

Reguły/przepisy na wykrywanie zagrożeń na podstawie działań grup cyberprzestępczych z bloku wschodniego

Kurs:

Monitorowanie i Detekcja
Zagrożeń

Autor:

Grzegorz Kędra

Cel projektu

Celem projektu było przeprowadzenie symulacji oraz wykrycie rzeczywistych ataków dokonywanych przez grupy cyberprzestępcze z bloku wschodniego. Symulowane ataki musiały zostać potwierdzone raportami nie starszymi niż z 2021 rok. W celu symulacji ataków wykorzystano narzędzie Atomic Red Team. Do wykrywania ataków użyto narzędzi Sysmon połączony ze Splunk.

Rozpoznanie zagrożeń oraz analiza potencjalnych dowodów cyfrowych

1. Informacje o realnych zagrożeniach

- Mitre Att&ck
- Mitre DataSources
- Mitre Navigator

2. Wybrane grupy:

- APT28
- APT29
- Sandworm
- Indrik Spider
- Gamaredon
- Ember Bear

3. Wybrane narzędzia i systemy

- Windows 10 Pro zainstalowany na HyperV
- AtomicRedTeam
- Invoke-AtomicRedTeam
- Sysmon
- Splunk
- SigmaHQ

APT28

Grupa APT28, znana również jako Fancy Bear została przyporządkowana do rosyjskich służb specjalnych, a konkretniej do Głównego Zarządu Wywiadowczego Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU).

APT28 istnieje od co najmniej 2007 roku i jest znana z szerokiego zakresu operacji cybernetycznych, które mają na celu osiągnięcie różnorodnych celów, w tym wywiadu, infiltracji, propagandy oraz destabilizacji. Grupa ta jest aktywna na arenie międzynarodowej i jej cele obejmują głównie instytucje rządowe, organizacje wojskowe, dyplomatyczne, think tanki, a także firmy z sektora prywatnego.

APT28 zdobyła rozgłos ze względu na swoje zaangażowanie w wiele znaczących kampanii. Była podejrzewana o udział w atakach na organizacje polityczne i instytucje związane z wyborami, takie jak włamanie do Komitetu Narodowego Partii Demokratycznej w Stanach Zjednoczonych w 2016 roku.

Grupa APT28 słynie z wykorzystywania zaawansowanych technik ataku, takich jak phishing, eksploatowanie podatności, wykorzystanie złośliwego oprogramowania, a także wykorzystanie tzw. "zero-day vulnerabilities" (podatności nieznanych publicznie). Wykazuje również umiejętność kamuflażu i zacierania swojego śladu w sieci.

APT28 jest stale monitorowana i analizowana przez organizacje zajmujące się bezpieczeństwem cybernetycznym na całym świecie. Jej działalność stanowi poważne zagrożenie dla sektora publicznego i prywatnego, a zrozumienie jej taktyk i metod jest kluczowe w celu skutecznej obrony przed jej atakami.

APT29

Grupa APT29, znana również jako Cozy Bear lub NOBELIUM, jest częścią rosyjskiej Służby Wywiadu Zagranicznego (SVR). Działają od co najmniej 2008 roku i są znane z szerokiego zakresu działań cyberprzestępczych.

APT29 skupia się głównie na atakowaniu sieci rządowych w Europie i krajach członkowskich NATO, a także instytutów badawczych i think tanków. Ich cele obejmują pozyskiwanie poufnych informacji, wywiad gospodarczy, a także podejmowanie działań mających na celu osłabienie potencjalnych przeciwników politycznych lub militarnych.

Grupa APT29 zyskała znaczną uwagę ze względu na swoje zaangażowanie w wiele znaczących incydentów. Jednym z najbardziej znanym jest atak na Komitet Narodowy Partii Demokratycznej w Stanach Zjednoczonych w lecie 2016 roku. Ten incydent miał duże konsekwencje polityczne i stał się przedmiotem intensywnych dochodzeń.

W kwietniu 2021 roku rządy Stanów Zjednoczonych i Wielkiej Brytanii przypisały grupie APT29 atak na SolarWinds, w którym naruszono łańcuch dostaw oprogramowania firmy SolarWinds. Ten atak spowodował szeroko zakrojone włamania i kradzieże danych.

Grupa APT29 jest uważana za zaawansowaną i długotrwałą grupę zagrożeń, posiadającą zaawansowane umiejętności techniczne i szeroki zasób narzędzi. Ich działania mają na celu osiągnięcie strategicznych celów dla rosyjskiego wywiadu zagranicznego. APT29 nadal pozostaje aktywna, a ich działania są obiektem monitorowania i analizy przez organizacje zajmujące się bezpieczeństwem cybernetycznym.

APT29 (Cozy bear)

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (1/3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (4/5)	Abuse Elevation Control Mechanism (1/4)	Abuse Elevation Control Mechanism (1/4)	Adversary-in-the-Middle (2/3)	Account Discovery (1/8)	Exploitation of Remote Services	Adversary-in-the-Middle (2/3)	Application Layer Protocol (1/4)	Automated Exfiltration (2/1)	Account Access Removal
Gather Victim Host Information (2/4)	Acquire Infrastructure (2/8)	Exploit Public-Facing Application	Command and Scripting Interpreter (5/9)	BITS Jobs	Access Token Manipulation (2/3)	Access Token Manipulation (2/3)	Brute Force (2/4)	Application Window Discovery	Internal Spoolphishing	Archive Collected Data (1/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (1/3)	Compromise Accounts (2/3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (1/14)	Boot or Logon Autostart Execution (1/14)	BITS Jobs	Credentials from Password Stores (1/8)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2/2)	Exfiltration Over Alternative Protocol (1/3)	Data Encrypted for Impact
Gather Victim Network Information (2/5)	Compromise Infrastructure (1/7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (2/5)	Boot or Logon Initialization Scripts (1/14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Automated Collection	Remote Service Session Hijacking (2/2)	Data Obfuscation (1/3)	Exfiltration Over C2 Channel	Data Manipulation (2/3)
Gather Victim Org Information (2/4)	Develop Capabilities (2/4)	Phishing (3/3)	Replication Through Removable Media	Browser Extensions	Deobfuscate/Decode Files or Information (2/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (4/7)	Browser Session Hijacking	Dynamic Resolution (2/3)	Exfiltration Over Other Network Medium (2/1)	Defacement (2/2)
Phishing for Information (2/3)	Establish Accounts (1/3)	Supply Chain Compromise (1/3)	Inter-Process Communication (2/3)	Compromise Client Software Binary	Create or Modify System Process (2/4)	Deploy Container	Forge Web Credentials (2/2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2/2)	Endpoint Denial of Service (2/4)	Disk Wipe (2/2)
Search Closed Sources (2/2)	Obtain Capabilities (1/4)	Trusted Relationship	Native API	Create Account (1/3)	Domain Policy Modification (1/2)	Direct Volume Access	Input Capture (2/4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Physical Medium (2/1)	Firmware Corruption
Search Open Technical Databases (2/5)	Stage Capabilities (2/4)	Valid Accounts (1/4)	Scheduled Task/Job (1/5)	Create or Modify System Process (2/4)	Escape to Host	Execution Guardrails (2/1)	Modify Authentication Process (1/8)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (2/2)	Ingress Tool Transfer	Exfiltration Over Web Service (2/3)	Inhibit System Recovery
Search Open Websites/Domains (2/3)			Serverless Execution	Event Triggered Execution (2/18)	Event Triggered Execution (2/18)	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (1/8)	Data from Information Repositories (1/8)	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (2/2)
Search Victim-Owned Websites			Shared Modules	External Remote Services	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2/2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
			Software Deployment Tools	Hijack Execution Flow (2/12)	Hijack Execution Flow (2/12)	Hide Artifacts (2/12)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port	System Shutdown/Reboot	Service Stop
			System Services (2/2)	Implant Internal Image	Process Injection (2/12)	Impair Defenses (3/18)	OS Credential Dumping (1/8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		System Shutdown/Reboot
			User Execution (2/3)	Scheduled Task/Job (1/5)	Scheduled Task/Job (1/5)	Indicator Removal (3/8)	Steal Application Access Token	Network Service Discovery		Data Staged (1/2)	Remote Access Software		
			Windows Management Instrumentation	Office Application Startup (2/8)	Office Application Startup (2/8)	Indirect Command Execution	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (1/2)	Traffic Signaling (2/2)		
				Pre-OS Boot (2/3)	Pre-OS Boot (2/3)	Masquerading (3/8)	Steal or Forge Kerberos Tickets (1/4)	Password Policy Discovery		Input Capture (2/4)	Web Service (1/3)		
				Scheduled Task/Job (1/5)	Scheduled Task/Job (1/5)	Modify Authentication Process (1/8)	Steal Web Session Cookie	Peripheral Device Discovery		Screen Capture			
				Server Software Component (1/5)	Server Software Component (1/5)	Modify Cloud Compute Infrastructure (2/4)	Unsecured Credentials (1/8)	Permission Groups Discovery (1/3)		Video Capture			
				Traffic Signaling (2/2)	Traffic Signaling (2/2)	Modify Registry		Process Discovery					
				Valid Accounts (1/4)	Valid Accounts (1/4)	Modify System Image (2/2)		Query Registry					
						Network Boundary Bridging (2/1)		Remote System Discovery					
						Obfuscated Files or Information (4/11)		Software Discovery (2/1)					
						Plist File Modification		System Information Discovery					
								System Location Discovery (2/1)					
								System Network					

UAC-0082 (Sandworm)

UAC-0082, znana również jako Sandworm, to grupa cyberprzestępcza, która jest odpowiedzialna za przeprowadzanie zaawansowanych ataków cybernetycznych na cele międzynarodowe. Grupa ta była aktywna od co najmniej 2009 roku i jest związana z rosyjskimi interesami. Otrzymała swoją nazwę od wykorzystania przez nią złośliwego oprogramowania o nazwie "BlackEnergy", które wykorzystuje podatność w systemie Windows zwanej "Sandworm". Grupa UAC-0082 jest znana z wielu działań, w tym ataków na organizacje rządowe, sektor energetyczny, infrastrukturę krytyczną i instytucje badawcze. Jej cele obejmują kraje europejskie, Stany Zjednoczone i kraje bliskowschodnie. Grupa jest zaangażowana w różne formy ataków, w tym wykorzystywanie exploitów, inżynierię społeczną, phishing, ataki DDoS i skomplikowane kampanie szpiegowskie.

