Threat Intelligence

Darien Kindlund
darien.kindlund@fireeye.com

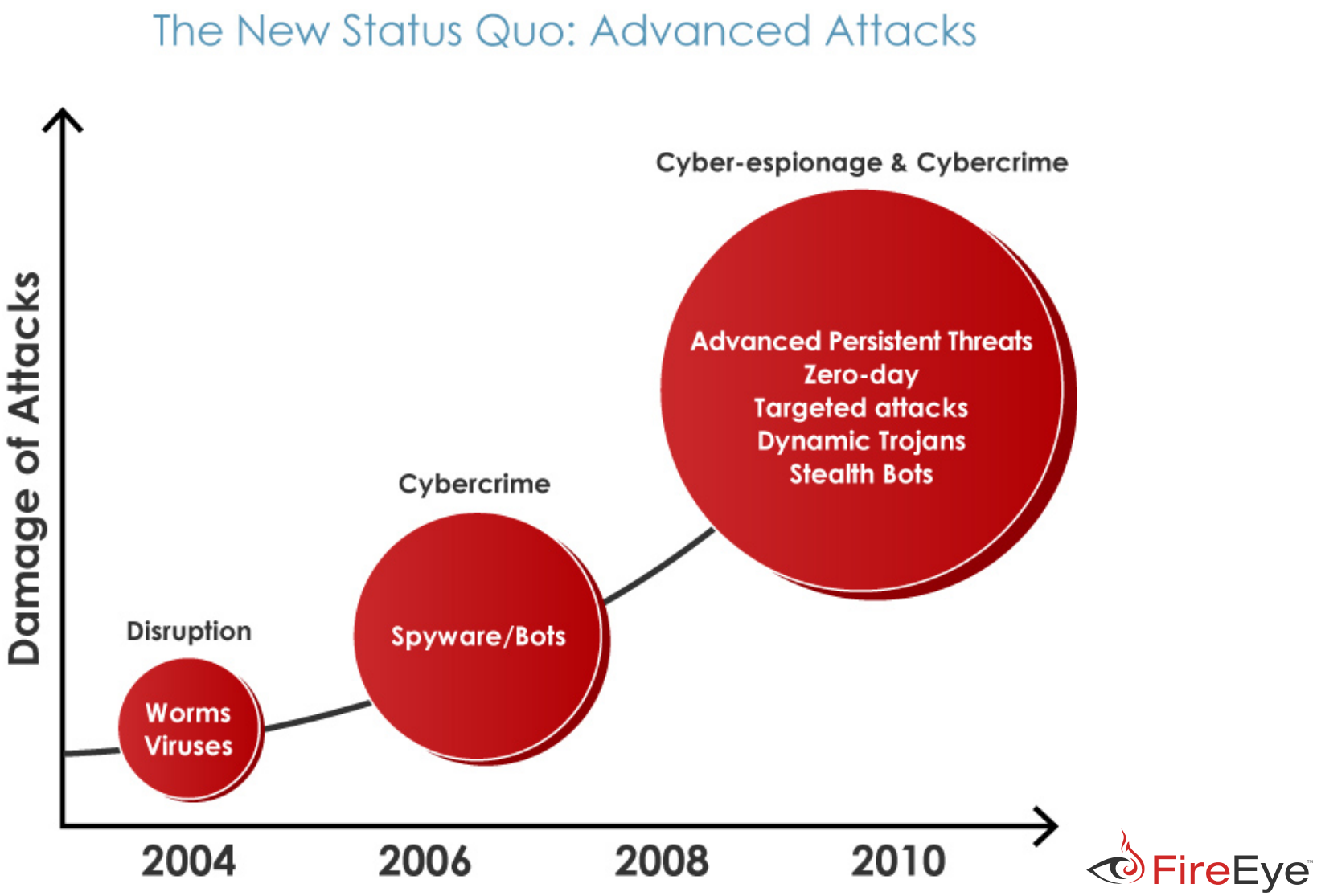
11/25/2013

Who am I?

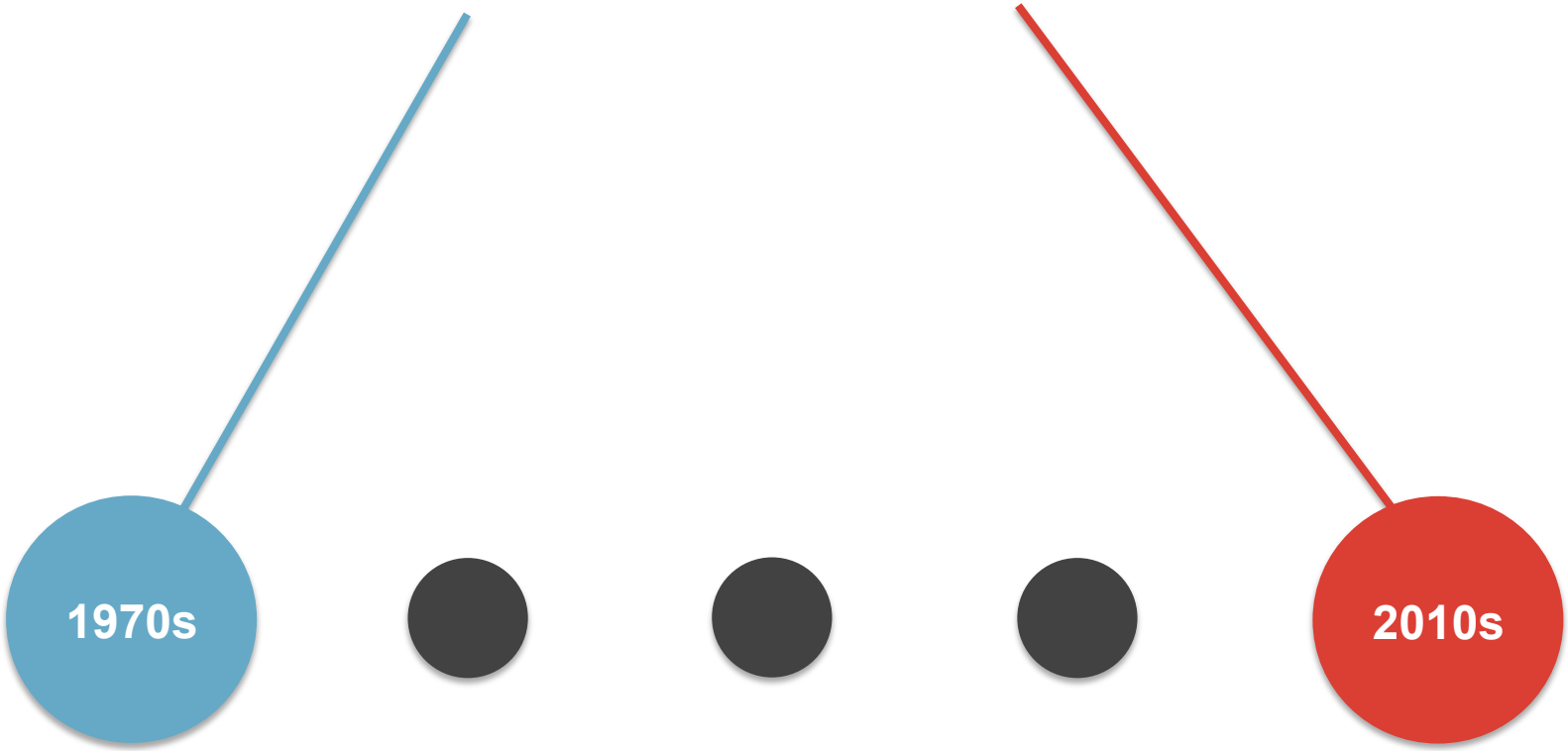
- Manager of Threat Intelligence at FireEye
- Infosec Scientist at MITRE
- Worked in Security Industry for 10+ years
- Cornell - BS 2002, M.Eng 2003

FireEye

History Lesson…



Why did this happen?



Security **Usability**

http://jnd.org/dn.mss/when_security_gets_in_the_way.html

FireEye

Defense has been losing…

- Write secure code from the start
- Patch as quickly as possible
- Try to proactively identify vulnerabilities (fuzzing)
- Audit code quality (after the fact)
- Validate code/communication reputation/provenance
- Employ bad code signatures
- Learn more about who is attacking us

FireEye

Old Assumption

- Write secu
- Patch as c
- Try to proa
- Audit code
- Validate c
- Employ ba
- Learn more about who is attacking us

We could detect and block these attacks before they succeed.

FireEye

New Assumption

Assume the attackers succeed and the infrastructure is already compromised.

- Learn more about who is attacking us

FireEye

The epiphany in sum…

- 1990s-2000s:
  - What does this bad **code** have in common?
  - Can we profile and detect bad **code**?
  - How can we prevent bad **code** from propagating?
  - Focus: It is a **code** problem.
- 2000s-2010s:
  - **Who** is attacking us?
  - Why are **they** successful?
  - How often do **they** change tactics?
  - What do **they** want?
  - Focus: It is a **human** problem.

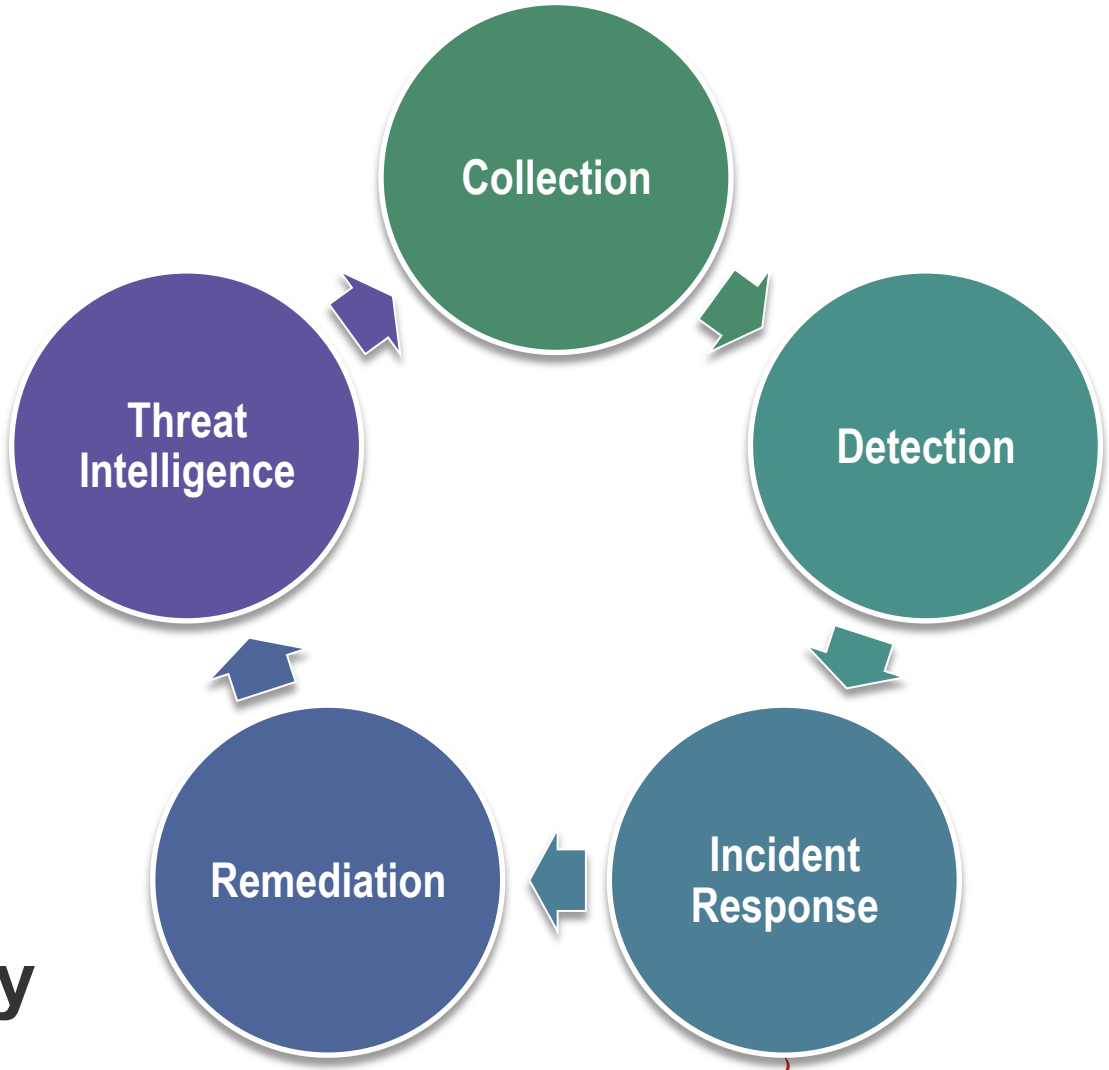
Ref: Reflections on Trusting Trust – Ken Thompson

FireEye

What is Threat Intelligence?

