Proactive Defense.

Using Deception, Automated Response and Threat Emulation

Vince Urias & Will Stout

October 2019

.conf19

splunk>

Vince Urias

Sandia National Laboratories

Will Stout

Sandia National Laboratories

What are we talking about today?

- Deception and Threat Intelligence (TI)
- Dynamic Deception
- Automation-in-Depth to Enable TI
- Putting the pieces together…
- … and showing it work

Key Takeaways

1. Threat intelligence (TI) gathering tools and techniques must evolve
2. Deception is a method to improve TI
3. Automation can provide numerous ways to refine and gather TI with non-intrusive methods

Deception

Making the Case for Deception and Threat Intelligence

.conf19
splunk>

Identifying Needs

DEFENDERS
Operational needs
Gaps in actionable threat intelligence • Modern tools are often are reactionary (signatures, etc.) and do not enable proactive strategies to combat threat • Traditional techniques of unplugging compromised boxes—lose value intelligence into adversary motivation
Few/no mechanisms to interact and learn about our adversaries
Better tools to gather information about our adversaries

THREAT INTELLIGENCE COMMUNITY
Threat feed landscape changing • LookingGlass acquisition *Cyveillance* • FireEye purchase of *iSight Partners* • Accenture purchase of *Arismore* and *iDefense*
What will the landscape look like 3-5 years from now?
Closed feeds by disparate vendors • Purchase them all? • Pick out the relevant threat feeds from the noise?
Consider tailoring intelligence based on security posture and threat profile • Roll-your-own based what is important to you

The Case for Deception

Table 1. Deception Providers and Their Primary Domains of Deception

Deception Provider	Network	Endpoint	Application	Data
Allure Security Technology	-	-	-	X
Attivo Networks	-	X	X	Partial
CyberTrap	-	X	X	Partial
Cymmetria	-	X	X	Partial
ForeScout	X	-	-	-
GuardiCore	X	X	X	Partial
Hexis Cyber Solutions	X	-	-	-
illusive networks	-	X	-	Partial
LogRhythm	-	X	-	-
Percipient Networks	X	-	-	-
Rapid7	-	X	-	-
Shape Security	-	-	X	-
Specter	-	X	X	Partial
TrapX Security	-	X	X	Partial
TopSpin Security	-	X	X	X

Source: Gartner (July 2015)

http://www.gartner.com/technology/reprints.do?id=1-2LSQOX3&ct=150824&st=sb&aliId=174399

From 2015: "Emerging Technology Analysis: Deception Techniques and Technologies Create Security Technology Business Opportunities"

- Advanced threat detection
- N/S, E/W
- Actionable intelligence

To today

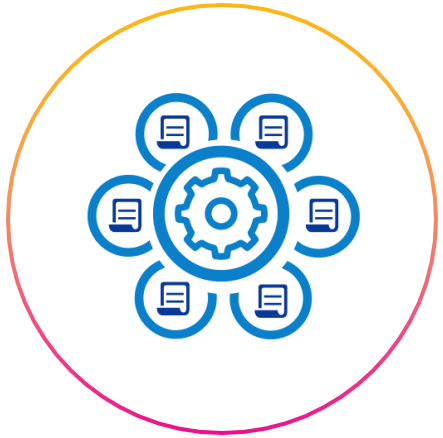
- This year, 10% of enterprises will use deception tools and tactics, and actively participate in deception operations against attackers

And Tomorrow

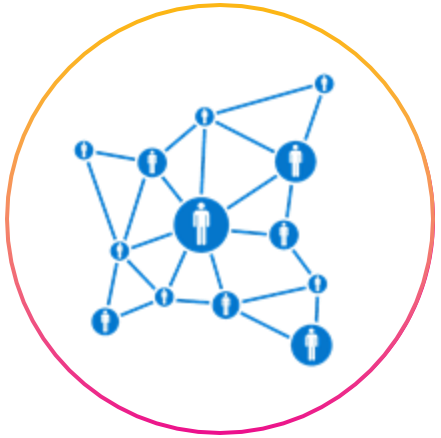
- The market value of deception-based cybersecurity will be at 12B (2019-2024), and grow steadily at 19% CAGR

https://www.marketanalysis.com/?p=398

Changing the Conversation with the Adversary



Data collection, for both network and host



Environment creation, including specification, user, traffic generation, and behavior modeling