Indrik Spider

Indrik Spider, znana również jako Evil Corp, to notoryczna grupa cyberprzestępcza, która działa co najmniej od 2014 roku. Grupa ta jest znana ze swojego udziału w różnych skalach działań przestępczych w sferze cybernetycznej, w tym kampaniach związanych z malwarem bankowym, atakach ransomware i oszustwach finansowych.

Indrik Spider zyskała dużą uwagę za swoje zaangażowanie w rozwój i dystrybucję bankowego trojana Dridex, który miał na celu atakowanie instytucji finansowych na całym świecie. Dridex był głównie wykorzystywany do kradzieży wrażliwych danych uwierzytelniających w bankowości i przeprowadzania fałszywych transakcji, co prowadziło do znacznych strat finansowych dla osób i organizacji.

Indrik Spider

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (10)	Acquire Access (8)	Drive-by Compromise (9)	Cloud Administration Command (14)	Account Manipulation (19)	Abuse Elevation Control Mechanism (13)	Abuse Elevation Control Mechanism (42)	Adversary-in-the-Middle (17)	Account Discovery (31)	Exploitation of Remote Services (9)	Adversary-in-the-Middle (17)	Application Layer Protocol (16)	Automated Exfiltration (9)	Account Access Removal (13)
Gather Victim Host Information (10)	Acquire Infrastructure (8)	Exploit Public-Facing Application (9)	Command and Scripting Interpreter (14)	BITS Jobs (19)	Access Token Manipulation (13)	Access Token Manipulation (42)	Brute Force (17)	Application Window Discovery (31)	Archive Collected Data (9)	Internal Spearphishing (17)	Communication Through Removable Media (16)	Data Transfer Size Limits (9)	Data Destruction (13)
Gather Victim Identity Information (10)	Compromise Accounts (8)	External Remote Services (9)	Container Administration Command (14)	Boot or Logon Autostart Execution (19)	Boot or Logon Autostart Execution (13)	Boot or Logon Autostart Execution (42)	Credentials from Password Stores (17)	Browser Information Discovery (31)	Audio Capture (9)	Remote Service Session Hijacking (9)	Data Encoding (16)	Exfiltration Over Alternative Protocol (9)	Data Encrypted for Impact (13)
Gather Victim Network Information (10)	Compromise Infrastructure (8)	Hardware Additions (9)	Deploy Container (14)	Boot or Logon Initialization Scripts (19)	Boot or Logon Initialization Scripts (13)	Boot or Logon Initialization Scripts (42)	Exploitation for Credential Access (17)	Cloud Infrastructure Discovery (31)	Automated Collection (9)	Remote Service Session Hijacking (9)	Data Obfuscation (16)	Exfiltration Over C2 Channel (9)	Data Manipulation (13)
Gather Victim Org Information (10)	Develop Capabilities (8)	Prishing (9)	Exploitation for Client Execution (14)	Browser Extensions (19)	Browser Extensions (13)	Browser Extensions (42)	Debugger Evasion (17)	Cloud Service Dashboard (31)	Remote Service Session Hijacking (9)	Remote Service Session Hijacking (9)	Dynamic Resolution (16)	Exfiltration Over Other Network Medium (9)	Defacement (13)
Phishing for Information (10)	Establish Accounts (8)	Replication Through Removable Media (9)	Inter-Process Communication (14)	Compromise Client Software Binary (19)	Create or Modify System Process (13)	Create or Modify System Process (42)	Forge Web Credentials (17)	Cloud Storage Object Discovery (31)	Replication Through Removable Media (9)	Replication Through Removable Media (9)	Encrypted Channel (16)	Exfiltration Over Physical Medium (9)	Endpoint Denial of Service (13)
Search Closed Sources (10)	Obtain Capabilities (8)	Supply Chain Compromise (9)	Native API (14)	Create Account (19)	Domain Policy Modification (13)	Domain Policy Modification (42)	Input Capture (17)	Cloud Storage Object Discovery (31)	Software Deployment Tools (9)	Software Deployment Tools (9)	Fallback Channels (16)	Exfiltration Over Web Service (9)	Firmware Corruption (13)
Search Open Technical Databases (10)	Stage Capabilities (8)	Trusted Relationship (9)	Scheduled Task/Job (14)	Create or Modify System Process (19)	Event Triggered Execution (13)	Event Triggered Execution (42)	Modify Authentication Process (17)	Container and Resource Discovery (31)	Taint Shared Content (9)	Taint Shared Content (9)	Multi-Stage Channels (16)	Exfiltration Over Web Service (9)	Inhibit System Recovery (13)
Search Open Websites/Domains (10)		Valid Accounts (9)	Serverless Execution (14)	Event Triggered Execution (19)	Evade to Host (13)	Evade to Host (42)	Multi-Factor Authentication Indication (17)	Device Driver Discovery (31)	Use Alternate Authentication Material (9)	Use Alternate Authentication Material (9)	Non-Application Layer Protocol (16)	Scheduled Transfer (9)	Resource Hijacking (13)
Search Victim-Owned Websites (10)			Software Deployment Tools (14)	External Remote Services (19)	Exploitation for Privilege Escalation (13)	Exploitation for Privilege Escalation (42)	Multi-Factor Authentication Request Generation (17)	Domain Trust Discovery (31)	File and Directory Discovery (9)	File and Directory Discovery (9)	Non-Standard Port (16)	Transfer Data to Cloud Account (9)	Service Stop (13)
			System Services (14)	Hijack Execution Flow (19)	Hijack Execution Flow (13)	Hijack Execution Flow (42)	Network Sniffing (17)	Group Policy Discovery (31)	Network Service Discovery (9)	Network Service Discovery (9)	Protocol Tunneling (16)		System Shutdown/Reboot (13)
			User Execution (14)	Implant Internal Image (19)	Process Injection (13)	Process Injection (42)	OS Credential Dumping (17)	Network Share Discovery (31)	Network Share Discovery (9)	Network Share Discovery (9)	Proxy (16)		
			Windows Management Instrumentation (14)	Modify Authentication Process (19)	Scheduled Task/Job (13)	Scheduled Task/Job (42)	Steal Application Access Token (17)	Network Sniffing (31)	Network Sniffing (9)	Network Sniffing (9)	Remote Access Software (16)		
				Office Application Startup (19)	Valid Accounts (13)	Valid Accounts (42)	Steal or Forge Authentication Certificates (17)	Peripheral Device Discovery (31)	Peripheral Device Discovery (9)	Peripheral Device Discovery (9)	Traffic Signaling (16)		
				Pre-OS Boot (19)	Indirect Command Execution (13)	Indirect Command Execution (42)	Steal or Forge Kerberos Tickets (17)	Permitted Groups Discovery (31)	Permitted Groups Discovery (9)	Permitted Groups Discovery (9)	Web Service (16)		
				Server Software Component (19)	Process Injection (13)	Process Injection (42)	Steal Web Session Cookie (17)	Process Discovery (31)	Process Discovery (9)	Process Discovery (9)			
				Traffic Signaling (19)	Modify Cloud Compute Infrastructure (13)	Modify Cloud Compute Infrastructure (42)	Unsecured Credentials (17)	Query Registry (31)	Query Registry (9)	Query Registry (9)			
				Valid Accounts (19)	Modify Registry (13)	Modify Registry (42)		Software Discovery (31)	Software Discovery (9)	Software Discovery (9)			
					Modify System Image (13)	Modify System Image (42)		System Information Discovery (31)	System Information Discovery (9)	System Information Discovery (9)			
					Network Boundary Bridging (13)	Network Boundary Bridging (42)		System Location Discovery (31)	System Location Discovery (9)	System Location Discovery (9)			
					Obfuscated Files or Information (13)	Obfuscated Files or Information (42)		System Network Configuration Discovery (31)	System Network Configuration Discovery (9)	System Network Configuration Discovery (9)			
					Plist File Modification (13)	Plist File Modification (42)		System Network Connections Discovery (31)	System Network Connections Discovery (9)	System Network Connections Discovery (9)			
					Pre-OS Boot (13)	Pre-OS Boot (42)		System Owner/User Discovery (31)	System Owner/User Discovery (9)	System Owner/User Discovery (9)			
					Process Injection (13)	Process Injection (42)		System Service Discovery (31)	System Service Discovery (9)	System Service Discovery (9)			
					Reflective Code Loading (13)	Reflective Code Loading (42)		System Time Discovery (31)	System Time Discovery (9)	System Time Discovery (9)			
					Rogue Domain Controller (13)	Rogue Domain Controller (42)		Virtualization/Sandbox Evasion (31)	Virtualization/Sandbox Evasion (9)	Virtualization/Sandbox Evasion (9)			
					Rootkit (13)	Rootkit (42)							
					Subvert Trust Controls (13)	Subvert Trust Controls (42)							
					System Binary Proxy Execution (13)	System Binary Proxy Execution (42)							
					System Script Proxy Execution (13)	System Script Proxy Execution (42)							
					Template Injection (13)	Template Injection (42)							

Gamaredon

Gamaredon to grupa cyberprzestępcza, która działa głównie na terenie Ukrainy. Grupa jest aktywna od co najmniej 2013 roku i jest uważana za powiązaną z rosyjskimi interesami. Jej działania koncentrują się na przeprowadzaniu ataków hakerskich o charakterze szpiegowskim i dezinformacyjnym.