A mix of:

- Computer science
- Software engineering
- Information security
- Intelligence analysis
- Malware analysis
- Reverse engineering
- Risk analysis
- Statistics
- **Criminal Psychology**



FireEye

Advanced Persistent Threat (APT) Actors

Spectrum of State Responsibility

1. State-prohibited. The national government will help **stop** the third-party attack.
2. State-prohibited-but-inadequate. The national government is cooperative but **unable** to stop the third-party attack.
3. State-ignored. The national government knows about the third-party attacks but is **unwilling** to take any official action.
4. State-encouraged. Third parties control and conduct the attack, but the national government **encourages** them as a matter of policy.
5. State-shaped. Third parties control and conduct the attack, but the state **provides** some support.

Ref: Jason Healey's concept of a ”Spectrum of State Responsibility"

FireEye

Spectrum of State Responsibility

6. State-coordinated. The national government coordinates third-party attackers such as by "**suggesting**" operational details.
7. State-ordered. The national government **directs** third-party proxies to conduct the attack on its behalf.
8. State-rogue-conducted. **Out-of-control** elements of cyber forces of the national government conduct the attack.
9. State-executed. The national government **conducts** the attack using cyber forces under their direct control.
10. State-integrated. The national government attacks using **integrated** third-party proxies and government cyber forces.

Ref: Jason Healey's concept of a "Spectrum of State Responsibility"

FireEye

Crux: Classic Asymmetric Warfare

- Can’t defend everything, all the time
- Defenders need to succeed **every time**
- Attackers only need to succeed **once**

FireEye

Sounds bad, right?

- Well, attackers are human, also
- They sometimes make **mistakes** (surprised?)
- Despite media hype, their operations are conducted similar to a **business**
- They use the least sophisticated methods to accomplish their mission objectives
- Why?

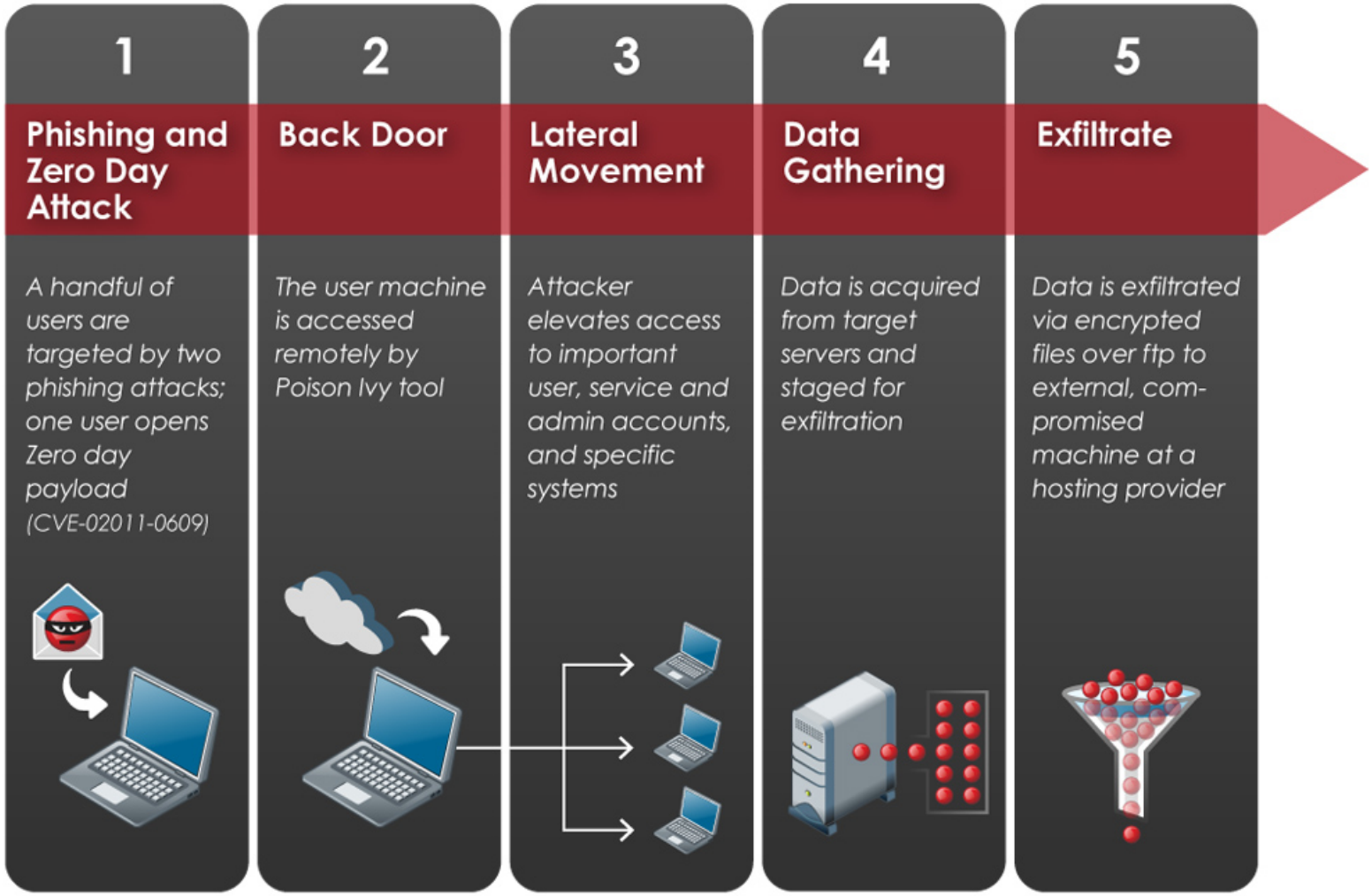
FireEye

K.I.S.S. Principle – Applies to Attackers, Too

- Complex attacks are **harder** to detect
- But complexity makes the attack more **costly** to develop/test
- Complexity also can make it **easier** to identify **portions** of the attack
  - Why do we not see more attackers using proper SSL comms? (Hint: How costly is it to implement PKI?)
  - Why is there not more signed malware?

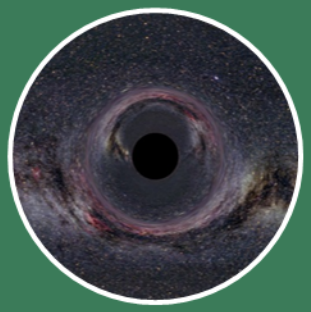
FireEye

Example Attacker/APT Playbook



Next-generation threats like the RSA attack use successive inbound and outbound stages

Spectrum of Frequent Advanced Attacks For 2012/2013



Mass Website Compromises

- Exploit toolkits
- 0-day exploits (rare)
- Sophisticated crimeware

Watering Hole Attacks

- Compromised site specific to industry vertical
- 0-day exploits more common
- Frequently nation state driven

Weaponized Email Attachments

- Common file formats
- Legit work product presented (decoy)
- Preferred by nation states

Malicious URLs in Email (Spearphish)

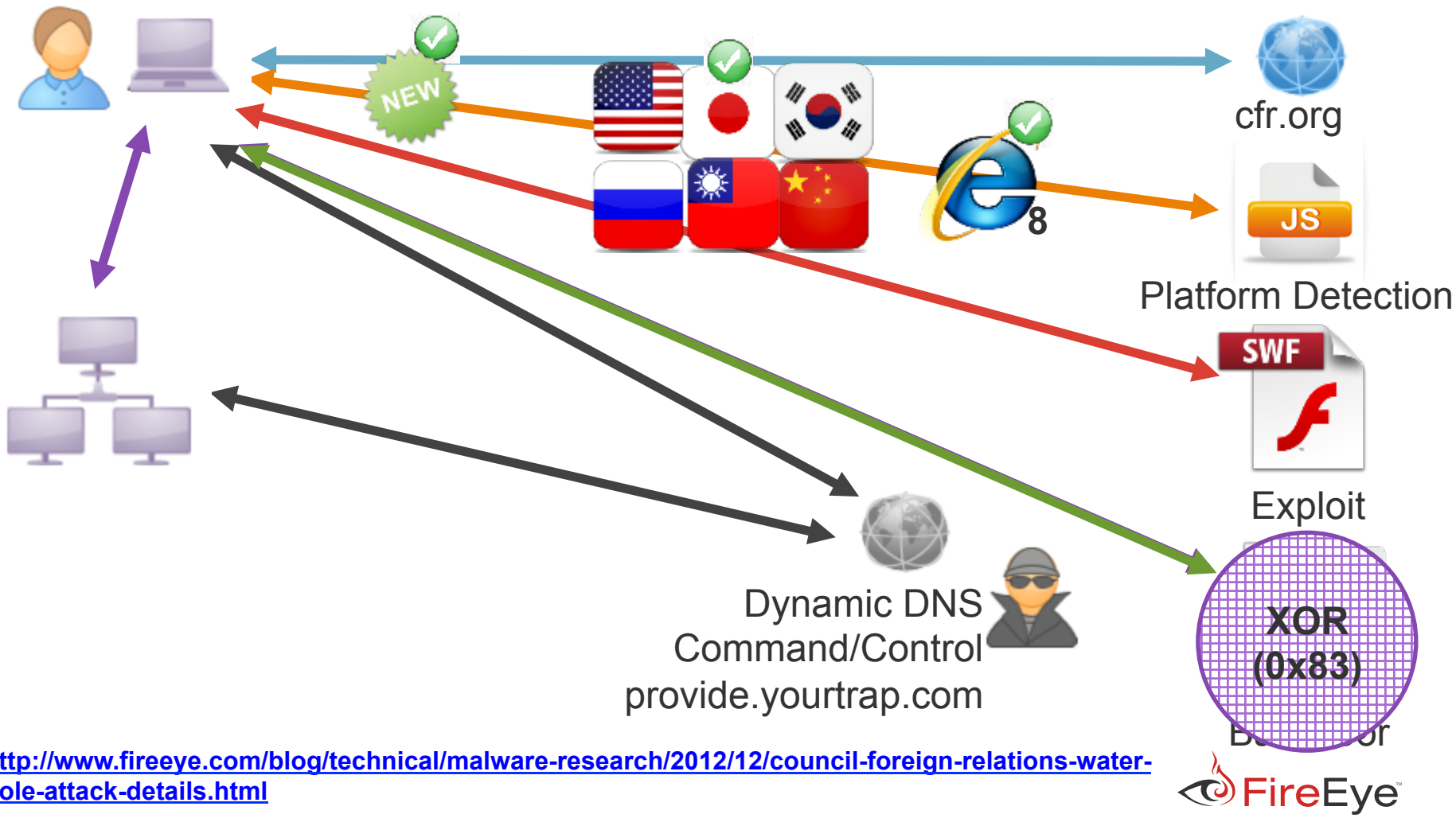
- Exploits specific to target environment
- Only exploit if visited from target network(s)
- Use existing trust relationships

1000+ Victims
(Easiest to Detect)

~1-2 Victims
(Hardest to Detect)