Capabilities to **analyze adversary tactics, techniques, and procedures** (TTPs)

The Need to Evolve Threat Intelligence

Defenders need to think like the attackers

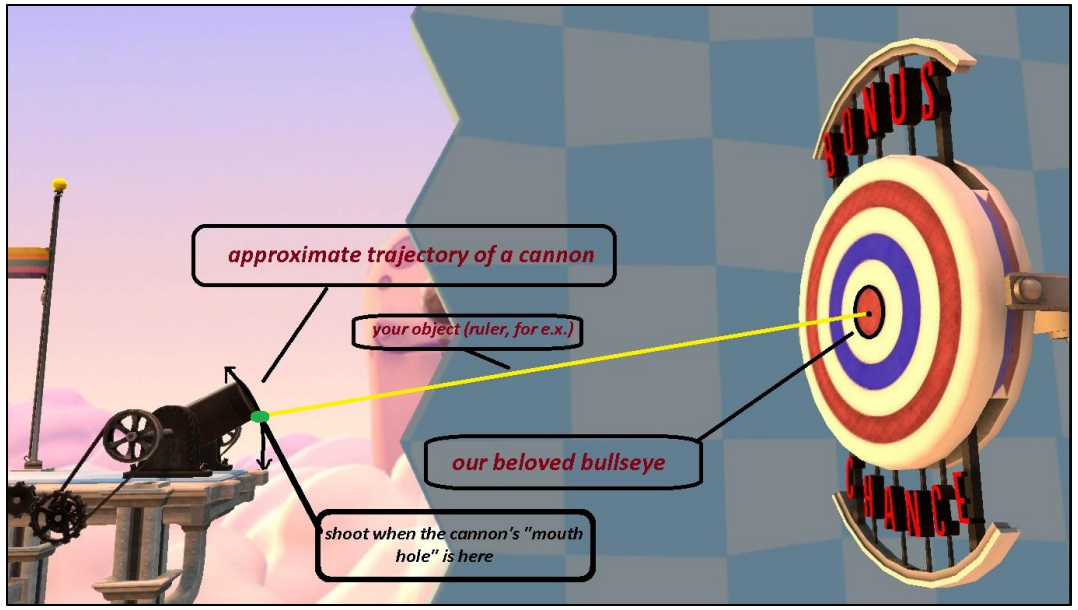
The gap between TI and Action is getting wider

Threat Profiling

- Who is your adversary?
  - Nation State
  - Hacktivists
  - Employees (Insiders)
  - Partners
  - Crimeware
  - King Koopa?

Targeting

- What are you trying to protect?
- What are common targets for your adversary?
  - Executives?
  - Web Servers?
  - Database Servers?
  - Users?



How do we reinforce our defenses against people attacking those targets?