Grupa Gamaredon znana jest z wykorzystywania zaawansowanych narzędzi i technik ataków, takich jak phishing, dostarczanie złośliwego oprogramowania, a także infiltracja i wykorzystywanie infrastruktury komunikacyjnej. Jej celem są głównie instytucje rządowe, siły zbrojne, przedsiębiorstwa energetyczne, a także organizacje pozarządowe.

Gamaredon

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0.1%)	Acquire Access (0.1%)	Drive-by Compromise (0.1%)	Cloud Administration Command (0.1%)	Account Manipulation (0.1%)	Abuse Elevation Control Mechanism (0.1%)	Abuse Elevation Control Mechanism (0.1%)	Adversary-in-the-Middle (0.1%)	Account Discovery (0.1%)	Exploitation of Remote Services (0.1%)	Adversary-in-the-Middle (0.1%)	Application Layer (0.1%)	Automated Exfiltration (0.1%)	Account Access Removal (0.1%)
Gather Victim Host Information (0.1%)	Acquire Infrastructure (0.1%)	Exploit Public-Facing Application (0.1%)	Command and Scripting Interpreter (0.1%)	BITS Jobs (0.1%)	Access Token Manipulation (0.1%)	Access Token Manipulation (0.1%)	Brute Force (0.1%)	Application Window Discovery (0.1%)	Archive Collected Data (0.1%)	Audio Capture (0.1%)	Communication Through Removable Media (0.1%)	Data Transfer Size Limits (0.1%)	Data Destruction (0.1%)
Gather Victim Identity Information (0.1%)	Compromise Accounts (0.1%)	External Remote Services (0.1%)	Container Administration Command (0.1%)	Boot or Logon Autostart Execution (0.1%)	Boot or Logon Autostart Execution (0.1%)	Boot or Logon Autostart Execution (0.1%)	Credentials from Password Stores (0.1%)	Browser Information Discovery (0.1%)	Automated Collection (0.1%)	Browser Session Hijacking (0.1%)	Exfiltration Over Alternative Protocol (0.1%)	Data Encrypted for Impact (0.1%)	Data Manipulation (0.1%)
Gather Victim Network Information (0.1%)	Compromise Infrastructure (0.1%)	Hardware Additions (0.1%)	Deploy Container (0.1%)	Boot or Logon Initialization Scripts (0.1%)	Boot or Logon Initialization Scripts (0.1%)	Boot or Logon Initialization Scripts (0.1%)	Exploitation for Credential Access (0.1%)	Cloud Infrastructure Discovery (0.1%)	Remote Service Session Hijacking (0.1%)	Clipboard Data (0.1%)	Data Obfuscation (0.1%)	Exfiltration Over CS Channel (0.1%)	Defacement (0.1%)
Gather Victim Org Information (0.1%)	Develop Capabilities (0.1%)	Finishing (0.1%)	Exploitation for Client Execution (0.1%)	Browser Extensions (0.1%)	Create or Modify System Process (0.1%)	Create or Modify System Process (0.1%)	Forced Authentication (0.1%)	Cloud Service Dashboard (0.1%)	Remote Services (0.1%)	Data from Cloud Storage (0.1%)	Fallback Channels (0.1%)	Exfiltration Over Physical Medium (0.1%)	Disk Wipe (0.1%)
Finishing for Information (0.1%)	Establish Accounts (0.1%)	Replication Through Removable Media (0.1%)	Inter-Process Communication (0.1%)	Compromise Client Software Binary (0.1%)	Create or Modify System Process (0.1%)	Create or Modify System Process (0.1%)	Forge Web Credentials (0.1%)	Cloud Service Discovery (0.1%)	Replication Through Removable Media (0.1%)	Data from Configuration Repositories (0.1%)	Encrypt Channel (0.1%)	Exfiltration Over Web Service (0.1%)	Endpoint Denial of Service (0.1%)
Search Closed Sources (0.1%)	Obtain Capabilities (0.1%)	Stage Capabilities (0.1%)	Native API (0.1%)	Create Account (0.1%)	Domain Policy Modification (0.1%)	Domain Policy Modification (0.1%)	Input Capture (0.1%)	Cloud Storage Object Discovery (0.1%)	Software Deployment Tools (0.1%)	Data from Information Repositories (0.1%)	Ingress Tool Transfer (0.1%)	Exfiltration Over Web Service (0.1%)	Firmware Corruption (0.1%)
Search Open Technical Databases (0.1%)	Valid Accounts (0.1%)	Trusted Relationship (0.1%)	Scheduled Task/Job (0.1%)	Create or Modify System Process (0.1%)	Escape to Host (0.1%)	Escape to Host (0.1%)	Modify Authentication Process (0.1%)	Container and Resource Discovery (0.1%)	Use Alternate Authentication Material (0.1%)	Data from Local System (0.1%)	Multi-Stage Channels (0.1%)	Scheduled Transfer (0.1%)	Network Denial of Service (0.1%)
Search Open Websites/ Domains (0.1%)		Valid Accounts (0.1%)	Serverless Execution (0.1%)	Event Triggered Execution (0.1%)	Exploitation for Defense Evasion (0.1%)	Exploitation for Defense Evasion (0.1%)	Multi-Factor Authentication Interception (0.1%)	Device Driver Discovery (0.1%)		Data from Network Shared Drive (0.1%)	Non-Application Layer Protocol (0.1%)	Transfer Data to Cloud Account (0.1%)	Resource Hijacking (0.1%)
Search Victim-Owned Websites (0.1%)			Shared Modules (0.1%)	External Remote Services (0.1%)	Exploitation for Privilege Escalation (0.1%)	Exploitation for Privilege Escalation (0.1%)	Multi-Factor Authentication Request Generation (0.1%)	Domain Trust Discovery (0.1%)		Data from Removable Media (0.1%)	Protocol Tunneling (0.1%)		Service Stop (0.1%)
			Software Deployment Tools (0.1%)	Hijack Execution Flow (0.1%)	Hide Artifacts (0.1%)	Hide Artifacts (0.1%)	Network Sniffing (0.1%)	File and Directory Permissions Modification (0.1%)		Data Staged (0.1%)			System Shutdown/Reboot (0.1%)
			System Services (0.1%)	Implant Internal Image (0.1%)	Hijack Execution Flow (0.1%)	Hijack Execution Flow (0.1%)	OS Credential Dumping (0.1%)	Hide Artifacts (0.1%)		Email Collection (0.1%)			
			User Execution (0.1%)	Modify Authentication Process (0.1%)	Scheduled Task/Job (0.1%)	Scheduled Task/Job (0.1%)	Steal Application Access Token (0.1%)	Impair Defenses (0.1%)		Input Capture (0.1%)			
			Windows Management Instrumentation (0.1%)	Office Application Startup (0.1%)	Valid Accounts (0.1%)	Valid Accounts (0.1%)	Steal or Forge Authentication Certificates (0.1%)	Indicator Removal (0.1%)		Screen Capture (0.1%)			
				Pre-OS Boot (0.1%)			Steal or Forge Kerberos Tickets (0.1%)	Indirect Command Execution (0.1%)		Video Capture (0.1%)			
				Scheduled Task/Job (0.1%)			Steal Web Session Cookie (0.1%)	Masquerading (0.1%)					
				Server Software Component (0.1%)			Unsecured Credentials (0.1%)	Modify Authentication Process (0.1%)					
				Traffic Signaling (0.1%)				Modify Cloud Compute Infrastructure (0.1%)					
				Valid Accounts (0.1%)				Modify Registry (0.1%)					
								Modify System Image (0.1%)					
								Network Boundary Bridging (0.1%)					
								Obfuscated Files or Information (0.1%)					
								Host File Modification (0.1%)					
								Pre-OS Boot (0.1%)					
								Process Injection (0.1%)					
								Reflective Code Loading (0.1%)					
								Rogue Domain Controller (0.1%)					
								Rootkit (0.1%)					
								Subvert Trust Controls (0.1%)					
								System Binary Proxy Execution (0.1%)					
								System Script Proxy Execution (0.1%)					
								Template Injection (0.1%)					
								Traffic Signaling (0.1%)					
								Trusted Developer Utilities Proxy Execution (0.1%)					

Ember Bear

Ember Bear, znana również jako TEMP.Veles lub Berserk Bear, to podejrzana rosyjska grupa cyberprzestępcza wspierana przez państwo, która działa od co najmniej marca 2021 roku. Grupa ta jest uważana za silnie powiązaną z rosyjskim rządem i działa w celu prowadzenia operacji szpiegowskich i cyberataków o charakterze dezorganizacyjnym.

