



Counterintelligence in  
Red Teaming using  
**MITRE ENGAGE**  
in 15min

OWASP Meetup Frankfurt #51, Oct 27th 2021



# Who am I



# Johannes Schönborn

Penetration Testing since 2006  
2016 Founded Exploit Labs  
@johnny\_sec, @xpltlabs

OWASP Frankfurt

ENISA's Ad-Hoc Working Group on Cyber  
Threat Landscapes

johannes@exploitlabs.de

## APT “Happy Turtle”

- Targets Power Plants PP
- Wants to disrupt
- Knows Robby is an OT Op
- Knows PP uses certain tech
- Knows PP uses cool WebApp OT



Who we are

# Agenda

1. How We Attack: MITRE ATT&CK
2. How Enterprises Can Defend: MITRE Engage
3. Adjusted Red Team Attack Playbooks
4. Key Takeaways

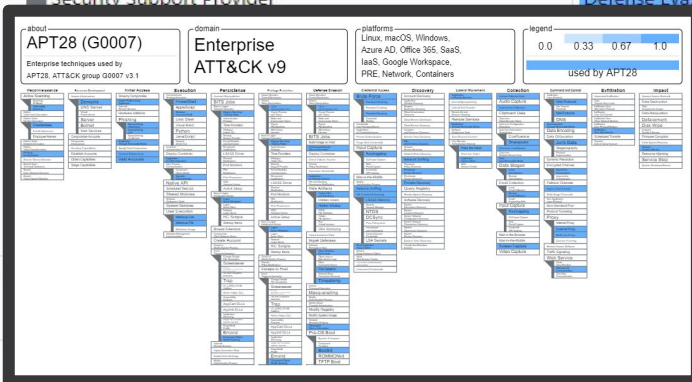




# 1. How We Attack: MITRE ATT&CK

# 1. How We Attack: MITRE ATT&CK

Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Credential Stuffing	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)
Create Process with Token	Access Token Manipulation (1/5)	Brute Force (2/4)	Application Window Discovery	Internal Spearphishing	Audio Capture
Make and Impersonate Token	Parent PID Spoofing	Make and Impersonate Token	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection
Parent PID Spoofing	SID-History Injection	Parent PID Spoofing	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data
SID-History Injection	Token Impersonation/Theft	SID-History Injection	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object
Token Impersonation/Theft	BITS Jobs	Token Impersonation/Theft	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)
Active Setup	Build Image on Host	Exploitation for Credential Access	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (1/2)
Authentication Package	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Taint Shared Content	Confluence
Kernel Modules and Extensions	Deobfuscate/Decode Files or Information (T1140)	Forge Web Credentials (0/2)	File and Directory Discovery	Application Access Token	Sharepoint
LSASS Driver	Score: 1	Man-in-the-Middle (0/2)	Network Service Scanning	Pass the Hash	Data from Local System
Plist Modification	Comment: An [APT28] macro uses the command certutil -decode to decode contents of a .txt file, storing the base64 encoded payload. (Citation: Unit 42 Sofacy Feb 2018) (Citation: Palo Alto Sofacy 06-2018)	Modify Authentication Process (0/4)	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive
Port Monitors	Deploy Container	Network Sniffing	Peripheral Device Discovery	Web Session Cookie	Data from Removable Media
Print Processors	Direct Volume Access	OS Credential Dumping (1/2)	Password Policy Discovery	Local Data Staging	Data Staged (1/2)
Re-opened Applications	Domain Policy Modification (0/2)	Hidden File System	Process Discovery	Remote Data Staging	Email Forwarding f
Registry Run Keys / Startup Folder	Execution Guardrails (0/1)	Hidden Files and Directories	Query Registry	Local Email Collect	Remote Email Coll
Security Support Provider	Exploitation for Defense Evasion	Hidden Users	Remote System Discovery	Credential API Hoc	GUI Input Capture
		Hidden Window	Software	Keylogging	Web Portal Capt
		NTFS File Attributes			
		Run Virtual Instance			
		VBA Stomping			



# 1. How We Attack: MITRE ATT&CK

<b>Credential Access</b> 15 techniques	<b>Discovery</b> 27 techniques
Credential Stuffing	Account Discovery (0/4)
Password Cracking	Application Window Discovery
Password Guessing	Browser Bookmark Discovery
Password Spraying	Cloud Infrastructure Discovery
...	Cloud Service Dashboard
...	Cloud Service

*Browser bookmarks may also highlight additional targets after an adversary has access to valid credentials, especially Credentials In Files associated with logins cached by a browser.*



