How to Submit a Threat Profile to MITRE ATT&CK

Walker Johnson

September 2018

Disclaimer

- I am not here in the name of or speaking on behalf of my employer.

- All opinions expressed here are my own.

Agenda

1. Background
2. ATT&CK framework
3. Threat research & submissions
4. Indicators and techniques
5. Takeaways

Background

- In 2010 began 18 month adventure.
- One client was a repeated victim.
- We did DFIR work all over the world.
- We got to know the attacker's methods.
- Almost 4 years go by..

Limited References

1. Publicly Available Tools Used in Targeted Attacks = 16 known tools

Mandiant 2012 M-Trends Report

http://www.utdallas.edu/~mxk055100/courses/dbsec12f_files/trend-report.pdf

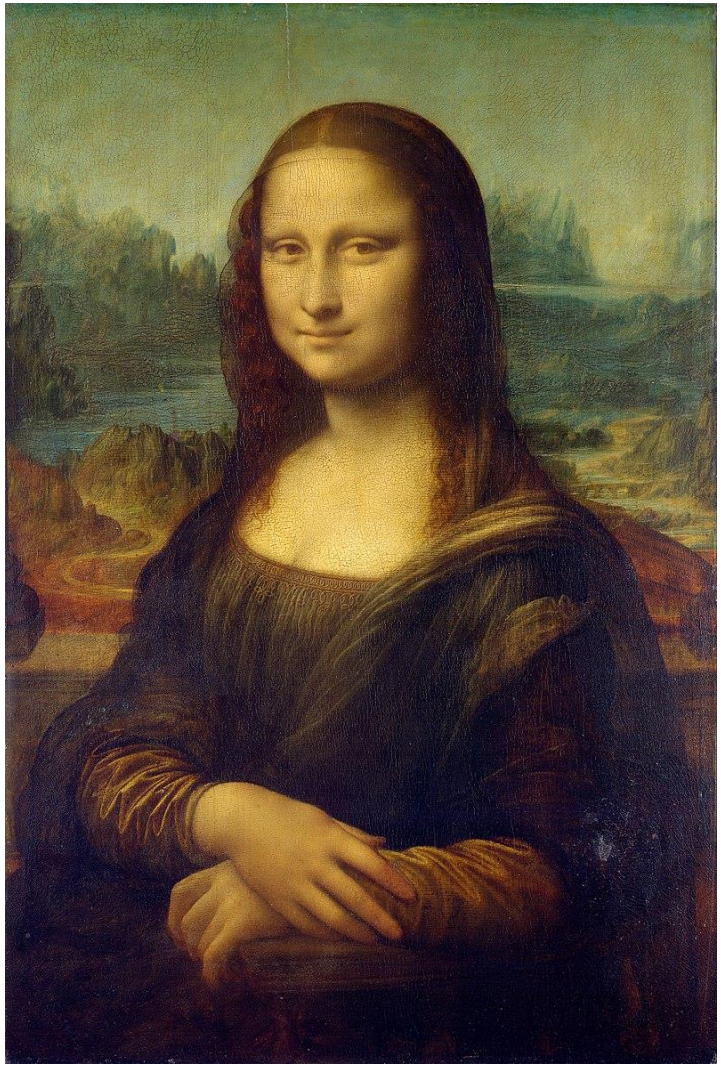
2. In-Depth Look: APT Attack Tools of the Trade = 18 known tools

Trend Micro 2013 Blog Post

http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade

MITRE ATT&CK

- **May 2015**
- **ATT&CK now:**
  - **11 Tactics**
  - **70+ Threat Groups**
  - **200+ Techniques**
  - **230+ Tools & Utilities**
  - **500 References**



MITRE ATT&CK

August 2015

Do you have public references that:

1. Associates the malware & tools to the group?
2. Associates the techniques to the group?
3. Can the references be definitively linked?
4. Are they clear and not open to interpretation?

Response

- They basically just wanted ***proof***.
- Proof is simply ***evidence*** of the truth.

Empirical evidence that supports science-based investigation = ***Forensic evidence***

October 2015

MITRE – "don't think there is enough public reporting to assert with high confidence"

In other words..

Cyber Threat Group Named

- ***Threat group named***:
  - **October 13, 2015**
    FireEye researchers shed more light on infamous cybercriminals associated with ***RawPOS*** malware. and christen it '***FIN5***.'
    http://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645

- ***Another mention one day later***
  - **October 14, 2015**
    FIN5 hacking crew steals 150,000 credit cards from casino
    http://securityaffairs.co/wordpress/41044/cyber-crime/fin5-hacked-a-casino.html

GrrCon 2016 Presentation

- ***One year later a great presentation:***

  Attacking the Hospitality and Gaming Industries
  Tracking an Attacker Around the World in 7 Years
  https://www.youtube.com/watch?v=fevGZs0EQu8

- ***55 Minute talk with tons of details***

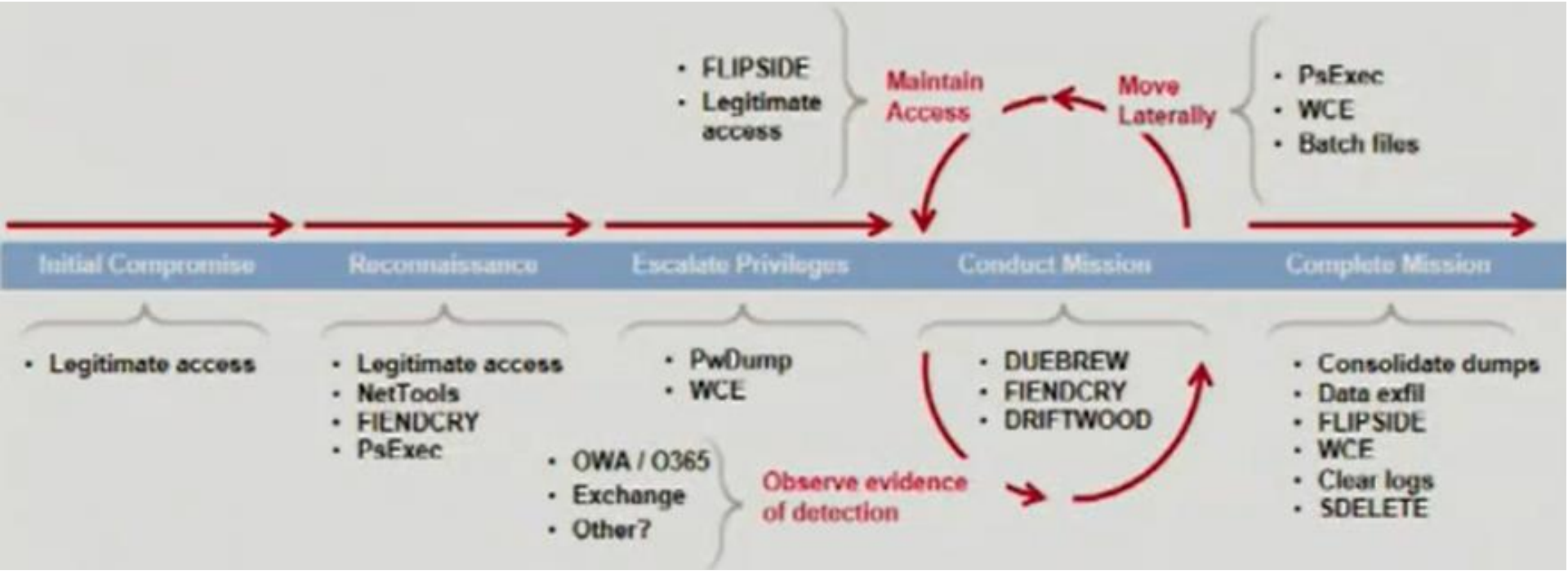
- ***Required some name decoding***

Mandiant Name	Public Name	Purpose
FIENDCRY	MemPDumper by DiabloHorn	Memory Searching
DUEBREW	Perl2Exe launcher	Execution & Persistence
DRIFTWOOD	Perl2Exe data encoder	Data Obfuscation (XOR)

GrrCon 2016 Presentation Cont.

- ***Details on tactics and techniques:***

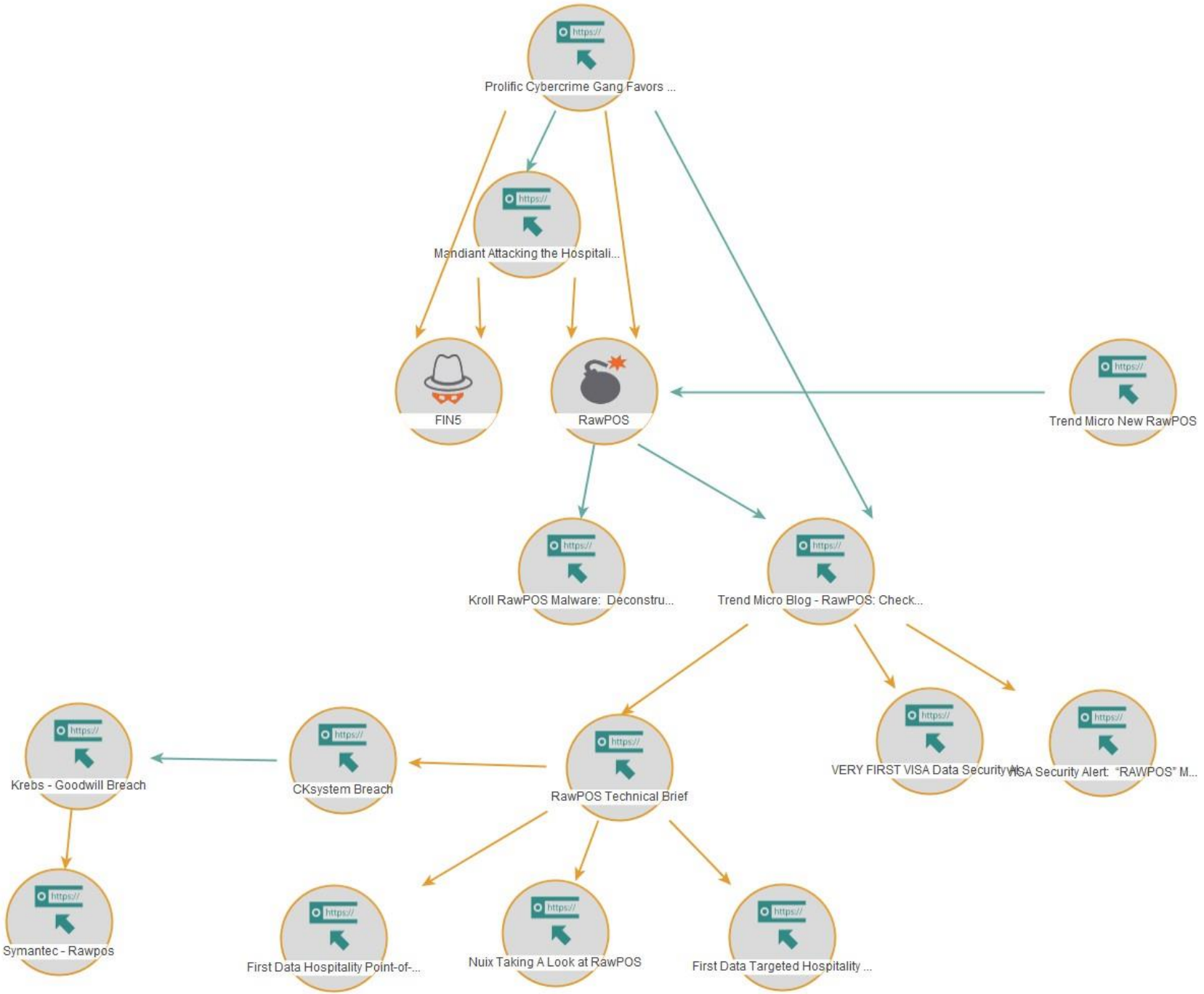
  - They use **RawPOS**. Since 2008. "slow maturity cycle.. still works."
  - **FIN5** by and large uses legitimate access . Most likely via vendors..
  - Very high statistical chance if **RawPOS** then.. most likely **FIN5**..



Threat Research with a Direct Link

- ***Research leads to related reports:***

Date	Reference Link
10/2008	http://usa.visa.com/download/merchants/d**ebugging_software_memory.pdf**
05/2009	https://www.firstdata.com/downloads/partners/**fd_gpm_notice_visa_security_alert_28may09_partnersupport.doc**
06/2009	https://www.firstdata.com/downloads/partners/**fd_gpm_notice_discover_alert_12june09_partnersupport.pdf**
02/2014	https://www.symantec.com/security_response/writeup.jsp?d**ocid=2014-021819-4159-99**
09/2014	https://krebsonsecurity.com/2014/09/**breach-at-goodwill-vendor-lasted-18-months/**
10/2014	https://www.nuix.com/2014/10/09/**taking-a-look-at-rawpos**
03/2015	https://usa.visa.com/dam/VCOM/download/**merchants/alert-rawpos.pdf**
04/2015	http://blog.trendmicro.com/trendlabs-security-intelligence/**rawpos-checking-in-at-a-hotel-near-you**
04/2015	http://www.trendmicro.com/vinfo/resources/images/tex/pdf/**RawPOS%20Technical%20Brief.pdf**
01/2017	http://www.kroll.com/CMSPages/GetAzureFile.aspx?path=~%5Cmedia%5Cfiles%5Cintelligence-center%5Ckroll_**malware-analysis-report.pdf**
04/2017	http://blog.trendmicro.com/trendlabs-security-intelligence/**rawpos-new-behavior-risks-identity-theft**


Prolific Cybercrime Gang Favors ...
Mandiant Attacking the Hospitali...
FIN5
RawPOS
Trend Micro New RawPOS
Kroll RawPOS Malware: Deconstru...
Trend Micro Blog - RawPOS: Check...
Krebs - Goodwill Breach
CKsystem Breach
RawPOS Technical Brief
VERY FIRST VISA Data Security Al...
VISA Security Alert: "RAWPOS" M...
Symantec - Rawpos
First Data Hospitality Point-of-...
Nuix Taking A Look at RawPOS
First Data Targeted Hospitality ...

Pivot #1 - Researching Presenters

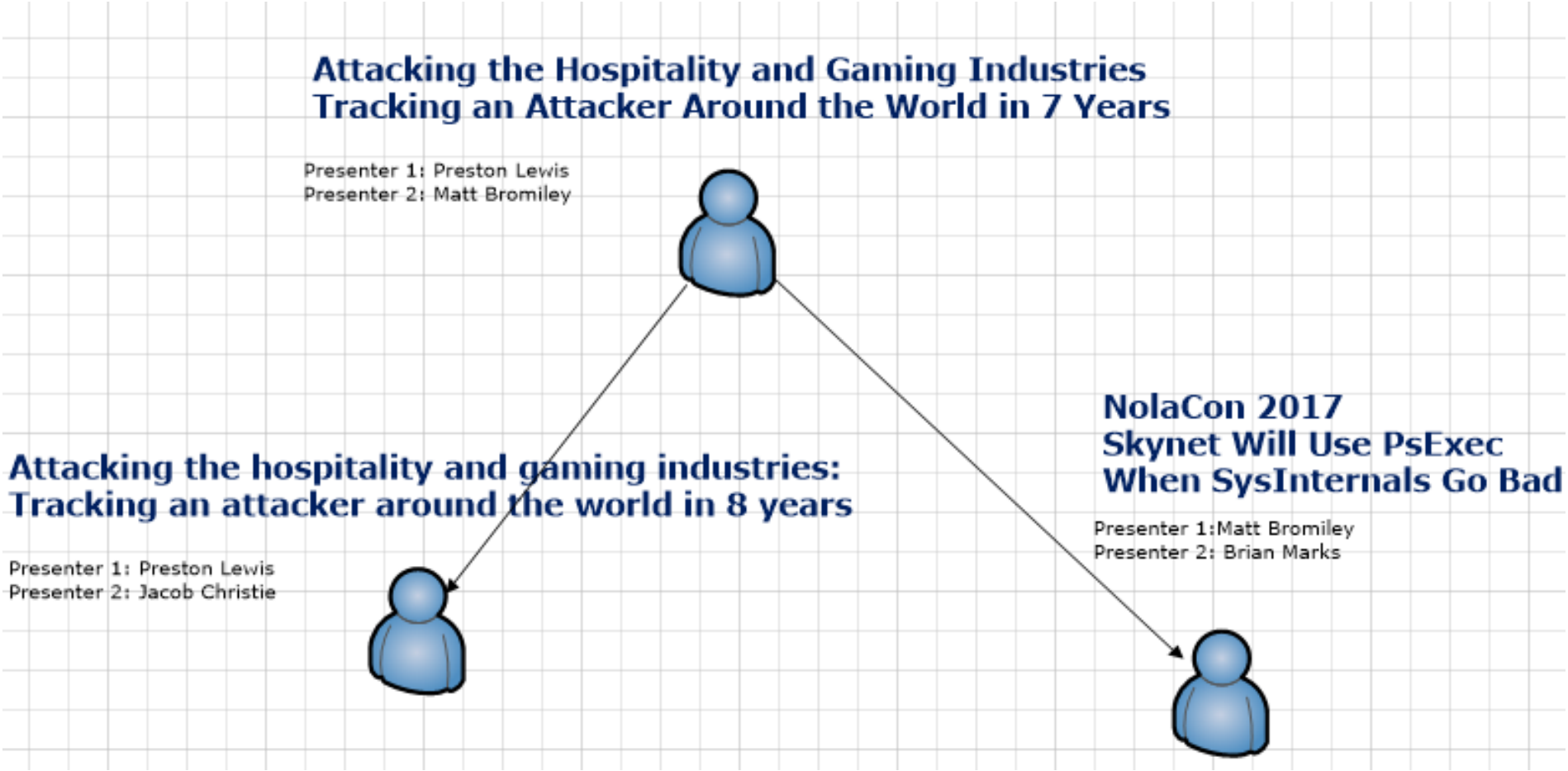
Presentation: INHOSPITALITY INDUSTRY: APT in hospitality and gaming industry

Date: **October 13, 2015**
Conference: Cyber Defense Summit (formerly Mircon)
Presenter 1: Emmanuel Jean-Georges
Presenter 2: Barry Vengerik

Presentation: Attacking the Hospitality and Gaming Industries Tracking an Attacker Around the World in 7 Years

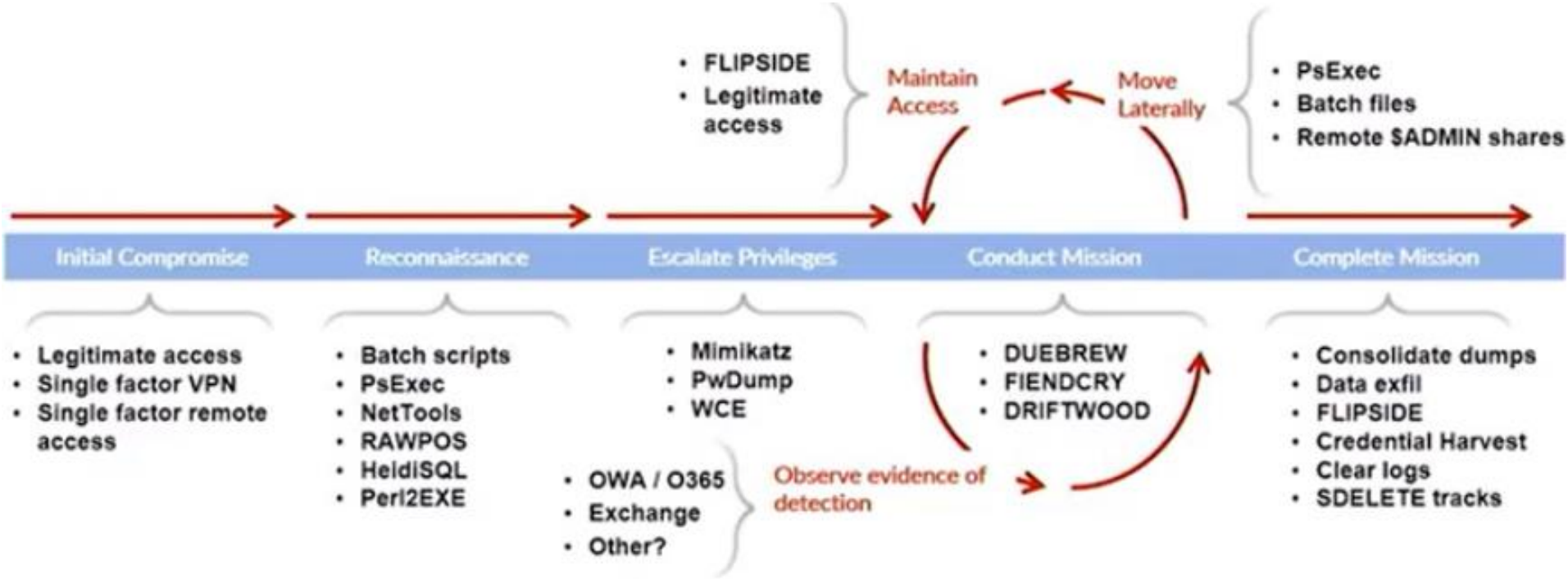
Date: **October 7, 2016**
Conference: GrrCon 2016
Presenter 1: Preston Lewis
Presenter 2: Matt Bromiley

Researching Presenters Cont.



Researching Presenters Cont.

- Attacking the hospitality and gaming industries: Tracking an attacker around the world in 8 years
  https://www.youtube.com/watch?v=lu2cBSItSZ4



Pivot #2 - IOC Exports

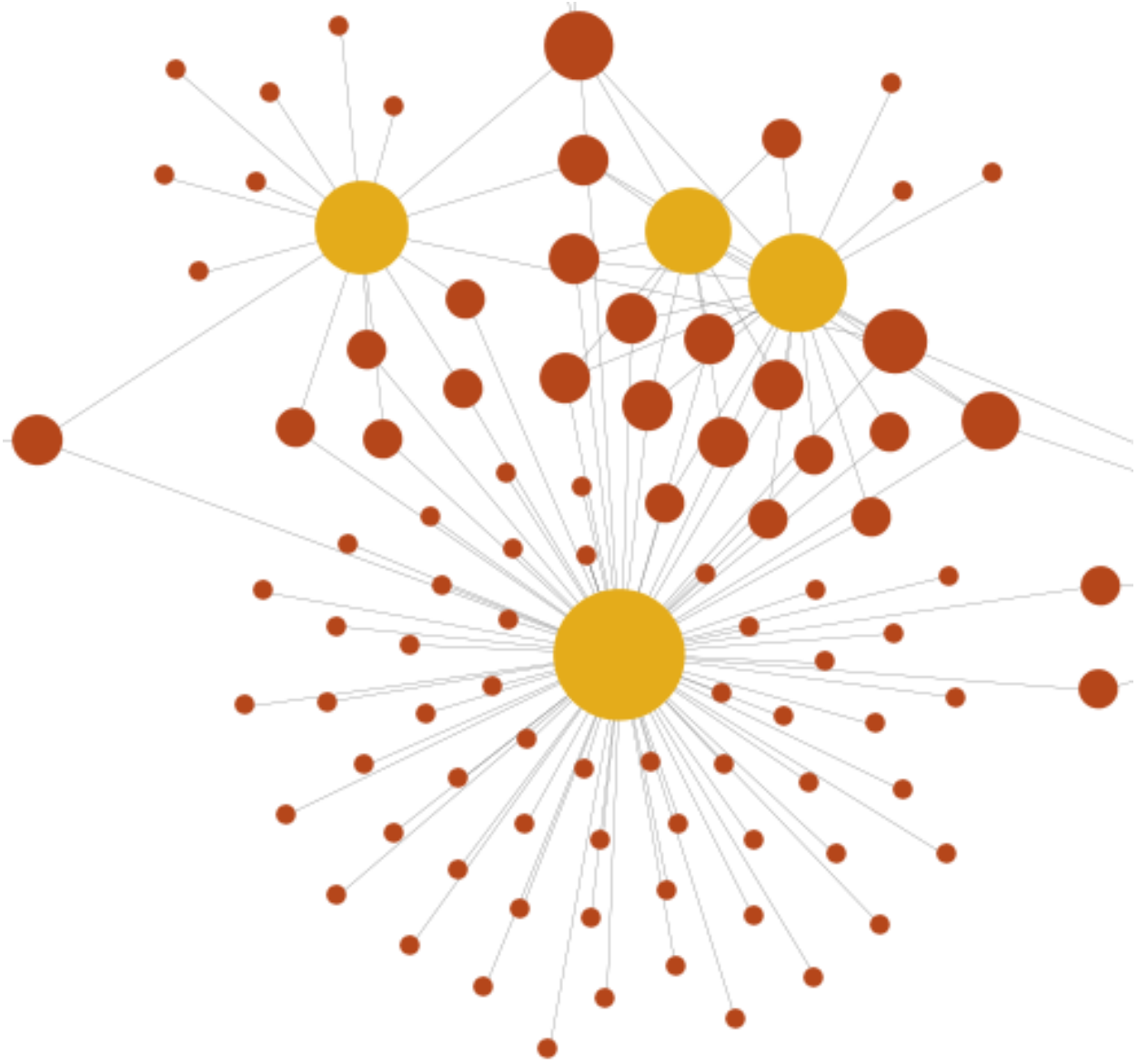
Report Name	Hash Values
Carbon Black Attack on Memory 012014	**12**
First Data Visa Targeted Hospitality 052009	**21**
First Data Visa Targeted Hospitality 062009	**37**
Kroll RawPOS Malware Report 012017	**44**
NUIX RawPOS Alert 092014	**14**
Trend Micro RawPOS Technical Brief 042015	**9**
Trustwave Spider Labs Malware Freakshow 062010	**4**
Trustwave Spider Labs Malware Freakshow 082009	**16**
VISA Malicious Software 042009	**26**
VISA RAWPOS Targeting Lodging 032015	**32**
VISA Targeted Hospitality Sector Vulnerabilities 122009	**80**
	295

Additional Threat Research Reports Found

- ***Initial results on the hash values:***

Date	Link
11/2008	https://www.bankcardcentral.com/resources/pdfs/visa-alerts/VisaDataSecurity**Alert-MaliciousSoftware.pdf**
04/2009	https://www.visa.com.ua/ua/ukua/merchants/riskmanagement/includes/uploads/**AP040109_malicious_ip_add.pdf**
08/2009	https://www.defcon.org/images/defcon-17/dc-17-presentations/**defcon-17-nicholas_percoco-jibran_ilyas-malware_freak_show.pdf**
12/2009	http://www.visa.com.ua/ua/uk-ua/merchants/riskmanagement/includes/uploads/**AP120109_targeted_hosp_vulnerabilities.pdf**
06/2010	https://media.blackhat.com/bh-us-10/whitepapers/Percoco_Ilyas/**Trustwave%20-%20SpiderLabs%20-%20BlackHat-USA-2010-Percoco-Ilyas-Malware%20Freakshow-2010-wp.pdf**
01/2014	https://www.carbonblack.com/2014/01/17/**the-attack-on-retailers-memory-and-how-to-prevent-it**

MD5 Hash Correlations



Additional Threat Research Reports Found

- ***Results from new searches:***

The not so boring land of Borland executables
http://www.hexacorn.com/blog/2014/12/18/the-not-so-boring-land-of-borland-executables-part-2

Data Security Alert - Retail Data Security Breaches
https://www.moneris.com/~/media/Files/SecurityAlerts/Discover%20Retail%20Data%20Security%20Breaches%202015FEB.ashx

TELUS Security Labs - Backdoor.Win32.Rawpos.A
http://telussecuritylabs.com/threats/show/TSL20140219-03

Understanding malware targeting Point Of Sale Systems
https://blogs.bromium.com/understanding-malware-targeting-point-of-sale-systems

Visa issues security alert
https://www.merchantequip.com/merchant-account-blog/641/visa-issues-security-alert

Malicious Software, Tools, Hash(s) Value, and Registry Key
http://www.abacuspos.com/eAlerts/Malicious-Software-Jan-2009.pdf

Authoritative Threat Group Techniques

October 2017

- Second submission
- 10 Tactics
- 14 Techniques
- 30 References
- 13 Security organizations

Initially Accepted Techniques (Jan, 2018)

File Name	Description	ATT&CK Technique	Stage in Lifecycle
wce64.exe	This 64-bit version of Windows Credential Editor is modified/slimmed down. The file had been obfuscated to appear as though it was part of Apache Open Office3.	Valid Accounts (T1078)	Initial Compromise
ENT.exe	ENT (Essential NetTools) is a set of network scanning, security and admin tools useful in diagnosing networks and monitoring network connections.	Remote System Discovery (T1018)	Reconnaissance
get2.exe	GET2 Penetrator Version 1.9.9d - Windows Authentication information exfiltrator.	Credential Dumping (T1003)	Escalate Privileges
PsExec.exe	The SysInternals tool also has myriad legitimate uses to allow system administrators to remotely invoke executable file across a network.	Service Execution (T1035)	Conduct Mission
sdelete.exe	SDelete 1.51 by SysInternals. Securely deletes data.	File Deletion (T1107)	Complete Mission

Anti Forensic Techniques Observed

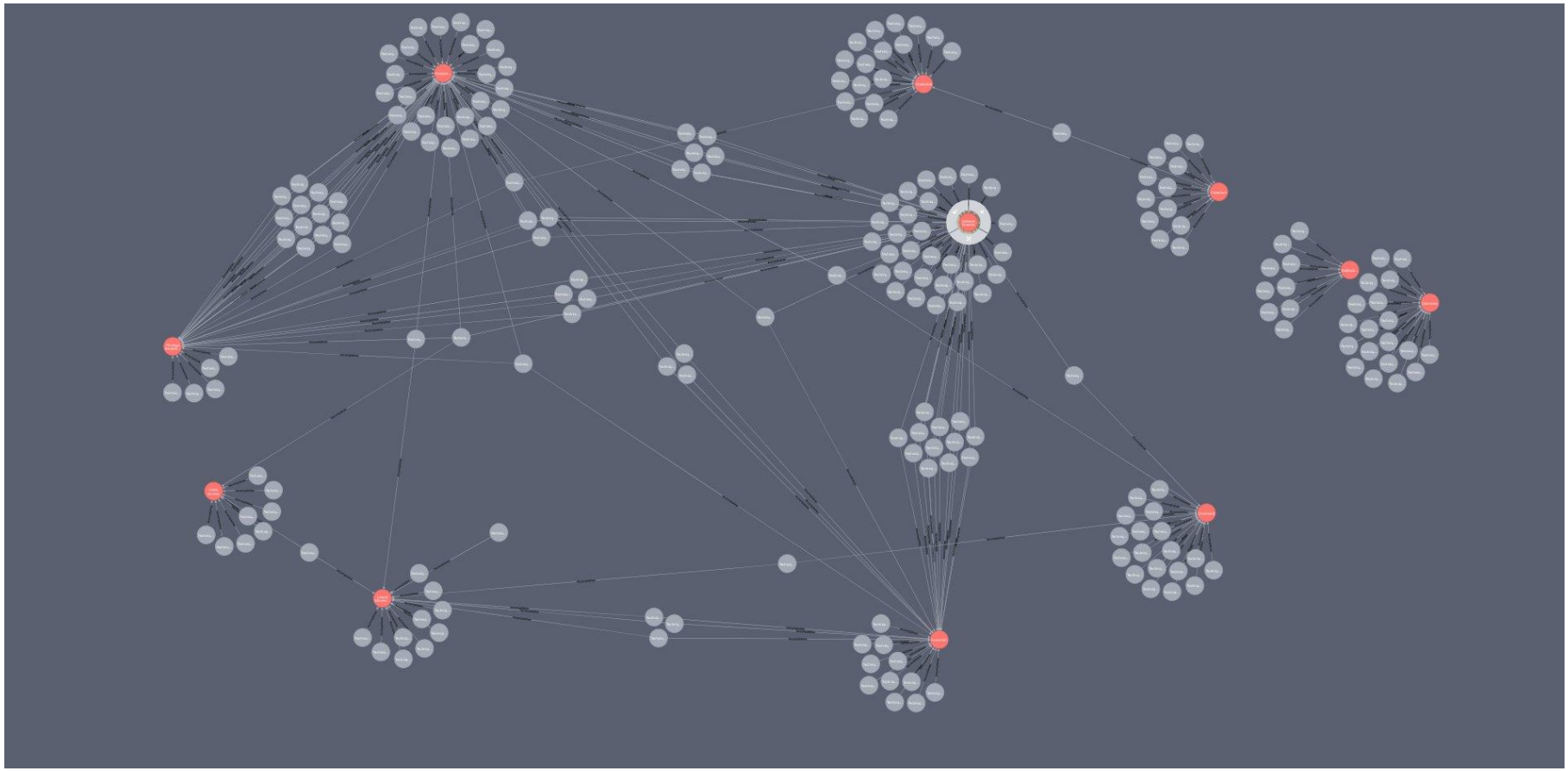
- **T1070 - Indicator Removal on Host**
  Description: Adversaries may delete.. event files.

- **T1027 - Obfuscated Files or Information**
  Description: Adversaries may attempt to make or file difficult to discover or analyze by encrypting,.

- **T1099 – Timestomp**
  Description: Timestomping is a technique that modifies the timestamps of a file..

- **T1107 - File Deletion**
  Description: Adversaries may remove these files over the course of an intrusion..

Tactics and Techniques



Best Practices

1. Incident Response Best Practices

- Identify adversary's footprint.., c2., and ***tools and techniques***.
- the attackers' ***tactics, techniques, and tools***

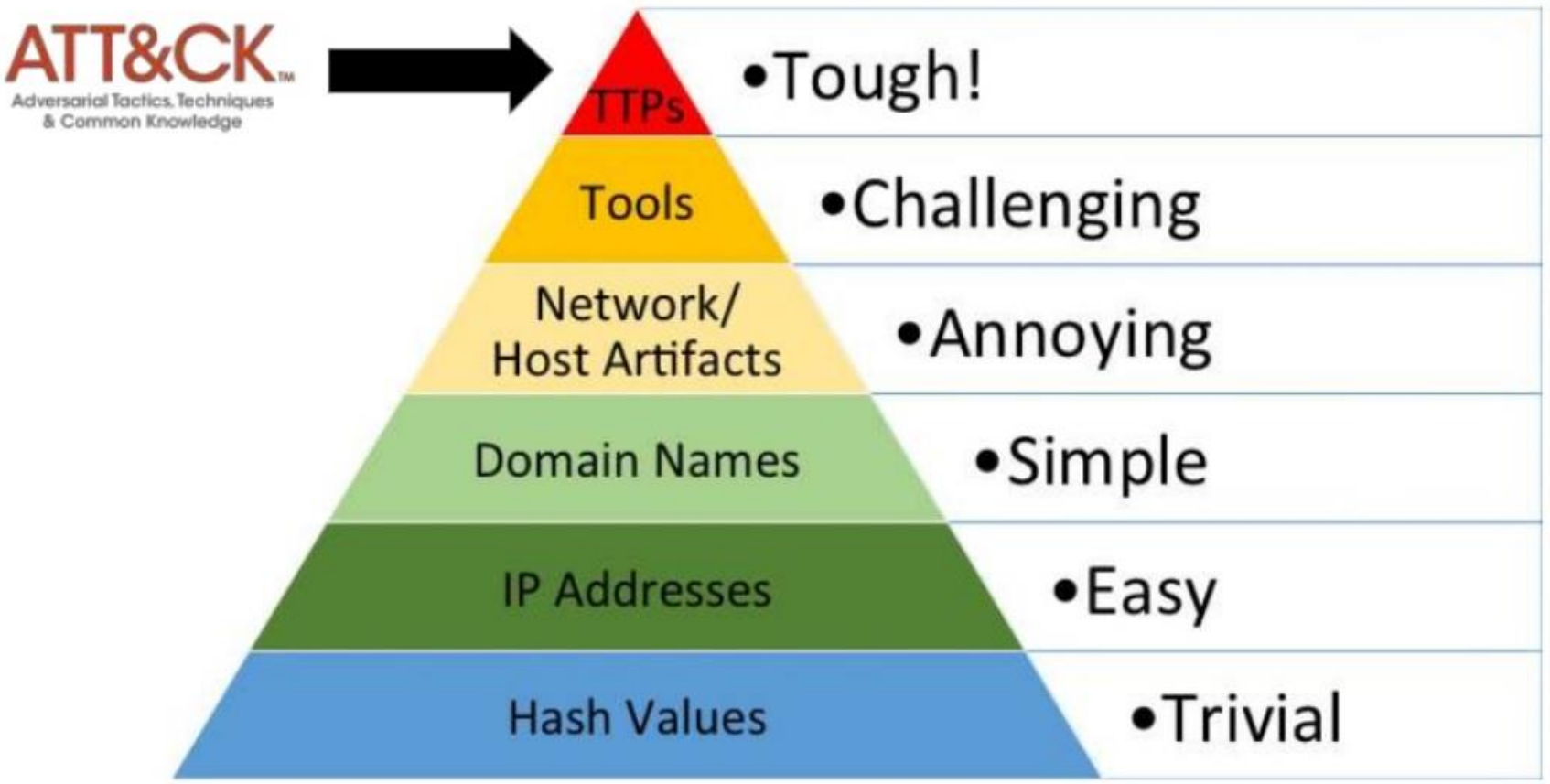
NIST Guide for Cybersecurity Event Recovery
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

2. CTI Sharing Best Practices

- Cyber threat information includes indicators of compromise; ***tactics, techniques***, and ***procedures***

NIST Guide to Cyber Threat Information Sharing
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

IR Pyramid of Pain



- Joe Slowik – "IOCs essentially 'expire'.. the very moment they are discovered"

IOC Shelf Life

Threat Connect

- "most IOCs have a relatively short shelf life, often lasting only hours between their first and last observation in the wild."

https://www.threatconnect.com/blog/what-the-verizon-dbir-says-about-threat-intelligence-sharing

Webroot

- **2015** over 97% of malware encountered by Webroot customers was seen on only a single endpoint.
- **2016**, approximately 94% of the malware observed by Webroot were only seen once
- **2017**, 93% of the malware encountered was seen on only one machine

Adversary Emulation

Open-source ATT&CK test tools

PRODUCT	MAIN PURPOSE	STRUCTURE	INSTALLATION*	ENDPOINTS SUPPORTED
Endgame Red Team Automation	Testing EDR products	Python scripts	Minimal	Windows only
Mitre Caldera	State preservation of attack origins	Python scripts, agents and Linux/Win server	Detailed instructions	Windows 64-bit only
Red Canary Atomic Red	Wiki, testing resources reference	No scripts	None	Windows, Mac, Linux
Uber Metta	Playbooks for adversary simulation and testing EDR products	Python, Redis, Celery, Vagrant, VirtualBox	Complex with lots of config file editing	Windows, Mac, Linux

Worst Case Scenario

State Dept. hack the 'worst ever'

"suspected Russian hackers have bedeviled State Department's email system for much of the past year"
https://www.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html

No Easy Breach: Challenges and Lessons Learned from an Epic Investigation
https://www.youtube.com/watch?v=cF9MeFhNn-w

Lessons Learned

1. All actors leave behind ***evidence***.
2. You can determine how your attacker likes to operate and ***get left*** of them.
3. A little ***persistence*** will pay off.
4. You now have a great way to ***share***!

Questions?

Thank You!

Email: wjohnsonsled@gmail.com

Twitter: wjohnsonsled