By thinking like ~~the~~ **YOUR** Adversary

Dynamic Deception

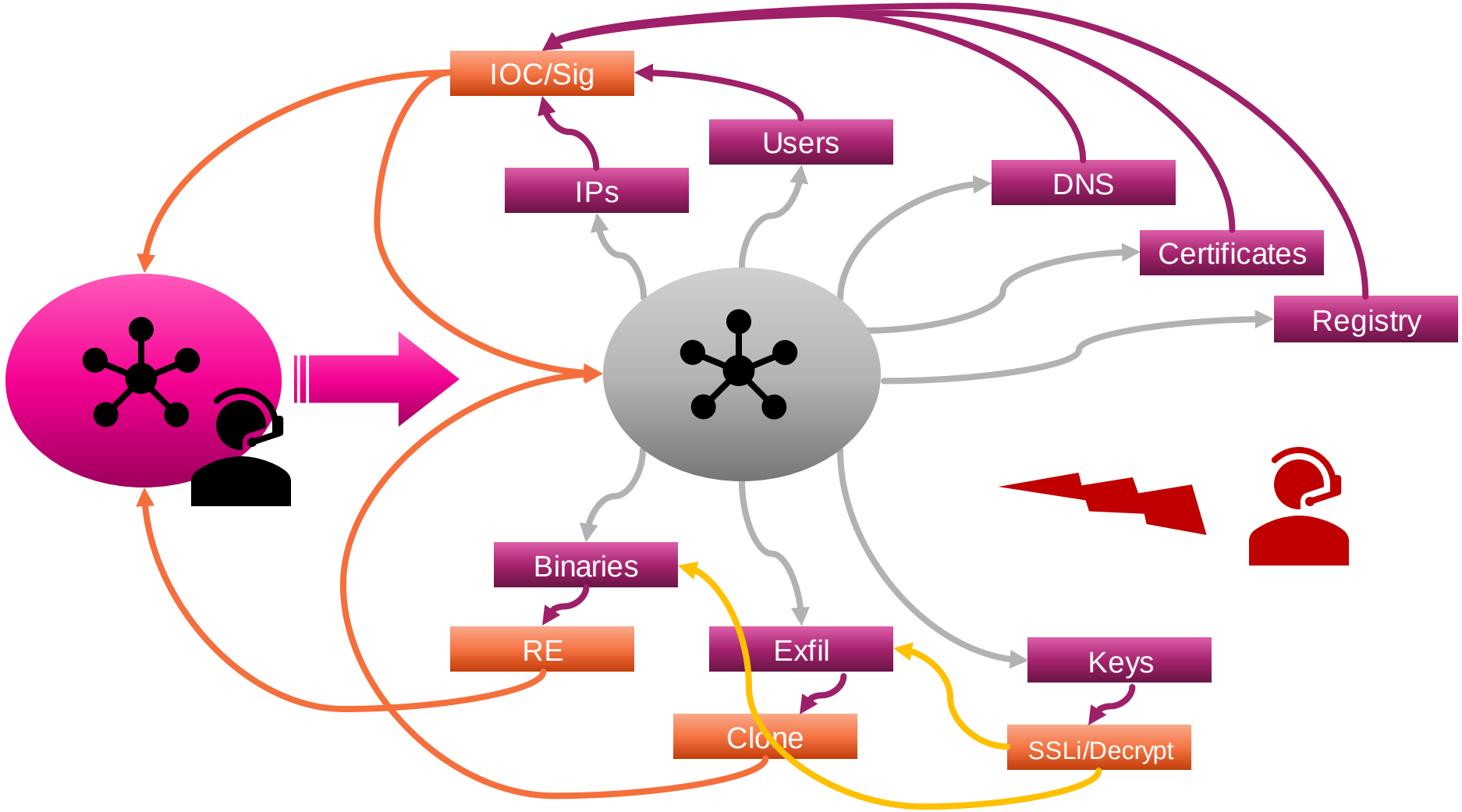
Networks are living, breathing entities. Really.

.conf19
splunk>

Dynamic Deception

- Creating a deception on the fly:
  - Leveraging sensor data
  - Software Defined Networking (SDN)
  - Virtualization
  - Machine Learning (ML)
  - …

Dynamic Deception




WHAT
WHO
WHY
HOW
WHEN
WHERE

Automation

Putting machines to work so you don’t have to.

.conf19
splunk>

What are some challenges ?

Creating DD at net-speed requires net-speed tools.

- Enter automation for:
  - Sensing
  - Responding
  - Creating
  - Continuing…

Underlying this is net-speed automated data exploitation to develop near real-time threat intel

Automation

Automation consists of three techniques or areas:

1. Binary Analysis Pipeline (BAP)
2. Dynamic Deception (DD)
3. Automated Response (AR)

Automation

Dynamic Deception (DD)

DD is revolves around changing the deception environment based on input from the defender or observed actions of the adversary.

Observation

- DD in based on the notion of changing the deception environment based on input from the defender or observed actions of the adversary.

Creation

- Using creation tools (such as SDN, VM generation, file generation, service deployment, user generation, emulated device deployment, etc.), artifacts are created in the platform to further engagement with the adversary.

Enrichment

- Outputs from adversary actions (accesses files, attack resources, surveying logs/files/devices) are two-fold:
- (1) Validating intelligence or TTPs of the adversary (e.g., APT3 is knows to do X; X is confirmed to have been done in deception environment);
- (2) providing new intelligence and TTPs to defenders

Automation

Binary Analysis Pipeline (BAP)

BAP is a technique used to dynamically/statically analyze binary data

Extraction

- Binaries are automatically extracted from VMs and downloaded to the platform, based on predefined “trigger” criteria.

