DEFENSIVE SECURITY

Rozwój pracowników SOC/CERT z wykorzystaniem narzędzi typu Cyber Range / Cyber Lab

Leszek Miś - Security Researcher/Trener,
lm@defensive-Security.com

whoami

- Security Researcher / uid=0 @ **Defensive-Security.com**
- OSCP / RHCA / Sec+
- Trener / Przeszkolonych osób łącznie powyżej 1000 osób
- Polska + warsztaty podczas Black Hat USA, Hack In The Box AMS / Singapore / Abu Dhabi / Dubai, OWASP Appsec USA, Flocon USA, BruCON BE, 44CON UK
- Obszary zainteresowania:
  - Cyber Range / Cyber Labs
  - Offensive Security Research
  - Adversary Emulations and Post-Exploitation Red/Blue Actions
  - Threat Hunting and Incident Response
  - Behavioral / Statistic / ML network analysis → Features Extraction
  - Hardening of Linux / Web Application / Infrastructure
  - Penetration testing / OSINT / Security audits
  - Open Source Security Projects

Wyzwania

- Proaktywna analiza zachowania krytycznych systemów i usług nie tylko z perspektywy **ps uax** czy też **tasklist.exe** i automatyzacja

Wyzwania

- Widoczność na wielu różnych warstwach od sieciowej po “syscallową” + automatyzacja

Wyzwania

- Aktywna analiza zagrożeń, typów i rodzajów technik, taktyk i procedur, w tym pełnych kompletnych kampanii ofensywnych → MITRE ATTACK Framework oraz **automatyzacja**
  - **https://thedfirreport.com/**

Wyzwania

- Obsługa incydentów i SOAR-owa **automatyzacja:**
  - Stos otwartoźródłowy:
    - Security Onion + n8n + Velociraptor
      - https://github.com/weslambert/DinoSOARLab

Wyzwania

- RE oraz dostarczanie pokrycia poszczególnych poziomów w procesie inżynierii detekcji + **automatyzacja**

Wyzwania

- Bycie na bieżąco z aktualnym spektrum zagrożeń, nowych podatności, narzędzi ofensywnych oraz rozwiązań prewencyjnych i detekcyjnych zwiększających widoczność, a przede wszystkim dostarczających kontekst oraz kluczowe metadane

Gra przyspieszyła

- A na pewno stała się dużo bardziej zaawansowana technicznie, ale i też bardziej dostępna - trzeba działać, nie gadać i tyle :D

Gra przyspieszyła

- Getting and executing an arbitrary payload from an attacker's controlled NTP server
- Can work on hardened networks since NTP is usually allowed in FW
- Impersonating a legitimate NTP server via IP spoofing

- https://github.com/Idov31/Sandman

Sandman

C# PYTHON WINDOWS

Sandman is a backdoor that is meant to work on hardened networks during red team engagements.

Sandman works as a stager and leverages NTP (a protocol to sync time & date) to get and run an arbitrary **shellcode** from a pre-defined server.

Since NTP is a protocol that is overlooked by many defenders resulting in wide network accessibility.

Usage

Gra przyspieszyła

- **BadOutlook**
  - email jako wyzwalacz uruchomienia kodu, a konkretnie to zdefiniowane pole **Subject** jako trigger
  - wykorzystuje Outlook Application Interface (COM) do uruchomienia shellcodu
  - pełny dostęp do struktury i danych Outlooka

- https://github.com/aahmad097/BadOutlook

Gra przyspieszyła

- **AtomPePacker : A Highly Capable Pe Packer**
  - no crt imports
  - api hashing library
  - direct syscalls (ntdll unhooking)
  - ntdll unhooking from \KnownDlls\
  - support tls callbacks
  - support reallocation
  - no rwx section allocation
  - and more

- https://github.com/ORCx41/AtomPePacker

Gra przyspieszyła

- **ScareCrow**
  - Payload creation framework for side loading (not injecting) into a legitimate Windows process (bypassing Application Whitelisting controls). Once the DLL loader is loaded into memory, it utilizes a technique to flush an EDR’s hook out of the system DLLs running in the process's memory

- https://github.com/optiv/ScareCrow

ScareCrow

Gra przyspieszyła

- **Freeze**
  - Payload creation tool used for circumventing EDR security controls to execute shellcode in a stealthy manner. Freeze utilizes multiple techniques to not only remove Userland EDR hooks, but to also execute shellcode in such a way that it circumvents other endpoint monitoring controls.

- https://github.com/optiv/Freeze

Freeze

Gra przyspieszyła

https://github.com/improsec/SharpEventPersist

SharpEventPersist

Persistence by writing/reading shellcode from Event Log.

Usage

The SharpEventPersist tool takes 4 case-sensitive parameters:

- -file "C:\path\to\shellcode.bin"
- -instanceid 1337
- -source Persistence
- -eventlog "Key Management Service".

Gra przyspieszyła

- VirusTotalC2:
  - Abusing VirusTotal API to host our C2 traffic, useful for bypassing blocking firewall rules if VirusTotal is in the target white list , and in case you don't have C2 infrastructure , now you have a free one
  - https://github.com/D1rkMtr/VirusTotalC2

C2

- C2Matrix jako dobre miejsce na zderzenie się z dostępnymi frameworkami ofensywnymi typu Command and Control:
  - **https://www.thec2matrix.com/**
- Uzbrojenie C2:
  - boff-ami, coff-ami,
  - szyfrowanymi DLL-kami i .so → celem bypasowania EDRow i innych AV.