# 1. How We Attack: MITRE ATT&CK

Playbook	T1217	Browser Bookmark Discovery
Goal	<ol style="list-style-type: none"><li>1. Enumerate local browsers</li><li>2. Extract history</li><li>3. Extract passwords from browser</li><li>4. Identify often used OT control interfaces</li><li>5. Identify how the operator authenticates i.e. via SSO or local credentials</li></ol>	
Method	SharpWeb, Browserloot.ps1 Metasploit: post/multi/gather/firefox_creds	
ATT&CK Defense	<i>“This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.”</i>	



# 1. How We Attack: MITRE ATT&CK

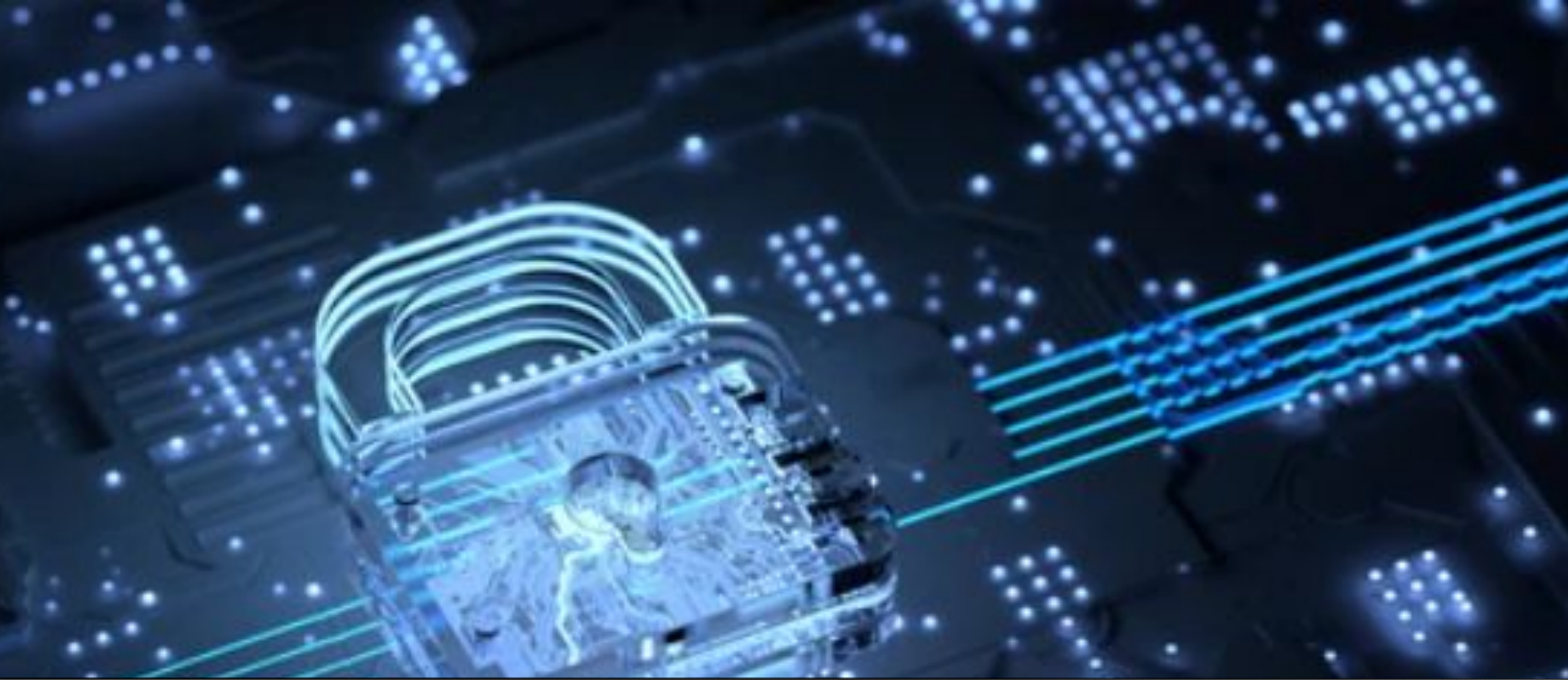


History:

Heatingcontrols.kplant

Browser Credentials:

XN5896 / Nioij()/&\*



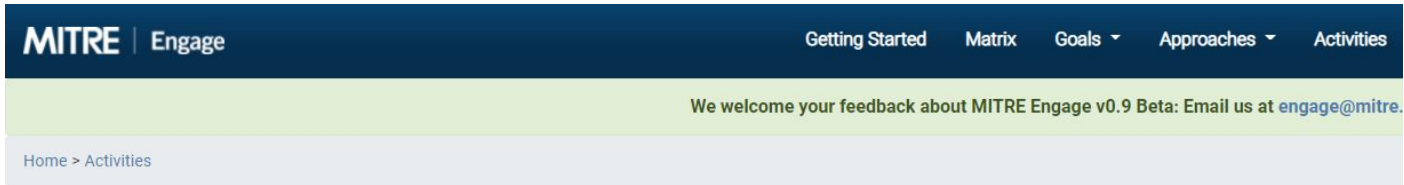
## 2. How Enterprises Can Defend: MITRE Engage

