



OST

Eastern Switzerland
University of Applied Sciences

Cyber Defense - Frameworks

CAS Cyber Security

Ivan Bütler

HS2024 – Cyber Defense

Documenting Attacks and Adversaries

- Documentation is today still text based (think emails, incident reports in Word/PDF, news articles)
- Framework needed to have a common description language
 - ① **“Cyber Kill Chain”**, Developed by Lockheed Martin
 - ② **“Diamond Model”**, Developed by Caltagirone, Pendergast, and Betzis
 - ③ **STIX/TAXII**, Sponsored by the U.S. Department of Homeland Security are heavily supported by MITRE corporation
 - ④ **MISP** Malware Information Sharing Project, MISP is an open source software
 - ⑤ **MITRE “ATT&CK”**, Developed by MITRE

Cyber Kill Chain

<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

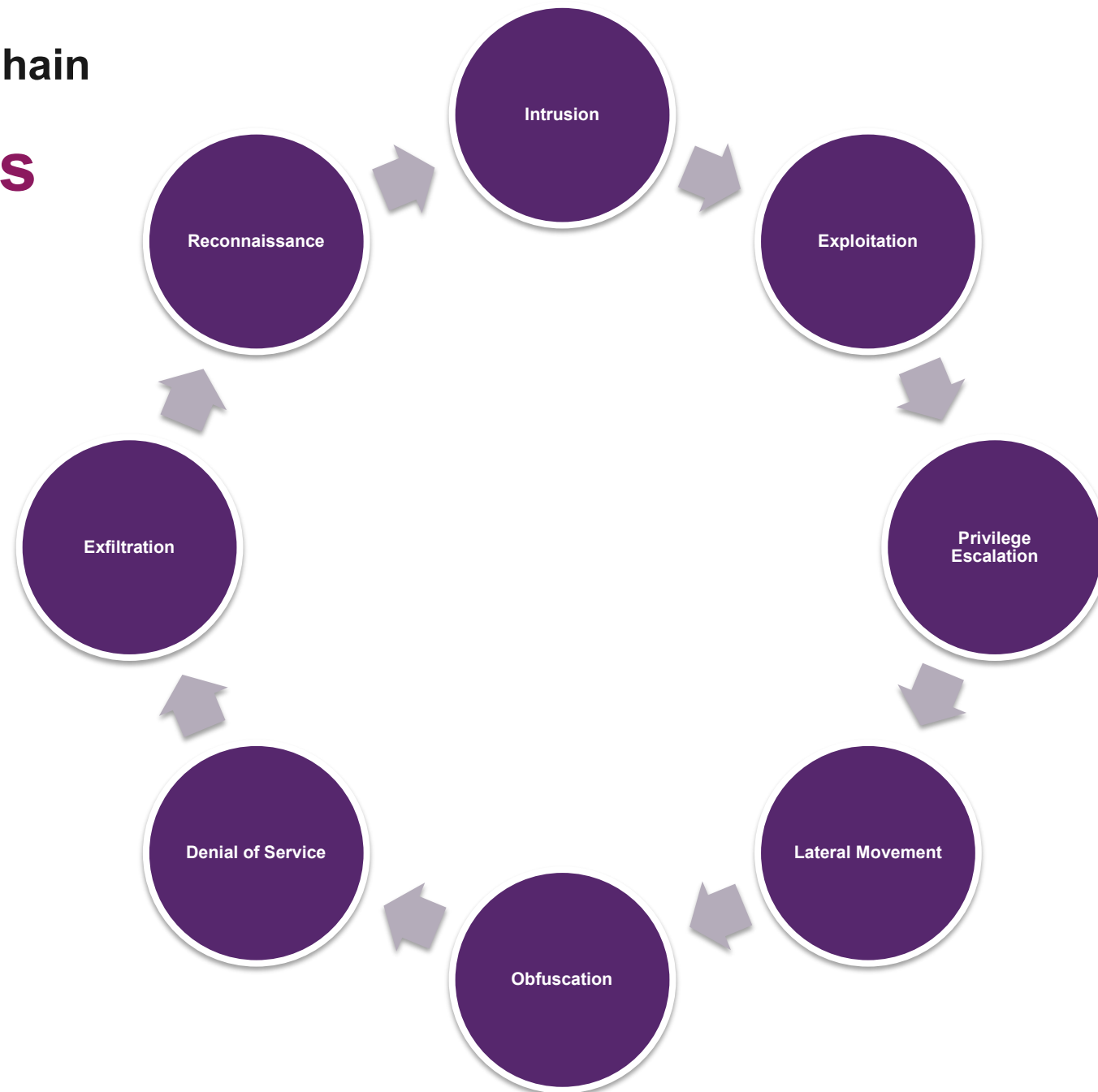


Cyber Kill Chain



The **Improved** Cyber Kill Chain

The Eight Phases



Cyber Kill Chain

- Series (8) of phases an attacker performs, that defenders can trace
- Implement security controls at each phase, break the chain and stop the attack
- **Reconnaissance**
 - The observation stage: attackers typically assess the situation from the outside-in, in order to identify both targets and tactics for the attack.
- **Intrusion**
 - Based on what the attackers discovered in the reconnaissance phase, they're able to get into your systems: often leveraging malware or security vulnerabilities.
- **Exploitation**
 - The act of exploiting vulnerabilities, and delivering malicious code onto the system, in order to get a better foothold.
- **Privilege Escalation**
 - Attackers often need more privileges on a system to get access to more data and permissions: for this, they need to escalate their privileges often to an Admin.

Cyber Kill Chain

- **Lateral Movement**

- Once they're in the system, attackers can move laterally to other systems and accounts in order to gain more leverage: whether that's higher permissions, more data, or greater access to systems.

- **Obfuscation / Anti-forensics**

- In order to successfully pull off a cyberattack, attackers need to cover their tracks, and in this stage they often lay false trails, compromise data, and clear logs to confuse and/or slow down any forensics team.

- **Denial of Service**

- Disruption of normal access for users and systems, in order to stop the attack from being monitored, tracked, or blocked

- **Exfiltration**

- The extraction stage: getting data out of the compromised system.