C2

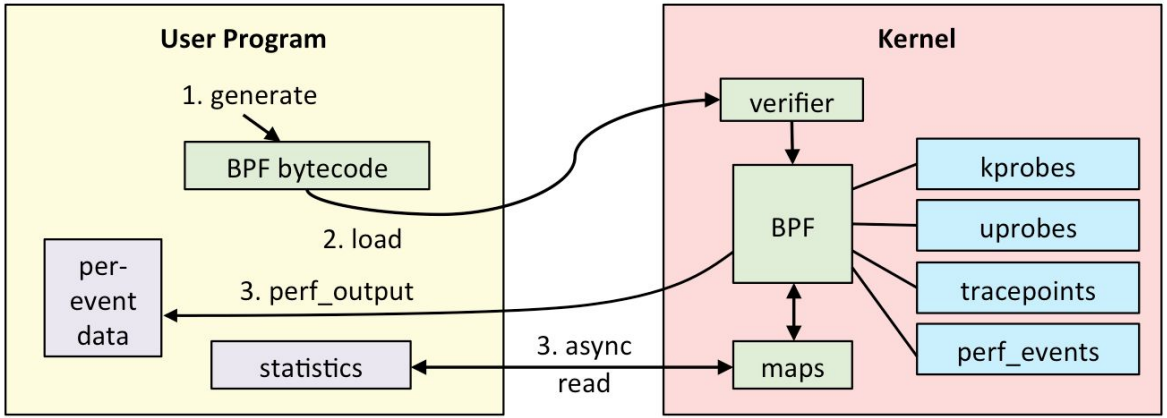
	C2 Info					C2 Matrix Info							Language		UI			
Name	License	Price	GitHub	Site	Twitter	Evaluator	Date	Version	Implementation	How-To	Slingshot	Kali	Server	Implant	Multi-User	UI	Dark Mode	API	Win
AirStrike	NA	NA	https://github.com/smokeme/airstrike		@q8fawazo	Contribute	10/2/2022												
Alan	Created Commons	NA	https://github.com/enkomio/AlanFramework		@s4tan	@s4tan	9/10/2021	4	binary				.NET	C/Asm	No	No	No	No	
Ares	NA	NA	https://github.com/sweetsoftware/Ares			@nas_bench	5/27/2021	N/A	Python				Python	Python	No	Web	Yes and only	Yes	
AsyncRAT-C#	MIT	NA	https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp			Contribute													
AtlasC2	MIT	NA	https://github.c	https://grimmie.net/atlasc2-ca	@gr1mmie	@Adam_Mashinch	3/20/2022		C#	Yes			**C#**	**C#**		CLI			
BabyShark	NA	NA	https://github.com/UnkL4b/BabyShark		@UnkL4b	@nas_bench	6/8/2021	Beta 1.0					Python	Bash	No	Web	Yes and only	No	
Badrats	GNU GPL3	NA	https://gitlab.com/KevinJClark/badrats		@GuhnooPlusLi	Contribute													
BlackMamba	MIT	NA	https://github.com/loseys/BlackMamba			Contribute													
Brute Ratel	Commercial	$2,500		https://bruteratel.com/	@NinjaParanoid	@NinjaParanoid	3/19/2021	0.3	binary				Golang	C, x64 Asm	Yes	GUI	Yes	Yes	
Bunraku	Apache 2	NA	https://github.com/theshadowboxers/bunraku			Contribute													
C3	BSD3	NA	https://github.c	https://labs.f-secure.com/tools	@FSecureLabs	@ajpc500	6/30/2021	1.3					.NET Core	C++	Yes	GUI	Yes	Yes	
CALDERA	Apache 2	NA	https://github.com/mitre/caldera			@jorgeorchilles	10/6/2019	2	pip3	Yes			Python	Go	Yes	Web		Yes	
Callidus	GNU GPL3	NA	https://github.com/3xpl01tc0d3r/Callidus		@chiragsavla94	@chiragsavla94	5/8/2020			Yes			.Net Core	.Net Core	No	CLI		No	
CHAOS	BSD3	NA	https://github.com/tiagorlampert/CHAOS		@tiagorlampert	@leekirkpatrick4	5/14/2020	3	Go		No		Go	Go	No	CLI		No	
Cobalt Strike	Commercial	$5,900		https://www.cobaltstrike.com/		@TimMedin	11/20/2019	3.14	binary				Java	C	Yes	GUI		No	
Covenant	GNU GPL3	NA	https://github.c	https://cobbr.io/tags#covenant	@cobbr_io	@jorgeorchilles	10/6/2019	0.3	Docker	Yes	Yes	Yes	C#	C#	Yes	Web	Yes	Yes	
DaaC2	NA	NA	https://github.com/crawl3r/DaaC2			Contribute													
Dali	MIT	NA	https://github.c	https://h0mbre.github.io/Imag	@h0mbre_	@jorgeorchilles	12/24/2019	POC	pip3				Python	Python	No	CLI		No	
DarkFinger	MIT	NA	https://github.com/hyp3rlinx/DarkFinger-C2		@hyp3rlinx	@nas_bench	7/4/2021	POC	Python				Python	Batch	No	No	No	No	
DBC2	NA	NA	https://github.com/Arno0x/DBC2			Contribute													
DcRat	MIT	NA	https://github.com/qwqdanchun/DcRat		@qwqdanchun	Contribute													
DeimosC2	MIT	NA	https://github.com/DeimosC2/DeimosC2		@CharlesDardar	@jasc22	9/17/2020	1.1.0 Beta	Golang				Golang	Golang	Yes	Web	Yes	Yes	
Disctopia	GNU GPL3	NA	https://github.com/3ct0s/disctopia-c2			Contribute													
Eggshell	GNU GPL2	NA	https://github.com/neoneggplant/EggShell			Contribute													
emp3r0r	MIT	NA	https://github.com/jm33-m0/emp3r0r			Contribute													
Empire	BSD3	NA	https://github.com/BC-SECURITY/Empire		@BCSecurity1	@jorgeorchilles	1/30/2020	3.0.5	install.sh	Yes	Yes	Yes	Python	PowerShell	Yes	GUI	Yes	Yes	
EvilOSX	GNU GPL3	NA	https://github.com/Marten4n6/EvilOSX			@cabbagesalad2	11/12/2019	7.2.1	pip3			Yes	Python	Python	No	GUI		No	
Faction C2	BSD3	NA	Taken down	https://c2lol.blob.core.windows.net/text/faction		@jorgeorchilles	10/30/2019	NA	install.sh	Yes	Yes	Yes	.NET	.NET	Yes	Web		Yes	
FlyingAFalseFlag	GNU GPL3	NA	https://github.com/monoxgas/FlyingAFalseFlag			@jorgeorchilles	11/12/2019	POC	pip3				Python	C++	No	CLI		No	

C2

- Bo już nie chodzi tylko o Cobalt Strike, Slivera czy Metasploita →
  - Brute-Ratel-C4
  - Havoc C2
  - Mythic C2
  - + 100 tych bardziej znanych
- Phishing NG → evilnginx2 + gophish / true Reverse Proxy i przekazanie połączenia do serwisu efektywnie zapisując dane sesyjne - pozostaje import do browsera → pełne bypassy MFA

