sweepatic SECURITY

An introduction to the PRE-ATT&CK framework

EU ATT&CK Workshop (lux)

25th October 2019

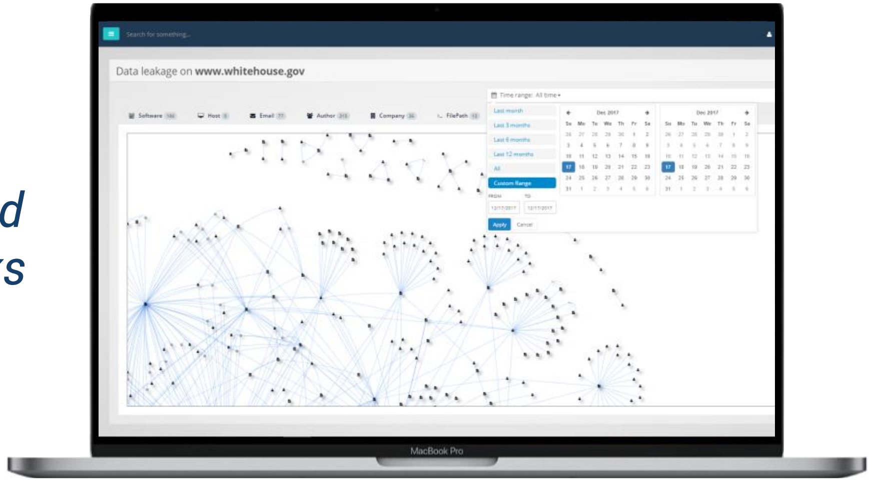
TLP: WHITE

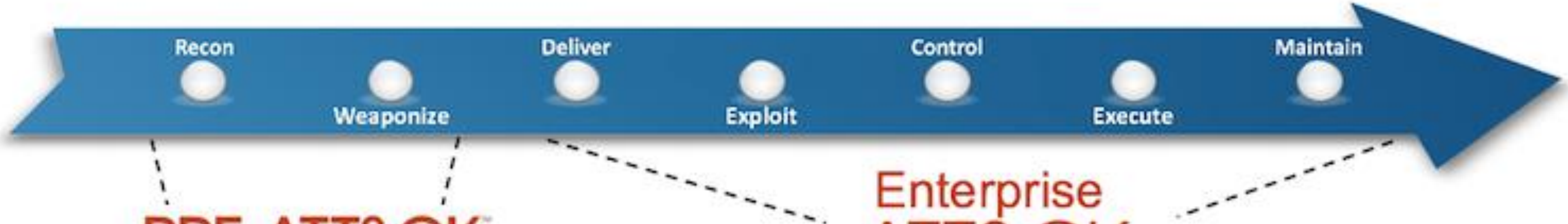
whoami

- *Stijn Vande Casteele*
- *18 years professional experience*
- *Co-founder & CEO at Sweepatic*
- *E-mail: stijn@sweepatic.com*
- *@securityworld*

About Sweepatic

- *Sweepatic is a data driven cybersecurity venture*
- *We developed a cloud based reconnaissance platform discovering and analyzing internet facing assets and checking their exposure to attacks ("attack surface monitoring")*
- *Website: https://www.sweepatic.com*