FireEye

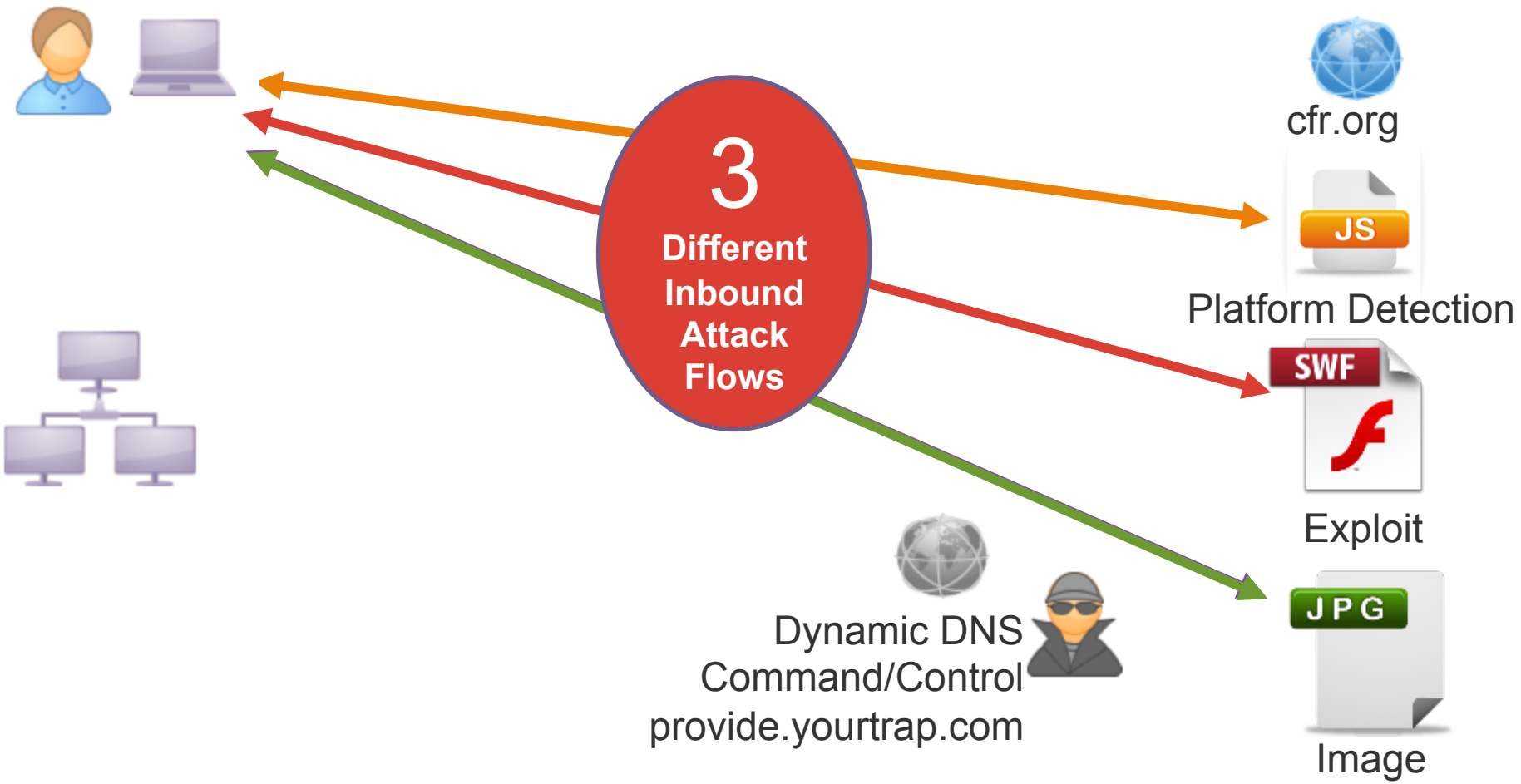
Watering Hole / Strategic Web Compromise
CFR Attack (CVE-2012-4792)



http://www.fireeye.com/blog/technical/malware-research/2012/12/council-foreign-relations-water-hole-attack-details.html

FireEye

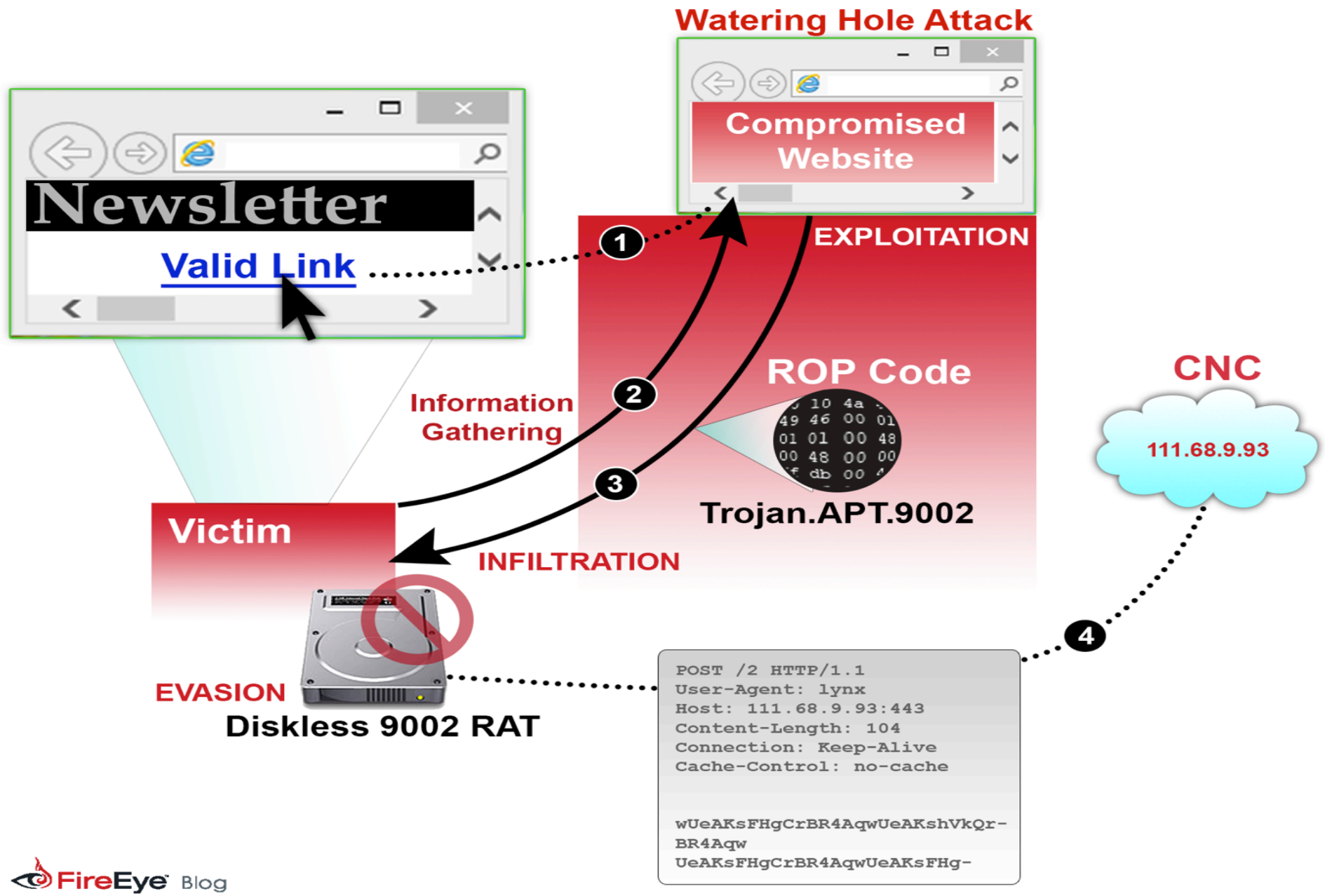
Watering Hole / Strategic Web Compromise
CFR Attack (CVE-2012-4792)



http://www.fireeye.com/blog/technical/malware-research/2012/12/council-foreign-relations-water-hole-attack-details.html

FireEye

OPERATION EPHEMERAL HYDRA



FireEye Blog

Email Attack
Operation Beebus

update.exe Apr 2011

UNKNOWN Sept 2011

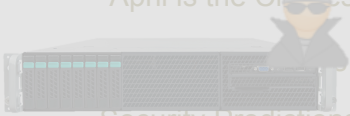
Key Attack Characteristics

1. Nation state driven attack using multiple vectors & files in campaigns spread over 2 years
2. Exploits known vulnerabilities in several Adobe products such as Reader and Flash Player
3. Targeted attacks - each campaign tried to compromise few specific individuals
4. Obfuscated callback communications to hide exfiltrated data

April is the Cr…est Month.pdf

…China.pdf Jul 2012

Security Predictions…2013.pdf Aug 2012



C&C Server:
worldnews.alldownloads.ftpserver.biz

rundll32.exe
UNKNOWN Sept 2012

сообщить.doc Nov 2012

install_flash_player.ex
install_flash_player.tmp2
Global_A&D_outlook_2012.pdf Jan 2013

Timeline of attack – multiple v

Aerospace Industry

3

Encrypted callback

Multi-vectored attacked

1 – Email/Web with weaponized malware
2 – Backdoor DLL dropped
3 – Encrypted callback over HTTP to C&C

FireEye

How can we defend against these attacks?

- Remember: Most attackers make **mistakes**, yes even APT. They like to reuse certain tactics/methods.
- Psych: Humans are creatures of **habit**.
- We have limited resources for defense.
- Key: **Align** your defenses to best match attackers' common tactics.
- Goal: Can't "win", but can force **stalemate**.

FireEye

How do we accomplish this?

- Collect as much intel for each attack
  - **Indicators of Compromise (IOC)**
- Correlate related attacks by identifying **common** tools, techniques, and procedures (**TTPs**) across multiple attacks
  - Pivot on IOCs to identify overlap (e.g., IP->DNS->IP)
- Threat actors reuse multiple TTPs/attack infrastructures
- And they evolve their methods fairly **slowly**

FireEye

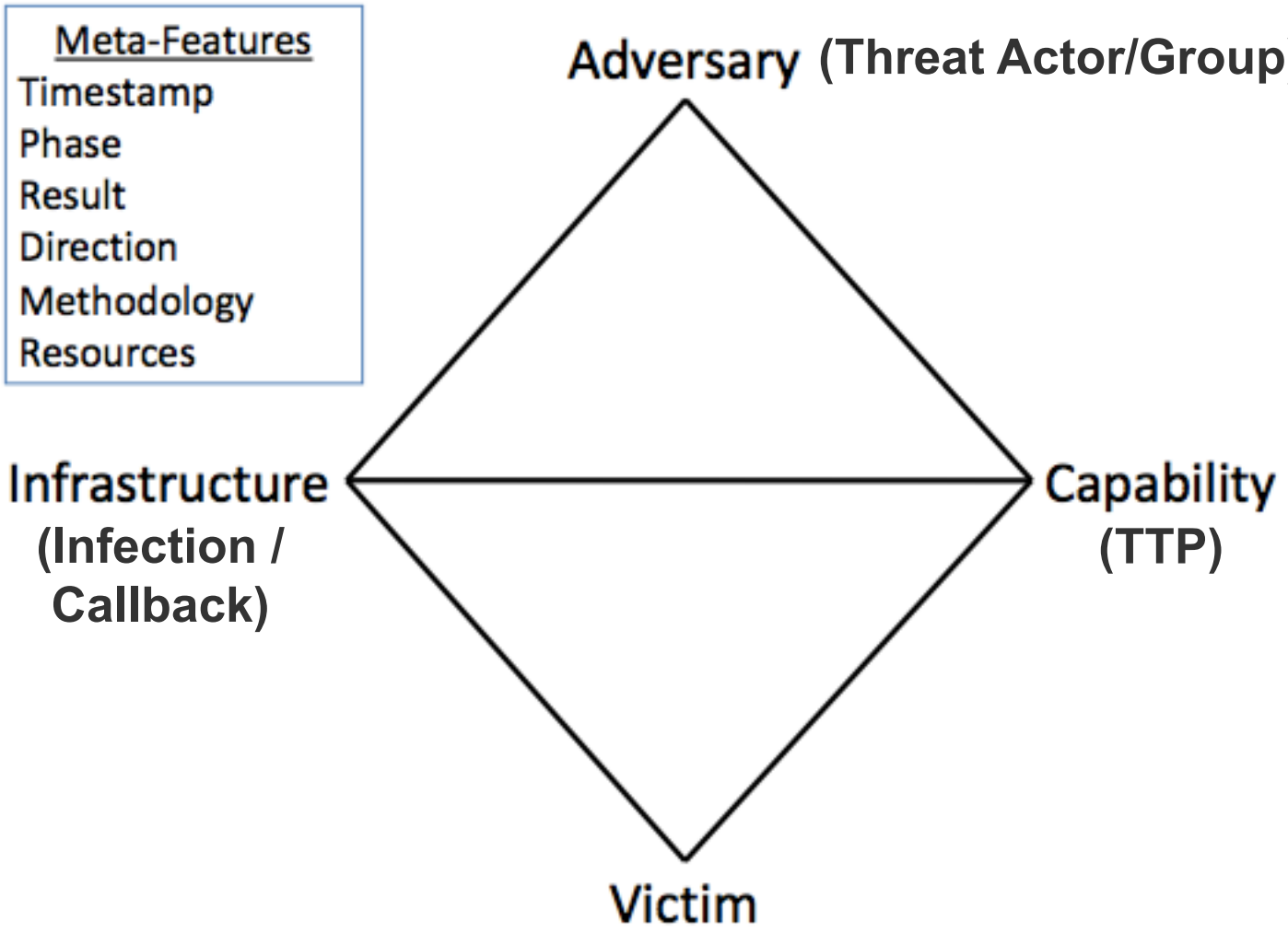
Map IOCs to Standard “Kill Chain”/Playbook

