Know your enemy

Martin Stanek

2025

Table of Contents

Motivation

- adversary tactics, techniques, and procedures (TTP)
  - replicate in your testing (pentest, resilience assessment)
  - improve security monitoring and incident response
- changing security landscape
  - new TTPs
  - evolving IT infrastructure (*aaS, upgrades, new systems etc.)

(Cyber) Threat intelligence

Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
[NIST SP 800-150]

- strategic (trends, general info)
  - long-term plans, CISO level
- tactical (TTPs of recent threats)
- operational (indicators of compromise IOCs, URLs, IP addresses, etc.)
  - often machine readable, consumed by firewalls, SIEM, IPS etc.

(Cyber) Threat intelligence

- relevant up to date information, often tailored for specific organization
  - who is likely to attack, what assets, and how
  - how to detect
  - recommended actions to defend
- prioritize effort and spending
  - avoid neglecting *old and obvious* weaknesses
- commercial services, offered by many security vendors
- OSINT sources: *see next lecture*

Cyber Kill Chain

- Lockheed Martin [1]
- model: what the adversaries must complete in order to achieve their objective

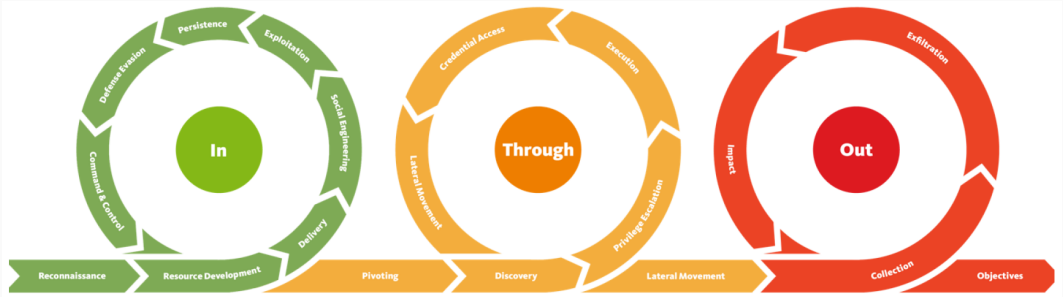
Reconnaissance	Harvest email addresses, Discover internet-facing servers, ...
Weaponization	Coupling exploit with backdoor into deliverable payload, ...
Delivery	E-mail, USB, web server, ...
Exploitation	Software, hardware, or human vulnerability, ...
Installation	Backdoor, webshell, persistence, ...
Command and Control	Two way communications to C2 infrastructure (web, DNS, mail), ...
Actions on Objectives	Achieve the goal: exfiltrate data, privilege escalation, destroy, ...

Cyber Kill Chain – remarks

- high level and (strictly) sequential model
- idea: stop attack at any stage, plan and test controls for each stage
  "*Stopping adversaries at any stage breaks the chain of attack!*"
- weaknesses of this model
  - only high level info (details are missing)
  - rigid structure (many attacks skips or combine stages)
  - focus on perimeter (insider threats do not fit the model)
  - focus on malware/payload (web app vulnerabilities, DoS, etc. are different)

The Unified Kill Chain

- P. Pols, 18 attack phases; grouped into In, Through, and Out objectives
- limited usability for operational and tactical planning/testing



source: https://www.unifiedkillchain.com

MITRE ATT&CK

"*globally-accessible knowledge base of adversary tactics and techniques based on real-world observations*" [2]

- established, mid-level adversary model
- use cases
  - Threat Intelligence
  - Detection and Analytics
  - Adversary Emulation and Red Teaming
  - Assessments and Engineering
- tactic: (why) the reason for performing an action
- technique: *how* an adversary achieves a tactical goal by performing an action.

MITRE ATT&CK cont.

- domains:
  - Enterprise (subsets for various OS, cloud services, network, containers)
  - Mobile (iOS, Android)
  - ICS (industrial control systems)
- ATT&CK v16.1 (October 2024):
  - Enterprise: 14 Tactics, 203 Techniques, 453 Sub-Techniques, 159 Groups, 710 Pieces of Software, 34 Campaigns, 44 Mitigations, and 37 Data Sources
- ATT&CK Navigator – interactive tool

Enterprise (14 tactics)

- Reconnaissance (10 techniques)
- Resource Development (8)
- Initial Access (10)
- Execution (14)
- Persistence (20)
- Privilege Escalation (14)
- Defense Evasion (44)
- Credential Access (17)
- Discovery (32)
- Lateral Movement (9)
- Collection (17)
- Command and Control (18)
- Exfiltration (9)
- Impact (14)