# 2. How Enterprises Can Defend: MITRE Engage

Prepare	Expose		Affect			Elicit		Understand
Planning	Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation	Analysis
Define Exit Criteria	API Monitoring	Decoy Artifacts and Systems	Baseline	Decoy Artifacts and Systems	Decoy Artifacts and Systems	Application Diversity	Application Diversity	Distill Intelligence
Develop Threat Model	Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity	Hotwash
Persona Creation	Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware	Inform Threat Model
Strategic Goal	System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation	Refine Operation Activities
Storyboarding			Security Controls	Network Manipulation		Information Manipulation	Personas	
				Peripheral Management		Network Diversity	Network Diversity	
				Security Controls		Peripheral Management		
				Software Manipulation		Pocket Litter		



# 2. How Enterprises Can Defend: MITRE Engage



## Decoy Artifacts and Systems

Introduce impersonations to expand the scope of a deceptive story.

Decoy Artifacts and Systems allow the defender to increase the attack surface of their environment to expose more of the deception story. Additionally, they can be used to adjust the adversary's sense of ambiguity to increase or decrease their level of uncertainty towards the environment. Investigation of these decoy artifacts may introduce a resource cost on the adversary, enable or block the adversary's intended actions, encourage or discourage a specific action or response, etc.

Decoy artifacts can take a variety of forms including credentials, accounts, files/directories, browser extensions/bookmarks, system processes, etc. Decoy systems can be real, virtual, or simulated. They can be presented as one of a variety of IT devices, including user workstations, servers, networking systems, IOT (embedded devices), mobile devices, etc. Regardless of form, these decoy artifacts and systems provide a variety of opportunities for the defender. For example, decoy artifacts can be used as tripwires to produce a high-fidelity alert when accessed.

Careful planning should guide the creation and deployment of these tripwires to ensure effectiveness. For example, understanding the adversary's known TTPs will highlight which resources the adversary is likely to touch, and therefore where decoy artifacts should be placed. A thorough assessment of the defender's priority cyber assets and intellectual property should guide the placement of decoy artifacts used as tripwires.

A decoy artifact can provide several means to influence adversary activity. The following examples illustrate the powerful effects decoy artifacts and systems can have on the adversary. First, by planting decoy artifacts and systems that align with known adversary TTPs, the defender can influence adversary activities. For example, if a target adversary has a capability against a specific application, the defender can place this vulnerable application in the environment to motivate the adversary to exploit the decoy.

As a second example, a defender may install AV or some other security or monitoring tool in a way that is easy for the adversary to remove. If an adversary removes the tool, they may be emboldened to act more openly believing they can't be monitored.

The defender can attempt to demotivate the adversary by strategically placing decoy artifacts. For example, a defender could place a selection of reverse engineering tools or monitoring applications on a known vulnerable target. This may sow confusion and raise ambiguity, demotivating the adversary's desire to go after that target even if it is vulnerable.

Decoy artifacts can take a variety of forms including credentials, accounts, files/directories, browser extensions/bookmarks, system processes, etc. Decoy systems can be real, virtual, or simulated.