Grupa jest znana z wykorzystywania zaawansowanych technik ataków i szerokiego zakresu narzędzi hakerskich oraz różnych wariantów złośliwego oprogramowania. Obserwowano, że używają własnego złośliwego oprogramowania i zestawów narzędzi dostosowanych do ich konkretnych celów. Taktyki, techniki i procedury (TTP) stosowane przez Ember Bear są stale rozwijane, co utrudnia ich identyfikację i wykrycie.

Ember Bear

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Access (0/8)	Drive-by Compromise (0/3)	Cloud Administration Command (0/4)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services (0/4)	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal (0/1)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Exploit Public-Facing Application (0/3)	Command and Scripting Interpreter (0/6)	BITS Jobs (0/1)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery (0/3)	Internal Spearphishing (0/3)	Archive Collected Data (0/3)	Communication Through Removable Media (0/2)	Data Transfer Size Limits (0/1)	Data Destruction (0/1)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/7)	External Remote Services (0/3)	Container Administration Command (0/4)	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	Credentials from Password Stores (0/5)	Browser Information Discovery (0/3)	Lateral Tool Transfer (0/3)	Audio Capture (0/3)	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/1)	Data Encrypted for Impact (0/1)
Gather Victim Network Information (0/3)	Compromise Infrastructure (0/7)	Hardware Additions (0/3)	Deploy Container (0/3)	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host (0/1)	Exploitation for Credential Access (0/3)	Cloud Infrastructure Discovery (0/3)	Remote Service Session Hijacking (0/2)	Automated Collection (0/3)	Data Obfuscation (0/3)	Exfiltration Over C2 Channel (0/2)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Phishing (0/3)	Exploitation for Client Execution (0/3)	Browser Extensions (0/3)	Create or Modify System Process (0/4)	Debugger Evasion (0/3)	Forced Authentication (0/3)	Cloud Service Dashboard (0/3)	Remote Services (0/2)	Browser Session Hijacking (0/3)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Establish Accounts (0/3)	Replication Through Removable Media (0/3)	Inter-Process Communication (0/3)	Compromise Client Software Binary (0/3)	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information (0/3)	Forge Web Credentials (0/2)	Cloud Storage Object Discovery (0/3)	Replication Through Removable Media (0/3)	Clipboard Data (0/3)	Encrypted Channel (0/2)	Firmware Corruption (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/6)	Supply Chain Compromise (0/3)	Native API (0/3)	Create Account (0/3)	Escape to Host (0/1)	Deploy Container (0/3)	Input Capture (0/4)	Container and Resource Discovery (0/3)	Software Deployment Tools (0/3)	Data from Cloud Storage (0/3)	Fallback Channels (0/3)	Inhibit System Recovery (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/4)	Trusted Relationship (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Event Triggered Execution (0/10)	Direct Volume Access (0/3)	Modify Authentication Process (0/8)	Debugger Evasion (0/3)	Taint Shared Content (0/3)	Data from Configuration Repository (0/2)	Ingress Tool Transfer (0/3)	Network Denial of Service (0/2)	Resource Hijacking (0/1)
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Serverless Execution (0/3)	Event Triggered Execution (0/10)	Exploitation for Privilege Escalation (0/10)	Execution Guardrails (0/1)	Multi-Factor Authentication Interception (0/3)	Device Driver Discovery (0/3)	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels (0/3)	Scheduled Transfer (0/1)	Service Stop (0/1)
Search Victim-Owned Websites (0/3)			Software Deployment Tools (0/3)	External Remote Services (0/3)	Hijack Execution Flow (0/12)	Exploitation for Defense Evasion (0/10)	Multi-Factor Authentication Request Generation (0/3)	File and Directory Discovery (0/3)		Data from Local System (0/3)	Non-Application Layer Protocol (0/3)	Transfer Data to Cloud Account (0/1)	System Shutdown/Reboot (0/1)
			System Services (0/2)	Hijack Execution Flow (0/12)	Process Injection (0/12)	File and Directory Permissions Modification (0/2)	Network Sniffing (0/3)	Group Policy Discovery (0/3)		Data from Network Shared Drive (0/3)	Non-Standard Port (0/3)		
			User Execution (0/3)	Implant Internal Image (0/3)	Scheduled Task/Job (0/5)	Hide Artifacts (0/10)	OS Credential Dumping (0/8)	Network Service Discovery (0/3)		Data from Removable Media (0/3)	Protocol Tunneling (0/3)		
			Windows Management Instrumentation (0/3)	Valid Accounts (0/4)	Valid Accounts (0/4)	Hijack Execution Flow (0/12)	Steal Application Access Token (0/3)	Network Share Discovery (0/3)		Data Staged (0/2)	Remote Access Software (0/3)		
						Impair Defenses (0/10)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing (0/3)		Email Collection (0/3)	Traffic Signaling (0/2)		
						Indicator Removal (0/3)	Steal or Forge Web Session Cookie (0/4)	Password Policy Discovery (0/3)		Input Capture (0/4)	Web Service (0/3)		
						Masquerading (0/8)	Unsecured Credentials (0/8)	Peripheral Device Discovery (0/3)		Screen Capture (0/3)			
						Modify Authentication Process (0/8)		Permission Groups Discovery (0/3)		Video Capture (0/3)			
						Modify Cloud Compute Infrastructure (0/4)		Process Discovery (0/3)					
						Modify Registry (0/2)		Query Registry (0/3)					
						Modify System Image (0/2)		Remote System Discovery (0/3)					
						Network Boundary Bridging (0/1)		Software Discovery (0/1)					
						Obfuscated Files or Information (0/11)		System Information Discovery (0/1)					
						Plist File Modification (0/1)		System Location Discovery (0/1)					
						Pre-OS Boot (0/5)		System Network Configuration Discovery (0/1)					
						Process Injection (0/12)		System Network Connections Discovery (0/1)					
						Reflective Code Loading (0/12)		System Owner/User Discovery (0/1)					
						Rogue Domain Controller (0/1)		System Service Discovery (0/1)					

Defense Evasion - Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)

Opis techniki:

Wykorzystanie podszycia się pod wyszukiwanie DLL pozwala na uruchomienie skopiowanych plików z lokalizacji, która jest bardziej podatna na pominięcie przez mechanizmy bezpieczeństwa. To podejście ma na celu uniknięcie wykrycia i pozwala na uruchomienie modyfikowanych lub złośliwych wersji tych plików.

Sposób emulacji:

```
copy %windir%\System32\windowspowershell\v1.0\powershell.exe %APPDATA%\updater.exe
```

```
copy %windir%\System32\amsi.dll %APPDATA%\amsi.dll
```

```
%APPDATA%\updater.exe -Command exit
```

Sposób detekcji:

```
sourcetype="wineventlog:Microsoft-Windows-Sysmon/Operational" (EventCode=11 OR EventCode=12)  
(TargetFilename="*\\windowspowershell\\v1.0\\powershell.exe" OR TargetFilename="*\\amsi.dll" OR TargetFilename="*\\updater.exe") OR  
(CommandLine="copy %windir%\\System32\\windowspowershell\\v1.0\\powershell.exe %APPDATA%\\updater.exe" OR CommandLine="copy  
%windir%\\System32\\amsi.dll %APPDATA%\\amsi.dll" OR CommandLine="%APPDATA%\\updater.exe -Command exit")
```

Dowód cyfrowy:

SNOWYAMBER wykorzystał złośliwą bibliotekę DLL załadowaną poprzez Dll

Hijacking do procesu utworzonego z legalnego pliku binarnego w celu wykonania złośliwego oprogramowania

<https://www.gov.pl/attachment/ee91f24d-3e67-436d-aa50-7fa56acf789d>

Hijack Execution Flow: DLL Search Order Hijacking (T1574.001)

New Search

sourceType="winEventlog:Microsoft-Windows-Sysmon/Operational" (EventCode=11 OR EventCode=12) (TargetFileName!="\\windowspowershell\\v1.0\\powershell.exe" OR TargetFileName!="amsi.dll" OR TargetFileName!="\\updater.exe") OR CommandLine="copy %windir%\\System32\\windowspowershell\\v1.0\\powershell.exe %APPDATA%\\updater.exe" OR CommandLine="copy %windir%\\System32\\amsi.dll %APPDATA%\\amsi.dll" OR CommandLine="%APPDATA%\\updater.exe -Command exit")