Pipeline

- A RE pipeline is then executed to unwrap the binary; using features of interest, automation of the RE environment’s variables and tools is conducted.

Enrichment

- The RE environment then is tailored to provide applicable outputs, in that the data is enriched by those features of interest.

Automation

Automated Response (AR)

AR consists of mechanisms to deter or thwart attacks in the networks.

Informing

- The root for these types of actions may be driven by such factors as well-known/established attack vectors (e.g., spearfish or known URLs).

Relief

- Automated responses aids in “clearing up the noise” so defenders need not get bogged down in the rush of cyber monitoring data.

…and how can we get there?

- Create actions off the data we are collecting
- Enable the integration of custom tools and workflows
- Automate the creation of sensor specific signatures
  - Using VMI for YARA, CB, …
  - Using DPI for suricata, snort, …
- Create Phantom playbooks encode informed understanding of the adversary
  - Creates higher confidence in the playbook
  - Enables defenders to create “risker” responding (we’re moving beyond blocks)
  - Enables the actioning off near-real time detection with the sensors on the operational system

Considerations…

… to keep in mind when developing automated platforms

- How do we use data sources to automate processes?
  - E.g., A product like Phantom is normally used today for FW blocks
- How can we use it for more specific automated response(s) ?

- Using Threat Emulation, we have a good idea of what the TTPs are of certain APTs.
- Based on those TTPs (e.g., SMB exploitation by APT*x*), we can create environments that are conducive to the TTP (e.g., create SMB shares for APT*x*) for both APT validation, containment, threat intelligence gathering (new techniques, threat surfaces)

Adversary Emulation

Getting to know your threats.

.conf19
splunk>

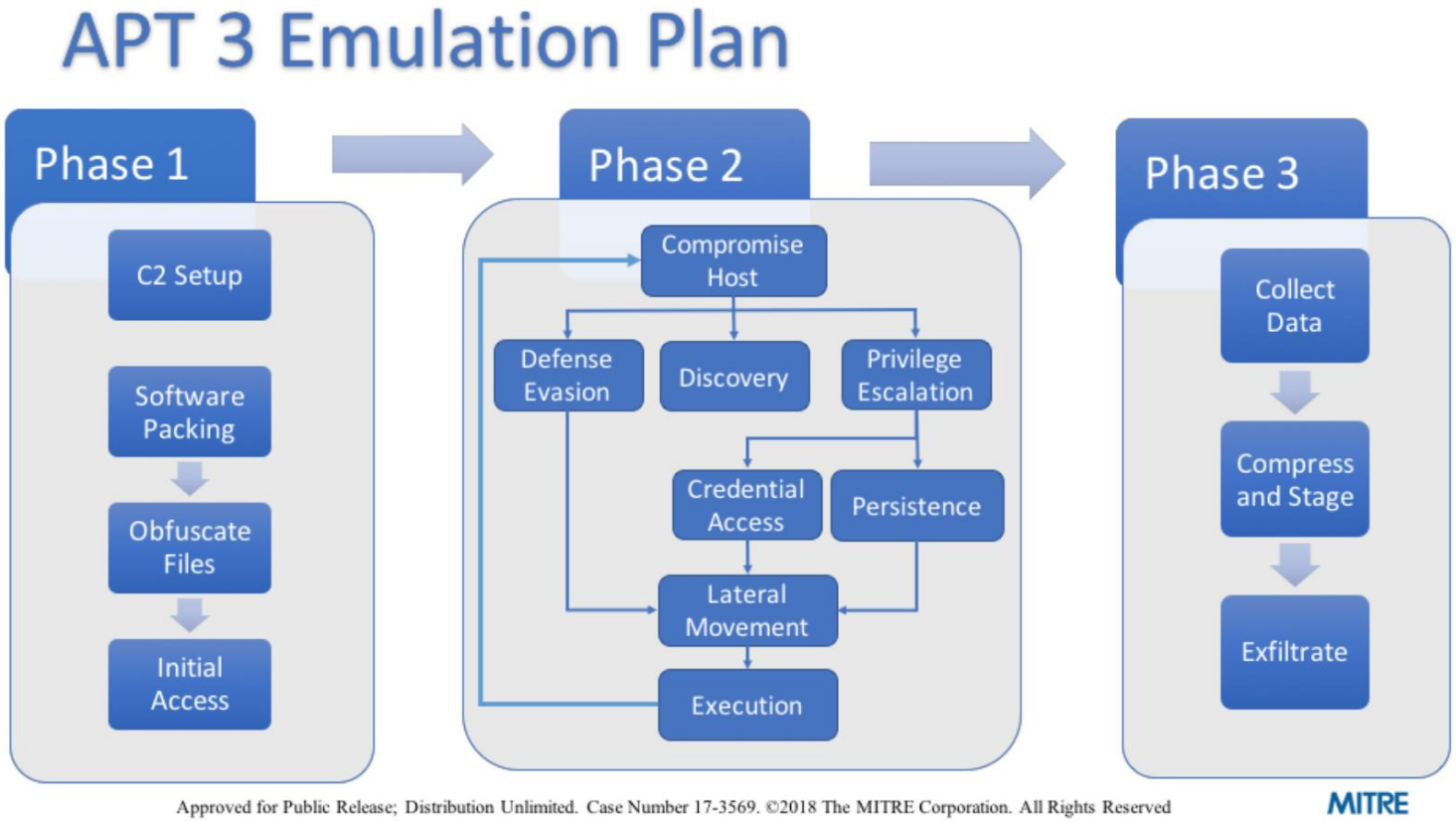
What is Adversary Emulation

- Adversary emulation is an activity where security experts emulate how an adversary operates.
- Adversary activities are described using TTPs (Tactics, Techniques & Procedures)
- Focused on the execution of a scenario

https://attack.mitre.org/w/img_auth.php/6/6c/APT3_Adversary_Emulation_Plan.pdf

Adversary Emulation

- Train the tools
- Test the tools
- Profile the adversary
- Enrich data
- Extrapolate data to fill in the gaps
- What did we do ?
  - Created a framework to encode and replay all the actions in a cyber range



https://attack.mitre.org/w/img_auth.php/6/6c/APT3_Adversary_Emulation_Plan.pdf

Techniques Example: APT3

Techniques Used

- System Owner/User Discovery - An **APT3** downloader uses the Windows command `"cmd.exe" /C whoami` to verify that it is running with the elevated privileges of "System."[3]
- Command-Line Interface - An **APT3** downloader uses the Windows command `"cmd.exe" /C whoami`.[3] The group also uses a tool to execute commands on remote computers.[4]
- Scheduled Task - An **APT3** downloader creates persistence by creating the following scheduled task: `schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"`.[3]
- Uncommonly Used Port - An **APT3** downloader establishes SOCKS5 connections to two separate IP addresses over TCP port 1913 and TCP port 81.[3]
- Standard Non-Application Layer Protocol - An **APT3** downloader establishes SOCKS5 connections for its initial C2.[3]
- Multi-Stage Channels - An **APT3** downloader first establishes a SOCKS5 connection to 192.157.198[.]103 using TCP port 1913; once the server response is verified, it then requests a connection to 192.184.60[.]229 on TCP port 81.[3]
- PowerShell - **APT3** has used PowerShell on victim systems to download and run payloads after exploitation.[3]
- Scripting - **APT3** has used PowerShell on victim systems to download and run payloads after exploitation.[3]
- Input Capture - **APT3** has used a keylogging tool that records keystrokes in encrypted files.[4]
- System Network Configuration Discovery - A keylogging tool used by **APT3** gathers network information from the victim, including the MAC address, IP address, WINS, DHCP server, and gateway.[4] [6]
- Credential Dumping - **APT3** has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig." The group has also used a tools to dump passwords from browsers.[4]

https://attack.mitre.org/wiki/Group/G0022

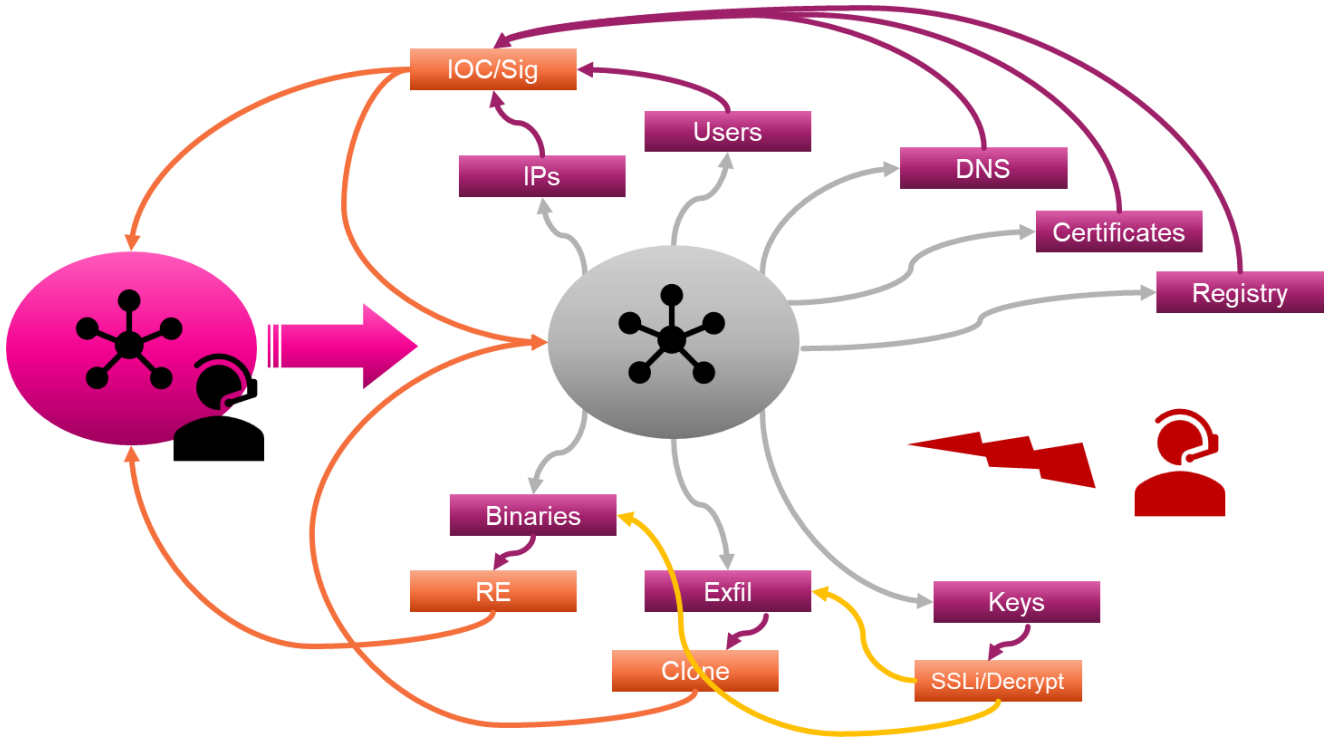
Putting the Pieces Together

APT3 in Action

.conf19
splunk>

Putting Together the Pieces

Using APT3 as a use-case, how would we leverage dynamic deception to identify, thwart, and learn from such an attack?



- Create the environment
- Emulate the attack
- Execute the attack
- Migrate and isolate
- Learn from the attack
- Create interest
- Continue the engagement

APT3 in Action

Environment/components: HADES, Director, Splunk, Phantom

VMs: Kali, Win7a, Win7b, VYOS, Win2012

- 1. Attack is initiated by Kali
  - Demonstrates threat emulation techniques
- 2. Malicious scans identified targeting SMB searches
- 3. Notification sent to HADES API to establish new SMB shares on-the-fly
- 4. Attack is identified
  - Method 1: known malicious URL identified in Splunk logs (through L7 DPI)
  - Method 2: mimikatz identified through CB/CS
- 5. Response based on playbook
  - Signature developed (Suricata)
- 6. Notification sent to HADES API to start migration/cloning process
- 7. New environment established, network flows installed

Demo

Conclusions

.conf19
splunk>

Summary & Conclusions

- … Threat data exploitation is important to becoming predictive
- Dynamic Deception is enhanced through Automation
  - React in realtime
  - Reduce defender overhead
  - Continue the enticement
  - Continue the engagement
- Automating workflows (binary analysis) brings tools to the front
  - Customization
  - Data/output extraction (e.g., into repositories)
- Automation of threats gives us understanding and the means to test defenses

Thank You!

Vince, vince@sandia.gov
Will, wmstout@sandia.gov

Go to the .conf19 mobile app to

RATE THIS SESSION