Critique by Security Professionals

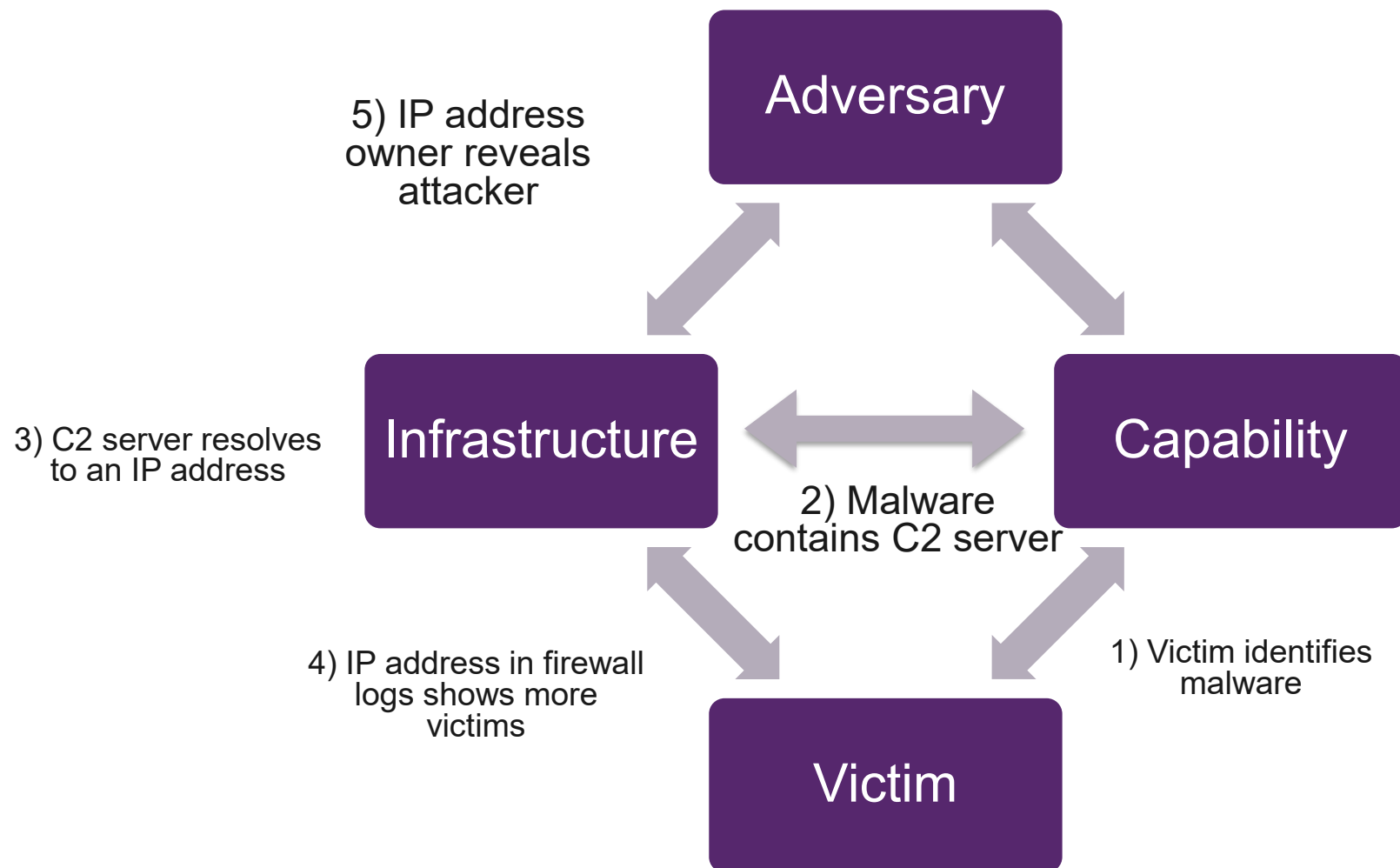
Cyber Kill Chain

- Not every phase is performed inside a victim network, more difficult to detect
 - The later iterations (as shown here) improved on some identified problems
- Difficult to detect non-external threat actors
 - e.g., how to detect insider threat abusing legitimate access?
- The chain represents a series: this, then that
 - It is very linear
- Lack of description for detection rules, little community effort around it

Diamond Model

- Consists of four basic components: **adversary**, **infrastructure**, **victim**, **capability**
- Developed by Caltagirone, Pendergast, and Betzis
- You group information to the basic components
 - Adversary: name (and aliases), origin, motivation, description
 - Infrastructure: IP addresses, malware, email addresses
 - Victim: location, vertical, goal, person, organization
 - Capability: methods, targets, operational manual, malware
- “An adversary deploys a capability over some infrastructure against a victim. These activities are called events. Events are phase-ordered by adversary-victim pair into activity threads representing the flow an adversary’s operations.”

Diamond Model



STIX

STIX & TAXII

- STIX: for **S**tructured **T**hreat **I**nformation **eX**pression
 - Describes cyber threat information i
 - Motivation
 - Abilities
 - Capabilities
 - Response
- JSON based document



STIX and TAXII are standards developed in an effort to improve the prevention and mitigation of cyber-attacks. STIX states the “**what**” of threat intelligence, while TAXII defines “**how**” that information is relayed. Unlike previous methods of sharing, STIX and TAXII are machine-readable and therefore easily automated.

STIX & TAXII

- TAXII: **T**rusted **A**utomated **eX**change of **I**ntelligence **I**nformation
 - STIX, short for Structured Threat Information eXpression, is a standardized language developed by MITRE and the OASIS Cyber Threat Intelligence (CTI) Technical Committee
 - STIX and TAXII are open community efforts sponsored by the U.S. Department of Homeland Security are heavily supported by MITRE corporation
 - Used to exchange intelligence information (mostly via STIX) in a standardized format
 - Four services offered to users:
 - **Discovery** – a way to learn what services an entity supports and how to interact with them
 - **Collection Management** – a way to learn about and request subscriptions to data collections
 - **Inbox** – a way to receive content (push messaging)
 - **Poll** – a way to request content (pull messaging)