2 events (5/20/23 10:00:00.000 AM to 5/21/23 10:00:00.000 AM) No Event Sampling

Events (2) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 20 Per Page

	i	Time	Event
>	5/21/23 9:42:30.000 AM	05/21/2023 09:42:30 AM	LogName=Microsoft-Windows-Sysmon/Operational EventCode=11 EventType=4 ComputerName=DESKTOP-QQLTL4U User=NOT_TRANSLATED Sid=5-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=237394 Keywords=None TaskCategory=File created (rule: FileCreate) OpCode=Info Message=File created: RuleName: DLL UtcTime: 2023-05-21 16:42:30.780 ProcessGuid: {95d4801c-49ec-646a-cb5c-030000000200} ProcessId: 12760 Image: C:\\Windows\\system32\\cmd.exe TargetFileName: C:\\Users\\GrzegorzKedra(253413\\AppData\\Roaming\\amsi.dll CreationUtcTime: 2023-05-21 16:42:30.779 User: AzureAD\\GrzegorzKedra(253413 Collapse host = DESKTOP-QQLTL4U source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourceType = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	5/21/23 9:42:27.000 AM	05/21/2023 09:42:27 AM	LogName=Microsoft-Windows-Sysmon/Operational EventCode=11 EventType=4 ComputerName=DESKTOP-QQLTL4U User=NOT_TRANSLATED Sid=5-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=237393 Keywords=None TaskCategory=File created (rule: FileCreate) OpCode=Info Message=File created: RuleName: DLL UtcTime: 2023-05-21 16:42:27.000 ProcessGuid: {95d4801c-49ec-646a-cb5c-030000000200} ProcessId: 12760 Image: C:\\Windows\\system32\\cmd.exe TargetFileName: C:\\Users\\GrzegorzKedra(253413\\AppData\\Roaming\\amsi.dll CreationUtcTime: 2023-05-21 16:42:27.000 User: AzureAD\\GrzegorzKedra(253413 Collapse host = DESKTOP-QQLTL4U source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourceType = WinEventLog:Microsoft-Windows-Sysmon/Operational

Administrator: Command Prompt

```
C:\Windows\system32>copy %windir%\System32\windowspowershell\v1.0\powershell.exe %APPDATA%\updater.exe
Overwrite C:\Users\GrzegorzKedra(253413\AppData\Roaming\updater.exe? (Yes/No/All): y
1 file(s) copied.

C:\Windows\system32>copy %windir%\System32\amsi.dll %APPDATA%\amsi.dll
Overwrite C:\Users\GrzegorzKedra(253413\AppData\Roaming\amsi.dll? (Yes/No/All): y
1 file(s) copied.

C:\Windows\system32>%APPDATA%\updater.exe -Command exit

C:\Windows\system32>
```

Defense Evasion Impair Defenses - Disable or Modify Tools (T1562.001)

Opis techniki:

Przeciwnicy mogą modyfikować lub dezaktywować narzędzia zabezpieczeń w celu uniknięcia wykrycia swojego złośliwego oprogramowania/narzędzi i działań. Może to przybrać różne formy, takie jak zabicie procesów lub usług oprogramowania zabezpieczającego, modyfikacja/usunięcie kluczy rejestru lub plików konfiguracyjnych, aby narzędzia nie działały poprawnie, lub inne metody interferencji w skanowanie narzędzi zabezpieczeń lub raportowanie informacji. Przeciwnicy mogą również dezaktywować aktualizacje, aby zapobiec dotarciu najnowszych łatek zabezpieczeń do narzędzi na systemach ofiar.

Sposób emulacji:

```
sc stop WinDefend
```

```
sc config WinDefend start=disabled
```

```
sc query WinDefend
```

Sposób detekcji:

```
index=main WinDefend EventCode=1 ParentCommandLine=\"%cmd.exe\" /c \"%sc stop WinDefend & sc config WinDefend start=disabled & sc query WinDefend\" OriginalFileName=\"sc.exe\"
```

Dowód cyfrowy:

Ember Bear wykonał skrypt wsadowy zaprojektowany w celu wyłączenia Windows Defender na zainfekowanym gościu.

<https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/>

Defense Evasion Impair Defenses: Disable or Modify Tools (T1562.001)

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

New Search

Save As ▾ Create Table View Close

index=main WinDefend EventCode=1 ParentCommandLine=""cmd.exe" /c \"sc stop WinDefend & sc config WinDefend start=disabled & sc query WinDefend\" OriginalFileName="sc.exe"

Last 24 hours 🔍

✓ 6 events (5/21/23 5:00:00.000 AM to 5/22/23 5:27:23.000 AM) No Event Sampling ▾

Job ▾ || ▮ ↶ ↷ ⬇ ⬆ ⬇ Smart Mode ▾

Events (6) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ ✓ Format 20 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS

- a CommandLine 3
- # EventCode 1
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Company 1
- a ComputerName 1
- a CurrentDirectory 1
- # date_hour 1
- # date_mday 1
- # date_minute 2
- a date_month 1
- # date_second 1
- a date_wday 1

i	Time	Event
>	5/22/23 5:26:27.000 AM	... 24 lines omitted ... OriginalFileName: sc.exe CommandLine: sc query WinDefend CurrentDirectory: C:\Users\Splunk\AppData\Local\Temp\ ... 9 lines omitted ... ParentCommandLine: "cmd.exe" /c "sc stop WinDefend & sc config WinDefend start=disabled & sc query WinDefend" ParentUser: DESKTOP-STF49S7\Splunk Show all 38 lines CommandLine = sc query WinDefend EventCode = 1 host = DESKTOP-STF49S7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	5/22/23 5:26:27.000 AM	... 24 lines omitted ... OriginalFileName: sc.exe CommandLine: sc config WinDefend start=disabled CurrentDirectory: C:\Users\Splunk\AppData\Local\Temp\ ... 9 lines omitted ... ParentCommandLine: "cmd.exe" /c "sc stop WinDefend & sc config WinDefend start=disabled & sc query WinDefend" ParentUser: DESKTOP-STF49S7\Splunk

Defense Evasion - Modify Registry (T1112)

Opis techniki:

Technika odnosi się do działań podejmowanych przez przeciwników w celu modyfikacji zawartości rejestru systemu operacyjnego. Rejestr jest centralnym miejscem przechowywania konfiguracji, ustawień, informacji o programach i wielu innych danych w systemie Windows.

Sposób emulacji:

```
reg add HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ImmersiveShell /v UseActionCenterExperience /t REG_DWORD /d 0 /f
```

Sposób detekcji:

```
sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=13
```

```
TargetObject=HKLM\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\CurrentVersion\\ImmersiveShell\\UseActionCenterExperience
```

Dowód cyfrowy:

Ember Bear wykorzystał skrypt wsadowy o otwartym kodzie źródłowym do modyfikacji kluczy rejestru programu Windows Defender.

<https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/>

Defense Evasion - Modify Registry (T1112)

splunk>enterprise Apps Administrator Messages Settings Activity Help

Search Analytics Datasets Reports Alerts Dashboards

New Search

Save As Create T

index=main EventCode=1 EventType=4 "HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ImmersiveShell" Image="C:\Windows\System32\reg.exe"

✓ 15 events (5/21/23 6:00:00.000 AM to 5/22/23 6:05:41.000 AM) No Event Sampling

Events (15) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 20 Per Page

< Hide Fields

≡ All Fields

SELECTED FIELDS

- CommandLine 2
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- Company 1
- ComputerName 1
- CurrentDirectory 2

i	Time	Event
>	5/21/23 2:57:02.000 PM	<p>05/21/2023 02:57:02 PM ... 22 lines omitted ... Company: Microsoft Corporation OriginalFileName: reg.exe CommandLine: reg add HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\ImmersiveShell /v UseActionCenterExperience /t REG_DWORD /d 0 /f CurrentDirectory: C:\Windows\system32\</p> <p>Show all 38 lines</p> <p>CommandLine = reg add HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion... host = DESKTOP-QOLTL4U source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational</p>
>	5/21/23	05/21/2023 02:56:46 PM

Impact Service stop (T1489)

Opis techniki:

Atakujący mogą zatrzymać lub wyłączyć usługi w systemie, aby uczynić je niedostępnymi dla legalnych użytkowników. Zatrzymanie krytycznych usług lub procesów może zahamować lub uniemożliwić reakcję na incydent lub pomóc w realizacji ogólnych celów przeciwnika polegających na wyrządzeniu szkód w środowisku

Sposób emulacji:

```
taskkill /f /im ONENOTE.EXE
```

Sposób detekcji:

```
index=main EventCode=1 EventType=4 OriginalFileName="taskkill.exe" Image="C:\\Windows\\System32\\taskkill.exe"
```

Dowód cyfrowy:

Indrik Spider wykorzystał PsExec do zatrzymania usług przed wykonaniem ransomware

<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us>

Impact - Service stop (T1489)

The screenshot shows the Splunk Enterprise web interface. At the top, the navigation bar includes 'splunk>enterprise', 'Apps', and user options like 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'New Search' and contains a search query: `index=main EventCode=1 EventType=4 OriginalFileName="taskkill.exe" Image="C:\\Windows\\System32\\taskkill.exe"`. Below the search bar, it indicates '8 events' found for the specified time range. The 'Events (8)' tab is selected, showing a list of search results. The interface includes various controls like 'Format Timeline', 'Zoom Out', 'Zoom to Selection', and 'Deselect'. On the left, there are sections for 'SELECTED FIELDS' and 'INTERESTING FIELDS'. The search results table has columns for 'Time' and 'Event'.

Search Query: `index=main EventCode=1 EventType=4 OriginalFileName="taskkill.exe" Image="C:\\Windows\\System32\\taskkill.exe"`

Results Summary: 8 events (5/21/23 9:00:00.000 AM to 5/22/23 9:33:23.000 AM) No Event Sampling

Selected Fields: `CommandLine` 8, `host` 1, `source` 1, `sourcetype` 1

Interesting Fields: `CommandLine` 1

i	Time	Event
>	5/22/23 9:12:28.000 AM	05/22/2023 09:12:28 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DESKTOP-Q0LTL4U Show all 38 lines CommandLine = taskkill /f /im host = DESKTOP-Q0LTL4U source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

Credential Access - OS Credential Dumping - LSASS Memory (T1003.001)

Opis techniki:

Polega na wykradaniu danych uwierzytelniających (credential) z systemu operacyjnego poprzez wydobycie ich z pamięci procesu Local Security Authority Subsystem Service (LSASS). LSASS jest komponentem systemu Windows, który zarządza uwierzytelnianiem użytkowników i przechowuje informacje o loginach, hasłach i innych danych uwierzytelniających.

