In Supply Chain Attacks. Retrieved August 4, 2021. CrowdStrike. (2022, January 27). Early Bird Catches the Wormhole: Observations from the StellarParticle Campaign. Retrieved February 7, 2022. Microsoft Threat Intelligence Center (MSTIC). (2021, May 27). New sophisticated email-based attack from NOBELIUM. Retrieved May 28, 2021. MSTIC. (2021, May 28). Breaking down NOBELIUM's latest early-stage toolset. Retrieved August 4, 2021. MSRC. (2021, June 25). New Nobelium activity. Retrieved August 4, 2021. Microsoft Defender Research Team. (2018, December 3). Analysis of cyberattack on U.S. think tanks, non-profits, public sector by unidentified attackers. Retrieved April 15, 2019. Faou, M., Tartare, M., Dupuy, T. (2019, October). OPERATION GHOST. Retrieved September 23, 2020. National Cyber Security Centre. (2020, July 16). Advisory: APT29 targets COVID-19 vaccine development. Retrieved September 29, 2020. Dunwoody, M. and Carr, N.. (2016, September 27). No Easy Breach DerbyCon 2016. Retrieved October 4, 2016. Microsoft Threat Intelligence Center. (2021, October 25). NOBELIUM targeting delegated administrative privileges to facilitate broader attacks. Retrieved March 25, 2022. MSRC. (2020, December 13). Customer Guidance on Recent Nation-State Cyber Attacks. Retrieved December 30, 2020. Smith, L., Leathery, J., Read, B. (2021, March 4). New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeting U.S.-Based Entity; Possible Connection to UNC2452. Retrieved March 12, 2021. FireEye Labs. (2015, July). HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group. Retrieved September 17, 2015. MSTIC, CDOC, 365 Defender Research Team. (2021, January 20). Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop . Retrieved January 22, 2021. Dunwoody, M., et al. (2018, November 19). Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign. Retrieved November 27, 2018. MSTIC. (2020, December 18). Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers . Retrieved January 5, 2021. Symantec Security Response. (2015, July 13). "Forkmeiamfamous": Seaduke, latest weapon in the Duke armory. Retrieved July 22, 2015. ESET. (2022, February). THREAT REPORT T3 2021. Retrieved February 10, 2022. ANSSI. (2021, December 6). PHISHING CAMPAIGNS BY THE NOBELIUM INTRUSION SET. Retrieved April 13, 2022. MSRC Team. (2021, February 18). Microsoft Internal Solorigate Investigation – Final Update. Retrieved May 14, 2021. Symantec Threat Hunter Team. (2021, January 18). Raindrop: New Malware Discovered in SolarWinds Investigation. Retrieved January 19, 2021. PWC. (2020, July 16). How WellMess malware has been used to target COVID-19 vaccines. Retrieved September 24, 2020. PWC. (2020, August 17). WellMess malware: analysis of its Command and Control (C2) server. Retrieved September 29, 2020. Microsoft 365 Defender Team. (2020, December 28). Using Microsoft 365 Defender to protect against Solorigate. Retrieved January 7, 2021. Dunwoody, M. (2017, March 27). APT29 Domain Fronting With TOR. Retrieved March 27, 2017. Luke Jenkins, Sarah Hawley, Parnian Najafi, Doug Bienstock. (2021, December 6). Suspected Russian Activity Targeting Government and Business Entities Around the Globe. Retrieved April 15, 2022. Secureworks CTU. (2021, May 28). USAID-Themed Phishing Campaign Leverages U.S. Elections Lure. Retrieved February 24, 2022. Ramin Nafisi. (2021, September 27). FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor. Retrieved October 4, 2021. CISA. (2020, July 16). MAR-10296782-1.v1 – SOREFANG. Retrieved September 29, 2020. Dunwoody, M.. (2017, April 3). Dissecting One of APT29's Fileless WMI and PowerShell Backdoors (POSHSPY). Retrieved April 5, 2017. Adair, S.. (2016, November 9). PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs. Retrieved January 11, 2017. CISA. (2020, July 16). MAR-10296782-3.v1 – WELLMAIL. Retrieved September 29, 2020. CISA. (2020, July 16). MAR-10296782-2.v1 – WELLMESS. Retrieved September 24, 2020.