Structure

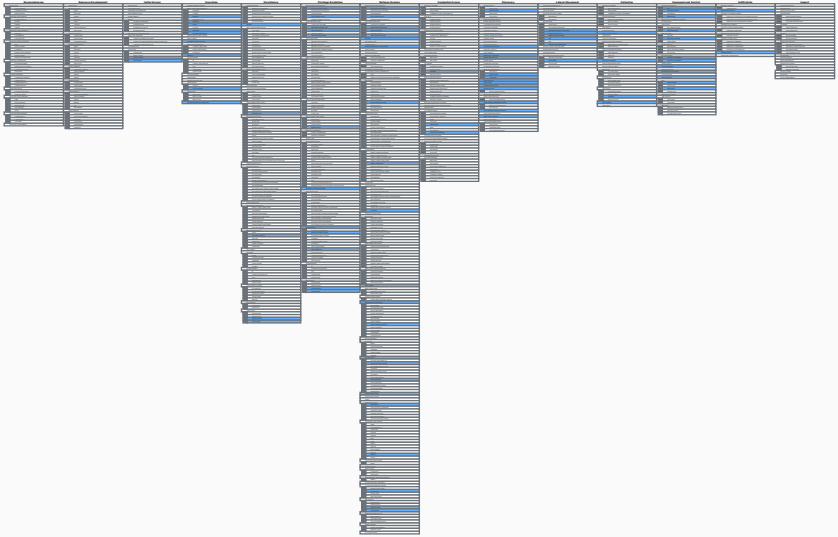
- Technique / sub-technique
  - description
  - info: platforms
  - procedure examples: what threat actors used the technique and how
  - mitigations: preventive measures
  - detection: what to monitor
  - references
  - previous ATT&CK versions: CAPEC cross reference
- CAPEC (Common Attack Pattern Enumerations and Classifications)
  - comprehensive dictionary of known patterns of attack employed by adversaries
  - approx. 560 attack patterns
  - crosslinked world: CAPEC $\mapsto$ ATT&CK, CWE

Example – Discovery / Network Service Discovery (T1046)

- Tactic: Discovery
- Platforms: Containers, IaaS, Linux, Network, Windows, macOS
- Procedures (57)
  - e.g. *APT39 has used CrackMapExec and a custom port scanner known as BLUETORCH for network scanning.*
- Mitigations (3)
  - Ensure that unnecessary ports and services are closed ...
  - Use network intrusion detection/prevention systems ...
  - Ensure proper network segmentation ...
- Detection (3)
  - Monitor cloud service usage for anomalous behavior ...
  - Monitor executed commands and arguments ...
  - Monitor network data for uncommon data flows ...

Example – Tactics and Techniques – threat actor (Lapsus$)

Example – Tactics and Techniques – software (Cobalt Strike)



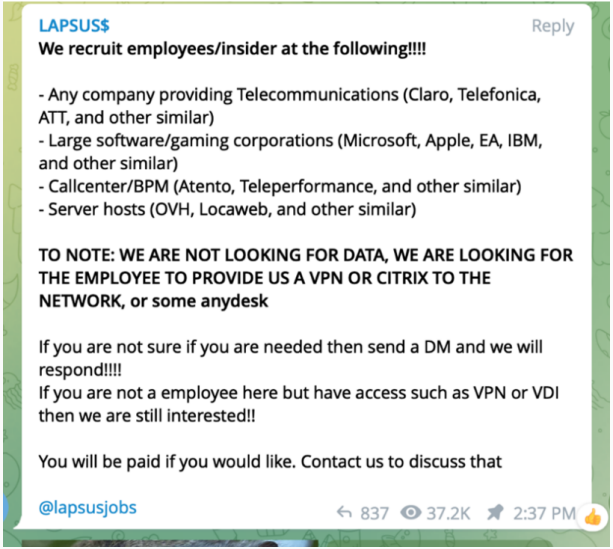
Lapsus$ (DEV-0537)

- stealing data, threatening to publish, demanding ransom
- victims (2021-2022):
  - Brazil's Ministry of Health and other targets (deleting data)
  - Microsoft, Okta, T-Mobile, Nvidia, Samsung, Uber, etc.
- arrests: UK and Brazil (mostly teenagers)
- Telegam channel
- analysis by Microsoft [3] (other reports and observations exist)

Initial Access

- obtaining credentials:
  - password stealer
  - purchasing credentials
  - paying employees (company, suppliers, business partners) for credentials and MFA approval
  - searching public code repositories
- VPN, RDP, VDI
- MFA: replay session tokens, MFA fatigue
- SIM swapping

Lapsus$ – recruiting (Telegram channel)



Lapsus$ – Tactics and Techniques (2)