Rosnące zainteresowanie eBPF

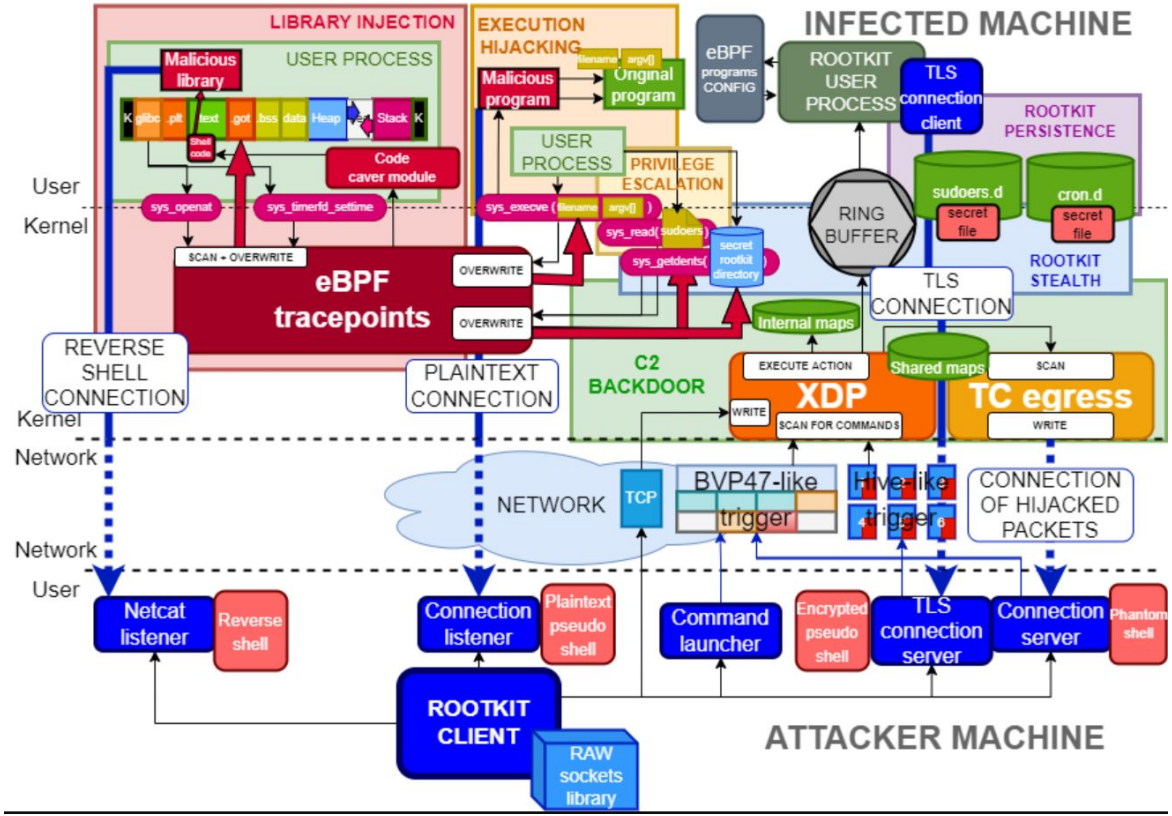
- eBPF Summit 2022 ponownie dowiodła, że eBPF w Linuksie to przyszłość osiągania wysokich wydajności sieciowych, widoczności i bezpiecznego dostępu do kernel space bez potrzeby ładowania modułu do jądra



Rosnące zainteresowanie eBPF

- Skoro popularność technologii rośnie to zwiększa się również zainteresowanie atakujących:
  - LPE / RCE
  - Persistence
- Dostępne kody źródłowe rootkitów wykonujących syscall hooking na warstwie eBPF:
  - **Tracee vs TripleCross** :>
    - Library injection module
    - An execution hijacking module
    - A local privilege escalation module that allows for running malicious programs with root privileges.
    - A backdoor with C2 capabilities + rootkit client
    - A persistence module
    - https://github.com/h3xduck/TripleCross

TripleCross



DEFENSIVE SECURITY

Jak i gdzie trenować takie umiejętności?

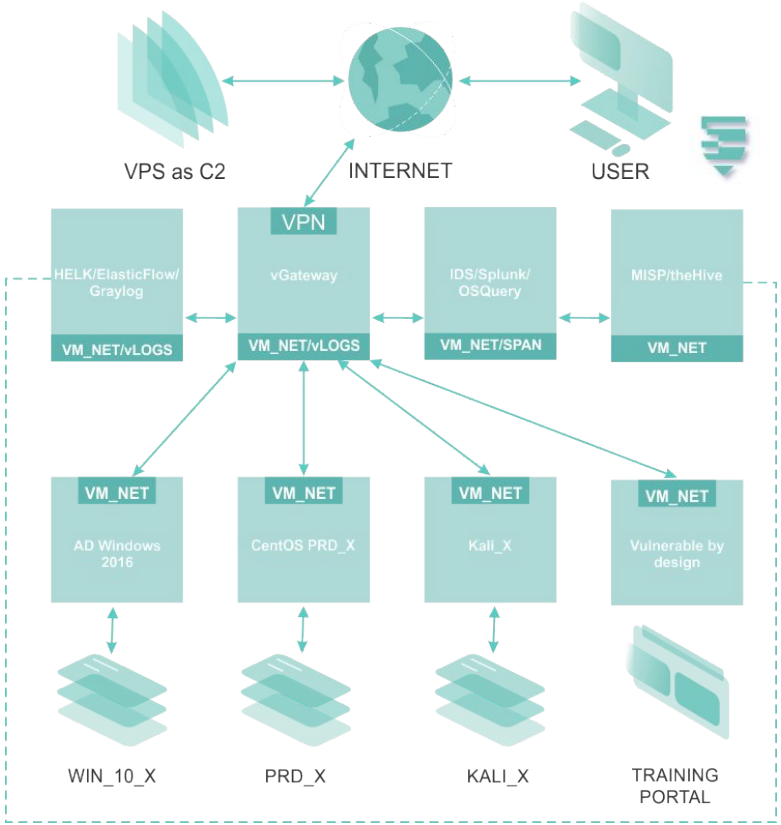
Cyber Range

Dedykowana infrastruktura pozwalająca na przeprowadzanie detekcji i analiz zachowania atakujących pod kątem wykorzystywanych technik, taktyk, procedur oraz narzędzi ofensywnych.

Sysmon & Windows events | Firewall logs | Netflow | Zeek | Suricata

OSquery | System/ authlogs | PowerShell logs | WAF logs | Proxy logs | Audit logs

Środowisko służyć ma stałemu podnoszeniu kompetencji w zakresie wyszukiwania zagrożeń (threat hunting) oraz poznawania aktualnych trendów działań ofensywnych (red teaming) w bezpośrednim ujęciu detekcyjnym (blue teaming)