### 3. Adjusted Red Team Attack Playbooks

### 3. Adjusted Red Team Attack Playbooks



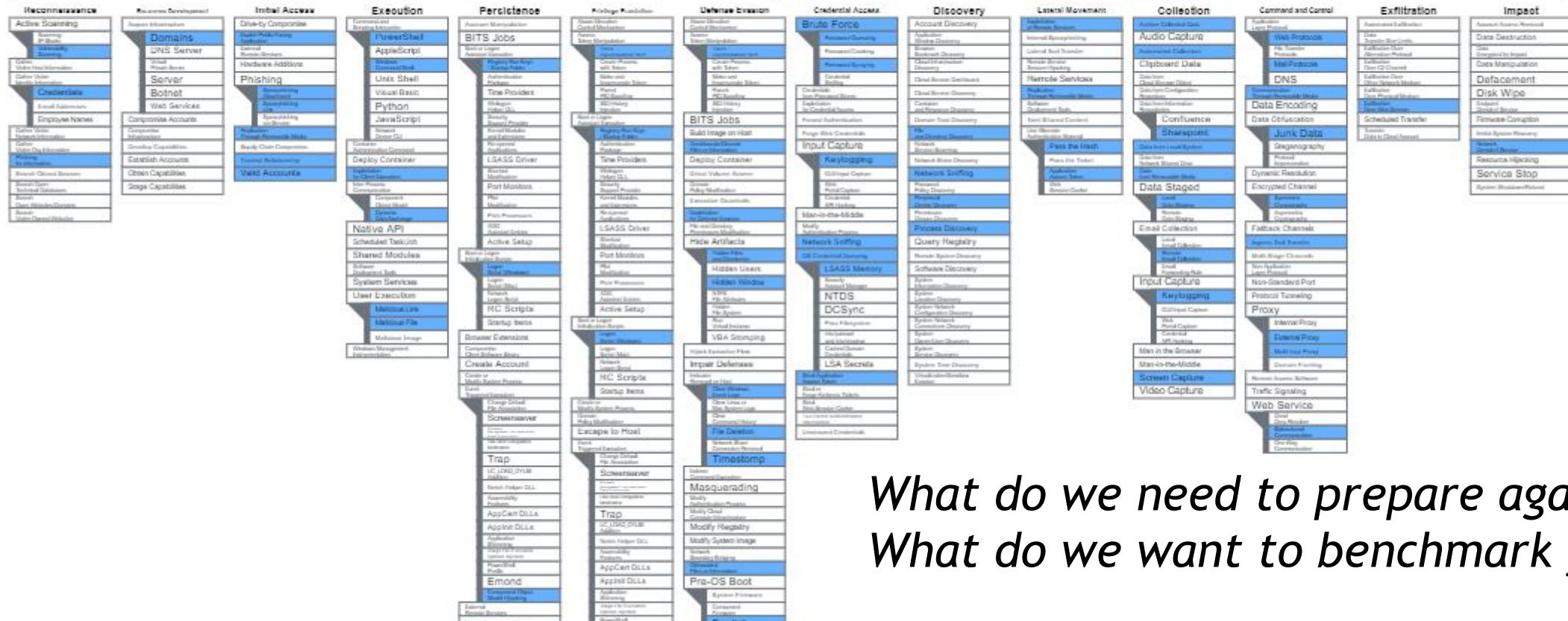
# 3. Adjusted Red Team Attack Playbooks

about **APT28 (G0007)**  
Enterprise techniques used by APT28, ATT&CK group G0007 v3.1

domain **Enterprise ATT&CK v9**

platforms Linux, macOS, Windows, Azure AD, Office 365, SaaS, IaaS, Google Workspace, PRE, Network, Containers

legend 0.0 0.33 0.67 1.0  
used by APT28



What do we need to prepare against?  
What do we want to benchmark for?<sub>14</sub>



# 3. Adjusted Red Team Attack Playbooks

Playbook	T1217	Browser Bookmark Discovery
Goal	<ol style="list-style-type: none"><li>1. Enumerate local browsers</li><li>2. Extract history</li><li>3. Extract passwords from browser</li><li>4. Identify often used OT control interfaces</li><li>5. Identify how the operator authenticates i.e. via SSO or local credentials</li></ol> <p>Do not engage before: Compare browsing history between browsers to identify honeypot URLs, i.e. a browser that only surfs to two, three high impact websites is suspicious Compare credentials from browsers against standard credentials: If they seem very different it could be a honeypot</p>	
Method	SharpWeb, Browserloot.ps1 Metasploit: post/multi/gather/firefox_creds	
ATT&CK Defense	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	
Engage	Decoy artifacts can take a variety of forms including credentials, accounts, files/directories, browser extensions/bookmarks, system processes, etc.	



### 3. Adjusted Red Team Attack Playbooks



History:

Heatingcontrols.kplant

Browser Credentials:

XN5896 / Nioij()/&\*



History:

maintenance.kplant

Browser Credentials:

Kplant\Johnny.s / Start2021!



## 4. Key Takeaways

# 4. Key Takeaways

## Use MITRE Engage to augment your Red Teaming TTPs

Understand the options the Blue Team has to defend, i.e. if a single security control is not available, it does not mean there is not defense in place

Identify Engage controls in place to derive further controls: If they have honeypot credentials in the browser, what about Active Directory?

## Align your results

We are now able to better advise on remediations by citing MITRE Engage and how it would have impacted the engagement

Prepare
Planning
Define Exit Criteria
Develop Threat Model
Persona Creation
Strategic Goal
Storyboarding





[BlackHills: OPSEC Fundamentals for Remote Red Teams](#)

[X33fCon: OPSEC Obsessed](#)

[CYBV436 Counter Cyber Threat Intelligence](#)

# Questions?

[johannes@exploitlabs.de](mailto:johannes@exploitlabs.de)