Reconnaissance and privilege escalation

- AD enumeration (AD Explorer)
- searching for SharePoint, Confluence, JIRA, GitLab, Teams, Slack
- discover privileged accounts, credentials and secrets
- exploiting publicly known vulnerabilities
- DCSync attack, Mimikatz
- after obtaining domain admin: ntdsutil to extract the AD database
- observed: calling helpdesk to get password reset (privileged accounts)

Lapsus$ – Tactics and Techniques (3)

Exfiltration, destruction, and extortion

- group operated dedicated infrastructure in known VPS provider
- usage of NordVPN to geographically match the target
- with access to target's cloud environment – creating own virtual machines
- if successful, redirect all e-mails
- removing all other global admin accounts
- deleting systems and resources
  - on-prem, e.g. VMware vShpere/ESXi, as well as in the cloud
- in some cases extortion, in others just public release of stolen data

Lessons learned – recommendations

- strengthen MFA implementation
- healthy and trusted endpoints
- better authentication options for VPNs
- strengthen and monitor your cloud security
- awareness of social engineering attacks

You can always do more, do better. Justify the resources (money, time, effort) and inconvenience. When is it enough?

Conti

- Conti: ransomware group (RaaS)
- playbook leaked in 2021 [4]:
  - exact procedures (not only tactics and techniques)
  - detailed, easy to follow (after some training), low expertise needed
  - known tools, techniques
- leaks of chat messages, tutorials, guides etc. started in February 2022
  - detailed view of inner workings of the group
  - guides written better than the playbook
  - various analyses, summaries, e.g. [5]

Conti playbook – excerpts (1)

3. Kerberoast attack

Objective is to receive admin hash for further brute attack. First method:

powershell-import /home/user/work/Invoke-Kerberoast.ps1

psinject 4728 x64 Invoke-Kerberoast -OutputFormat HashCat | fl | Out-File -FilePath c:\ProgramData\pshashes.txt -append -force - Encoding UTF8

- Cobalt Strike

Conti playbook – excerpts (2)

7. PrintNightmare

Fresh but known vulnerability. Use before patched) CVE-2021-34527 allows to create local administrator. Useful if agent returned with common user rights.

On agent:

powershell-import //import file CVE-2021-34527.ps1

powershell Invoke-Nightmare -NewUser "HACKER" -NewPassword "FUCKER" -DriverName "Xeroxxx" //create user HACKER with password FUCKER and add to local administrators

spawnas COMPNAME\HACKER FUCKER https // replace https with listener name. Getting agent from our new local administrator. There's a chance of getting agent from **SYSTEM***. After imprt run: **Invoke-Nightmare -DLL "\polniy\put\do\payload.dll"**

Dark Pink

- based on https://www.group-ib.com/blog/dark-pink-apt
- Vietnam, Malaysia, Indonesia, Cambodia, Philippines, Bosnia and Herzegovina
- victims: military bodies, government agencies, religious organizations, etc.
- goals:
  - corporate espionage
  - steal documents
  - capture the sound from the microphones
  - exfiltration of data from messengers
- communication: Telegram API

Initial access

- spear-phishing emails (job applicant)
  - shortened URL to ISO image, or ISO image as an attachment
  - content: non-malicious files (doc, pdf, jpg), malicious exe and dll files
  - DLL Sideloading (abusing the DLL search order mechanism in Windows)
- 3 different paths how to obtain persistence:
  - ISO contains all files
  - malicious template document download from the Github
  - MSBuild project XML file with task to execute the malware

Dark Pink – Tactics and Techniques (2)

Reconnaissance and lateral movement

- collect info (sysinfo, web browsers, installed SW, USB drives and network shares)
- lateral movement: network and USB drives

Data exfiltration

- self-made stealers Cucky and Ctealer
- passwords, history, logins, and cookies from web browsers
- three paths to exfiltrate data:
  - via Telegram API (extensions: doc, docx, xls, xlsx, ppt, pptx, pdf)
  - via Dropbox (HTTP request with hardcoded token)
  - vie e-mail

Testing based on attackers' TTPs

MITRE Engenuity – Cybersecurity

- Center for Threat-Informed Defense – Adversary Emulation Library
  - emulation plans for selected threat actors (available on Github)

ATT&CK Evaluations [6]

- evaluating vendors/tools
- open-book and minimally sized environment
- goal: to understand baseline capabilities of security tools
- screenshots, detections, data sources, protection results
- SW components, configuration
- examples:
  - Turla (2023), 31 vendors
  - Enterprise 2024, 4 smaller emulations, 19 vendors

