Intell917

Techniques Used by Lazarus Group

Domain	ID	Name	Use	Column1
Enterprise	T1134	.002	Access Token Manipulation: Create Process with Token	Lazarus Group keylogger KiloAlfa obtains user tokens from interactive sessions to execute itself with API call `CreateProcessAsUserA` under that user's context.[3][8]
Enterprise	T1087	.002	Account Discovery: Domain Account	Lazarus Group has queried an active directory server to obtain the list of accounts, including administrator accounts.[9]
Enterprise	T1098		Account Manipulation	Lazarus Group malware WhiskeyDelta-Two contains a function that attempts to rename the administrator's account.[3][10]
Enterprise	T1583	.001	Acquire Infrastructure: Domains	Lazarus Group has acquired domains related to their campaigns to act as distribution points and C2 channels.[11][9][12]
		.004	Acquire Infrastructure: Server	Lazarus Group has acquired servers to host their malicious tools.[9]
		.006	Acquire Infrastructure: Web Services	Lazarus Group has hosted malicious downloads on Github and Dropbox.[11][13]
Enterprise	T1557	.001	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	Lazarus Group executed Responder using the command `[Responder file path] -i [IP address] -rPv` on a compromised host to harvest credentials and move laterally.[14]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Lazarus Group has conducted C2 over HTTP and HTTPS.[15][16][17][18][19][20][21]
Enterprise	T1010		Application Window Discovery	Lazarus Group malware IndiaIndia obtains and sends to its C2 server the title of the window for each running process. The KilaAlfa keylogger also reports the title of the window in the foreground.[3][22][8]
Enterprise	T1560		Archive Collected Data	Lazarus Group has compressed exfiltrated data with RAR and used RomeoDelta malware to archive specified directories in .zip format, encrypt the .zip file, and upload it to C2. [22][23][15][9]
		.002	Archive via Library	Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is compressed with Zlib, encrypted, and uploaded to a C2 server.[23][15]
		.003	Archive via Custom Method	A Lazarus Group malware sample encrypts data using a simple byte based XOR operation prior to exfiltration.[3][22][23][15]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Lazarus Group has maintained persistence by loading malicious code into a startup folder or by adding a Registry Run key.[3][23][15][18][19]
		.009	Boot or Logon Autostart Execution: Shortcut Modification	Lazarus Group malware has maintained persistence on a system by creating a LNK shortcut in the user's Startup folder.[15][13]
Enterprise	T1110		Brute Force	Lazarus Group has performed brute force attacks against administrator accounts.[9]
		.003	Password Spraying	Lazarus Group malware attempts to connect to Windows shares for lateral movement by using a generated list of usernames, which center around permutations of the username Administrator, and weak passwords.[3][23]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Lazarus Group has used PowerShell to execute commands and malicious code.[9][12]
		.003	Command and Scripting Interpreter: Windows Command Shell	Lazarus Group malware uses cmd.exe to execute commands on a compromised host.[3][10][15][24][20] A Destover-like variant used by Lazarus Group uses a batch file mechanism to delete its binaries from the system.[25]
		.005	Command and Scripting Interpreter: Visual Basic	Lazarus Group has used VBA and embedded macros in Word documents to execute malicious code.[18][13][19][20]
Enterprise	T1584	.001	Compromise Infrastructure: Domains	Lazarus Group has compromised legitimate domains, including those hosted in the US and Italy, for C2.[26]
		.004	Compromise Infrastructure: Server	Lazarus Group has compromised servers to stage malicious tools.[14][13][9][18]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Several Lazarus Group malware families install themselves as new services.[3][10]
Enterprise	T1485		Data Destruction	Lazarus Group has used a custom secure delete function to overwrite file contents with data from heap memory.[3]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	A Lazarus Group malware sample encodes data with base64.[15]
Enterprise	T1005		Data from Local System	Lazarus Group has collected data and files from compromised networks.[3][22][23][14][13][18]
Enterprise	T1001	.003	Data Obfuscation: Protocol Impersonation	Lazarus Group malware also uses a unique form of communication encryption known as FakeTLS that mimics TLS but uses a different encryption method, potentially evading SSL traffic inspection/decryption.[3][10][15][25]
Enterprise	T1074	.001	Data Staged: Local Data Staging	Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is saved in the %TEMP% directory, then compressed, encrypted, and uploaded to a C2 server.[3][22]