Indicator for Malicious URL

Reading a STIX document

```

1  {
2    "type": "bundle",
3    "id": "bundle--56be2a3b-1534-4bef-8fe9-602926274089",
4    "objects": [
5      {
6        "type": "indicator",
7        "spec_version": "2.1",
8        "id": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4f",
9        "created": "2014-06-29T13:49:37.079Z",
10       "modified": "2014-06-29T13:49:37.079Z",
11       "name": "Malicious site hosting downloader",
12       "description": "This organized threat actor group operates to create profit from all types of crime.",
13       "indicator_types": [
14         "malicious-activity"
15       ],
16       "pattern": "[url:value = 'http://x4z9arb.cn/4712/']",
17       "pattern_type": "stix",
18       "valid_from": "2014-06-29T13:49:37.079Z"
19     },
20     {
21       "type": "malware",
22       "spec_version": "2.1",
23       "id": "malware--162d917e-766f-4611-b5d6-652791454fca",
24       "created": "2014-06-30T09:15:17.182Z",
25       "modified": "2014-06-30T09:15:17.182Z",
26       "name": "x4z9arb backdoor",
27       "description": "This malware attempts to download remote files after establishing a foothold as a back
28       oor.",
29       "malware_types": [
30         "backdoor",
31         "remote-access-trojan"
32       ],
33       "is_family": false,
34       "kill_chain_phases": [
35         {
36           "kill_chain_name": "mandiant-attack-lifecycle-model",
37           "phase_name": "establish-foothold"
38         }
39       ],
40     },
41     {
42       "type": "relationship",
43       "spec_version": "2.1",
44       "id": "relationship--864af2ea-46f9-4d23-b3a2-1c2adf81c265",
45       "created": "2020-02-29T18:03:58.029Z",
46       "modified": "2020-02-29T18:03:58.029Z",
47       "relationship_type": "indicates",
48       "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4f",
49       "target_ref": "malware--162d917e-766f-4611-b5d6-652791454fca"
50     }
51   ]
52 }

```

- Objects
 - Indicator
 - Name and description
 - **Pattern**
 - url:value
 - Malware
 - Name and description
 - Malware types
 - Killchain
 - Relationship
 - Source (indicator) and target (malware)
- Malicious URL is used to drop a malware

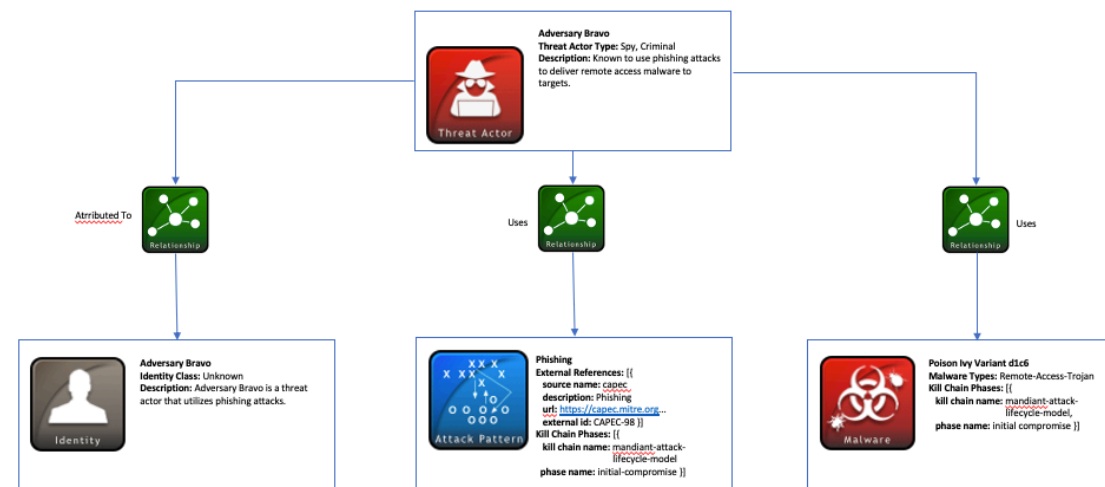
Threat Actor Leveraging Attack Patterns and Malware

Reading a STIX document

```

1 {
2   "type": "bundle",
3   "id": "bundle--0ecd8123-90d5-46e0-9cd4-65d4999b3a2e",
4   "objects": [
5     {
6       "type": "threat-actor",
7       "spec_version": "2.1",
8       "id": "threat-actor--9a8a0d25-7636-429b-a99e-b2a73cd0f11f",
9       "created": "2015-05-07T14:22:14.760Z",
10      "modified": "2015-05-07T14:22:14.760Z",
11      "name": "Adversary Bravo",
12      "description": "Adversary Bravo is known to use phishing attacks to deliver remote access malware to the targets.",
13      "threat_actor_types": [{}],
14    },
15    {
16      "type": "malware",
17      "spec_version": "2.1",
18      "id": "malware--d1c612bc-146f-4b65-b7b0-9a54a14150a4",
19      "created": "2015-04-23T11:12:34.760Z",
20      "modified": "2015-04-23T11:12:34.760Z",
21      "name": "Poison Ivy Variant d1c6",
22      "malware_types": [{}],
23      "is_family": false,
24      "kill_chain_phases": [{}],
25    },
26    {
27      "type": "attack-pattern",
28      "spec_version": "2.1",
29      "id": "attack-pattern--8ac90ff3-ecf8-4835-95b8-6aea6a623df5",
30      "created": "2015-05-07T14:22:14.760Z",
31      "modified": "2015-05-07T14:22:14.760Z",
32      "name": "Phishing",
33      "description": "Spear phishing used as a delivery mechanism for malware.",
34      "kill_chain_phases": [{}],
35      "external_references": [{}],
36    },
37  ],
38  {
39    {
40    },
41    {
42    },
43    {
44    },
45    {
46    }
47  }
48 }