Phase	Indicators
Reconnaissance	[Recipient List] Benign File: tcnom.pdf
Weaponization	Trivial encryption algorithm: Key 1
Delivery	dn...etto@yahoo.com Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]
Exploitation	CVE-2009-0658 [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp
C2	202.abc.xyz.7 [HTTP request]
Actions on Objectives	N/A

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

FireEye

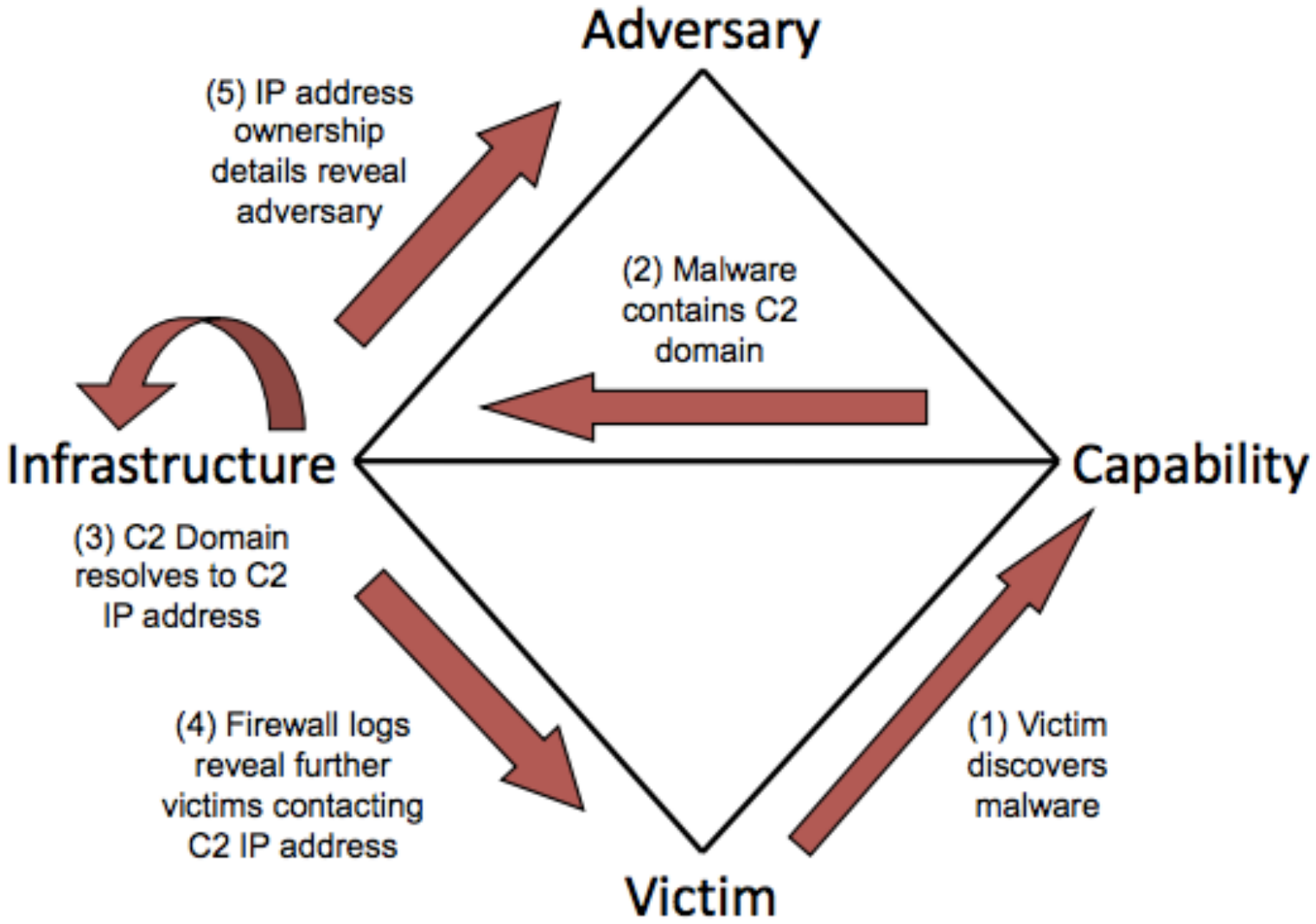
Diamond Model of Intrusion Analysis: How we connect the dots…



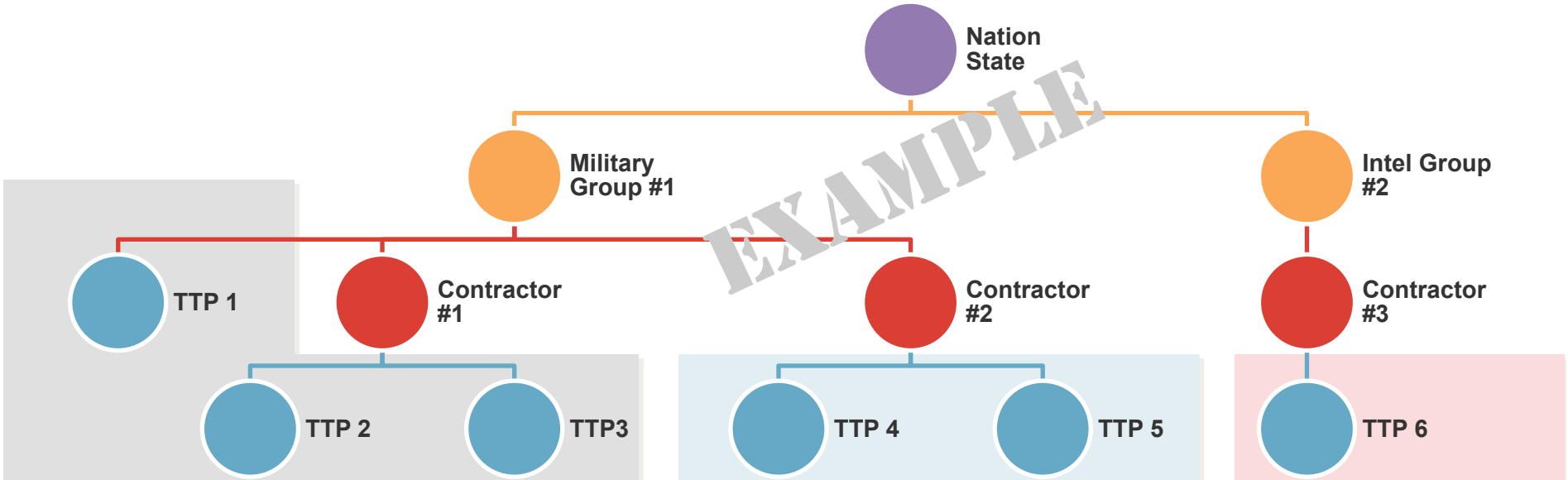
http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

FireEye

Simplified Methodology



The Big Picture (Simplified)



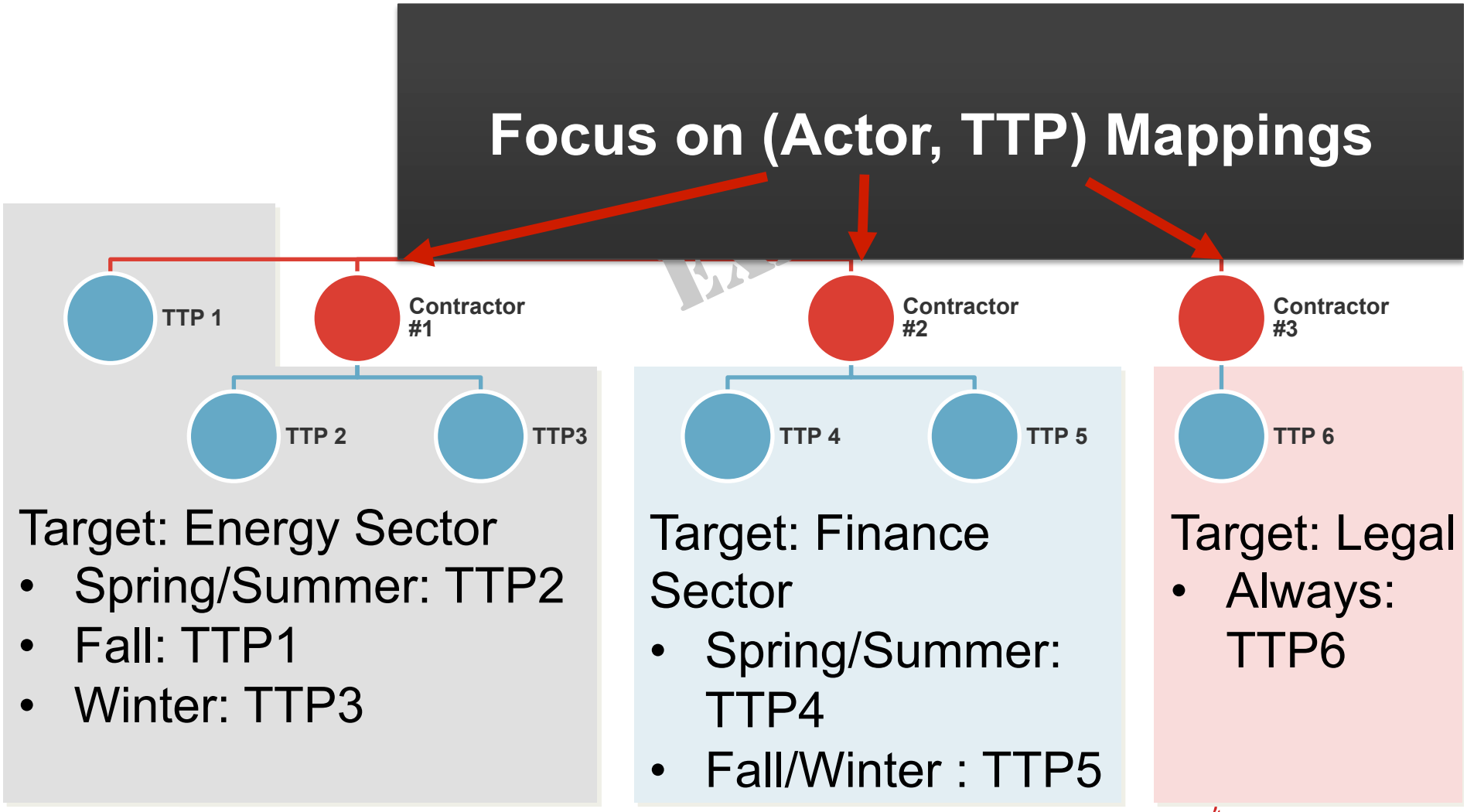
Target: Energy Sector
- Spring/Summer: TTP2
- Fall: TTP1
- Winter: TTP3

Target: Finance Sector
- Spring/Summer: TTP4
- Fall/Winter : TTP5

Target: Legal
- Always: TTP6

FireEye

What Actually Matters



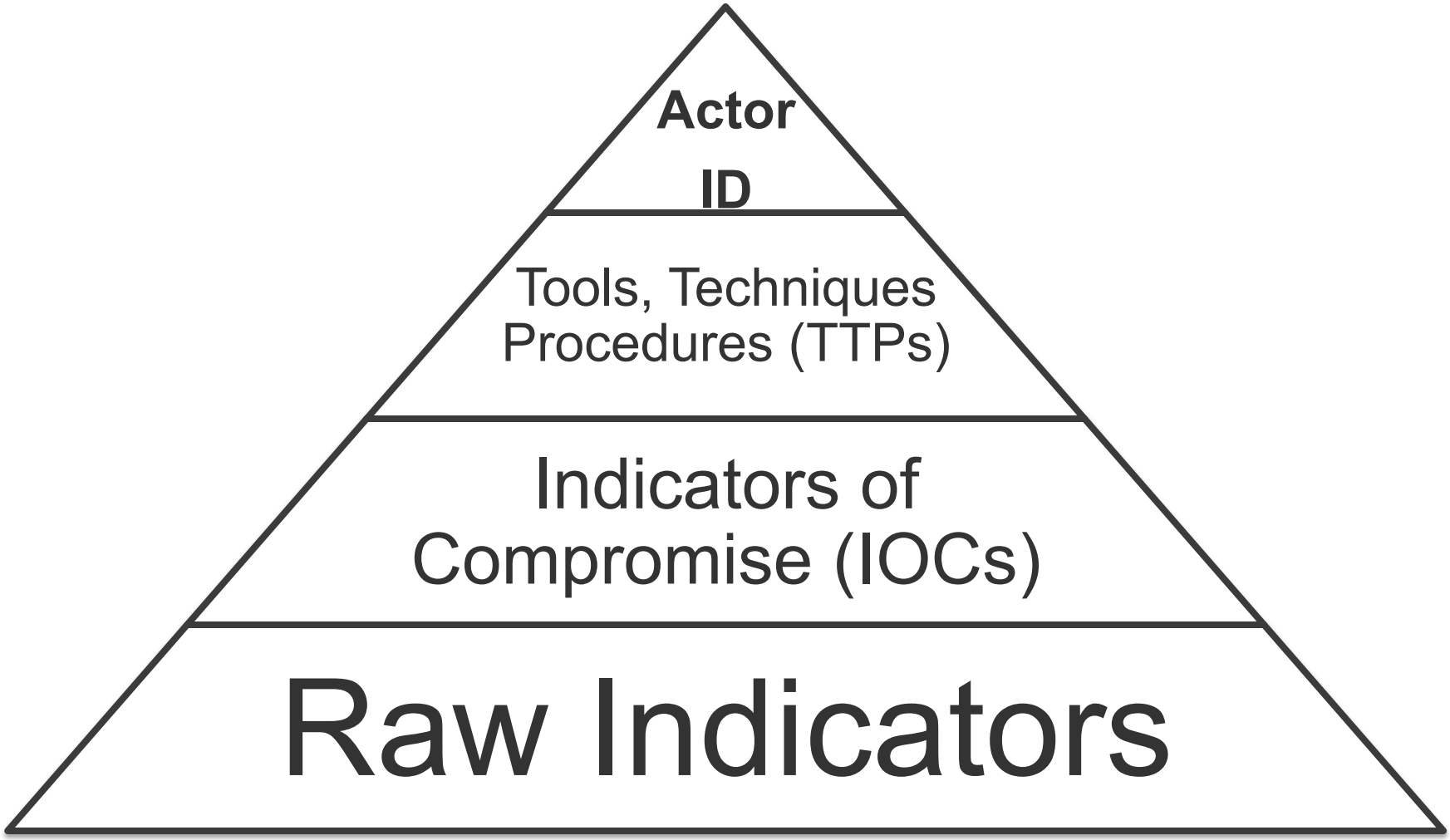
FireEye

Defender's Playbook (Custom Per Actor/Group's Collection of TTPs)

	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web Analytics	Policy to Prevent Forum Use			Create fake postings	
Weaponization						
Delivery	NIDS, User Education	Email AV Scanning		Email Queuing	Filter but respond with out-of-office message	
Exploitation	HIDS	Patch	DEP			
Installation						
C2	NIDS	HTTP Whitelist	NIPS	HTTP Throttling		
Action on Objectives	Proxy Detection	Firewall ACL	NIPS	HTTP Throttling	Honeypot	

eEye™

Analysts' Hierarchy of Needs



FireEye

FireEye™

Case Studies

Poison Ivy

Poison Ivy

- First released in 2005, last release 2008
- Developed by a Swedish coder named “ShapeLeSS”
- Has been part of the APT toolbox for a long time
- Has vulnerabilities of its own, but is still in use

FireEye

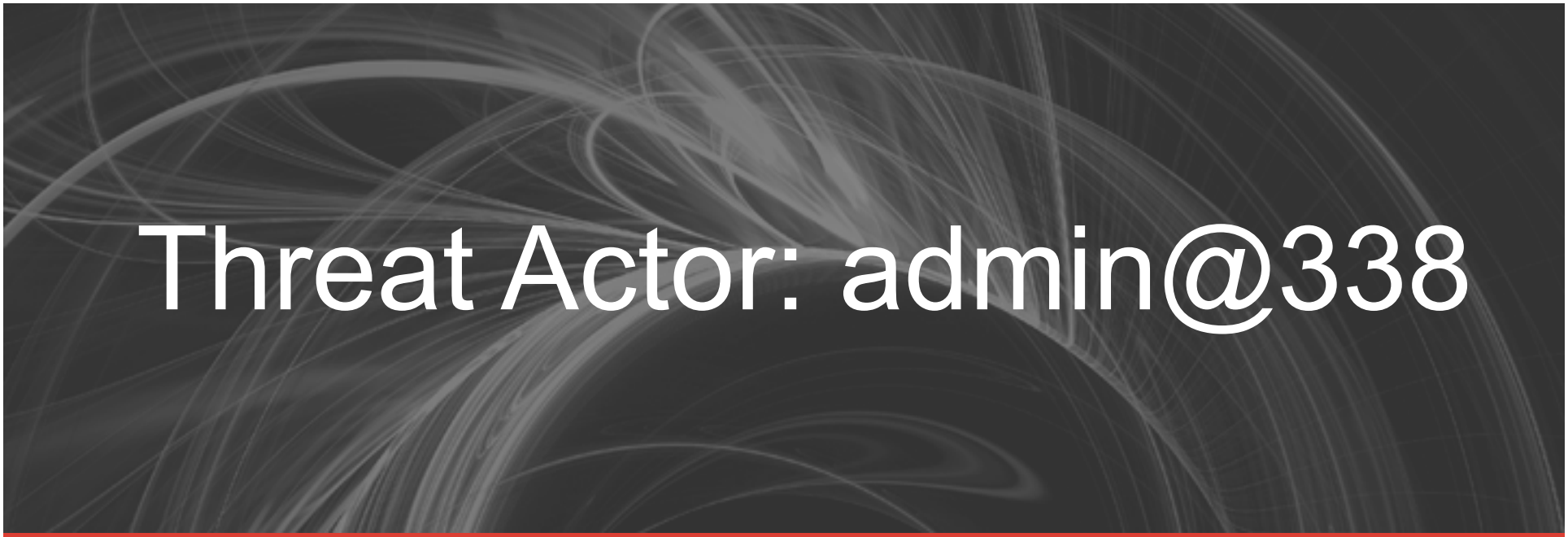
- BusinessWeek revealed that Booz Allen Hamilton was compromised with Poison Ivy (~2008)
- RSA revealed that it had been compromised; one of the tools used was Poison Ivy (2011)
- Symantec documented the “Nitro Campaign” against the chemical industry and others (2011/2012)

FireEye

Poison Ivy is Still Active

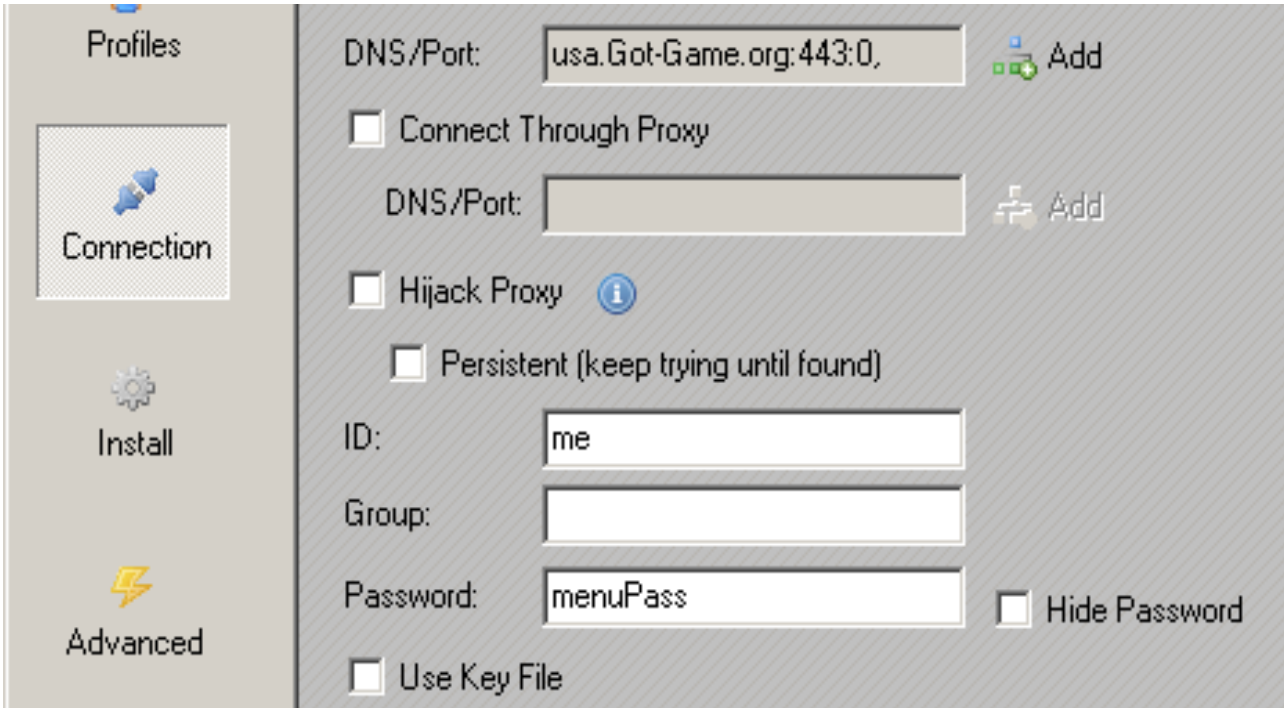
- Strategic compromises of CFR (2012), DoL (2013)
- Strategic web compromises by the “Sunshop” campaign (2013)
- Let’s focus on one campaign that has been active since ~2008: admin@338

FireEye


Threat Actor: admin@338

Gathering Intelligence from Poison Ivy

- When analyzing a Poison Ivy attack, the following attributes can be combined to form a unique fingerprint:



FireEye

Gathering Intelligence from Poison Ivy

- Poison Ivy ID/Group
- Mutex
- Password
- Command and Control Infrastructure
- Implant name/location
- Weaponization
- Delivery

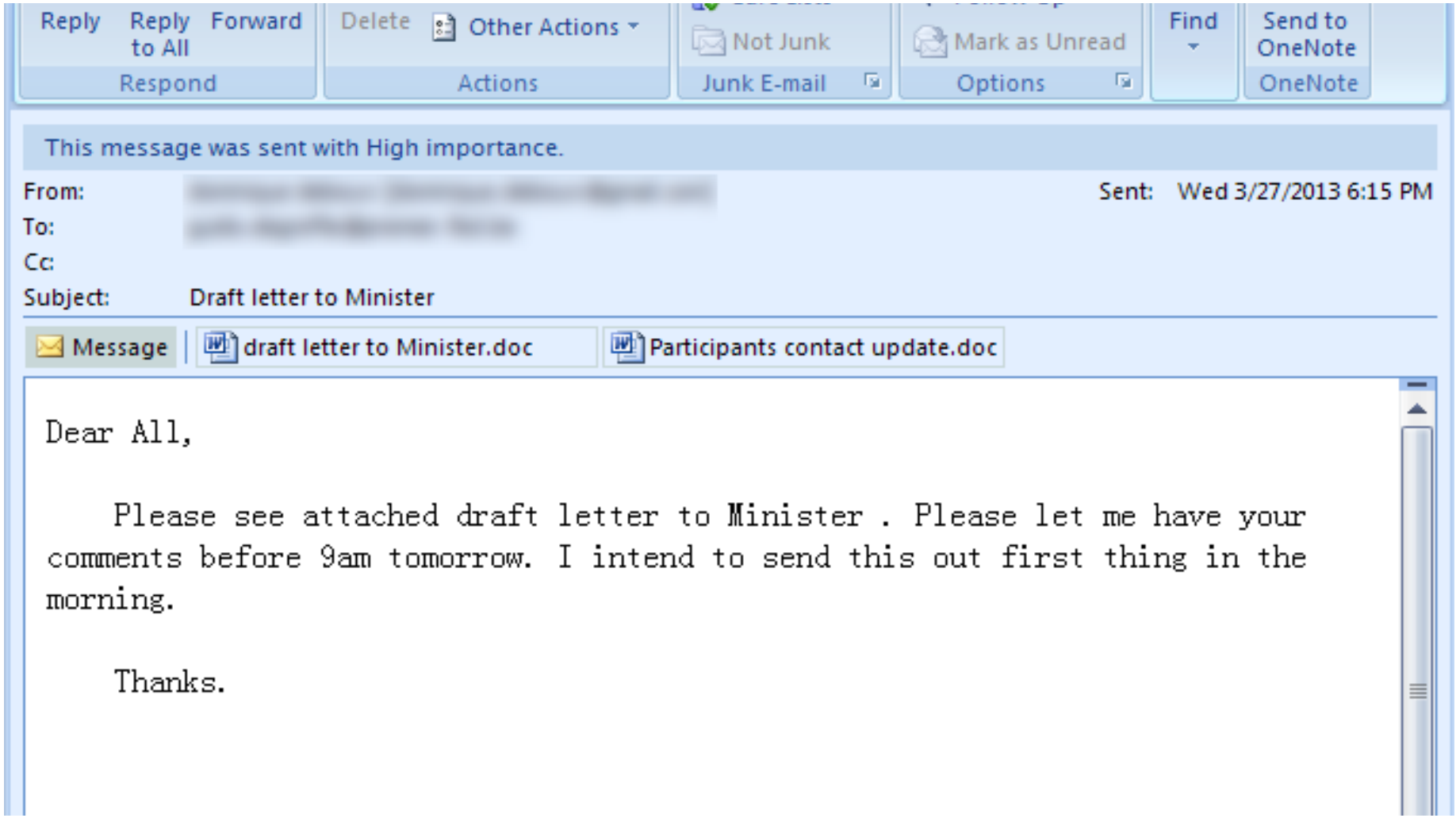
FireEye

admin@338 History

- Our data set for the admin@338 threat actor contains 21 Poison Ivy (PIVY) samples, 3 passwords and 43 command and control servers
- The earliest admin@338 PIVY sample we have is dated 2009-12-27
- We believe this actor uses a number of different tools in addition to Poison Ivy

FireEye

admin@338 Delivery



FireEye

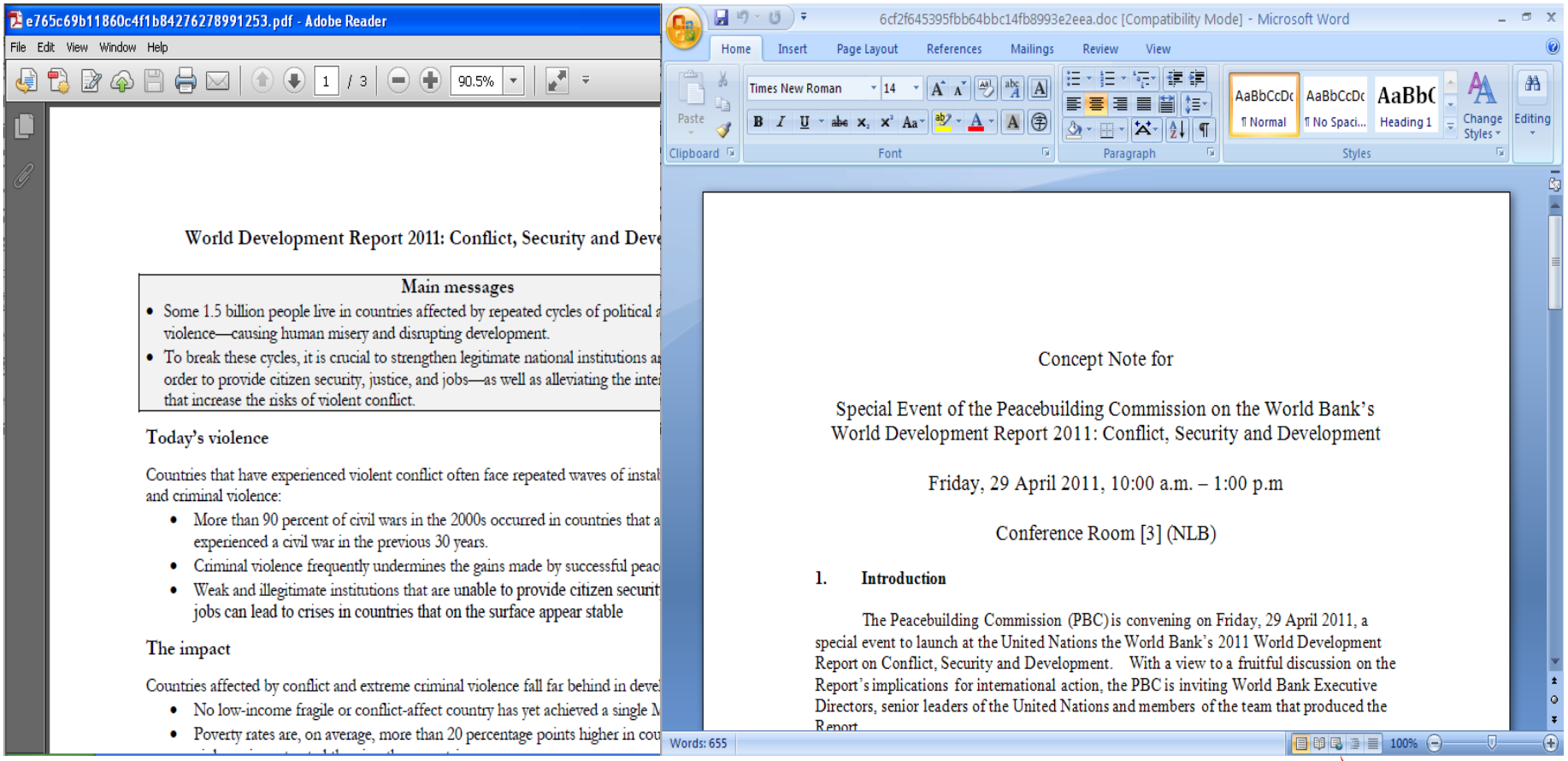
admin@338 Exploitation

- The admin@338 actor has weaponized Microsoft Office and Adobe PDF documents via the use of:
  - CVE-2010-3333
  - CVE-2009-4324
- This actor has also weaponized Microsoft Help Files

FireEye

admin@338 Delivery

- Decoy documents



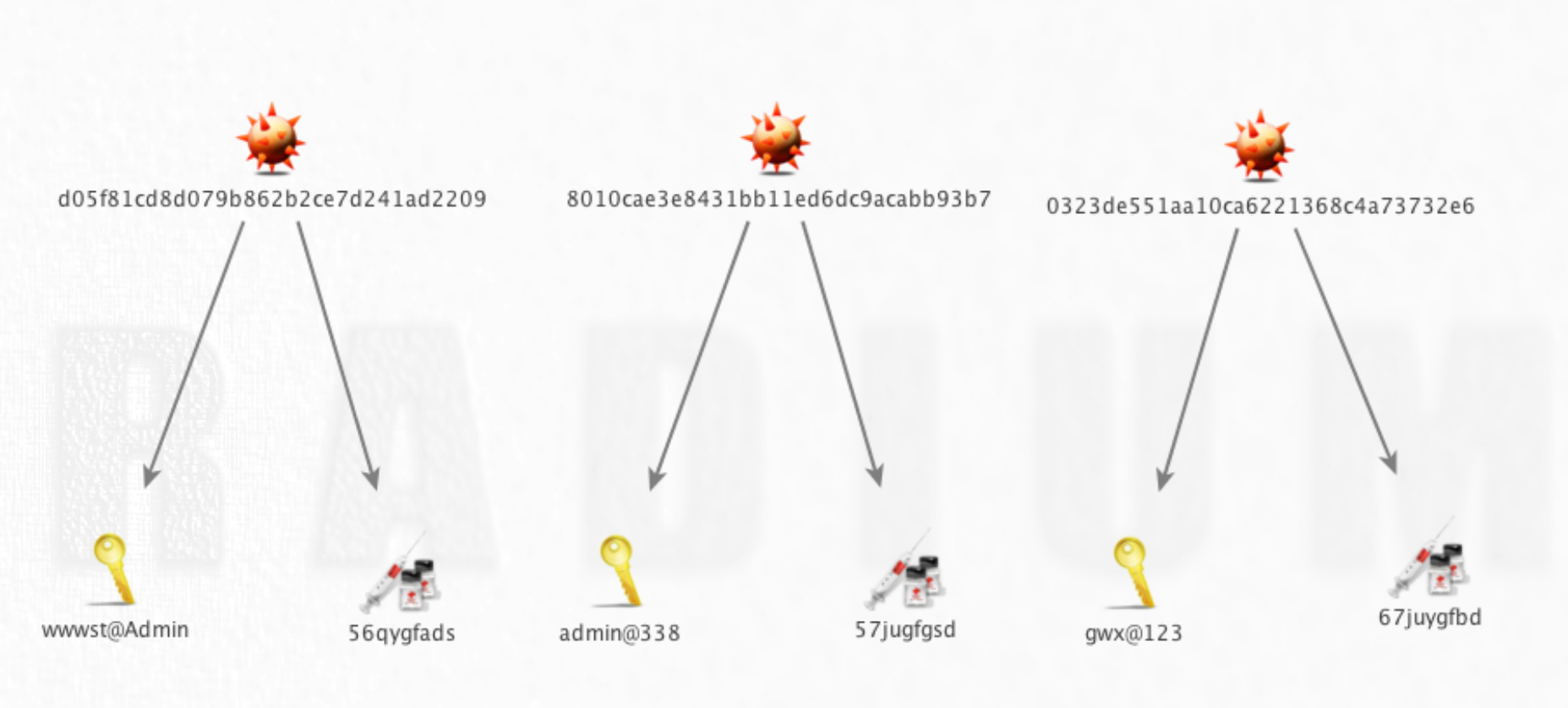
FireEye

admin@338 TTP Correlation

- Other passwords used by the admin@338 actor:
  - gwx@123
  - key@123
  - wwwst@Admin

FireEye

admin@338 TTP Identification
Attacker getting sloppy…



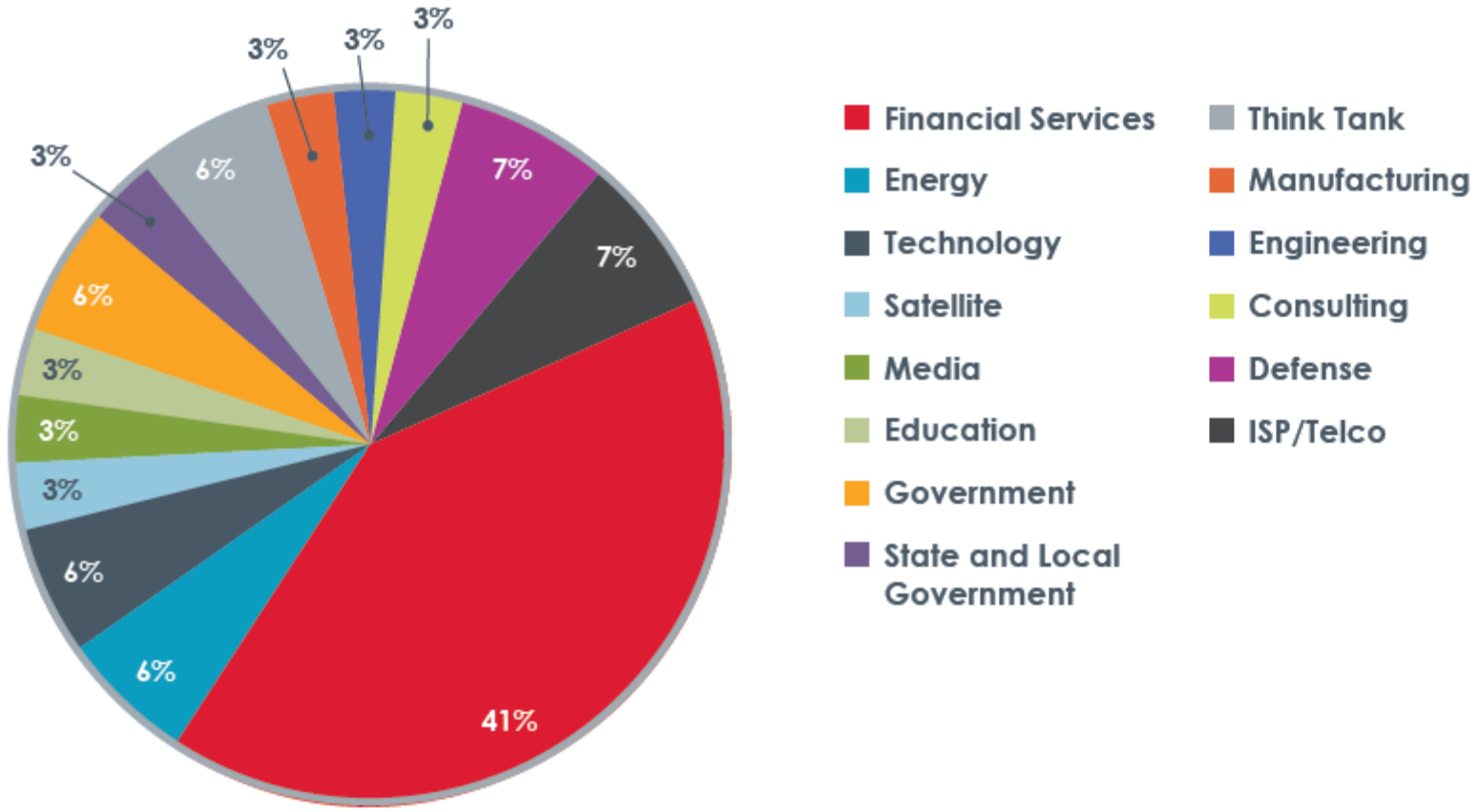
FireEye

admin@338 TTP Identifiers

- Common attributes:
  - Reuse of poison ivy passwords
  - Common mutex naming convention
  - Common targeting preferences
  - Reuse of c2 infrastructure
    - Network location
    - domains

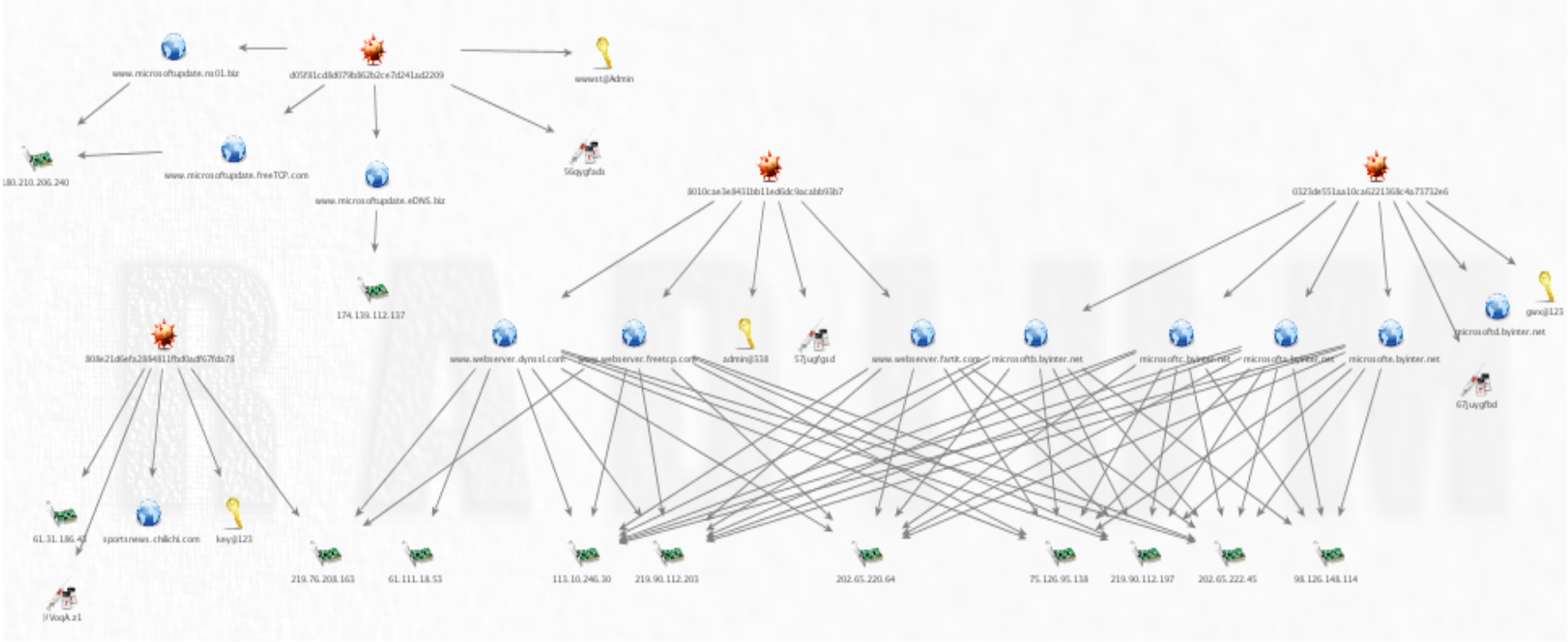
FireEye

admin@338 Target Verticals



FireEye

admin@338 Cluster Analysis



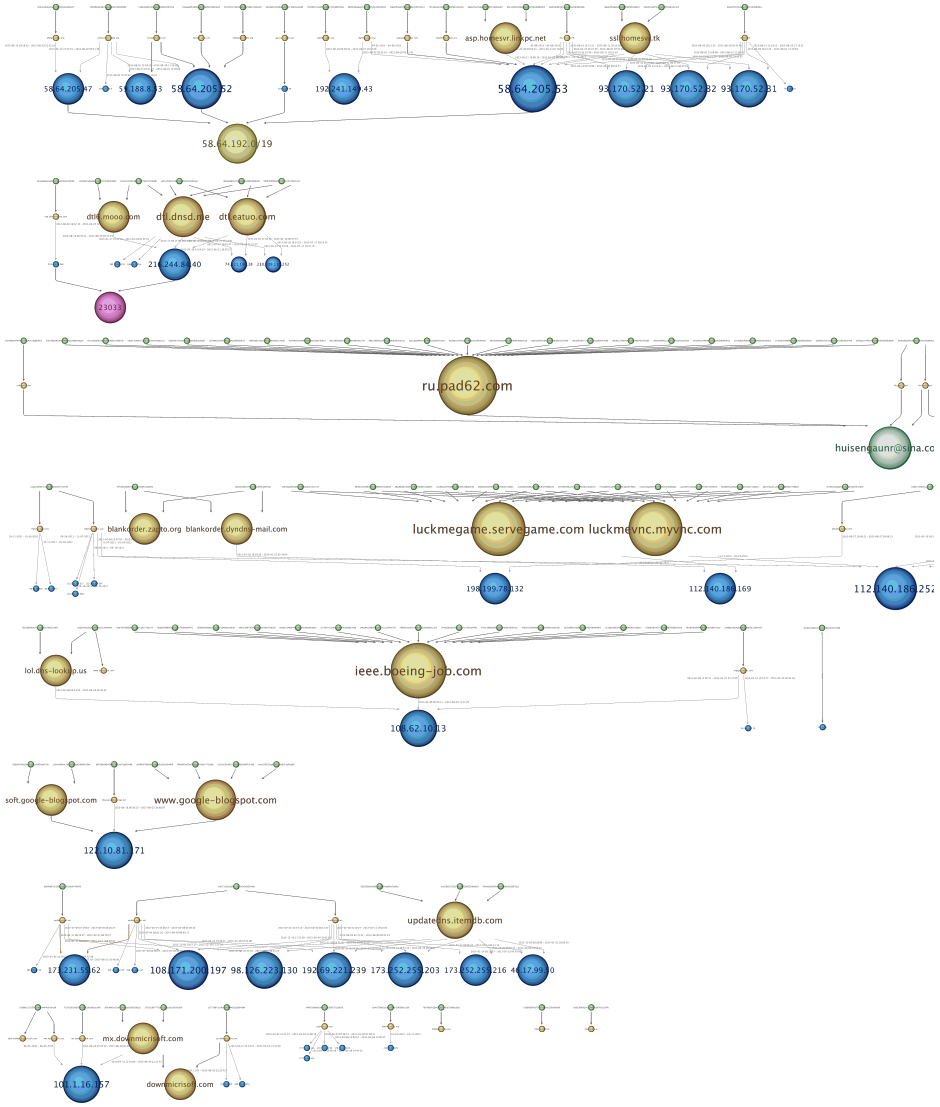
http://www.fireeye.com/resources/pdfs/fireeye-poison-ivy-report.pdf

FireEye

FireEye™

Sunshop Digital Quartermaster (DQ)

11 seemingly distinct APT campaigns…



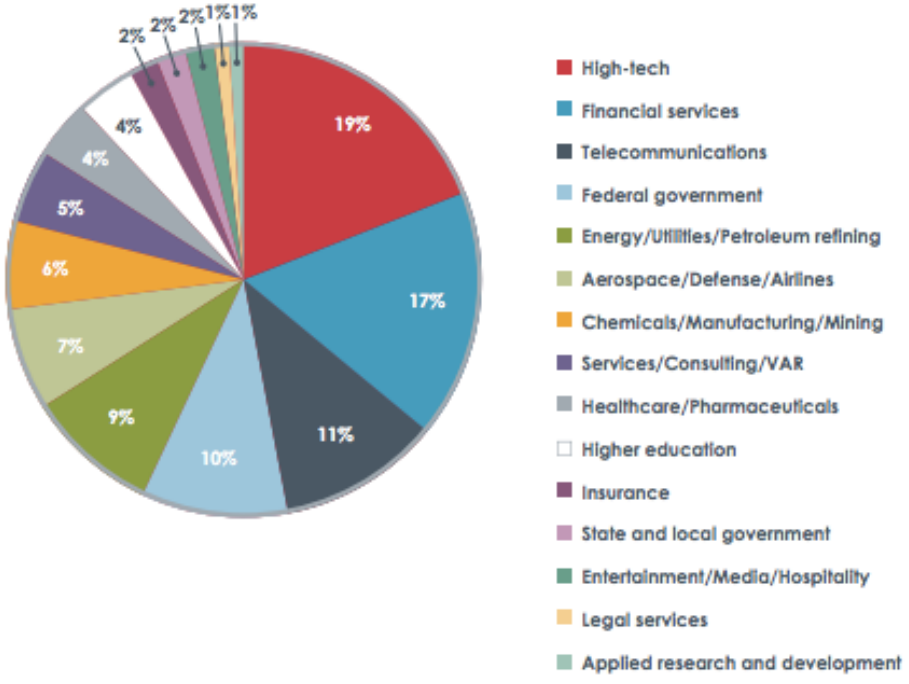


Figure 1: Percent of APT campaigns per industry

FireEye™

How the attacker got sloppy…

Sunshop vs DTL

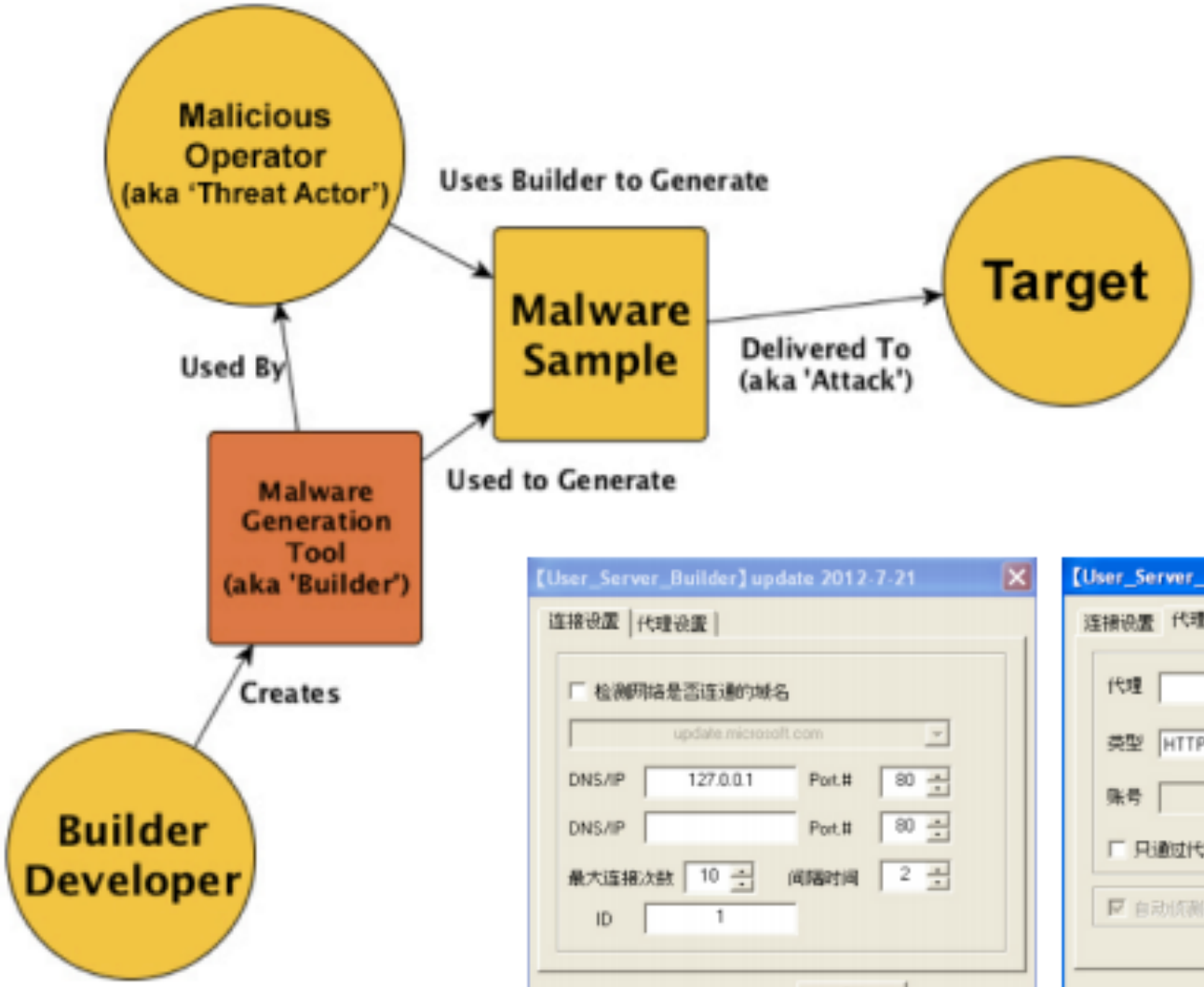
```
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2  <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion=
3  <assemblyIdentity version="1.0.0.0" processorArchitecture="X86" nam
4  <description>Nullsoft Install System v2.34</description>
5      <dependency><dependentAssembly>
6          <assemblyIdentity type="win32" name="Microsoft.Windows.Comm
7      </dependentAssembly>
8  </dependency>
9  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
10 <security>
11     <requestedPrivileges>
12     <requestedExecutionLevel level="asInvoker" uiAccess="false"/></
13 </security>
14 </trustInfo>
15 </assembly>
```

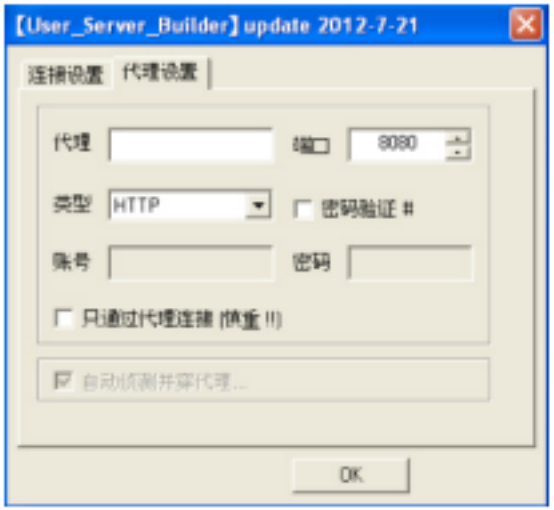
```
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2  <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion=
3  <assemblyIdentity version="1.0.0.0" processorArchitecture="X86" nam
4  <description>Nullsoft Install System v2.34</description>
5      <dependency><dependentAssembly>
6          <assemblyIdentity type="win32" name="Microsoft.Windows.Comm
7      </dependentAssembly>
8  </dependency>
9  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
10     <security>
11         <requestedPrivileges>
12         <requestedExecutionLevel level="asInvoker" uiAccess="false"
13     </security>
14 </trustInfo>
15 </assembly>
```

We discovered 64 total samples using these two PE resources. These samples were linked used in 11 different campaigns.

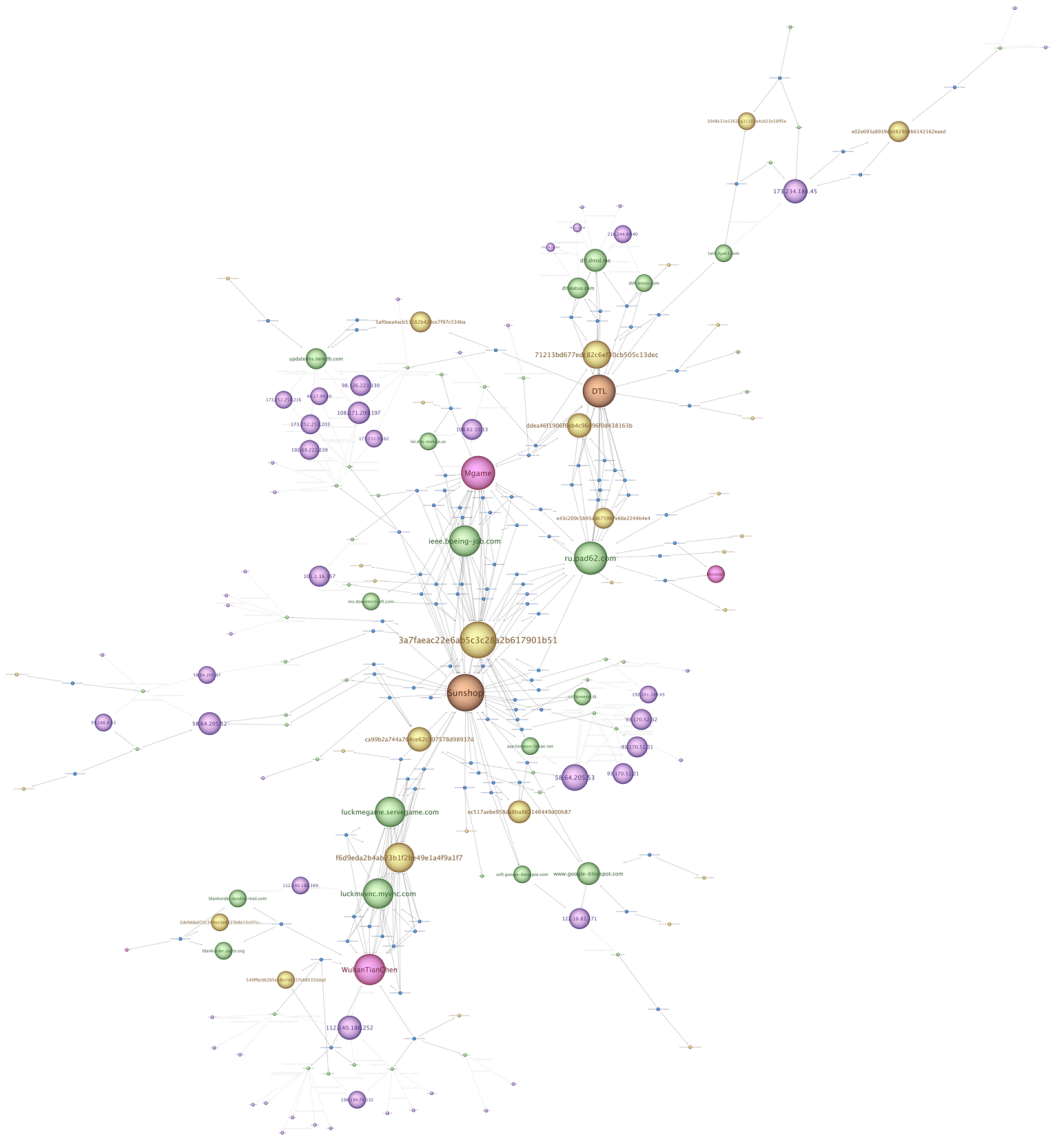
FireEye

Shared builder used across campaigns



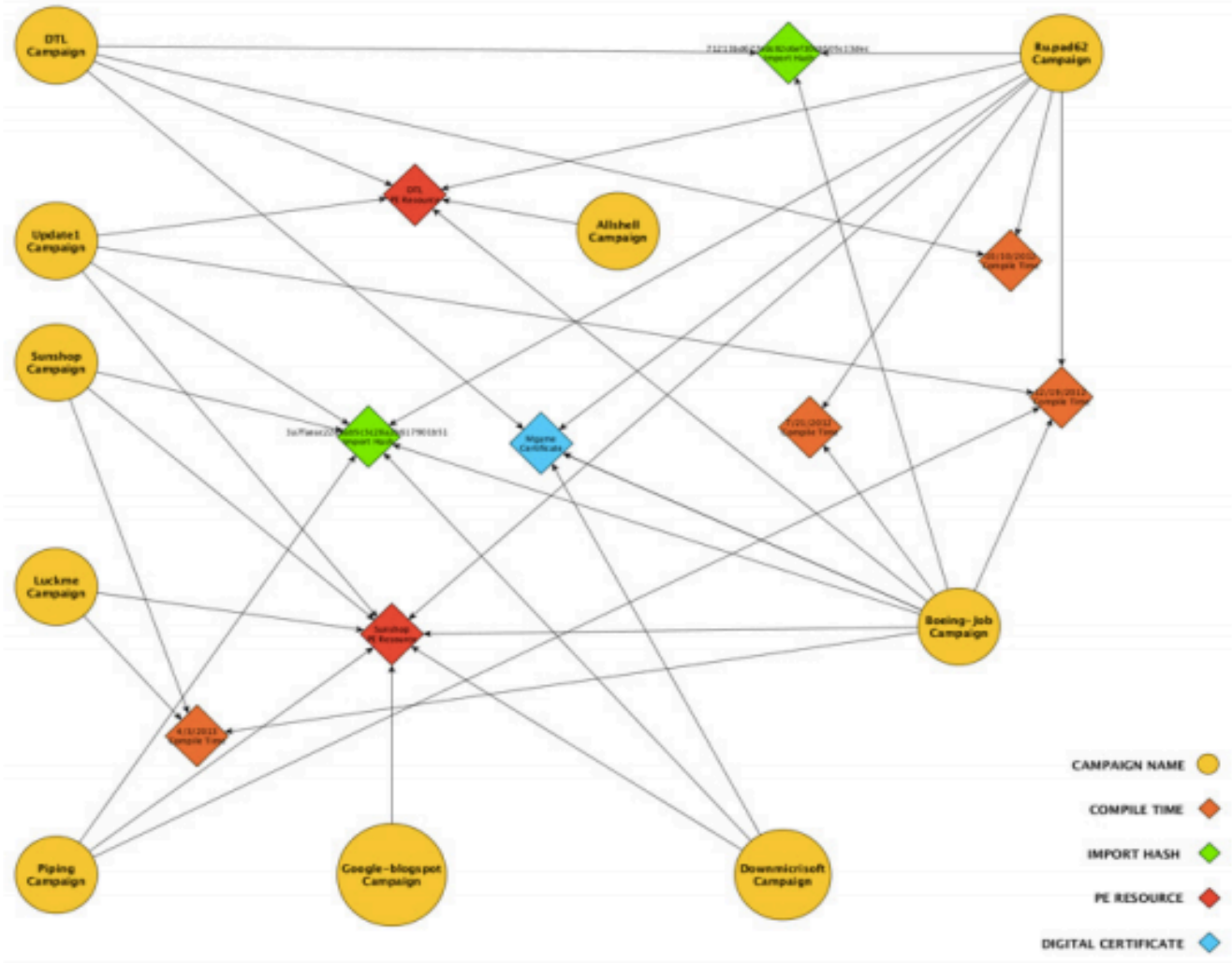


It’s actually all related…Sunshop DQ



FireEye

50,000 ft (Partial) View of Sunshop DQ



http://www.fireeye.com/resources/pdfs/fireeye-malware-supply-chain.pdf

In sum…

- Is this methodology perfect? No, but it is effective at detecting and defending against **unique attacks**.
- Defense in depth is still required
  - Multiple defensive strategies are needed
- However, Threat Intelligence is a tactical, **short-term mitigation**, while better, long-term methods are developed

FireEye

Closing thoughts…

- Why is it hard to measure security?
- Why isn't security embedded into most business operations?
- Why do most breaches not affect the market value of victim firms?

FireEye

Questions?

FireEye™

IGNITE

UNIVERSITY RELATIONS

Visit http://fireeye.jobs

UR@FireEye.com

"The spark starts here"