Data leakage on **www.whitehouse.gov**



PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection

Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec

Establish & Maintain Infrastructure

Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

Enterprise ATT&CK

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

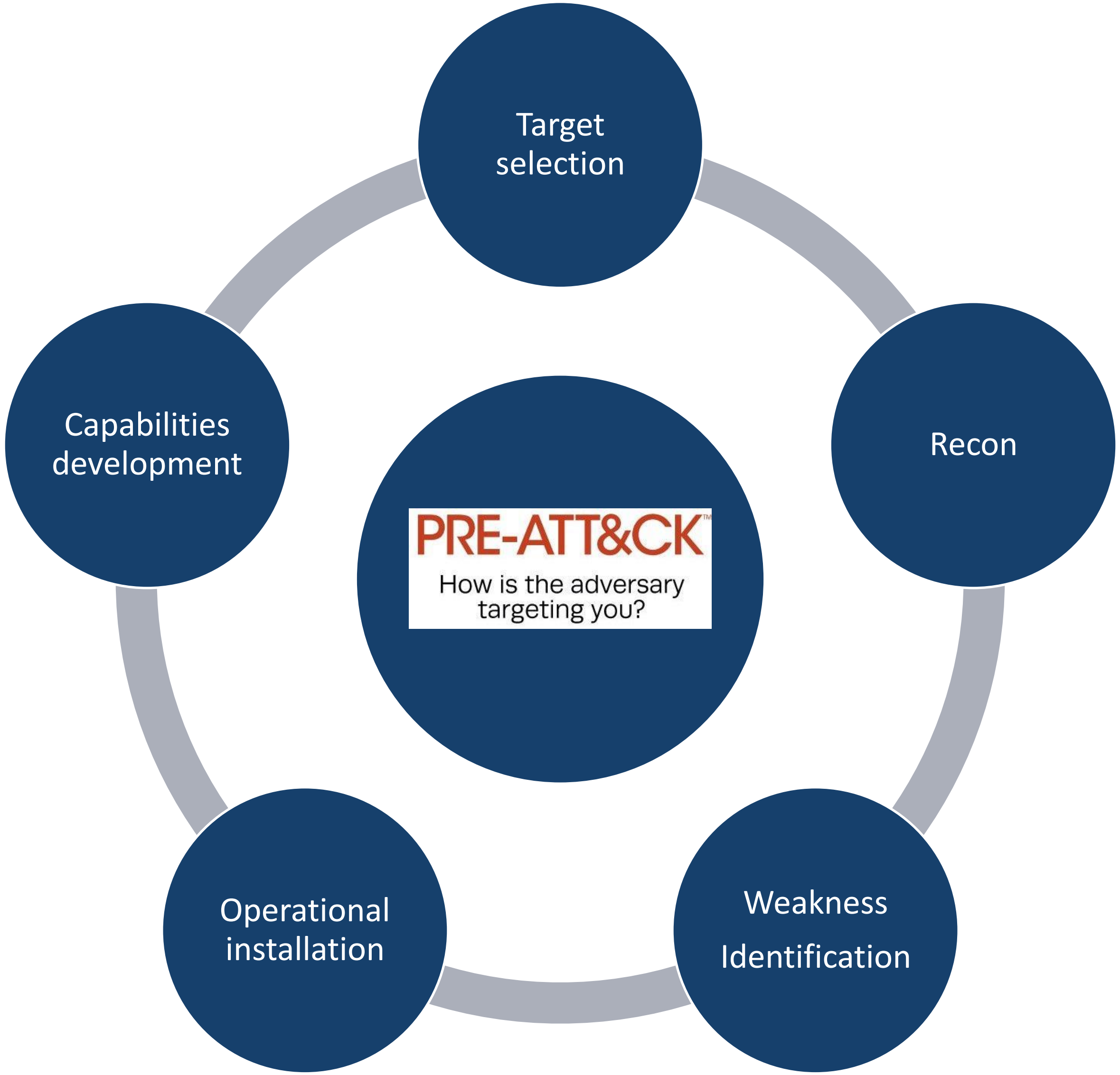
sweepatic SECURITY

PRE-ATT&CK Matrix

The MITRE PRE-ATT&CK Matrix™ is an overview of the tactics and techniques described in the PRE-ATT&CK model. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

