Cyber Range - podnoszenie technicznych kompetencji zespołów SOC/CSIRT w sposób ciągły.

Leszek Miś / Security Researcher

whoami

- Security Researcher / Founder / uid=0 @ Defensive Security
- Offensive Security Certified Professional (OSCP)
- Red Hat Certified Architect/RHCSS/RHCX/Sec+
- Trener / wykładowca podczas Black Hat US, Hack In The Box AMS / Singapore / Abu Dhabi, OWASP Appsec US, Flocon US, BruCON, Confidence PL
- Obszary zainteresowania:
  - Cyber Range Playgrounds
  - 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 Software

Agenda

I. Wprowadzenie:

- Czym jest środowisko Cyber Range?
- Cele, korzyści i wartości
- Stos technologiczny w wydaniu Open Source

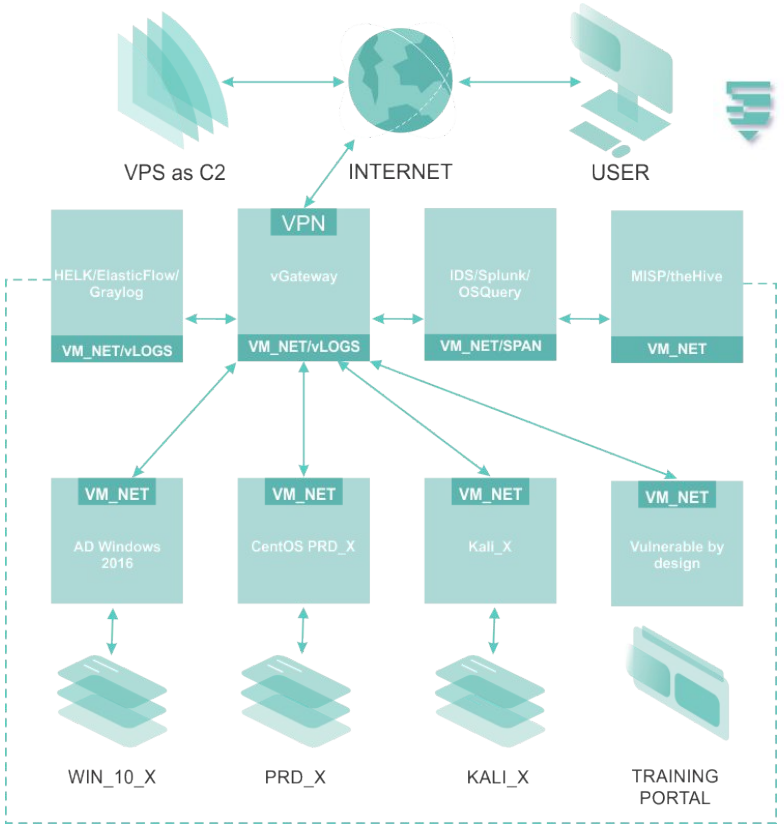
II. Sposoby transferu wiedzy:

- Emulacja zachowań grup APT
- Atak vs detekcja
- Przez detekcję do ataku
- CTF

III. Przykładowy scenariusz APT w ujęciu detekcyjnym

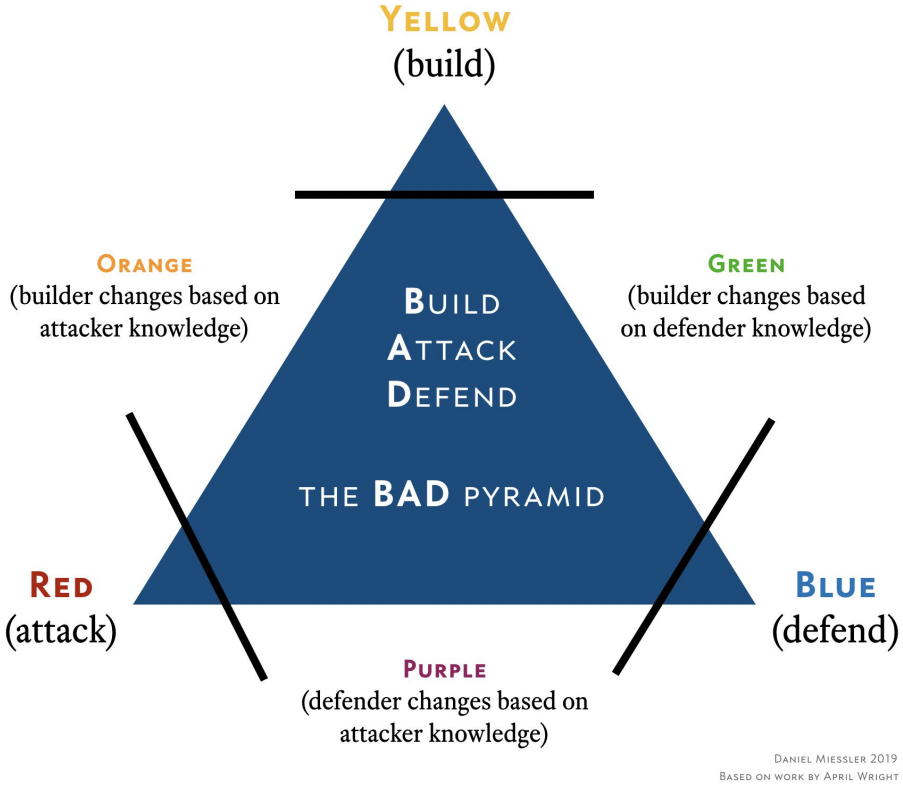
Cyber Range

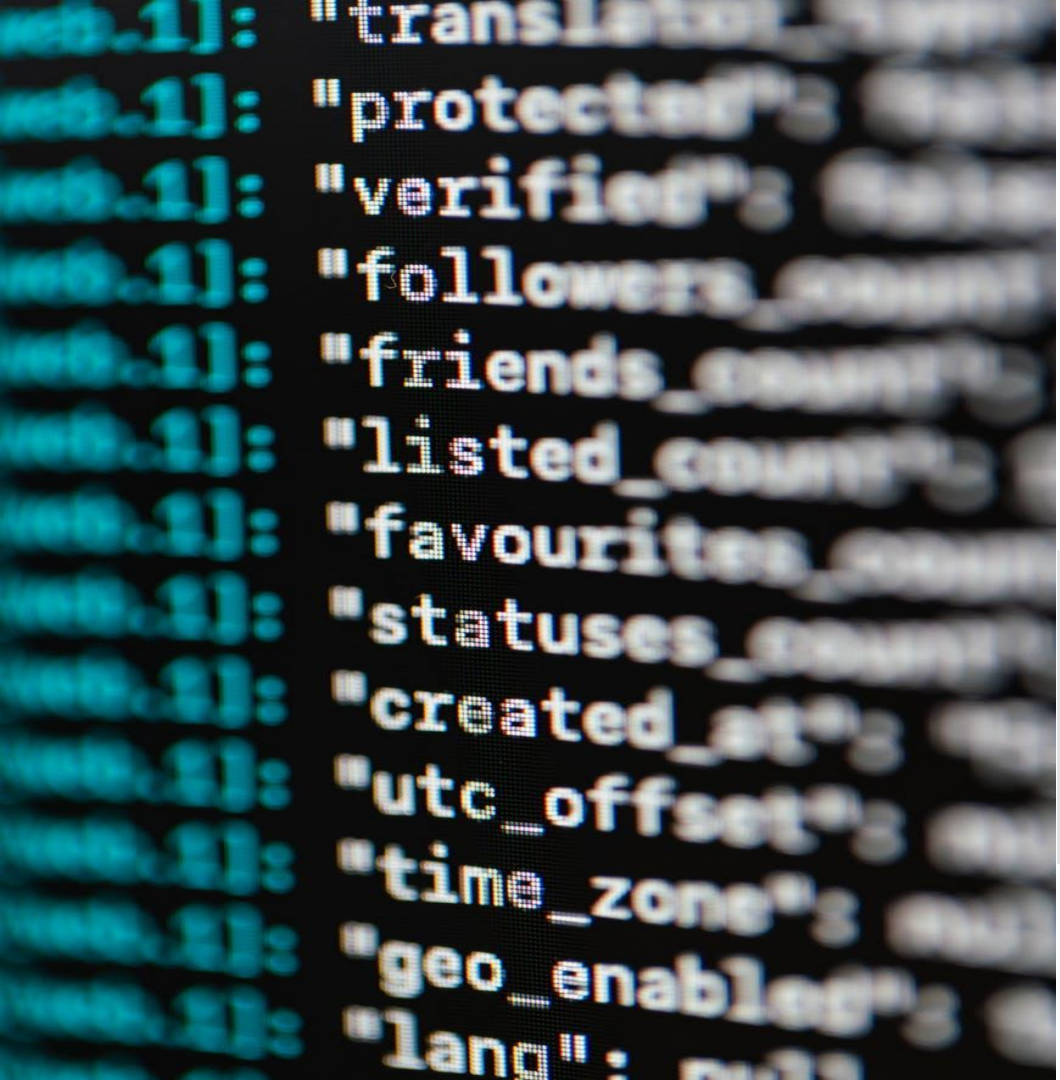
Dedykowana infrastruktura pozwalająca na przeprowadzanie detekcji i analiz zachowania atakujących pod kątem wykorzystywanych technik, taktyk, procedur oraz narzędzi ofensywnych.



Cyber Range

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





Wartości i korzyści

- Rozwinięcie umiejętności analitycznych wymaganych do pracy w środowisku Security Operation Center / CSIRT
- Zwiększenie świadomości skomplikowania i występujących zależności pomiędzy elementami kampanii APT i obszarami detekcji.
- Okresowy / ciągły transfer wiedzy z zakresu Red + Blue = Purple teaming.

Mapowanie ATT&CK Framework

Kategoryzacja ćwiczeń per taktyka:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact
- + Breach and Attack Simulations
- + Forensics

Stos technologiczny

- Widoczność na warstwie hosta i sieci:
  - SIEM → HELK / Graylog / Splunk
  - Zeek IDS / Suricata IDS
  - Wazuh HIDS + Sysmon / auditd
  - Falco / Tracee / Sysmon / eBPF
  - Velociraptor → DFIR client events
  - OSquery → active SQL-based OS data
  - Arkime / Moloch → Full Packet Capture
  - Elastiflow → Netflow Analytics
  - theHive Incident Response Mgmt
  - Sandfly → Linux Detection and IR

Transfer wiedzy

- Symulacje APT
- Atak vs detekcja
- Grywalność / CTF
- **Gry i zabawy z jeszcze gorącymi podatnościami / exploitami**
- Warsztaty stacjonarne, wirtualne i hybrydowe

Przykładowy scenariusz w stylu Purple

Atak		Detekcja
External enumeration → OSINT / attack preparation	1	Honeypots, WAF, Proactive DNS fuzzing
Initial Access → DNS Rebinding + local Docker API	2	Zeek DNS / Full Packet Capture + Falco
Discovery → PEASS-ng / nmap / cme	3	Suricata IDS, Falco, auditd + Wazuh
Privilege escalation → Kernel exploit / pkexec	4	Syscall filtering / Tracee eBPF
Defense Evasion → Process injection (ptrace())	5	Syscall filtering / Tracee eBPF / Velociraptor DFIR
Persistence → cron / rc.scripts / PAM / rootkit	6	File Integrity Monitoring, Yara, Sandfly, LKRG
Command and Control → Sliver / Covenant C2	7	JA3, beacon telemetry, Falco

Emulacje w stylu Purple

https://thedfirreport.com

From Zero to Domain Admin

CONTInuing the Bazar Ransomware Story

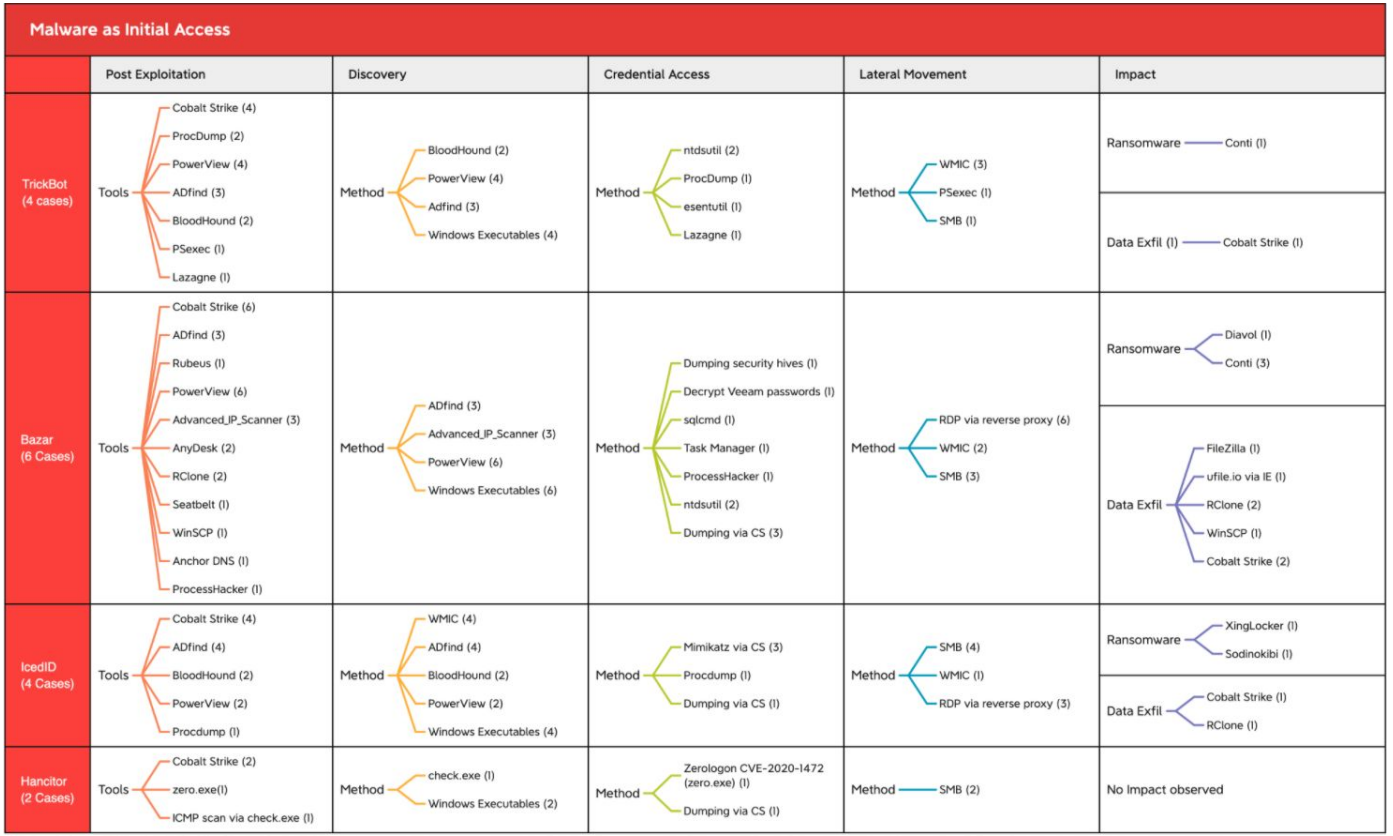
Qbot and Zerologon Lead To Full AD Compromise

From Word to Lateral Movement in 1 Hour

Trickbot Leads Up to Fake 1Password Installation

Dridex – From Word to Domain Dominance

Emulacje w stylu Purple - 2021



Przez detekcję do ataku

- Sigma Rules:
  - Generyczny format opisu zdarzeń bazujący na logach
  - **Opis logiki ataku i detekcji w jednym miejscu**
  - https://github.com/SigmaHQ/sigma


```
logsource:
  product: windows
  category: process_creation
detection:
  selection1:
    ParentImage|endswith: '\powershell.exe'
    Image|endswith: '\schtasks.exe'
    CommandLine|contains|all:
      - '/Create'
      - '/SC'
  selection2:
    CommandLine|contains:
      - 'ONLOGON'
      - 'DAILY'
      - 'ONIDLE'
      - 'Updater'
    CommandLine|contains|all:
      - '/TN'
      - 'Updater'
      - '/TR'
      - 'powershell'
  condition: selection1 and selection2
```

Podsumowanie

- Środowisko typu Cyber Range to kluczowy składnik służący do rozwoju umiejętności technicznych zespołów SOC/CSIRT:
  - Uzyskasz umiejętności związane z generowaniem podejrzanych zdarzeń na warstwie sieci i systemów operacyjnych Windows i Linux oraz sposobów ich wykrywania
  - Zdobędziesz umiejętności budowania ścieżek ataków (Attack Paths / Attack Lifecycles) oraz łańcuchów zdarzeń dzięki kombinacji pojedynczych technik, taktyk i procedur atakującego
  - Zrozumiesz wartości płynących z podejścia "Assume Breach" oraz symulacji zagrożeń po wczesnym uzyskaniu dostępu (C2, post-exploitation, Lateral Movement, Persistence, Evasion)
  - Zrozumiesz potencjał reguł Sigma i płynących z nich wartości dla rozwiązań SIEM
  - Przeprowadzisz walidację aktualnego stanu bezpieczeństwa sieci organizacji i występujących ryzyk

Dziękuję za uwagę i zapraszam do kontaktu:)

lm@defensive-security.com