Dowody cyfrowe:

Aktorzy grupy APT28 zrzucili pamięć procesu LSASS przy użyciu rundll32.exe do wykonania funkcji MiniDump eksportowanej przez natywną bibliotekę DLL systemu Windows® comsvcs.dll.

<https://orkl.eu/libraryEntry/6c652f88-62da-4e36-8659-eaf4ab90e55b>

https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

Emulacja zagrożenia:

Invoke-AtomicTest T1003.001 –CheckPrereq

Invoke-AtomicTest T1003.001 –GetPrereq

Invoke-AtomicTest T1003.001 –TestNumbers 2

Reguła detekcji dla testu 2:

index=main EventCode=1 ParentCommandLine="*lsass"

Credential Access - OS Credential Dumping - LSASS Memory (T1003.001)

New Search

Save As>Create Table View>Close

index=main EventCode=1 ParentCommandLine="*lsass*"Last 24 hours

4 events (5/22/23 4:00:00.000 AM to 5/23/23 4:37:48.000 AM) No Event SamplingJob|||Smart Mode

Events (4)PatternsStatisticsVisualization

Format TimelineZoom OutZoom to SelectionDeselect1 hour per column

ListFormat20 Per Page

< Hide FieldsAll Fields

SELECTED FIELDS

a CommandLine 2

EventCode 1

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Company 1

a ComputerName 1

a CurrentDirectory 1

date_hour 1

date_mday 1

date_minute 2

a date_month 1

date_second 4

a date_wday 1

date_year 1

a date_zone 1

a Description 2

EventType 1

a FileVersion 1

i	Time	Event
>	5/23/23 4:32:45.000 AM	05/23/2023 04:32:45 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DESKTOP-STF4957 Show all 38 lines Command Line = "C:\Windows\System32\rundll32.exe" C:\windows\System32\comsvcs.dll MiniDu... EventCode = 1 host = DESKTOP-STF4957 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	5/23/23 4:28:22.000 AM	05/23/2023 04:28:22 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DESKTOP-STF4957 Show all 38 lines Command Line = "C:\Windows\System32\rundll32.exe" C:\windows\System32\comsvcs.dll MiniDu... EventCode = 1 host = DESKTOP-STF4957 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	5/23/23 4:28:18.000 AM	05/23/2023 04:28:18 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DESKTOP-STF4957

Execution - Windows Management Instrumentation (T1047)

Opis techniki:

Polega na wykorzystaniu narzędzi i funkcji dostępnych w środowisku Windows do wykonywania złośliwych poleceń i payloadów. WMI jest funkcją administracyjną, która zapewnia jednolite środowisko dostępu do komponentów systemu Windows. Przeciwnik może wykorzystać WMI do interakcji z lokalnymi i zdalnymi systemami oraz używać go jako narzędzia do wykonania różnych działań, takich jak zbieranie informacji na temat zainstalowanego oprogramowania, urządzeń sieciowych, ustawień systemowych, użytkowników i grup, wersji systemu operacyjnego itp oraz zdalne wykonanie plików w ramach ruchu bocznego (Lateral Movement).

Dowody cyfrowe:

Grupa APT28 w ataku o nazwie Zebrocy wykorzystała WMI w celu uzyskania szczegółowych informacji na temat dysków atakowanego systemu.

<https://www.attackiq.com/2022/09/21/emulating-the-sophisticated-russian-adversary-apt28/>

<https://orkl.eu/libraryEntry/7d1a783e-34b9-4f36-9a88-494a35adb5cd>

Emulacja zagrożenia:

Invoke-AtomicTest T1047 -CheckPrereq

Invoke-AtomicTest T1047 -GetPrereq

Invoke-AtomicTest T1047 -TestNumbers 1

Reguła detekcji dla testu 1:

index=main EventCode=1 (Image="*\wmic.exe" CommandLine="*useraccount*" CommandLine="*get*")

Execution - Windows Management Instrumentation (T1047)

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

index=main EventCode=1 | (Image="*\wmic.exe" CommandLine="*useraccount*" CommandLine="*get*")

Last 24 hours

✓ 1 event (5/21/23 12:00:00.000 PM to 5/22/23 12:10:33.000 PM) No Event Sampling

Job || ↗ ⚙ ⬇ ⚡ Smart Mode

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- CommandLine 1
- # EventCode 1
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- Company 1

i	Time	Event
>	5/22/23 11:53:47.000 AM	05/22/2023 11:53:47 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DESKTOP-STF49S7 Show all 38 lines CommandLine = wmic useraccount get /ALL /format:csv EventCode = 1 host = DESKTOP-STF49S7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

Lateral Movement - Remote Services - SMB/Windows Admin Shares (T1021.002)

Opis techniki:

Wykorzystuje udostępniane zasoby w sieci Windows, takie jak administracyjne udziały SMB (Server Message Block) lub Windows Admin Shares. Przeciwnik może wykorzystać te zasoby do zdalnego zarządzania i przeprowadzania działań związanych z atakiem. Administracyjne udziały SMB (np. C\$, D\$) i Windows Admin Shares (np. Admin\$, IPC\$) są domyślnie udostępnione na systemach Windows w celu ułatwienia zarządzania i diagnostyki. Przez te udziały można uzyskać dostęp do plików, folderów, rejestrów systemowych i innych zasobów na zdalnych maszynach. Przeciwnik może wykorzystać te udziały do przeprowadzenia różnych działań, takich jak przechwytywanie danych, zdalne wykonanie plików, przeprowadzenie ataku typu pass-the-hash oraz przechwytywanie uwierzytelnienia.

Dowody cyfrowe:

Aktorzy grupy APT28 wykorzystali tę technikę w celu zmapowania dysków sieciowych. https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

Emulacja zagrożenia:

```
Invoke-AtomicTest T1021.002 -CheckPrereq  
Invoke-AtomicTest T1021.002 -GetPrereq  
Invoke-AtomicTest T1021.002 -TestNumbers 1
```

Reguła detekcji dla testu 1:

```
index=main net use EventCode=1 CommandLine="net use *"
```

Lateral Movement - Remote Services - SMB/Windows Admin Shares (T1021.002)

New Search

index=main net use EventCode=1 CommandLine="net use *

3 events (5/21/23 1:00:00.000 PM to 5/22/23 1:35:43.000 PM) No Event Sampling

Save As Create Table View Close

Last 24 hours

Job || → ⚙ ⬇ ⚡ Smart Mode

Events (3) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

Hide Fields All Fields

SELECTED FIELDS

a CommandLine 1

EventCode 1

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Company 1

a ComputerName 1

a CurrentDirectory 2

date_hour 2

date_mday 2

date_minute 3

a date_month 1

date_second 3

a date_wday 2

i	Time	Event
>	5/22/23 1:32:02.000 PM	<div>... 24 lines omitted ...</div> <div>OriginalFileName: net.exe</div> <div>CommandLine: net use \\Target\C\$ P\$ssw0rd1 /u:DOMAIN\Administrator</div> <div>CurrentDirectory: C:\Users\Splunk\AppData\Local\Temp\</div> <div>User: DESKTOP-STF49S7\Splunk</div> <div>... 8 lines omitted ...</div> <div>ParentCommandLine: cmd.exe /c "net use \\Target\C\$ P\$ssw0rd1 /u:DOMAIN\Administrator"</div> <div>Show all 38 lines</div> <div>CommandLine = net use \\Target\C\$ P\$ssw0rd1 /u:DOMAIN\Administrator EventCode = 1 host = DESKTOP-STF49S7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational</div>
>	5/22/23 1:31:03.000 PM	<div>... 24 lines omitted ...</div> <div>OriginalFileName: net.exe</div> <div>CommandLine: net use \\Target\C\$ P\$ssw0rd1 /u:DOMAIN\Administrator</div> <div>CurrentDirectory: C:\Users\Splunk\AppData\Local\Temp\</div> <div>User: DESKTOP-STF49S7\Splunk</div> <div>... 8 lines omitted ...</div> <div>ParentCommandLine: cmd.exe /c "net use \\Target\C\$ P\$ssw0rd1 /u:DOMAIN\Administrator"</div>

Impact - Data Destruction (T1485)

Opis techniki:

Dotyczy celowego niszczenia danych i plików na konkretnych systemach lub w dużej skali w sieci w celu zakłócenia dostępności systemów, usług i zasobów sieciowych. Niszczenie danych ma na celu uniemożliwienie odzyskania przechowywanych danych za pomocą technik forensycznych poprzez nadpisanie plików lub danych na lokalnych i zdalnych dyskach. Powszechne polecenia usuwania plików systemowych, takie jak `del` i `rm`, zazwyczaj tylko usuwają wskaźniki do plików bez nadpisywania ich zawartości, co umożliwia odzyskanie plików przy odpowiedniej metodologii forensycznej. Przeciwnicy mogą próbować nadpisać pliki i katalogi losowo generowanymi danymi, aby uczynić je nieodzyskiwalnymi. W niektórych przypadkach pliki obrazów o charakterze politycznym zostały użyte do nadpisywania danych.