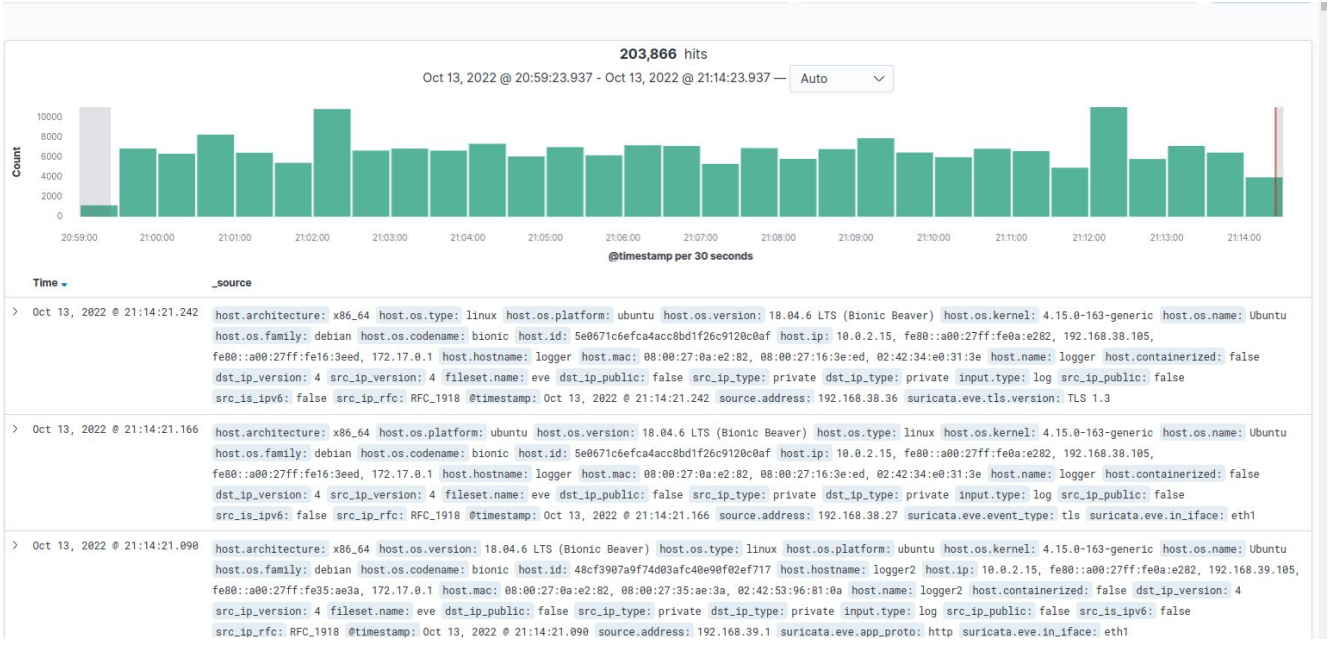


Transfer wiedzy

- **Atak vs detekcja + DFIR**
- Symulacje APT
- Gry i zabawy z nowymi podatnościami / exploitami
- Warsztaty stacjonarne, wirtualne i hybrydowe
- Spotkania cykliczne
- **Newsy z placu boju**
- **100% HANDS-ON**

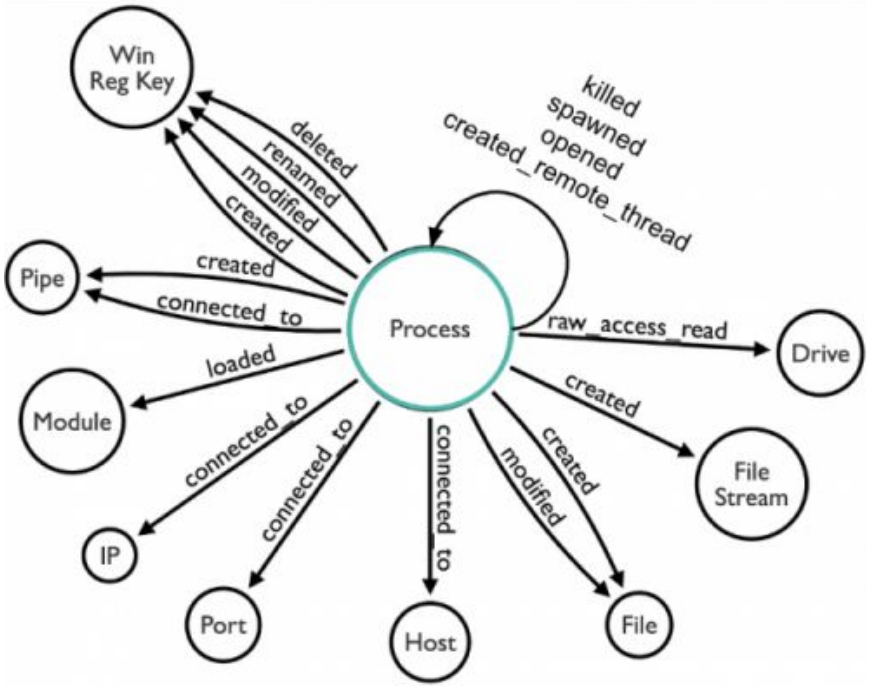
Cyber Range - SIEM

- Hunting ELK
- Splunk
- Graylog



Cyber Range - sysmon

- Rozszerzona widoczność systemowa / audytowa dla Windowsów i Linuxów:

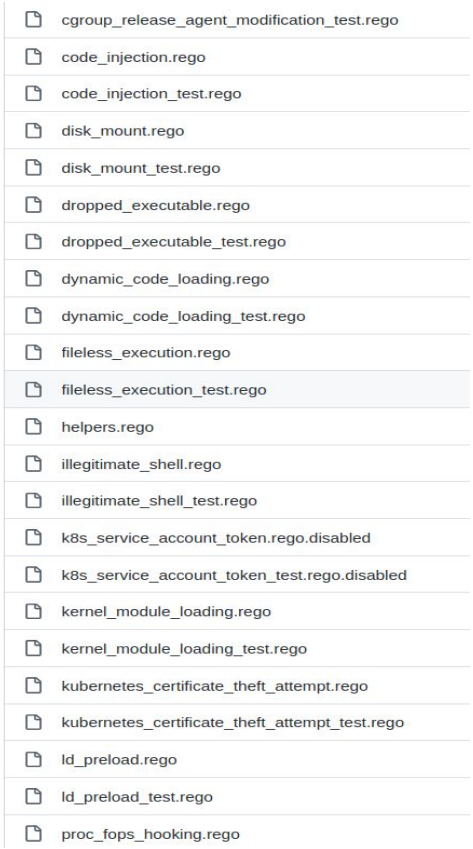


Cyber Range - Falco

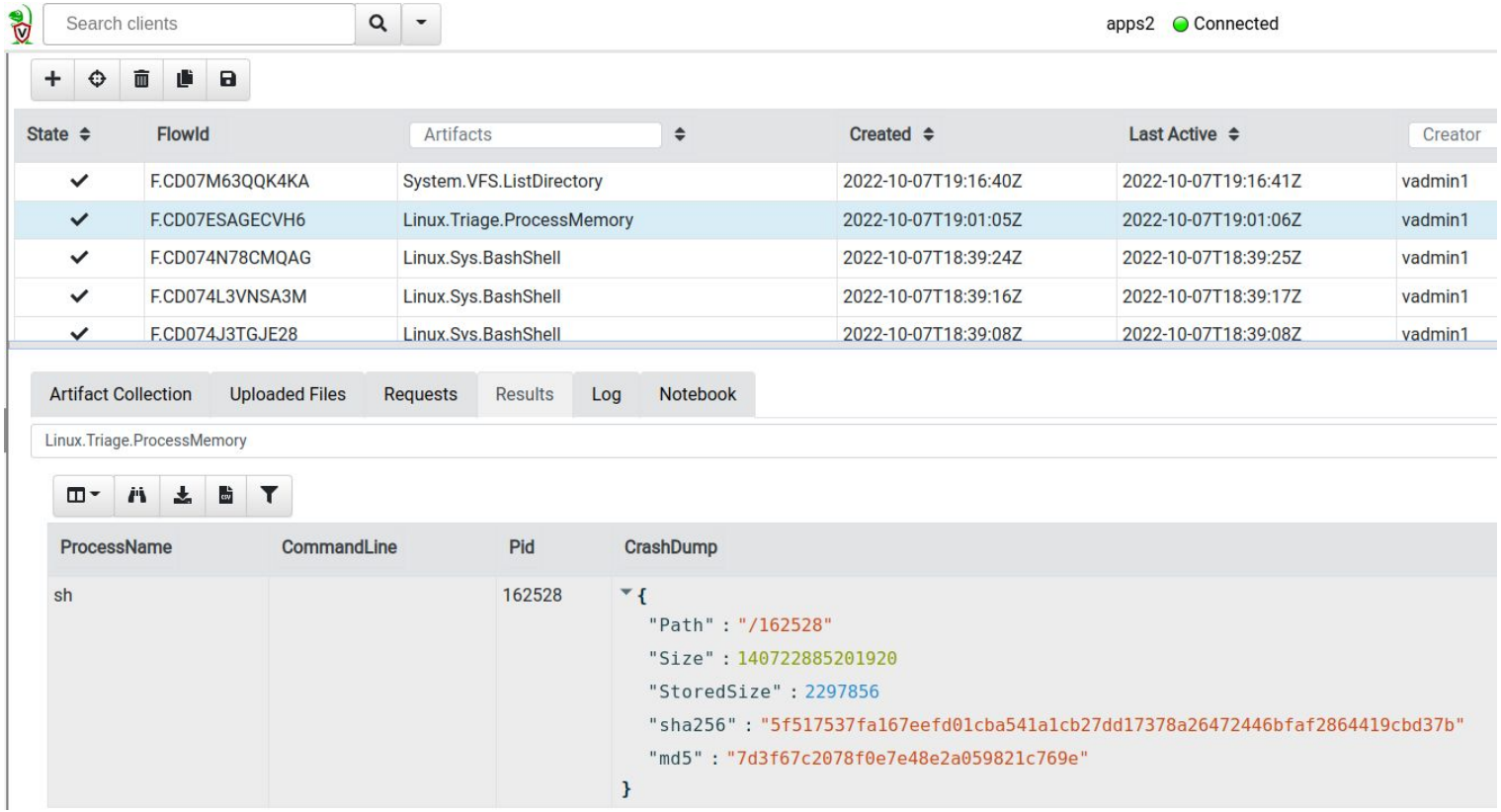
- Rozszerzona widoczność systemowa / audytowa dla Linuxów:
  - Falco:
    - Can detect and alert on any behavior that involves making Linux system calls
    - Alerts can be triggered by the use of specific system calls, their arguments, and by properties of the calling process
    - https://github.com/falcosecurity/falco

Cyber Range - Tracee

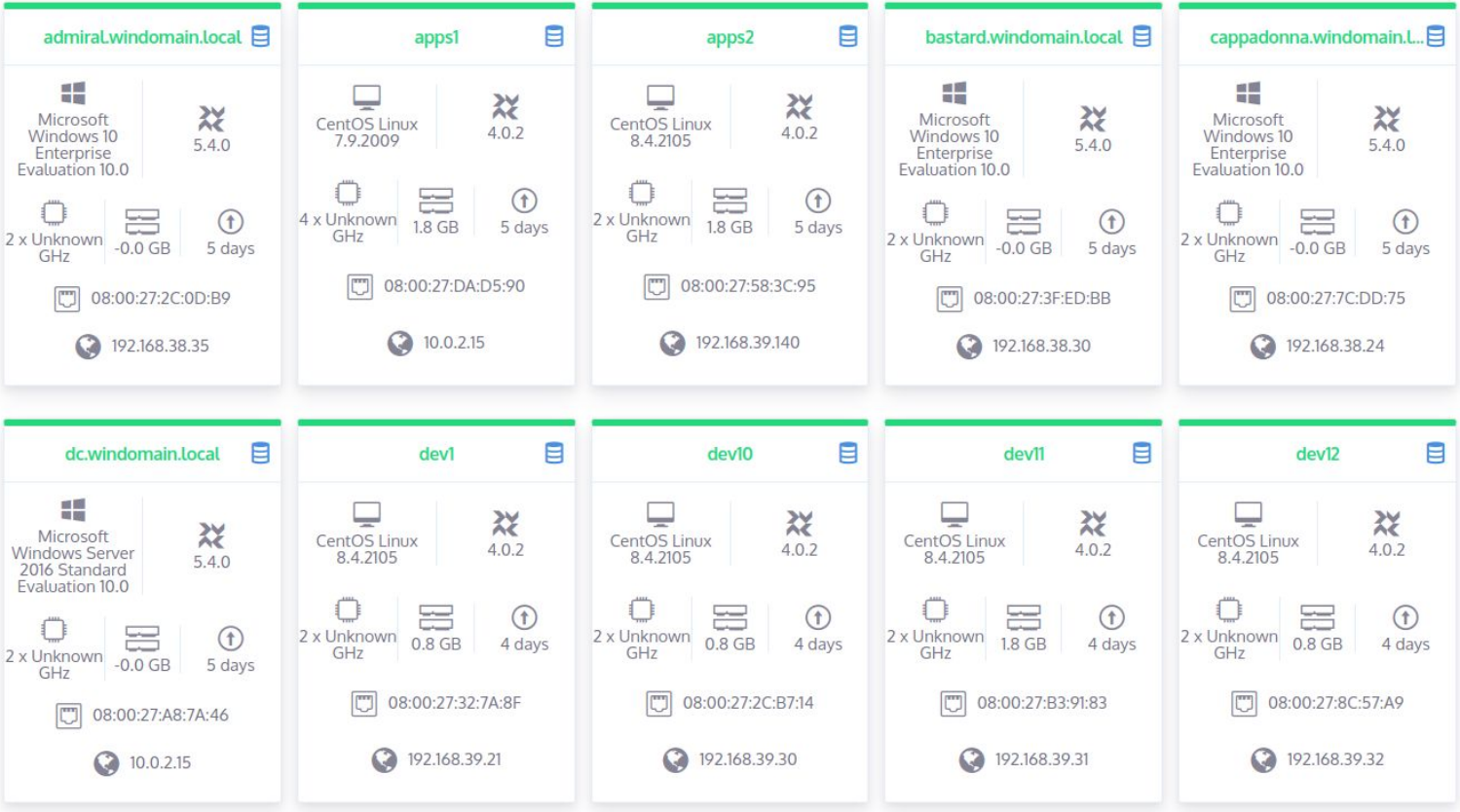
- Rozszerzona widoczność systemowa / audytowa dla Linuxów:
  - Tracee:
    - Runtime Security and forensics tool for Linux.
    - Uses Linux **eBPF** technology to trace your system and applications at runtime, and analyzes collected events in order to detect suspicious behavioral patterns.
    - https://github.com/aquasecurity/tracee



