digital shadows_

March 2019

ATT&CK™ Is The Best Form Of… Reconnaissance

Using MITRE PRE-ATT&CK™ To Enrich Your Threat Model

Dr. Richard Gold, Director of Security Engineering, Digital Shadow

digital shadows_

Mitre PRE-ATT&CK

- “This cyber threat framework captures the tactics, techniques, and procedures adversaries use to select a target, obtain information, and launch a campaign.”

Priority Definition
- **Planning, Direction**

Target Selection

Information Gathering
- **Technical, People, Organizational**

Weakness Identification
- **Technical, People, Organizational**

Adversary OpSec

Establish & Maintain Infrastructure

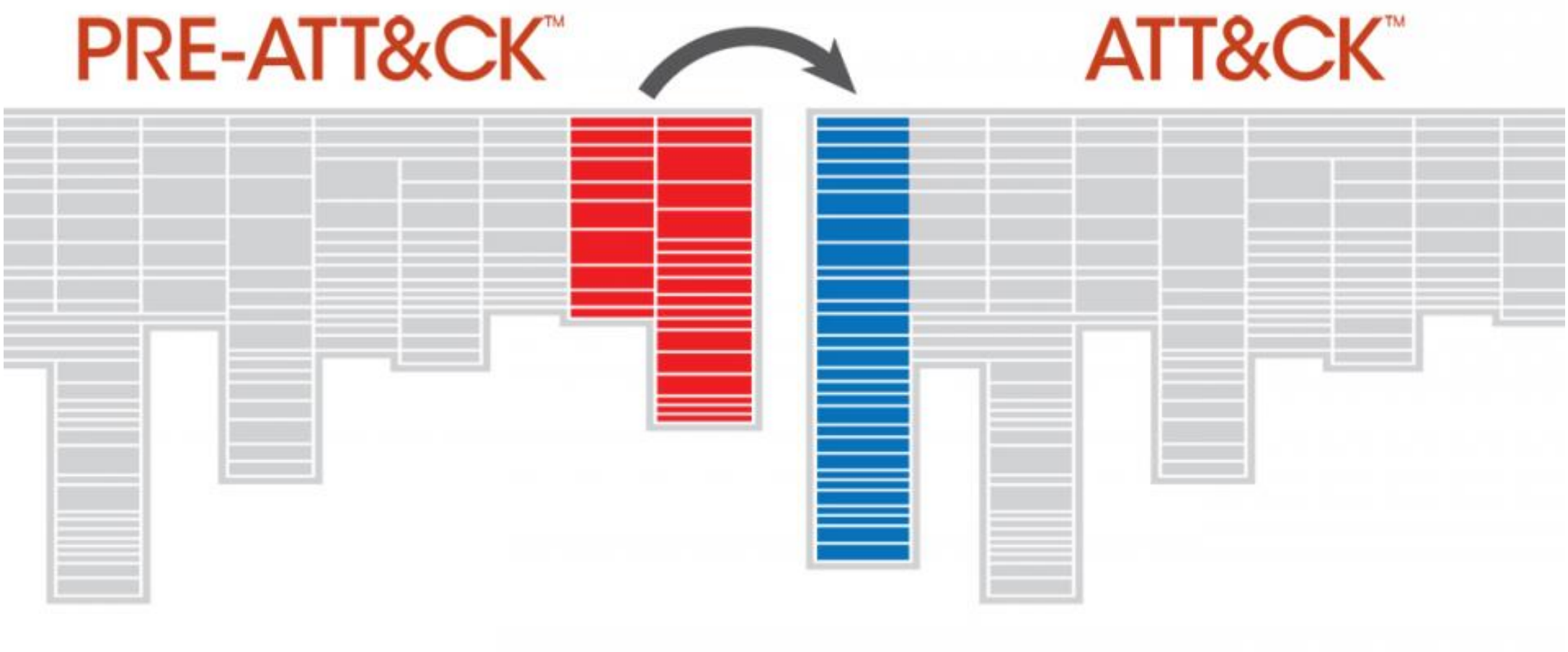
Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

PRE-ATT&CK meets ATT&CK



Explanation of terms and the problem

- What are the challenges with mapping PRE-ATT&CK?
  - Lack of open source reporting on the reconnaissance phase
  - Difficult to find evidence of PRE-ATT&CK TTPs
- ATT&CK is primarily for single, independent intrusions and not long-term campaigns
- Can we use PRE-ATT&CK for use-cases which help us protect our own organizations?

PRE-ATT&CK use cases

- Unlike Enterprise ATT&CK which can be used for generating detection use-cases, PRE-ATT&CK more useful for generating assessment use-cases
- Many real-world attacks have an extensive reconnaissance phase
- Many types of recon is performed beyond the perimeter:
  - **People**: social media, recruitment sites, sales prospecting tools, …
  - **Processes**: Google dorking, open S3 buckets, …
  - **Technology**: SHODAN, Censys, Github, Pastebin, …

Challenges

- OSINT recon by it's very nature is *passive* reconnaissance rather than *active*
- Instead of trying to detect it, how about *emulating* it?
- PRE-ATT&CK is a great way to structure your OSINT recon program against yourself
- Some good TTPs to start with:
  - Technical/People/Organizational Information Gathering
  - Technical/People/Organizational Weakness Identification

How do attackers perform recon for real-world attacks?