Impact - Data Destruction (T1485)

Dowody cyfrowe:

Grupa UAC-0082 (Sandworm) w ramach przeprowadzonego ataku na ukraińskie elektrownie użyła kilku narzędzi, w celu naruszenia integralności i dostępności informacji uniemożliwiając ich odzyskanie.

<https://cert.gov.ua/article/3718487?fbclid=IwAR1i0b3pmLOs8p8ObWwRwZFSjiuAV3ZSiA1otKrE4nDd3G7c3ghLSklZrsI>

<https://socprime.com/blog/latest-threats/uac-0082-sandworm-apt-group-targets-ukrainian-national-information-agency-ukrinform-in-a-series-of-cyber-attacks-leveraging-multiple-wiper-malware-strains/>

Emulacja zagrożenia:

Invoke-AtomicTest T1485 -CheckPrereq

Invoke-AtomicTest T1485 -GetPrereq

Invoke-AtomicTest T1485 -TestNumbers 1

Reguła detekcji dla testu 1:

index=main EventCode=1 CommandLine="*sdelete*

Impact - Data Destruction (T1485)

New Search

index=main EventCode=1 CommandLine="*sdelete*" |

✓ 3 events (5/21/23 1:00:00.000 PM to 5/22/23 1:20:21.000 PM) No Event Sampling

Save As Create Table View Close

Last 24 hours

Job ||| ↗ 🗑️ ⬇️ Smart Mode

Events (3) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

List Format 20 Per Page

< Hide Fields

≡ All Fields

SELECTED FIELDS
a CommandLine 3
EventCode 1
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Company 2
a ComputerName 1
a CurrentDirectory 1
date_hour 1
date_mday 1
date_minute 2
a date_month 1
date_second 3
a date_wday 1

i	Time	Event
>	5/22/23 1:04:06.000 PM	<div>05/22/2023 01:04:06 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DESKTOP-STF49S7 Show all 39 lines CommandLine = "C:\Users\Splunk\AppData\Local\Temp\Sdelete\sdelete.exe" -accepteula C:\User... sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational</div> <div>EventCode = 1 host = DESKTOP-STF49S7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational</div>
>	5/22/23 1:04:02.000 PM	<div>05/22/2023 01:04:02 PM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DESKTOP-STF49S7 Show all 38 lines CommandLine = "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" & {if (Test-Pat... sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational</div> <div>EventCode = 1 host = DESKTOP-STF49S7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational</div>

Collection - Screen Capture (T1113)

Opis techniki:

Polega na próbie przechwytywania zrzutów ekranu w celu pozyskania takich informacji jak dane uwierzytelniające, poufne dane biznesowe czy dane poufne klientów. Funkcjonalność przechwytywania ekranu może być zawarta jako funkcja narzędzi zdalnego dostępu wykorzystywanych w operacjach po kompromitacji. Wykonywanie zrzutu ekranu jest również możliwe za pomocą narzędzi natywnych lub wywołań interfejsów API, takich jak CopyFromScreen, xwd lub screencapture.

Dowody cyfrowe:

Grupa APT28 w ramach ataku Zebrocy użyła tej techniki w celu kradzieży danych, przesyłanych regularnie poprzez stworzone zaplanowane zadanie.
<https://orkl.eu/libraryEntry/c5e77536-f26c-469d-b1af-6de422c5f69a>

Emulacja zagrożenia:

Invoke-AtomicTest T1113 –CheckPrereq

Invoke-AtomicTest T1113 –GetPrereq

Invoke-AtomicTest T1113 –TestNumbers 5

Reguła detekcji dla testu 5:

index=main EventCode=1 OriginalFileName="psr.exe"

Collection - Screen Capture (T1113)

New Search

index=main EventCode=1 OriginalFileName="psr.exe"

Week to date

✓ 12 events (5/21/23 12:00:00.000 AM to 5/23/23 3:40:21.000 AM) No Event Sampling

Job

||

↗

⌵

Smart Mode

Save As

Create Table View

Close

Events (12)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

+ Zoom to Selection

× Deselect

1 hour per column

List

Format

20 Per Page

< Hide Fields

≡ All Fields

SELECTED FIELDS

a CommandLine 2

EventCode 1

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a Company 1

a ComputerName 1

a CurrentDirectory 1

date_hour 2

date_mday 2

date_minute 3

date_month 1

date_second 7

a date_wday 2

i	Time	Event
>	5/23/23 3:24:07.000 AM	<div>05/23/2023 03:24:07 AM</div> <div>LogName=Microsoft-Windows-Sysmon/Operational</div> <div>EventCode=1</div> <div>EventType=4</div> <div>ComputerName=DESKTOP-STF49S7</div> <div>Show all 38 lines</div> <div>CommandLine = "C:\Windows\system32\psr.exe" /start /output c:\temp\T1113_desktop.zip /sc 1/gu... EventCode = 1 host = DESKTOP-STF49S7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational</div>
>	5/23/23 3:24:06.000 AM	<div>05/23/2023 03:24:06 AM</div> <div>LogName=Microsoft-Windows-Sysmon/Operational</div> <div>EventCode=1</div> <div>EventType=4</div> <div>ComputerName=DESKTOP-STF49S7</div> <div>Show all 38 lines</div> <div>CommandLine = "C:\Windows\system32\psr.exe" /start /output c:\temp\T1113_desktop.zip /sc 1/gu... EventCode = 1 host = DESKTOP-STF49S7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational</div>

Persistence - Registry Run Keys / Startup Folder (T1547.001)

Opis techniki:

Napastnicy używają tej techniki do ustanowienia trwałej obecności na urządzeniu ofiary. Do tego celu wykorzystywany jest wbudowany w system operacyjny autostart uruchamiający program podrzucony przez atakujących podczas bootowania systemu. W tej technice realizowane jest to poprzez odwołanie się do kluczy rejestru. Dodanie ich pozwala na włączenie programu po zalogowaniu się przez użytkownika.

Sposób emulacji:

Invoke-AtomicTest T1547.001 -CheckPrereq

Invoke-AtomicTest T1547.001 -GetPrereq

Invoke-AtomicTest T1547.001 -TestNumbers 1

Sposób detekcji:

index=main EventCode=13 TargetObject="HKU\\S-1-5-21-3388779504-2943004340-2021762261-1001\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Atomic Red Team"

Dowód cyfrowy:

Grupa APT29 wykorzystywała narzędzie SNOWYAMBER do ustanowienia stałej obecności. Pozwoliła na to modyfikacja kluczy rejestru. Atak opisano w Raporcie CERT POLSKA i Służby Kontrwywiadu Wojskowego.

<https://www.gov.pl/attachment/ee91f24d-3e67-436d-aa50-7fa56acf789d>

Persistence - Registry Run Keys / Startup Folder (T1547.001)

index=main EventCode=13 Image="*reg.exe"

✓ 1 event (5/21/23 8:00:00.000 AM to 5/22/23 8:31:59.000 AM) No Event Sampling ▾

Job ▾ || ▢ ↻ 🗑️ ⬇️

Events (1) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ ✎ Format 20 Per Page ▾

< Hide Fields ≡ All Fields

SELECTED FIELDS

- a host 1
- a Keywords 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

i	Time	Event
>	5/22/23 7:15:41.000 AM	05/22/2023 07:15:41 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=13 EventType=4 ComputerName=DESKTOP-OOLFQ5G Show all 24 lines Keywords = None host = DESKTOP-OOLFQ5G source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

Initial Access - Spearphishing Attachment (T1566.001)

Opis techniki:

Atakującym udaje się uzyskać dostęp do komputerów ofiar poprzez wysyłanie fałszywych e-maili wyglądających jak prawdziwe, a zawierających złośliwe oprogramowanie. Wiadomości zawierają zazwyczaj zainfekowane załączniki lub linki do fałszywych stron internetowych, które wyglądają jak oryginalne. Gdy odbiorca otwiera załącznik lub kliknie na link, może zostać zainfekowany złośliwym oprogramowaniem, które pozwala atakującemu uzyskać dostęp do systemu lub kradnie poufne informacje.

Sposób emulacji:

Invoke-AtomicTest T1566.001 -CheckPrereq

Invoke-AtomicTest T1566.001 -GetPrereq

Invoke-AtomicTest T1566.001 -TestNumbers 1

Sposób detekcji:

index=main EventCode=11 TargetFilename="*.xlsm"

Dowód cyfrowy:

Grupa APT 29 wykonała atak skierowany przeciwko placówkom dyplomatycznym i dyplomatom pracującym w Europie. Atakujący wysyłali mail zawierający spreparowany plik PDF zawierający link do narzędzia ENVYSCOUT. Atak został opisany w raporcie przygotowanym przez CERT POLSKA i Służbę Kontrwywiadu Wojskowego.