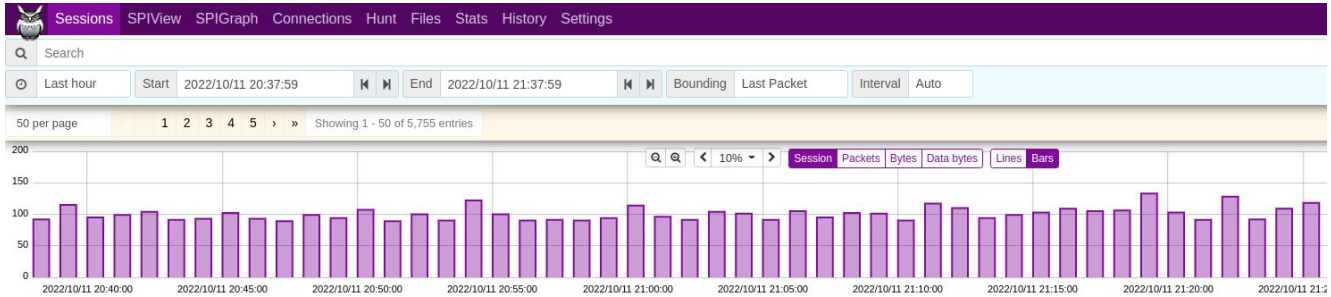
Cyber Range - Velociraptor DFIR



Cyber Range - OSQuery

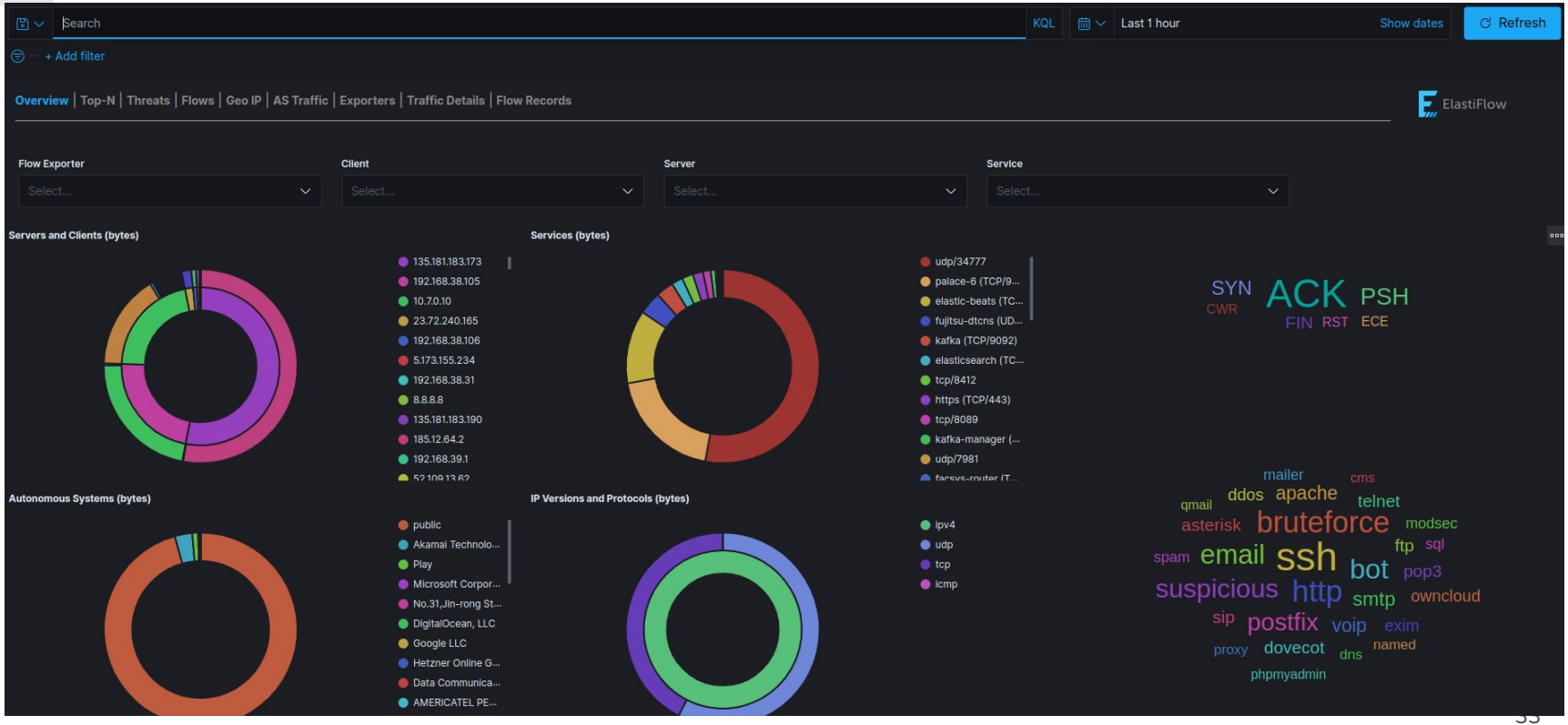


Cyber Range - Moloch/Arkime FPC



Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
udp 2022/10/11 21:37:01	2022/10/11 21:37:01	192.168.38.38	138	192.168.38.255	138	1	201 243	logger	
udp 2022/10/11 21:37:00	2022/10/11 21:37:00	192.168.38.232	35832	31.209.85.242	123	2	96 180	logger	
tcp 2022/10/11 21:36:58	2022/10/11 21:37:26	192.168.38.1	38274	192.168.38.105	8089	19	4,344 5,614	logger	
tcp 2022/10/11 21:36:56	2022/10/11 21:37:24	192.168.38.1	38268	192.168.38.105	8089	19	4,342 5,612	logger	
tcp 2022/10/11 21:36:54	2022/10/11 21:37:22	192.168.38.1	38266	192.168.38.105	8089	19	4,336 5,606	logger	
udp 2022/10/11 21:36:51	2022/10/11 21:36:51	192.168.38.225	44716	5.145.135.89	123	2	96 180	logger	
tcp 2022/10/11 21:36:50	2022/10/11 21:37:01	192.168.38.24	62030	192.168.38.102	445	25	6,082 7,486	logger	
tcp 2022/10/11 21:36:48	2022/10/11 21:37:16	192.168.38.1	38264	192.168.38.105	8089	19	4,334 5,604	logger	
tcp 2022/10/11 21:36:48	2022/10/11 21:36:48	192.168.38.30	57834	192.168.38.102	389	17	6,754 7,726	logger	
tcp 2022/10/11 21:36:48	2022/10/11 21:36:48	192.168.38.30	57833	192.168.38.102	389	250	315,947 329,585	logger	
tcp 2022/10/11 21:36:48	2022/10/11 21:36:59	192.168.38.30	57832	192.168.38.102	49678	20	2,108 3,248	logger	
tcp 2022/10/11 21:36:47	2022/10/11 21:37:15	192.168.38.1	38262	192.168.38.105	8089	19	4,333 5,603	logger	
icmp6 2022/10/11 21:36:47	2022/10/11 21:36:47	fe80::a00:27ff:fef7:e1a8	0	ff02::2	0	1	16 70	logger	
udp 2022/10/11 21:36:46	2022/10/11 21:36:46	192.168.38.234	35918	8.8.8.8	53	4	276 444	logger	Host new-fp-shed.wg1.b.yahoo.com www.yahoo.com
udp 2022/10/11 21:36:46	2022/10/11 21:36:46	192.168.38.228	56229	8.8.8.8	53	4	276 444	logger	Host new-fp-shed.wg1.b.yahoo.com www.yahoo.com
udp 2022/10/11 21:36:45	2022/10/11 21:36:45	192.168.38.27	65300	192.168.38.102	53	2	141 225	logger	Host wpad.windomain.local

Cyber Range - ElastiFlow



Cyber Range - Zeek IDS

- Zeek + customowe moduły:
  - JA3
  - HASSH
  - Community_ID
  - long-connections
  - Spicy-ipsec/wireguard
  - Anomalous-dns
  - Pingback
- Metadane z połączeń per protokół:

Network Protocols

Log File	Description	Field Descriptions
:file:`conn.log`	TCP/UDP/ICMP connections	:zeek:type:`Conn::Info`
:file:`dce_rpc.log`	Distributed Computing Environment/RPC	:zeek:type:`DCE_RPC::Info`
:file:`dhcp.log`	DHCP leases	:zeek:type:`DHCP::Info`
:file:`dnp3.log`	DNP3 requests and replies	:zeek:type:`DNP3::Info`
:file:`dns.log`	DNS activity	:zeek:type:`DNS::Info`
:file:`ftp.log`	FTP activity	:zeek:type:`FTP::Info`
:file:`http.log`	HTTP requests and replies	:zeek:type:`HTTP::Info`
:file:`irc.log`	IRC commands and responses	:zeek:type:`IRC::Info`
:file:`kerberos.log`	Kerberos	:zeek:type:`KRB::Info`
:file:`modbus.log`	Modbus commands and responses	:zeek:type:`Modbus::Info`
:file:`modbus_register_change.log`	Tracks changes to Modbus holding registers	:zeek:type:`Modbus::MemmapInfo`
:file:`mysql.log`	MySQL	:zeek:type:`MySQL::Info`
:file:`ntlm.log`	NT LAN Manager (NTLM)	:zeek:type:`NTLM::Info`
:file:`ntp.log`	Network Time Protocol	:zeek:type:`NTP::Info`
:file:`radius.log`	RADIUS authentication attempts	:zeek:type:`RADIUS::Info`
:file:`rdp.log`	RDP	:zeek:type:`RDP::Info`
:file:`rfb.log`	Remote Framebuffer (RFB)	:zeek:type:`RFB::Info`
:file:`sip.log`	SIP	:zeek:type:`SIP::Info`
:file:`smb_cmd.log`	SMB commands	:zeek:type:`SMB::CmdInfo`

Cyber Range - Suricata IDS

- Zestawy sygnatur:
  - # suricata-update enable-source et/open
  - # suricata-update enable-source ptresearch/attackdetection
  - # suricata-update enable-source tgreen/hunting
  - # suricata-update enable-source sslbl/ja3-fingerprints

Detekcja Linuksowa / IR

- eBPF:
  - Falco
  - Tracee
  - Sysmon for Linux
  - ebpf-monitor
- Wazuh HIDS
- auditd
- OSQuery
- Velociraptor:
  - Linux.Collection.CatScale
  - Yara na plikach / na procesach
  - Pełny DFIR w tym Memory Forensics
- Strelka
- unhide
- Sandfly

Detekcja Linuksowa #1

- Podejrzane procesy:
  - Proces nadal działa, ale binarka została usunięta
  - Proces komunikuje się poprzez sieć
  - Wysokie obciążenie CPU
  - Niespotykana nazwa procesu
  - Proces o nazwie bardzo podobnej lub identycznej do procesów systemowych czy wątków kernelowych np. **[kworker/1:2H]**
  - Poprawny proces systemowy, ale ze wstrzykniętym kodem poprzez:
    - ptrace() → https://github.com/gaffe23/linux-inject
    - dlinject.py → https://github.com/DavidBuchanan314/dlinject

```
ulexec@ubuntu:~/Documents$ ps -aux | grep kworker/u8
root        2303  0.0  0.0   2524  1940 ?        t    04:31   0:00 [kworker/u8:7-ev]
ulexec      4777  0.0  0.0  21536  1088 pts/0    S+   20:30   0:00 grep --color=auto kworker/u8
ulexec@ubuntu:~/Documents$
```

Detekcja Linuksowa #2

- User mode rootkit:
  - PAM-based + Telegram Exfil
    - /etc/pam.d/ , /lib64/security/
    - https://github.com/mthbernardes/sshLooterC/blob/master/looter.c
  - SSHD backdoor:
    - https://blog.xpnsec.com/linux-process-injection-aka-injecting-into-sshd-for-fun/
  - HTTPD:
    - mod_backdoor HTTPD Server:
      - https://github.com/VladRico/apache2_BackdoorMod
    - mod_authg:
      - https://github.com/ChristianPapathanasiou/apache-rootkit

Detekcja Linuksowa #3

- Webshells
  - uruchamianie kodu z kontekstu aplikacji / serwera HTTP:
    - SOCKS proxy z poziomu PHP/ASP/JSP:
      - https://github.com/sensepost/Regeorg
  - Warto zwrócić uwagę na → slopShell:
      - https://github.com/oldkingcone/slopShell
  - Generyczna detekcja webshelli na bazie relacji parent-child dla procesów:
    - https://github.com/SigmaHQ/sigma/blob/master/rules/linux/process_creation/proc_creation_lnx_webshell_detection.yml