Enterprise	T1491	.001	Defacement: Internal Defacement	Lazarus Group replaced the background wallpaper of systems with a threatening image after rendering the system unbootable with a Disk Structure Wipe.[10]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Lazarus Group has used shellcode within macros to decrypt and manually map DLLs and shellcode into memory at runtime.[19][20]
Enterprise	T1587	.001	Develop Capabilities: Malware	Lazarus Group has developed custom malware for use in their operations.[11][9][12][13]
Enterprise	T1561	.001	Disk Wipe: Disk Content Wipe	Lazarus Group has used malware like WhiskeyAlfa to overwrite the first 64MB of every drive with a mix of static and random buffers. A similar process is then used to wipe content in logical drives and, finally, attempt to wipe every byte of every sector on every drive. WhiskeyBravo can be used to overwrite the first 4.9MB of physical drives. WhiskeyDelta can overwrite the first 132MB or 1.5MB of each drive with random data from heap memory.[10]
		.002	Disk Wipe: Disk Structure Wipe	Lazarus Group malware SHARPKNOT overwrites and deletes the Master Boot Record (MBR) on the victim's machine and has possessed MBR wiper malware since at least 2009.[24][3]

Enterprise	T1189		Drive-by Compromise	Lazarus Group delivered RATANKBA and other malicious code to victims via a compromised legitimate website.[27][12]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Several Lazarus Group malware families encrypt C2 traffic using custom code that uses XOR with an ADD operation and XOR with a SUB operation. Another Lazarus Group malware sample XORs C2 traffic. Other Lazarus Group malware uses Caracachs encryption to encrypt C2 payloads. Lazarus Group has also used AES to encrypt C2 traffic.[3][10][15][25][18]
Enterprise	T1585	.001	Establish Accounts: Social Media Accounts	Lazarus Group has created new LinkedIn and Twitter accounts to conduct social engineering against potential victims.[13][9][12]
		.002	Establish Accounts: Email Accounts	Lazarus Group has created new email accounts for spearphishing operations.[9][14]
Enterprise	T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Lazarus Group malware SierraBravo-Two generates an email message via SMTP containing information about newly infected victims.[3][23]
Enterprise	T1041		Exfiltration Over C2 Channel	Lazarus Group has exfiltrated data and files over a C2 channel through its various tools and malware.[3][22][15][26]
Enterprise	T1567	.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Lazarus Group has exfiltrated stolen data to Dropbox using a customized version of dbxcli.[9][13]
Enterprise	T1203		Exploitation for Client Execution	Lazarus Group has exploited Adobe Flash vulnerability CVE-2018-4878 for execution.[28]
Enterprise	T1008		Fallback Channels	Lazarus Group malware SierraAlfa sends data to one of the hard-coded C2 servers chosen at random, and if the transmission fails, chooses a new C2 server to attempt the transmission again.[3][23]
Enterprise	T1083		File and Directory Discovery	Several Lazarus Group has conducted word searches on compromised machines to identify specific documents of interest. Lazarus Group malware can use a common function to identify target files by their extension, and some also enumerate files and directories, including a Destover-like variant that lists files and gathers information for all drives.[3][25][13][19][20]
Enterprise	T1589	.002	Gather Victim Identity Information: Email Addresses	Lazarus Group collected email addresses belonging to various departments of a targeted organization which were used in follow-on phishing campaigns.[14]
Enterprise	T1591		Gather Victim Org Information	Lazarus Group has studied publicly available information about a targeted organization to tailor spearphishing efforts against specific departments and/or individuals.[9][13][14]
		.004	Identify Roles	Lazarus Group has targeted specific individuals within an organization with tailored job vacancy announcements.[9][13]
Enterprise	T1564	.001	Hide Artifacts: Hidden Files and Directories	Lazarus Group has used a VBA Macro to set its file attributes to System and Hidden and has named files with a dot prefix to hide them from the Finder application.[15][16][17][19]
Enterprise	T1574	.002	Hijack Execution Flow: DLL Side-Loading	Lazarus Group has replaced `win_fw.dll`, an internal component that is executed during IDA Pro installation, with a malicious DLL to download and execute a payload.[21]
		.013	Hijack Execution Flow: KernelCallbackTable	Lazarus Group has abused the `KernelCallbackTable` to hijack process control flow and execute shellcode.[19][20]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	Lazarus Group malware TangoDelta attempts to terminate various processes associated with McAfee. Additionally, Lazarus Group malware SHARPKNOT disables the Microsoft Windows System Event Notification and Alerter services.[3][22][8][24].