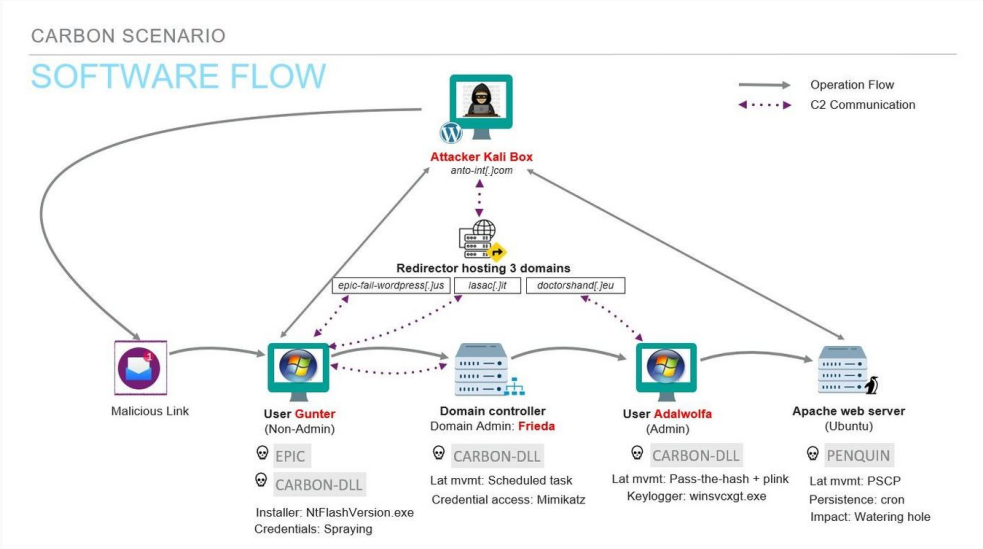
Turla 2023

- Turla – a threat group active since early 2000s
- victims in more than 50 countries
- targets: government agencies, diplomatic missions, military groups, research and education facilities, critical infrastructure, and media
- campaigns aimed at exfiltrating sensitive information from Linux and Windows infrastructure

Emulation plans, each contains detection and protection scenarios (details):

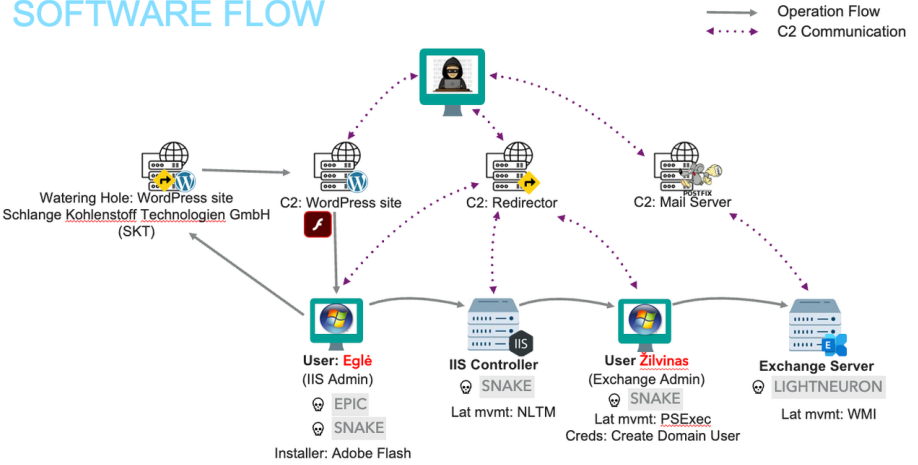
- Carbon
  - spearphishing, fake software installer, lateral movement (DC, Linux Apache server)
- Snake
  - drive-by compromise, malicious installer, privilege elevation, lateral movement (IIS, Exchange Server), email collection, exfiltration

Turla 2023 – Carbon



SNAKE SCENARIO

SOFTWARE FLOW



Exercises

1. TryHackMe: Moniker Link (CVE-2024-21413)
   - take a screenshot of the Net-NTLMv2 hash
   - read the original analysis by Check Point Research (link)
   - identify tactics and techniques from MITRE ATT&CK applicable for this exploit
2. Analyze the phishing e-mail available on course's web page (encrypted 7z archive, password: 'phish' followed by 4-digit number)
   - decrypt and unzip the archive
   - find the URL, domain and IP address for collecting credentials
   - validate the link with Virustotal, note the detections

Resources

1. Lockheed Martin, *The Cyber Kill Chain*
2. MITRE, *ATT&CK*
3. Microsoft, *DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*, 2022
4. W. Largent, *Translated: Talos' insights from the recently leaked Conti ransomware playbook*, Cisco Talos, 2021
5. S. Kupchik, *Conti's Hacker Manuals - Read, Reviewed & Analyzed*, Akamai Security Research, 2022
6. MITRE Engenuity, *ATT&CK Evaluations*