Detekcja Linuksowa #4

- Kernel mode rootkit → LKM → Loadable Kernel Modules:
  - ukrywanie plików, procesów, połączeń sieciowych
  - ukrywanie modułu /proc/modules
  - aktywacja keyloggera / drop2shell poprzez wysłanie specjalnego sygnału / pakietu sieciowego
  - Przykłady:
    - suterusu
    - rkduck
    - reptile
    - Diamorphine
    - krf
    - Umbra
    - Drovorub

https://github.com/milabs/awesome-linux-rootkits#hear_no_evil-kernel-mode-rootkits

Rekomendowany kierunek

- Sigma Rules:
  - Generyczny format opisu zdarzeń bazujący na logach i kontekstach, np. whoami uruchamiany z uprawnieniami SYSTEM
  - Konwerter reguł Sigma do dowolnego silnika SIEM:
    - sigmac
    - https://uncoder.io/
  - Sigma for Linux:
    - https://github.com/SigmaHQ/sigma/tree/master/rules/linux
  - Hayabusa:
    - https://github.com/Yamato-Security/hayabusa
  - Zircolite:
    - https://github.com/wagga40/Zircolite

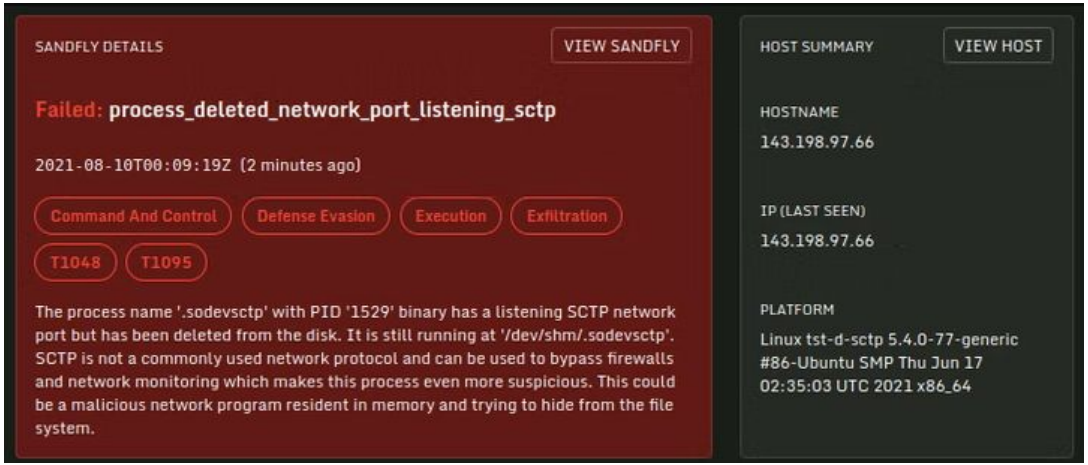
Rekomendowany kierunek

- Protections Artifacts:
  - aktywny projekt od Elastic zawierający:
    - reguły YARA,
      - np. Linux_Backdoor_Tinyshell_67ee6fae
    - reguły EQL opisujące złośliwe zachowanie:
      - np. cred_access_web_browsers_password_access_via_cmd
  - https://github.com/elastic/protections-artifacts

- Świetne źródło wiedzy i super przydatne do:
  - Analizy malware
  - Threat Hunting
  - IR / Forensics

Proaktywne skanowanie DFIR

- Sandfly Security + usługa cyklicznego skanowania:
  - skaner wykrywający podejrzane zachowanie dowolnego Linuksa
  - bezagentowy, ponad 2000 definicji i kombinacji wykrywania anomalii
  - kontekstowy opis wyników + mapowanie MITRE Attack Framework
  - https://www.sandflysecurity.com/ ← **WARTO sprawdzić!**



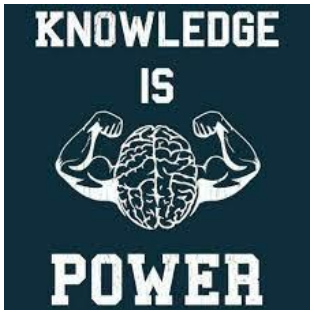
Podsumowanie - wartości

1. Rozwinięcie umiejętności analitycznych zespołu wymaganych do pracy w środowisku Security Operation Center.
2. Zwiększenie świadomości skomplikowania i występujących zależności pomiędzy elementami kampanii APT i obszarami detekcji.
3. Okresowy transfer wiedzy i systematyczne poszerzanie kompetencji zespołu z zakresu Red + Blue = Purple teaming.
4. Zdobycie umiejętności budowania ścieżek ataków (Attack Paths / Attack Lifecycles) oraz łańcuchów zdarzeń dzięki kombinacji pojedynczych technik, taktyk i procedur atakującego (Chain Attack Scenarios).
5. Zrozumienie wartości płynących z podejścia "Assume Breach" oraz symulacji zagrożeń po wczesnym uzyskaniu dostępu (C2, post-exploitation, Lateral Movement, Persistence, Evasion).
6. Zrozumienie czym jest threat hunting i dlaczego jest istotny.
7. Uzyskanie umiejętności związanych z generowaniem podejrzanych zdarzeń na warstwie sieci i systemów operacyjnych Windows i Linux oraz sposobów ich wykrywania.
8. Zrozumienie potencjału reguł Sigma i płynących z nich wartości dla rozwiązań SIEM.
9. Walidację aktualnego stanu bezpieczeństwa sieci organizacji i występujących ryzyk.
10. Uzyskanie wiedzy dt. zasilenia / utworzenia kompletnego środowiska SOC z wykorzystaniem oprogramowania Open Source.

Podsumowanie

- “Obrońcy muszą znać tysiące sposobów, na które system może zostać skompromitowany. Atakujący muszą znać tylko ten jeden właściwy.”

- “Atakujący muszą znać tysiące sposobów, aby zatrzeć po sobie ślady. Obrońcy muszą zauważyć tylko jedną nieprawidłowość.”



DEFENSIVE SECURITY

50% OFF: VY8ZAD2-MCC

Linux Attack and Forensics Inspection At Scale - https://edu.defensive-security.com/

Do poczytania

- VMware Exposing Malware in Linux-Based Multi-Cloud Environments:
  - https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
- My Methods To Achieve Persistence In Linux Systems:
  - https://flaviu.io/advanced-persistent-threat/
- Advanced Persistent Threat Techniques Used in Container Attacks:
  - https://blog.aquasec.com/advanced-persistent-threat-techniques-container-attacks
- Linux Compromise Detection:
  - https://2018.purplecon.nz/archive/craig-h-rowland/Linux.Compromise.Detection.Presentation.pdf
- Hunting for Persistence in Linux:
  - https://pberba.github.io/security/2021/11/22/linux-threat-hunting-for-persistence-sysmon-auditd-webshell/

DEFENSIVE SECURITY

Dziękuję za uwagę i zapraszam do kontaktu!

Leszek Miś
lm@defensive-security.com
https://defensive-security.com
https://edu.defensive-security.com