		.004	Impair Defenses: Disable or Modify System Firewall	Various Lazarus Group malware modifies the Windows firewall to allow incoming connections or disable it entirely using netsh. [3][22][8]
Enterprise	T1070		Indicator Removal	Lazarus Group has restored malicious KernelCallbackTable code to its original state after the process execution flow has been hijacked.[19]
		.003	Clear Command History	Lazarus Group has routinely deleted log files on a compromised router, including automatic log deletion through the use of the logrotate utility.[14]
		.004	File Deletion	Lazarus Group malware has deleted files in various ways, including "suicide scripts" to delete malware binaries from the victim. Lazarus Group also uses secure file deletion to delete files from the victim.[3][25]
		.006	Timestomp	Several Lazarus Group malware families use timestomping, including modifying the last write timestamp of a specified Registry key to a random date, as well as copying the timestamp for legitimate .exe files (such as calc.exe or mspaint.exe) to its dropped files.[3][10][22][25]
Enterprise	T1202		Indirect Command Execution	Lazarus Group persistence mechanisms have used `forfiles.exe` to execute .htm files.[20]
Enterprise	T1105		Ingress Tool Transfer	Lazarus Group has downloaded files, malware, and tools from its C2 onto a compromised host.[3][10][22][16][17][13][14][18][9][12][19][20][21]
Enterprise	T1056	.001	Input Capture: Keylogging	Lazarus Group malware KiloAlfa contains keylogging functionality.[3][8]
Enterprise	T1534		Internal Spearphishing	Lazarus Group has conducted internal spearphishing from within a compromised organization.[13]
Enterprise	T1036		Masquerading	Lazarus Group has disguised malicious template files as JPEG files to avoid detection.[18]
		.003	Rename System Utilities	Lazarus Group has renamed system utilities such as `wscript.exe` and `mshta.exe`.[20]
		.004	Masquerade Task or Service	Lazarus Group has used a scheduled task named `SRCheck` to mask the execution of a malicious .dll.[21]
		.005	Match Legitimate Name or Location	Lazarus Group has renamed malicious code to disguise it as Microsoft's narrator and other legitimate files.[29][9][20]
Enterprise	T1104		Multi-Stage Channels	Lazarus Group has used multi-stage malware components that inject later stages into separate processes.[19]
Enterprise	T1106		Native API	Lazarus Group has used the Windows API `ObtainUserAgentString` to obtain the User-Agent from a compromised host to connect to a C2 server.[18] Lazarus Group has also used various, often lesser known, functions to perform various types of Discovery and Process Injection.[19][20]
Enterprise	T1046		Network Service Discovery	Lazarus Group has used nmap from a router VM to scan ports on systems within the restricted segment of an enterprise network.[14]

Enterprise	T1571		Non-Standard Port	Some Lazarus Group malware uses a list of ordered port numbers to choose a port for C2 traffic, creating port-protocol mismatches.[3][23]
Enterprise	T1027		Obfuscated Files or Information	Lazarus Group has used multiple types of encryption and encoding for their payloads, including AES, Caracachs, RC4, XOR, Base64, and other tricks such as creating aliases in code for Native API function names.[3][22][23][15][17][9][18][26][13][19][20]
		.002	Software Packing	Lazarus Group has used Themida to pack malicious DLLs and other files.[13][26]
		.007	Dynamic API Resolution	Lazarus Group has used a custom hashing method to resolve APIs used in shellcode.[19]
Enterprise	T1588	.002	Obtain Capabilities: Tool	Lazarus Group has obtained a variety of tools for their operations, including Responder, PuTTy PSCP, Wake-On-Lan, ChromePass, and dbxcli.[9][13][14]
		.003	Obtain Capabilities: Code Signing Certificates	Lazarus Group has used code signing certificates issued by Sectigo RSA for some of its malware and tools.[9]
		.004	Obtain Capabilities: Digital Certificates	Lazarus Group has obtained SSL certificates for their C2 domains.[11]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Lazarus Group has targeted victims with spearphishing emails containing malicious Microsoft Word documents.[28][14][18][19][20]