```



Source: <https://oasis-open.github.io/cti-documentation/examples/threat-actor-leveraging-attack-patterns-and-malware>

Introduction

What is MISP

- MISP software facilitates the exchange and sharing of:
 - threat intelligence
 - Indicators of Compromise (IoCs)
 - Targeted malware and attacks
 - financial fraud
 - or any intelligence within your community of trusted members.
- Used by malware researchers and SOC's
- More than 6000 organisations worldwide are using MISP
- Open Source: <https://github.com/MISP/>
- About: <https://www.misp-project.org/>









MISP – Threat Intelligence Platform

- A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise (IOC) of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.
 - Store your IOCs in a structured manner, and thus enjoy the correlation, automated exports for IDS, or SIEM, in STIX or OpenIOC and synchronize to other MISP instances
 - Make it easier for you to share with, but also to receive from trusted partners and trust-groups
- Core development by [CIRCL](#), the Computer Incident Response Center in Luxembourg
 - Accepts commits and requests via GitHub

MISP Published Standards

- MISP core format: used to exchange indicators and threat information between MISP instances
- MISP object template format: describes a simple JSON format to represent the various templates used to construct MISP objects
- MISP taxonomy format: describes a simple JSON format to represent machine tag vocabularies
- MISP galaxy format: simple JSON format to represent galaxies and clusters that can be attached to MISP events or attributes
- SightingDB format: to give automated context to a given Attribute by counting occurrences and tracking times of observability

Filters: Tag: tlp:white X									
My Events Org Events									
ed	Creator org	Owner org	ID	Clusters	Tags	#Attr.	Creator user	Date	Info
	citizenlab	V	895		tlp:white osint:source-type="blog-post"	71	misp@riskmitigation.ch	2019-09-24	MISSING LINK: Tibetan Groups Targeted with Mobile
V	V	V	890	Malpedia Silence Q ≡ Threat Actor Silence group Q ≡ Tool Silence Q ≡	osint:source-type="technical-report" tlp:white	70	misp@riskmitigation.ch	2019-08-21	Silence 2.0 Going Global
V	V	V	319		tlp:white osint:source-type="automatic-collection"	1019	misp@riskmitigation.ch	2017-11-26	Das Malwerk Malware Feed feed
V	V	V	436		tlp:white osint:source-type="automatic-collection"	13308	misp@riskmitigation.ch	2018-10-15	Panels feed
V	V	V	381		tlp:white	1609716	misp@riskmitigation.ch	2018-02-25	Sanyalnet Mirai IPs feed
V	V	V	886	Threat Actor APT33 Q ≡ Charming Kitten Q ≡	tlp:white APT osint:source-type="blog-post"	77	misp@riskmitigation.ch	2019-07-06	OSINT: 'Twas the night before
V	V	V	385		tlp:white osint:source-type="block-or-filter-list" misp:confidence-level="usually-confident"	1945	misp@riskmitigation.ch	2018-02-28	Spamhaus DROP List feed
V	V	V	419		tlp:white osint:source-type="automatic-collection"	1417	misp@riskmitigation.ch	2018-09-20	SHA256 feed
V	V	V	418		tlp:white passivetotal:class="malicious"	1440	misp@riskmitigation.ch	2018-09-20	URLs feed