Last Modified: 2018-04-18 17:59:24.739000

Priority Definition Planning	Priority Definition Direction	Target Selection	Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification	Adversary OPSEC	Establish & Maintain Infrastructure	Persona Development	Build Capabilities	Test Capabilities	Stage Capabilities
Assess KITs/KIQs benefits	Assign KITs, KIQs, and/or intelligence requirements	Determine approach/attack vector	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Analyze application security posture	Analyze organizational skillsets and deficiencies	Analyze business processes	Acquire and/or use 3rd party infrastructure services	Acquire and/or use 3rd party infrastructure services	Build social network persona	Build and configure delivery systems	Review logs and residual traces	Disseminate removable media
Assess current holdings, needs, and wants	Receive KITs/KIQs and determine requirements	Determine highest level tactical element	Conduct active scanning	Aggregate individual's digital footprint	Conduct social engineering	Analyze architecture and configuration posture	Analyze social and business relationships, interests, and affiliations	Analyze organizational skillsets and deficiencies	Acquire and/or use 3rd party software services	Acquire and/or use 3rd party software services	Choose pre-compromised mobile app developer account credentials or signing keys	Build or acquire exploits	Test ability to evade automated mobile application security analysis performed by app stores	Distribute malicious software development tools
Assess leadership areas of interest	Submit KITs, KIQs, and intelligence requirements	Determine operational element	Conduct passive scanning	Conduct social engineering	Determine 3rd party infrastructure services	Analyze data collected	Assess targeting options	Analyze presence of outsourced capabilities	Acquire or compromise 3rd party signing certificates	Acquire or compromise 3rd party signing certificates	Choose pre-compromised persona and affiliated accounts	C2 protocol development	Test callback functionality	Friend/Follow/Connect to targets of interest
Assign KITs/KIQs into categories	Task requirements	Determine secondary level tactical element	Conduct social engineering	Identify business relationships	Determine centralization of IT management	Analyze hardware/software security defensive capabilities		Assess opportunities created by business deals	Anonymity services	Buy domain name	Develop social network persona digital footprint	Compromise 3rd party or closed-source vulnerability/exploit information	Test malware in various execution environments	Hardware or software supply chain implant
Conduct cost/benefit analysis		Determine strategic target	Determine 3rd party infrastructure services	Identify groups/roles	Determine physical locations	Analyze organizational skillsets and deficiencies		Assess security posture of physical locations	Common, high volume protocols and software	Compromise 3rd party infrastructure to support delivery	Friend/Follow/Connect to targets of interest	Create custom payloads	Test malware to evade detection	Port redirector
Create implementation plan			Determine domain and IP address space	Identify job postings and needs/gaps	Dumpster dive	Identify vulnerabilities in third-party software libraries		Assess vulnerability of 3rd party vendors	Compromise 3rd party infrastructure to support delivery	Create backup infrastructure	Obtain Apple iOS enterprise distribution key pair and certificate	Create infected removable media	Test physical access	Upload, install, and configure software/tools
Create strategic plan			Determine external network trust dependencies	Identify people of interest	Identify business processes/tempo	Research relevant vulnerabilities/CVEs			DNSCalc	Domain registration hijacking		Discover new exploits and monitor exploit-provider forums	Test signature detection for file upload/email filters	
Derive intelligence requirements			Determine firmware version	Identify personnel with an authority/privilege	Identify business relationships	Research visibility gap of security vendors			Data Hiding	Dynamic DNS		Identify resources required to build capabilities		
Develop KITs/KIQs			Discover target logon/email address format	Identify sensitive personnel information	Identify job postings and needs/gaps	Test signature detection			Dynamic DNS	Install and configure hardware, network, and systems		Obtain/re-use payloads		
Generate analyst intelligence requirements			Enumerate client configurations	Identify supply chains	Identify supply chains				Fast Flux DNS	Obfuscate infrastructure		Post compromise tool development		
Identify analyst level gaps			Enumerate externally facing software applications technologies, languages, and dependencies	Mine social media	Obtain templates/branding materials				Host-based hiding techniques	Obtain booter/stressor subscription		Remote access tool development		
Identify gap areas			Identify job postings and needs/gaps						Misattributable credentials	Procure required equipment and software				
Receive operator KITs/KIQs tasking			Identify security defensive capabilities						Network-based hiding techniques	SSL certificate acquisition for domain				
			Identify supply chains						Non-traditional or less attributable payment options	SSL certificate acquisition for trust breaking				
			Identify technology usage patterns						OS-vendor provided communication channels	Shadow DNS				
			Identify web defensive services						Obfuscate infrastructure	Use multiple DNS infrastructures				
			Map network topology						Obfuscate operational infrastructure					
			Mine technical blogs/forums						Obfuscate or encrypt code					
			Obtain domain/IP registration information						Obfuscation or cryptography					
			Spearphishing for Information						Private whois services					
									Proxy/protocol relays					
									Secure and protect infrastructure					



PRE-ATT&CK™

How is the adversary targeting you?

Target selection

Recon

Weakness Identification

Operational installation

Capabilities development

➢ https://blog.sweepatic.com/

An update (*)

<snap>

We are planning on ***merging*** *PRE-ATT&CK into Enterprise ATT&CK.*

If you take a look at the PRE-ATT&CK matrix, we're planning on deprecating what's currently covered by the ***first three PRE-ATT&CK tactics****, and folding the rest into* ***new tactics in Enterprise ATT&CK****.*

Our goal is to still represent all of ***the real-world****, technical activity that's covered by the other 12 Tactics, but inside of ATT&CK. I'll be previewing what that looks like at ATT&CKcon (**) next week (and that should be streamed live).*

That said, I wouldn't expect any visible changes to PRE-ATT&CK until ***early next year*** *as it's dependent on our release of sub-techniques, and I would expect the current version to remain published (but deprecated) even after that happens.*

</snap>

(*) E-mail thread 22/10/2019 with Adam Pennington - MITRE

(**) https://www.mitre.org/attackcon-streamed-live

Thank you for your attention!

Stijn Vande Casteele

stijn@sweepatic.com