<https://www.gov.pl/attachment/ee91f24d-3e67-436d-aa50-7fa56acf789d>

Initial Access - Spearphishing Attachment (T1566.001)

index=main EventCode=11 TargetFilename=*PhishingAttachment.xlsm*

✓ 2 events (5/21/23 9:00:00.000 AM to 5/22/23 9:03:37.000 AM) No Event Sampling

Events (2) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection x Deselect

List Format 20 Per Page

< Hide Fields	≡ All Fields	i	Time	Event
		>	5/22/23 8:55:58.000 AM	05/22/2023 08:55:58 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=11 EventType=4 ComputerName=DESKTOP-OOLFQ5G User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Microsoft-Windows-Sysmon Type=Information RecordNumber=44809 Keywords=None TaskCategory=File created (rule: FileCreate) OpCode=Info Message=File created: RuleName: - UtcTime: 2023-05-22 15:55:58.878 ProcessGuid: {33e57f41-908b-646b-d9aa-000000000200} ProcessId: 12012 Image: C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\MDIZ\AppData\Local\Temp\PhishingAttachment.xlsm CreationUtcTime: 2023-05-22 15:55:58.878 User: DESKTOP-OOLFQ5G\MDIZ Collapse EventCode = 11 Keywords = None host = DESKTOP-OOLFQ5G source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

SELECTED FIELDS
EventCode 1
a host 1
a Keywords 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a ComputerName 1
a CreationUtcTime 2
date_hour 2
date_mday 1
date_minute 2
a date_month 1
date_second 2
a date_wday 1
date_year 1
a date_zone 1
EventType 1
a Image 2
a index 1
linecount 1
a LogName 1
a Message 2
a OpCode 1

Defense Evasion - Deobfuscate/Decode Files or Information (T1140)

Opis techniki:

Atakujący wykorzystują tę technikę w celu ukrycia charakterystycznych cech ataku lub używanych narzędzi przed analizą. Deobfuskacja/dekodowanie ma na celu przywrócenie oryginalnego, czytelnego formularza plików lub informacji, które zostały celowo zamaskowane lub zakodowane w różnych celach, takich jak ochrona i unikanie wykrycia.

Sposób emulacji:

Invoke-AtomicTest T1140 -CheckPrereq

Invoke-AtomicTest T1140 -GetPrereq

Invoke-AtomicTest T1140 -TestNumbers 1

Sposób detekcji:

index=main CommandLine="* -decode*" EventCode=1

Dowód cyfrowy:

W lutym 2023 zaobserwowano użycie narzędzia HALFRIG, którego podobieństwo do QUARTERRIG sugeruje wykorzystywanie go przez grupę APT29.

Wykorzystano w nim szyfrowanie w celu utrudnienia wykrycia. Atak został opisany w raporcie przygotowanym przez CERT POLSKA i Służbę Kontrwywiadu Wojskowego.

<https://www.gov.pl/attachment/64193e8d-05e2-4cbf-bb4c-5f58da21fefb>

Defense Evasion - Deobfuscate/Decode Files or Information (T1140)

index=main EventCode=11 Image="*certutil.exe" TargetFilename="*.exe"

✓ 1 event (5/21/23 9:00:00.000 AM to 5/22/23 9:42:07.000 AM) No Event Sampling ▾ Job ▾ || ▮ ↻ ⚙

Events (1) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

< Hide Fields

≡ All Fields

SELECTED FIELDS
EventCode 1
a host 1
a Keywords 1
a source 1
a sourcetype 1

List ▾ ↗ Format 20 Per Page ▾

i	Time	Event
>	5/22/23 9:28:34.000 AM	05/22/2023 09:28:34 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=11 EventType=4 ComputerName=DESKTOP-OOLFQ5G Show all 23 lines EventCode = 11 Keywords = None host = DESKTOP-OOLFQ5G source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

Defense Evasion - HTML Smugling (T1027.006)

Opis techniki:

Technika ta jest wykorzystywana w celu ukrycia i przemycenia groźnych payloadów w uznawanych za niegroźne plikach html. Atakujący wykorzystują możliwość ukrycia w takim pliku dużych obiektów binarnych znanych jako JavaScript Blobs. Pozwala to na przemycenie takiego pliku przez zaporę, dzięki wykorzystaniu zwykłego tekstu.

Sposób emulacji:

Invoke-AtomicTest T1027.006 -CheckPrereq

Invoke-AtomicTest T1027.006 -GetPrereq

Invoke-AtomicTest T1027.006 -TestNumbers 1

Sposób detekcji:

index=main EventCode=1 CommandLine="*html"

Dowód cyfrowy:

Narzędzie QUARTERRIG wykorzystywało tę technikę od początku marca 2023. Opis narzędzia i sposób ataku zostały przedstawione w raporcie CERT POLSKA i Służby Kontrwywiadu Wojskowego.

<https://www.gov.pl/attachment/6f51bb1a-3ad2-461c-a16d-408915a56f77>

Defense Evasion - HTML Smugling (T1027.006)

New Search

Save As ▾Create Table VI

index=main EventCode=1 CommandLine="<html">

Last 24 h

✓ 1 event (5/21/23 1:00:00.000 PM to 5/22/23 1:19:57.000 PM) No Event Sampling ▾

Job ▾ || ▢ ↗ ↻ ⬇ ⚠

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection x Deselect

List ▾ ✓ Format 20 Per Page ▾

< Hide Fields ≡ All Fields

SELECTED FIELDS
EventCode 1
a host 1
a Keywords 1
a source 1
a sourcetype 1

i	Time	Event
>	5/22/23 10:49:02.000 AM	05/22/2023 10:49:02 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DESKTOP-OOLFQ5G Show all 38 lines EventCode = 1 Keywords = None host = DESKTOP-OOLFQ5G source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

Execution - Malicious File (T1204.002)

Opis techniki:

Atakujący często polegają na wykonaniu pewnych czynności po przez użytkowników. W przypadku tej techniki użytkownik zostanie prawdopodobnie zachęcony poprzez inżynierię społeczną do uruchomienia spreparowanego pliku.

Sposób emulacji:

Invoke-AtomicTest T1204.002 –CheckPrereq

Invoke-AtomicTest T1204.002 –GetPrereq

Invoke-AtomicTest T1204.002 –TestNumbers 8

Sposób detekcji:

index=main EventCode=1 CommandLine="\"powershell.exe\" & {Invoke-Webrequest*}"

Dowód cyfrowy:

Grupa ACTINIUM wykorzystała tę technikę podczas ataków na ukraińskie cele:


<https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/>

Execution - Malicious File (T1204.002)

New Search

Save As ▾Create Table ViewClose

index=main EventCode=1 CommandLine="\"powershell.exe\" & {Invoke-Webrequest*}"

Last 24 hours ▾

✓ 1 event (5/21/23 10:00:00.000 AM to 5/22/23 10:07:01.000 AM) No Event Sampling ▾


Job ▾ ||| ↻ ⚙ ⬇ ⚡ Smart Mode ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

1 hour per column

List ▾ ↗ Format 20 Per Page ▾

< Hide Fields  All Fields

SELECTED FIELDS

α CommandLine 1

EventCode 1

α host 1

α source 1

α sourcetype 1

INTERESTING FIELDS

α Company 1

i	Time	Event
>	5/22/23 2:31:42.000 AM	<div>05/22/2023 02:31:42 AM</div> <div>LogName=Microsoft-Windows-Sysmon/Operational</div> <div>EventCode=1</div> <div>EventType=4</div> <div>ComputerName=DESKTOP-STF49S7</div> <div>Show all 38 lines</div> <div>CommandLine = "powershell.exe" & {Invoke-Webrequest -Uri \"https://raw.githubusercontent.co... EventCode = 1 host = DESKTOP-STF49S7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational</div> <div>sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational</div>

Defense Evasion - Indicator Removal on Host: File Deletion (T1070.004)

Opis techniki:

Przeciwnicy mogą usuwać pliki pozostawione w wyniku działań ich intruzji. Malware, narzędzia lub inne pliki niezwiązane z systemem, które zostają przekazane lub utworzone na systemie przez przeciwnika (np. narzędzia transferu narzędzi dostępu), mogą pozostawiać ślady wskazujące na to, co zostało wykonane w sieci i w jaki sposób. Usuwanie tych plików może następować podczas intruzji lub jako część procesu po-intruzji w celu zminimalizowania śladów pozostawionych przez przeciwnika.

Sposób emulacji:

Invoke-AtomicTest T1070.004 –CheckPrereq

Invoke-AtomicTest T1070.004 –GetPrereq

Invoke-AtomicTest T1070.004 –TestNumbers 4

Sposób detekcji:

index=main EventCode=1 CommandLine="\"cmd.exe\" /c \"del /f *\" Image=\"C:\\Windows\\System32\\cmd.exe"

Dowód cyfrowy:

Narzędzia grupy Gamaredon mogą usuwać pliki używane podczas operacji.

<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine>

Defense Evasion - Indicator Removal on Host: File Deletion (T1070.004)

splunk>enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search & Reporting

New Search

Save As ▾ Create Table View Close

index=main EventCode=1 CommandLine="cmd.exe" /c %del /f % Image="C:\\Windows\\System32\\cmd.exe"

✓ 1 event (5/21/23 9:00:00.000 AM to 5/22/23 9:47:18.000 AM) No Event Sampling ▾

Job ▾ || ▢ → ⚙ ⬇ ⬆ Smart Mode ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

May 21, 2023 9:00 AM May 22, 2023 10:00 AM

1 day 1 hour

1 hour per column

List ▾ ✓ Format 20 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS

- α CommandLine 1
- # EventCode 1
- α host 1
- α source 1
- α sourcetype 1

INTERESTING FIELDS

- α Company 1

i	Time	Event
>	5/22/23 9:44:46.000 AM	05/22/2023 09:44:46 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=1 EventType=4 ComputerName=DESKTOP-STF49S7 Show all 38 lines CommandLine = "cmd.exe" /c %del /f %temp%%deleteme_T1551.004" EventCode = 1 host = DESKTOP-STF49S7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational