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, exploitowanie 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.

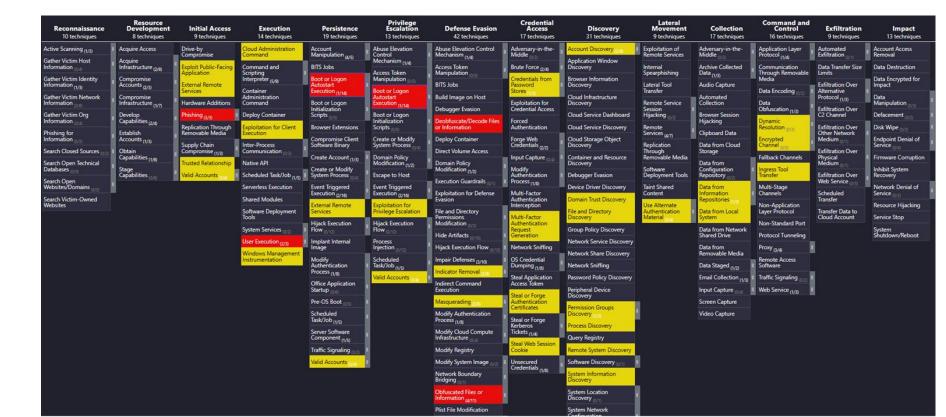
APT29 skupia się głównie na atakowaniu sieci rządowych w Europie i krajach członkowskich NATO, a także instytutów badawczych i think tanków. Ich cele obejmują pozyskiwanie poufnych informacji, wywiad gospodarczy, a także podejmowanie działań mających na celu osłabienie potencjalnych przeciwników politycznych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



UAC-0082 (Sandworm)

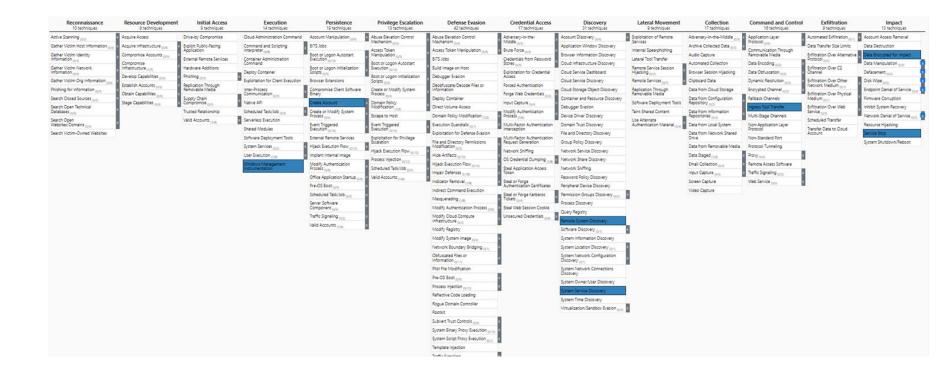
UAC-0082, znana również jako Sandworm, to grupa cyberprzestępcza, która jest odpowiedzialna za przeprowadzanie zaawansowanych ataków cybernetycznych na cele międzynarodowe. Grupa ta była aktywna od co najmniej 2009 roku i jest związana z rosyjskimi interesami. Otrzymała swoją nazwę od wykorzystania przez 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

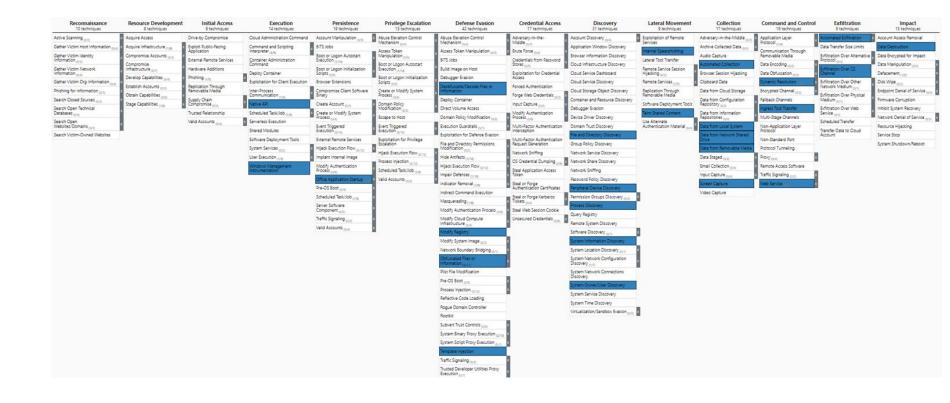


Gamaredon

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

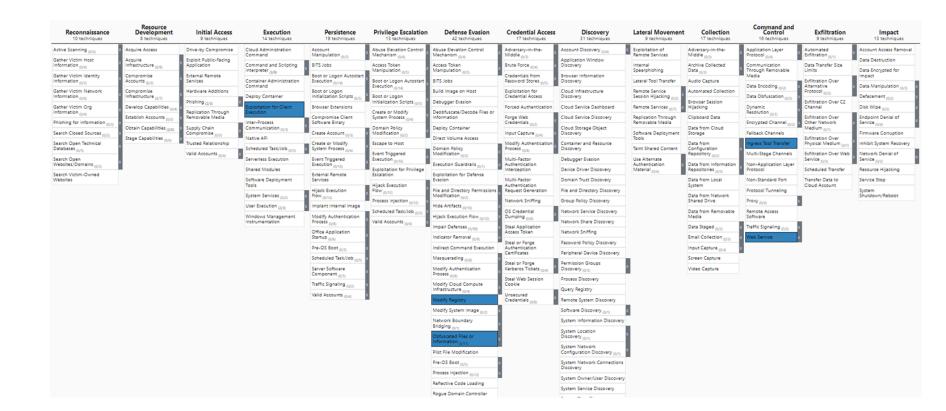


Ember Bear

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



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")

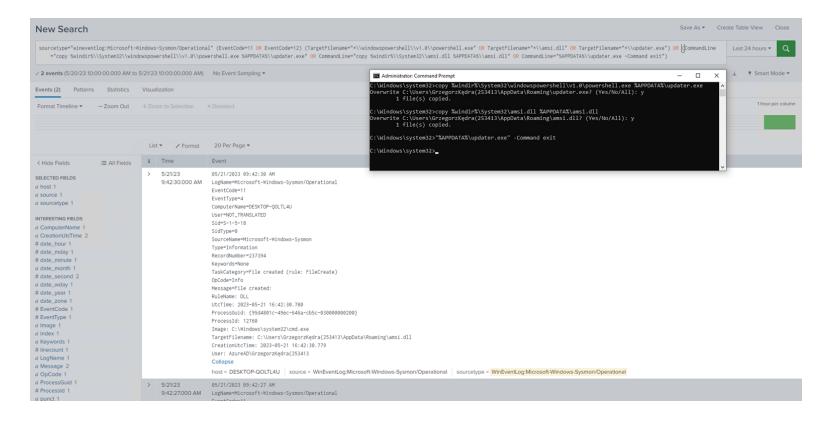
Dowód cyfrowy:

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)



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:

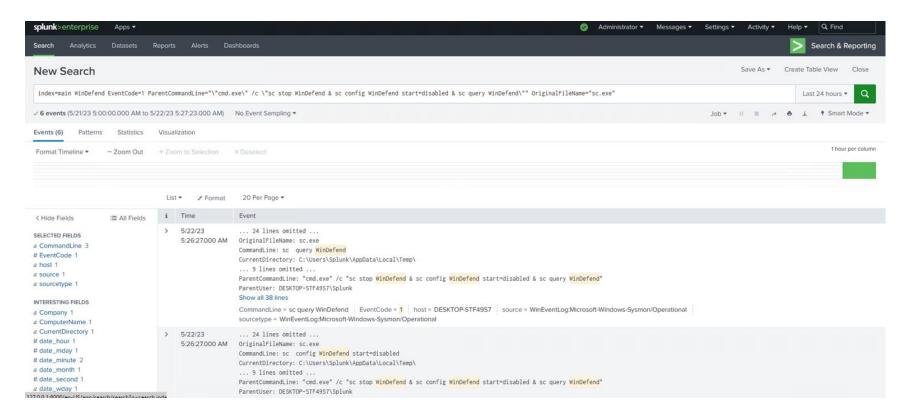
index=main WinDefend EventCode=1 ParentCommandLine="\"cmd.exe\" /c \"sc stop WinDefend & sc config WinDefend start=disabled & sc query WinDefend\"" OriginalFileName="sc.exe"

Dowód cyfrowy:

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

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

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



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:

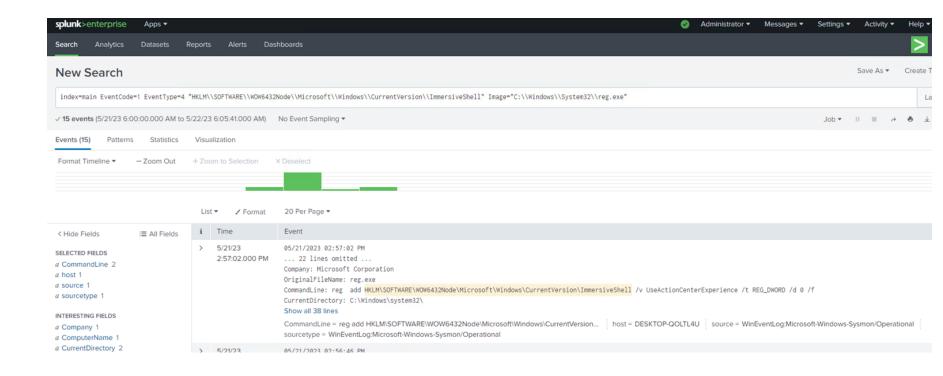
sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=13 TargetObject=HKLM\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\CurrentVersion\\ImmersiveShell\\UseActionCenterExperience

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)



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:

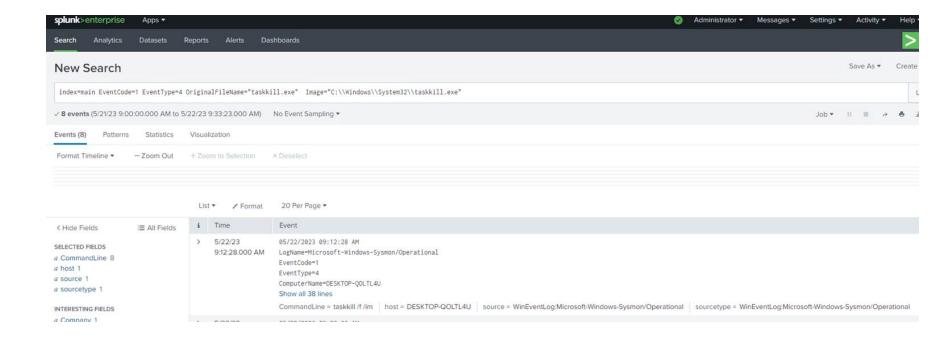
index=main EventCode=1 EventType=4 OriginalFileName="taskkill.exe" Image="C:\\Windows\\System32\\taskkill.exe"

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)



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

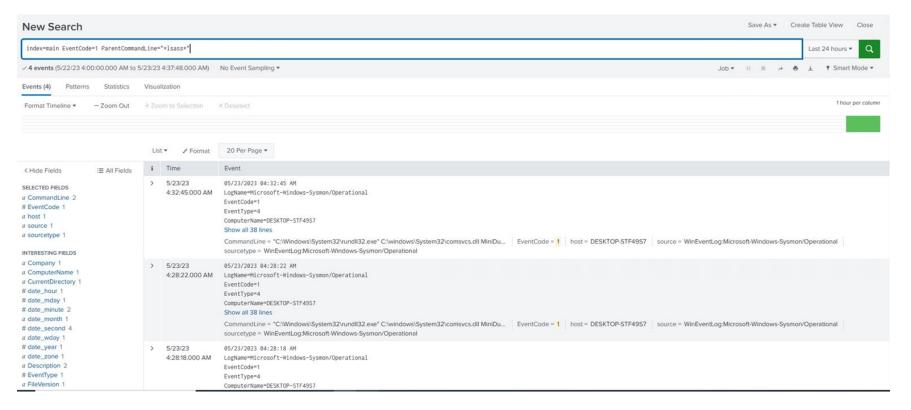
Invoke-AtomicTest T1003.001 -GetPrereq

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)



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

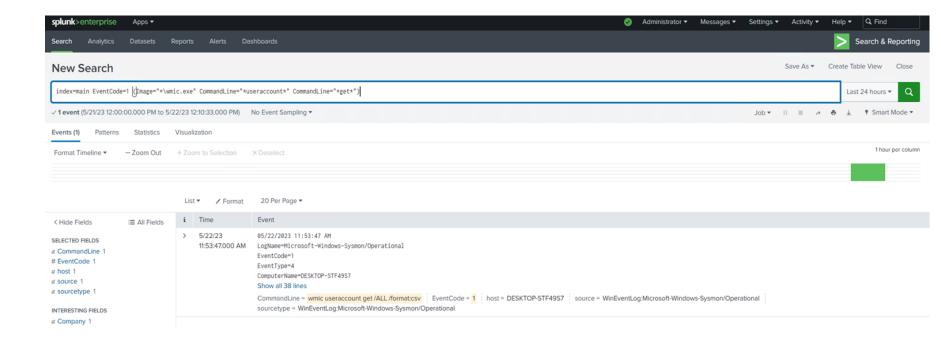
Emulacja zagrożenia:

Invoke-AtomicTest T1047 – CheckPrereq Invoke-AtomicTest T1047 – GetPrereq Invoke-AtomicTest T1047 – TestNumbers 1

Regula detekcji dla testu 1:

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

Execution - Windows Management Instrumentation (T1047)



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

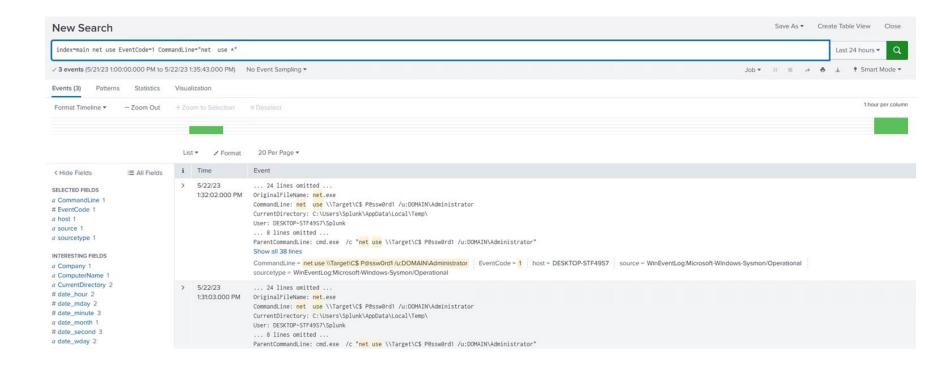
Emulacja zagrożenia:

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

Regula detekcji dla testu 1:

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

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



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

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

Emulacja zagrożenia:

Invoke-AtomicTest T1485 - CheckPrereq

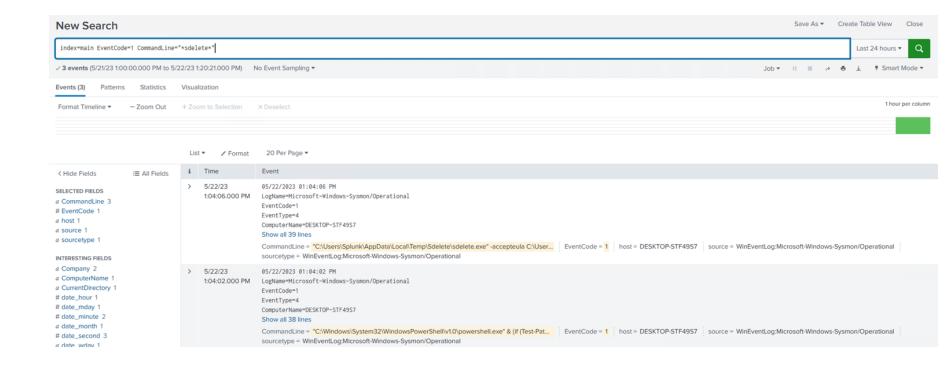
Invoke-AtomicTest T1485 -GetPrereq

Invoke-AtomicTest T1485 -TestNumbers 1

Reguła detekcji dla testu 1:

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

Impact - Data Destruction (T1485)



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

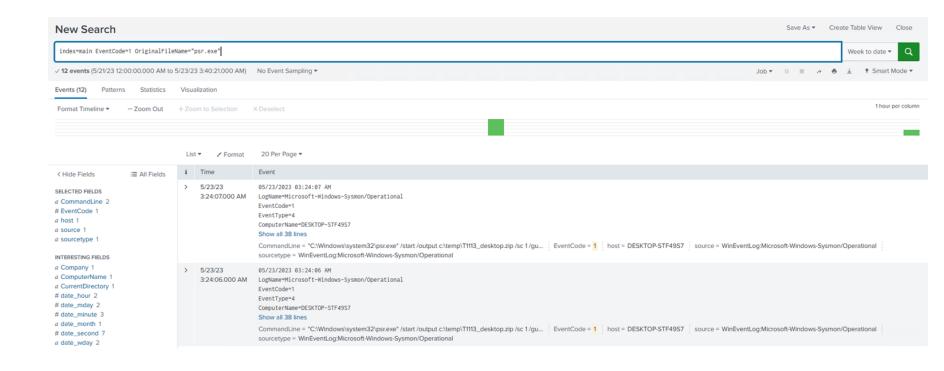
Invoke-AtomicTest T1113 -GetPrereq

Invoke-AtomicTest T1113 –TestNumbers 5

Reguła detekcji dla testu 5:

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

Collection - Screen Capture (T1113)



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 użytkowanika.

Sposób emulacji:

Invoke-AtomicTest T1547.001 -CheckPrereq Invoke-AtomicTest T1547.001 -GetPrereq Invoke-AtomicTest T1547.001 -TestNumbers 1

Sposób detekcji:

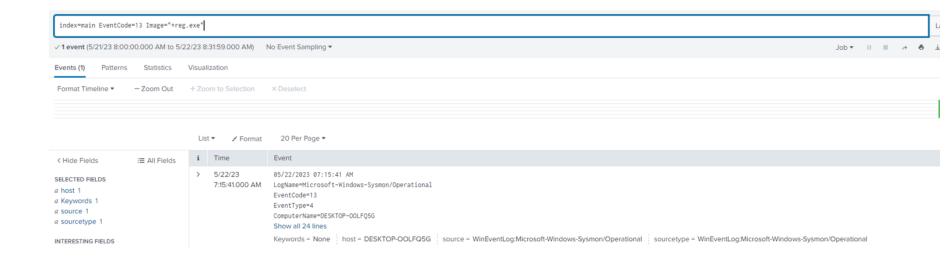
 $index=main\ EventCode=13\ TargetObject="HKU\\S-1-5-21-3388779504-2943004340-2021762261-1001\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Atomic\ Red\ Team"$

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)



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:

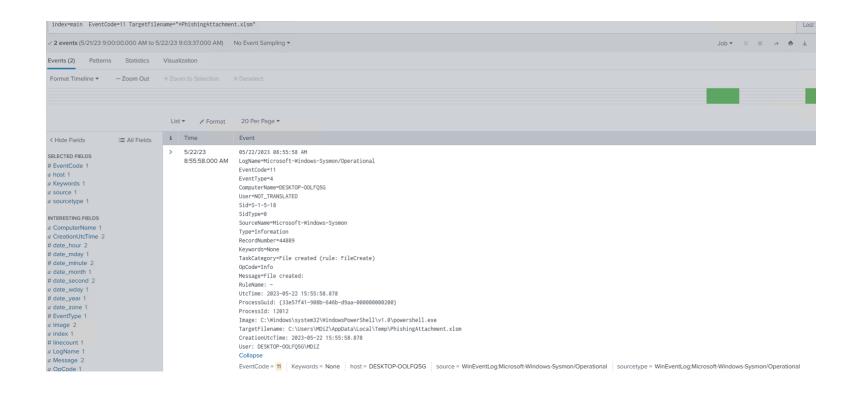
index=main EventCode=11 TargetFilename="*.xlsm"

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)



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:

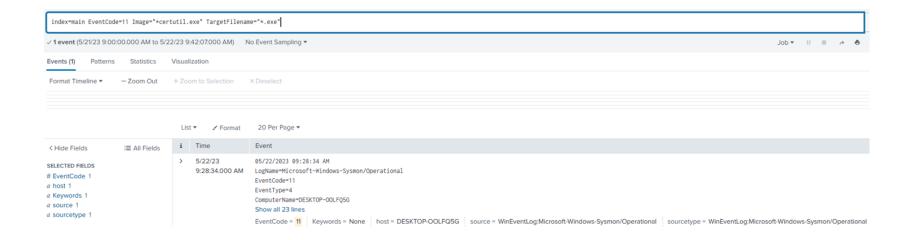
index=main CommandLine="* -decode*" EventCode=1

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)



Defense Evasion - HTML Smugling (T1027.006)

Opis techniki:

Technika ta jest wykorzystywana w celu ukrycia i przemycenia groźnych paylodów w uznawanych za niegroźne plikach html. Atakujący wykorzystują możliwość ukrycia w takim pliku dużych obiektów binarnych znanych jako JavaScirpt 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:

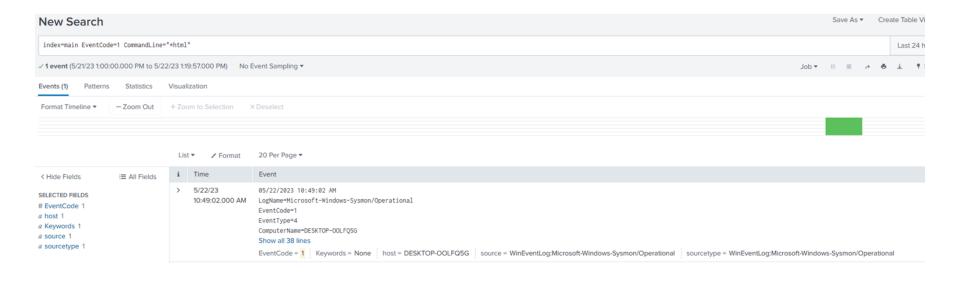
index=main EventCode=1 CommandLine="*html"

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)



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:

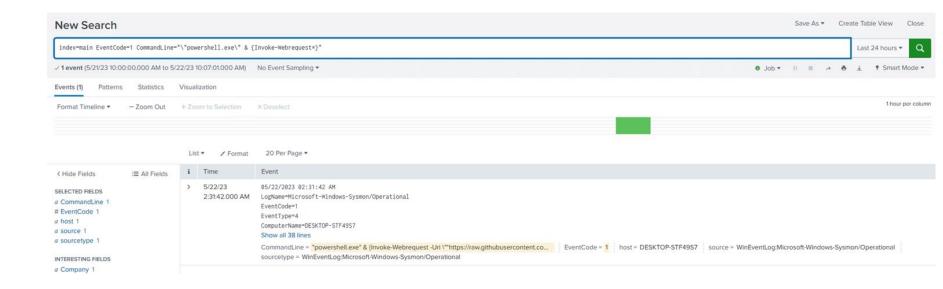
index=main EventCode=1 CommandLine="\"powershell.exe\" & {Invoke-Webrequest*}"

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)



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 narzędzia 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)