Owner org	vulnerability.ch research
Creator user	misp@riskmitigation.ch
Tags	<div><div> osint:source-type="technical-report" x</div><div> tlp:white x</div><div> +</div><div> +</div></div>
Date	2019-08-21
Threat Level	✔ Low
Analysis	Completed
Distribution	All communities <div><div></div><div> </div></div>
Info	Silence 2.0 Going Global
Published	Yes (2019-08-21 21:32:24)
#Attributes	70 (1 Object)
First recorded change	2019-08-21 18:30:05

ATT&CK

- Acronym for “Adversarial Tactics, Techniques, & Common Knowledge”
- Framework to document common tactics, techniques and procedures (TTPs) that advanced persistent threats use against Windows enterprise networks
- Based on real-life observations (published reports) and attributions (mostly by vendors such as FireEye, Sophos, Kaspersky, ...)
- Useful for “blue” and “red” teams to understand an attack or a simulation

ATT&CK – Examples Techniques

- Attacker sends email to employees
 - T1193: Initial Access - Spearphishing Attachment
 - T1192: Initial Access - Spearphishing Link
 - T1194: Initial Access - Spearphishing via Service
- Attacker uses Mimikatz to ...
 - T1178: Privilege Escalation - SID-History Injects
 - T1003: Credential Access - Credential Dumping
 - T1075: Lateral Movement - Pass the Hash

Phishing: Spearphishing Attachment

ATT&CK – Examples Techniques - T1193

- Spearphishing Attachment: Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.
- Attackers using this technique: APT12, APT29, Cobalt Group, ..., Lazarus Group, ..., Turla
- Mitigation: Antivirus, Network Intrusion Prevention (monitor network traffic for suspicious files), Restrict Web-Based Content (e.g. blocking attachment types), User Training

Source: <https://attack.mitre.org/techniques/T1566/>

ATT&CK – Examples Techniques - T1003

- Credential Access - Credential Dumping: Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.
- Attackers using this technique: APT33, APT39, FIN8, ..., Lazarus Group, ..., TEMP.Veles
- Mitigation: Active Directory Configuration, Credential Access Protection, Operating System Configuration, Password Policies, Privileged Account Management, Privileged Process Integrity, User Training

Source: <https://attack.mitre.org/techniques/T1003/>

Threat Actors

Threat Actor: Flash Card

- Threat actor name: Cobalt Group, Cobalt Gang, Cobalt Spider, TEMP.MetaStrike
- Motivation: financial, bank card/ATM fraud, SWIFT
- Victims: financial organisations across the globe
- Victims in Switzerland: several firms targeted, no successful attacks known
- Last attack against firm: 2020
- Modus operandi: sends emails with malicious links or attachments to victims, executes office or binary file, infects system with custom malware, moves laterally, escalates privileges, compromises internal applications and accounts
- Years active: 2016 – 2020 (suspected dormant)

Threat Actors

Threat Actor: G0080

- Cobalt Group
 - is a financially motivated threat group that has primarily targeted financial institutions. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organisations in order to use their access to then compromise additional victims. Reporting indicates there may be links between Cobalt Group and both the malware “Carbanak” and the group “Carbanak”.
- Techniques used
 - T1088, T1191, T1059, T1203, T1068, T1107, T1037, T1027, T1086, T1108, T1117, T1053, T1204, ...
- Software used
 - Cobalt Strike, Mimikatz, More_eggs, PsExec, SDelete, CobInt

Source: <https://attack.mitre.org/groups/G0080/>

ATT&CK - Word of Caution

- It is also important to understand what ATT&CK is not
 - Not a checklist: do not use this as a simple “can we detect this”, but understand the attack, translate it into your environment, compare to existing controls
 - Not a bingo-card: do not mark what you can cover
 - Documenting every possible attack: ATT&CK documents the known TTPs: when you document your own attacks/campaigns, you realise that you have more information about an attacker than what ATT&CK currently publicly describes
 - Static, final list: the ATT&CK matrixes are improved or modified regularly and now include PRE-ATT&CK (preparation attackers perform) and Mobile

ATT&CK vs. Kill Chain

- The tactics allow you to show the lifecycle/progress of an attack inside your enterprise
- Similar to what we saw with the Cyber Kill Chain
 - Some tactic are equal or very similar (intrusion and initial access, privilege escalation, exfiltration), others do not exists in one or the other (denial of service, discovery)
- The kill chain is more linear, as an attacker you move from left to right
- ATT&CK is more graph-like, move from left to right but also within the tactics up and down
 - Defenders need to think in graphs, not in lists