		.002	Phishing: Spearphishing Link	Lazarus Group has sent malicious links to victims via email.[14][13][9]
		.003	Phishing: Spearphishing via Service	Lazarus Group has used social media platforms, including LinkedIn and Twitter, to send spearphishing messages.[12][13][9]
Enterprise	T1542	.003	Pre-OS Boot: Bootkit	Lazarus Group malware WhiskeyAlfa-Three modifies sector 0 of the Master Boot Record (MBR) to ensure that the malware will persist even if a victim machine shuts down.[3][10]
Enterprise	T1057		Process Discovery	Several Lazarus Group malware families gather a list of running processes on a victim system and send it to their C2 server. A Destover-like variant used by Lazarus Group also gathers process times.[3][22][15][25][17][19]
Enterprise	T1055	.001	Process Injection: Dynamic-link Library Injection	A Lazarus Group malware sample performs reflective DLL injection.[15][19]
Enterprise	T1090	.001	Proxy: Internal Proxy	Lazarus Group has used a compromised router to serve as a proxy between a victim network's corporate and restricted segments.[14]
		.002	Proxy: External Proxy	Lazarus Group has used multiple proxies to obfuscate network traffic from victims.[30][17]
Enterprise	T1012		Query Registry	Lazarus Group malware IndiaIndia checks Registry keys within HKCU and HKLM to determine if certain applications are present, including SecureCRT, Terminal Services, RealVNC, TightVNC, UltraVNC, Radmin, mRemote, TeamViewer, FileZilla, pcAnyware, and Remote Desktop. Another Lazarus Group malware sample checks for the presence of the following Registry key:`HKEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt`.[3][22][15]
Enterprise	T1620		Reflective Code Loading	Lazarus Group has changed memory protection permissions then overwritten in memory DLL function code with shellcode, which was later executed via KernelCallbackTable hijacking. Lazarus Group has also used shellcode within macros to decrypt and manually map DLLs into memory at runtime.[19][20]
Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	Lazarus Group malware SierraCharlie uses RDP for propagation.[3][23]
		.002	Remote Services: SMB/Windows Admin Shares	Lazarus Group malware SierraAlfa accesses the `ADMIN$` share via SMB to conduct lateral movement.[3][23]
		.004	Remote Services: SSH	Lazarus Group used SSH and the PuTTy PSCP utility to gain access to a restricted segment of a compromised network.[14]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Lazarus Group has used `schtasks` for persistence including through the periodic execution of a remote XSL script or a dropped VBS payload.[9][20][21]
Enterprise	T1593	.001	Search Open Websites/Domains: Social Media	Lazarus Group has used LinkedIn to identify and target specific employees within a chosen organization.[9][13]
Enterprise	T1489		Service Stop	Lazarus Group has stopped the MSExchangeIS service to render Exchange contents inaccessible to users.[10]
Enterprise	T1608	.001	Stage Capabilities: Upload Malware	Lazarus Group has hosted malicious files on compromised as well as Lazarus Group-controlled servers.[13][9][26]
		.002	Stage Capabilities: Upload Tool	Lazarus Group has hosted custom and open-source tools on compromised as well as Lazarus Group-controlled servers.[9]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	Lazarus Group has digitally signed malware and utilities to evade detection.[9][19]
Enterprise	T1218		System Binary Proxy Execution	Lazarus Group lnk files used for persistence have abused the Windows Update Client (`wuauclt.exe`) to execute a malicious DLL.[19][20]
		.005	Mshta	Lazarus Group has used `mshta.exe` to execute HTML pages downloaded by initial access documents.[19][20]
		.010	Regsvr32	Lazarus Group has used rgsvr32 to execute custom malware.[9]
		.011	Rundll32	Lazarus Group has used rundll32 to execute malicious payloads on a compromised host.[18][9][21]
Enterprise	T1082		System Information Discovery	Several Lazarus Group malware families collect information on the type and version of the victim OS, as well as the victim computer name and CPU information. A Destover-like variant used by Lazarus Group also collects disk space information and sends it to its C2 server.[3][10][22][15][25][19]
Enterprise	T1614	.001	System Location Discovery: System Language Discovery	Lazarus Group has deployed malware designed not to run on computers set to Korean, Japanese, or Chinese in Windows language preferences.[13]
Enterprise	T1016		System Network Configuration Discovery	Lazarus Group malware IndiaIndia obtains and sends to its C2 server information about the first network interface card's configuration, including IP address, gateways, subnet mask, DHCP information, and whether WINS is available.[3][22]
Enterprise	T1049		System Network Connections Discovery	Lazarus Group has used `net use` to identify and establish a network connection with a remote host.[14]
Enterprise	T1033		System Owner/User Discovery	Various Lazarus Group malware enumerates logged-on users.[3][10][22][23][15][16][19]

Enterprise	T1529		System Shutdown/Reboot	Lazarus Group has rebooted systems after destroying files and wiping the MBR on infected systems.[24]
Enterprise	T1124		System Time Discovery	A Destover-like implant used by Lazarus Group can obtain the current system time and send it to the C2 server.[25]
Enterprise	T1221		Template Injection	Lazarus Group has used DOCX files to retrieve a malicious document template/DOTM file.[13][18]
Enterprise	T1204	.001	User Execution: Malicious Link	Lazarus Group has sent spearphishing emails in an attempt to lure users to click on a malicious link.[9][13]
		.002	User Execution: Malicious File	Lazarus Group has attempted to get users to launch a malicious Microsoft Word attachment delivered via a spearphishing email.[28][13][14][19][20]
Enterprise	T1078		Valid Accounts	Lazarus Group has used administrator credentials to gain access to restricted network segments.[14]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	Lazarus Group has used tools to detect sandbox or VMware services through identifying the presence of a debugger or related services.[13]
Enterprise	T1102	.002	Web Service: Bidirectional Communication	Lazarus Group has used GitHub as C2, pulling hosted image payloads then committing command execution output to files in specific directories.[19]
Enterprise	T1047		Windows Management Instrumentation	Lazarus Group has used WMIC for discovery as well as to execute payloads for persistence and lateral movement.[3][23][13][14][20]
Enterprise	T1220		XSL Script Processing	Lazarus Group has used WMIC to execute a remote XSL script to establish persistence.[9]
ICS	T0865		Spearphishing Attachment	Lazarus Group has been observed targeting organizations using spearphishing documents with embedded malicious payloads. [31] Highly targeted spear phishing campaigns have been conducted against a U.S. electric grid company. [32]
Total				111

Software

ID	Name	References	Techniques
S0584	AppleJeus	[11]	Abuse Elevation Control Mechanism: Bypass User Account Control, Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: Unix Shell, Create or Modify System Process: Windows Service, Create or Modify System Process: Launch Daemon, Deobfuscate/Decode Files or Information, Event Triggered Execution: Installer Packages, Exfiltration Over C2 Channel, Hide Artifacts: Hidden Files and Directories, Indicator Removal: File Deletion, Obfuscated Files or Information, Phishing: Spearphishing Link, Scheduled Task/Job: Scheduled Task, Subvert Trust Controls: Code Signing, System Binary Proxy Execution: Msiexec, System Information Discovery, System Services: Launchctl, User Execution: Malicious Link, User Execution: Malicious File, Virtualization/Sandbox Evasion: Time Based Evasion
S0347	AuditCred	[33]	Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, File and Directory Discovery, Indicator Removal: File Deletion, Ingress Tool Transfer, Obfuscated Files or Information, Process Injection, Proxy
S0245	BADCALL	[34]	Data Obfuscation: Protocol Impersonation, Encrypted Channel: Symmetric Cryptography, Impair Defenses: Disable or Modify System Firewall, Modify Registry, Non-Standard Port, Proxy, System Information Discovery, System Network Configuration Discovery
S0239	Bankshot	[28]	Access Token Manipulation: Create Process with Token, Account Discovery: Local Account, Account Discovery: Domain Account, Application Layer Protocol: Web Protocols, Automated Collection, Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Data Encoding: Non-Standard Encoding, Data from Local System, Data Obfuscation: Protocol Impersonation, Deobfuscate/Decode Files or Information, Exfiltration Over C2 Channel, Exploitation for Client Execution, File and Directory Discovery, Indicator Removal: Timestomp, Indicator Removal: File Deletion, Indicator Removal, Ingress Tool Transfer, Modify Registry, Native API, Non-Standard Port, Process Discovery, Query Registry, System Information Discovery

S0520	BLINDINGCAN	[35]	Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: Windows Command Shell, Data Encoding: Standard Encoding, Data from Local System, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Exfiltration Over C2 Channel, File and Directory Discovery, Indicator Removal: File Deletion, Indicator Removal: Timestomp, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information, Phishing: Spearphishing Attachment, Shared Modules, Subvert Trust Controls: Code Signing, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration Discovery, User Execution: Malicious File
S0498	Cryptoistic	[16]	Data from Local System, Encrypted Channel, File and Directory Discovery, Indicator Removal: File Deletion, Ingress Tool Transfer, Non-Application Layer Protocol, System Owner/User Discovery
S0497	Dacls	[16][17]	Application Layer Protocol: Web Protocols, Create or Modify System Process: Launch Daemon, Create or Modify System Process: Launch Agent, File and Directory Discovery, Hide Artifacts: Hidden Files and Directories, Ingress Tool Transfer, Masquerading, Obfuscated Files or Information, Process Discovery
S0567	Dtrack	[36]	Archive Collected Data, Boot or Logon Autostart Execution, Browser Bookmark Discovery, Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Data from Local System, Data Staged: Local Data Staging, Deobfuscate/Decode Files or Information, File and Directory Discovery, Hijack Execution Flow, Indicator Removal: File Deletion, Ingress Tool Transfer, Input Capture: Keylogging, Masquerading: Match Legitimate Name or Location, Obfuscated Files or Information: Embedded Payloads, Process Discovery, Process Injection: Process Hollowing, Query Registry, Shared Modules, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, Valid Accounts
S0593	ECCENTRICBANDWAGON	[37]	Command and Scripting Interpreter: Windows Command Shell, Data Staged: Local Data Staging, Indicator Removal: File Deletion, Input Capture: Keylogging, Obfuscated Files or Information, Screen Capture
S0181	FALLCHILL	[30]	Create or Modify System Process: Windows Service, Data Obfuscation: Protocol Impersonation, Encrypted Channel: Symmetric Cryptography, File and Directory Discovery, Indicator Removal: File Deletion, Indicator Removal: Timestomp, System Information Discovery, System Network Configuration Discovery
S0246	HARDRAIN	[38]	Command and Scripting Interpreter: Windows Command Shell, Data Obfuscation: Protocol Impersonation, Impair Defenses: Disable or Modify System Firewall, Non-Standard Port, Proxy
S0376	HOPLIGHT	[5]	Command and Scripting Interpreter: Windows Command Shell, Data Encoding: Standard Encoding, Exfiltration Over C2 Channel, Fallback Channels, File and Directory Discovery, Impair Defenses: Disable or Modify System Firewall, Ingress Tool Transfer, Modify Registry, Non-Standard Port, OS Credential Dumping: Security Account Manager, Process Injection, Proxy, Query Registry, System Information Discovery, System Services: Service Execution, System Time Discovery, Use Alternate Authentication Material: Pass the Hash, Windows Management Instrumentation
S0431	HotCroissant	[39]	Application Window Discovery, Command and Scripting Interpreter: Windows Command Shell, Encrypted Channel: Symmetric Cryptography, Exfiltration Over C2 Channel, File and Directory Discovery, Hide Artifacts: Hidden Window, Indicator Removal: File Deletion, Ingress Tool Transfer, Native API, Obfuscated Files or Information, Obfuscated Files or Information: Software Packing, Process Discovery, Scheduled Task/Job: Scheduled Task, Screen Capture, Service Stop, Software Discovery, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Service Discovery
S0271	KEYMARBLE	[40]	Command and Scripting Interpreter: Windows Command Shell, Encrypted Channel: Symmetric Cryptography, File and Directory Discovery, Indicator Removal: File Deletion, Ingress Tool Transfer, Modify Registry, Process Discovery, Screen Capture, System Information Discovery, System Network Configuration Discovery

S0108	netsh	[22]	Event Triggered Execution: Netsh Helper DLL, Impair Defenses: Disable or Modify System Firewall, Proxy, Software Discovery: Security Software Discovery
S0238	Proxysvc	[25]	Application Layer Protocol: Web Protocols, Automated Collection, Command and Scripting Interpreter: Windows Command Shell, Data Destruction, Data from Local System, Exfiltration Over C2 Channel, File and Directory Discovery, Indicator Removal: File Deletion, Process Discovery, Query Registry, System Information Discovery, System Network Configuration Discovery, System Services: Service Execution, System Time Discovery
S0241	RATANKBA	[41]	Account Discovery: Local Account, Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Ingress Tool Transfer, Process Discovery, Process Injection: Dynamic-link Library Injection, Query Registry, Remote System Discovery, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Owner/User Discovery, System Service Discovery, Windows Management Instrumentation
S0364	RawDisk	[3][10]	Data Destruction, Disk Wipe: Disk Content Wipe, Disk Wipe: Disk Structure Wipe
S0174	Responder	[13]	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Network Sniffing
S0103	route	[14]	System Network Configuration Discovery
S0586	TAINTEDSCRIBE	[29]	Archive Collected Data, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Data Obfuscation: Protocol Impersonation, Encrypted Channel: Symmetric Cryptography, Fallback Channels, File and Directory Discovery, Indicator Removal: File Deletion, Indicator Removal: Timestomp, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Obfuscated Files or Information: Binary Padding, Process Discovery, Remote System Discovery, System Information Discovery, System Time Discovery
S0665	ThreatNeedle	[14]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Create or Modify System Process: Windows Service, Data from Local System, Deobfuscate/Decode Files or Information, File and Directory Discovery, Ingress Tool Transfer, Masquerading: Match Legitimate Name or Location, Modify Registry, Obfuscated Files or Information, Phishing: Spearphishing Attachment, System Information Discovery, User Execution: Malicious File
S0678	Torisma	[26]	Application Layer Protocol: Web Protocols, Data Encoding: Standard Encoding, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Execution Guardrails, Exfiltration Over C2 Channel, Native API, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Time Discovery
S0263	TYPEFRAME	[42]	Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, File and Directory Discovery, Impair Defenses: Disable or Modify System Firewall, Indicator Removal: File Deletion, Ingress Tool Transfer, Modify Registry, Non-Standard Port, Obfuscated Files or Information, Proxy, System Information Discovery, User Execution: Malicious File
S0180	Volgmer	[43]	Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, Encrypted Channel: Asymmetric Cryptography, File and Directory Discovery, Indicator Removal: File Deletion, Ingress Tool Transfer, Masquerading: Masquerade Task or Service, Modify Registry, Native API, Obfuscated Files or Information, Process Discovery, Query Registry, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Service Discovery

S0366	WannaCry	[44][45][46][47]	Create or Modify System Process: Windows Service, Data Encrypted for Impact, Encrypted Channel: Asymmetric Cryptography, Exploitation of Remote Services, Exploitation of Remote Services, File and Directory Discovery, File and Directory Permissions Modification: Windows File and Directory Permissions Modification, Hide Artifacts: Hidden Files and Directories, Inhibit System Recovery, Lateral Tool Transfer, Lateral Tool Transfer, Peripheral Device Discovery, Proxy: Multi-hop Proxy, Remote Service Session Hijacking: RDP Hijacking, Remote System Discovery, Service Stop, System Network Configuration Discovery, Windows Management Instrumentation