- In order to emulate an adversary, we first need to study how they actually behave
- Indictments are a great initial source as we are provided with information on the recon phase which is usually not present in other open source reporting

- Lots of great indictments out there to learn from:
  - North Korean officers (Sony): https://www.justice.gov/usao-cdca/press-release/file/1091951/download
  - SamSam: https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public
  - FIN7: https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100
  - GRU officers (DCCC/DNC): https://www.justice.gov/file/1080281/download

Recent Indictment summary

- GRU/APT28/STRONTIUM/Fancy Bear/etc.
  - Intrusions to support influence operations
- FIN7
  - Intrusions to steal payment card data and/or non-public information
- North Korean programmer
  - Intrusions to steal non-public information (SPE)
  - Usage of wiper malware for destructive purposes (SPE)
  - Intrusions to gain a position to make fraudulent SWIFT transactions (Bangladesh Bank)
  - Self-propagating malware for destructive purposes (WannaCry)
- SamSam
  - Network intrusions to support extortion attempts

GRU indictment

- Personal accounts of key employees were targeted
- Social media profiles were used to create phishing pretexts
- "researched the DCCC and DNC computer networks to identify technical specifications and vulnerabilities”
- "ran a technical query for the DCCC’s internet protocol configurations to identify connected devices"

FIN7 indictment

- Employees that regularly dealt with customers or external partners were prime targets
- FIN7 looked for employees who dealt with catering requests, hotel or table reservations, or complaints about quality or service
- In certain cases, FIN7 would then make a follow up phone call to walk the target through the process of opening the malicious attachment containing malware

FIN7 indictment

- “sent phishing emails to personnel at victim companies who had unique access to internal proprietary and non-public company information, including, but not limited to, employees involved with making filings with the United States Securities and Exchange Commission (“SEC”)”
- One such FIN7 campaign targeted several hundred organizations and specifically targeted employees with the “*Financial Filing [Reporting] Analyst*” job title
  - H/T: Ryan Kalember, Proofpoint

North Korean indictment

- “online reconnaissance included research relating to the victim company or entity that the subjects were targeting, as well as relating to individual employees of the victim company”
- “The subjects have also used the services of websites that specialize in locating email accounts associated with specific domains and companies”
- “The subjects have registered for business records search services that offer career postings, business searches, and marketing services”

North Korean indictment

- The attackers “researched the time zone of a correspondent bank that the subjects intended and attempted to use for a fraudulent transfer from a victim bank in 2016, days before the cyber-heist there”

Mapping PRE-ATT&CK to assessment use-cases

1. Information Gathering
   - Many OSINT data sets are free or free for limited use
     - SHODAN, hunter.io, WHOIS, Certificate Transparency
   - Analyze these with existing OSINT tools or Python, Go, etc.
   - Can you find your own assets in these data sets?
2. Weakness identification
   - Vulnerable software versions – Mitre/NIST, ExploitDB, etc.
   - Employees sharing too much online
   - Documents accessible online which shouldn't be
3. Establish & Maintain Infrastructure
   - There are cases like registration of typosquat domains which *can* be detected

When ATT&CK becomes PRE-ATT&CK

- The relationship between one intrusion's ATT&CK and another's PRE-ATT&CK in long term campaigns
  - The North Korean actor used the Brambul worm to email stolen credentials and server information back to the attackers
  - The compromised servers for hop points and other activities, meaning they had a constant supply of infrastructure for future attacks and campaigns
- Blurring the lines between ATT&CK and PRE-ATT&CK
  - "Analysis of the operation suggests that the adversaries previously identified specific directories, file shares, servers, user accounts, employee full names, password policies, and group memberships on the network, likely during their detailed reconnaissance phase"
    - http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf
- Information stolen during one intrusion can be repurposed for subsequent ones

Mitigations

- What information about the organization and its employees should be made public?
  - email and telephone contact details, technical information, etc.
- Certain job titles may be of more interest to attackers
  - these employees may require dedicated training to educate them of the threats that they face
- Social media searches can be used by attackers to uncover these employees
  - public documents can also reveal these employees and their contact details.
- What information do you hold could be used against other organizations?

What this means for defenders

- It’s possible to use the ATT&CK framework for long term campaigns
- You can use open source reports and indictments to update your threat model
  - People
  - Processes
  - Technology
- Using (PRE) ATT&CK gives you a structured way of extracting the most significant points from unstructured text
- This gives a framework for generating assessment use-cases for understanding your own exposure online

Conclusions

- ATT&CK and PRE-ATT&CK are excellent tools for modelling intrusions
- Long-running campaigns can use ATT&CK as the PRE-ATT&CK phase for another intrusion
- Need to keep in mind our position relative to others
- Difficult to *detect* PRE-ATT&CK activity, but we can use our knowledge of attacker tradecraft to perform our own assessments
- A lot of this work can be done using free or low-cost tools and data sets