Threat Intelligence

Darien Kindlund
darien.kindlund@fireeye.com
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
History Lesson…

The New Status Quo: Advanced Attacks

- Disruption
- Worms/Viruses
- Spyware/Bots
- Cybercrime
- Advanced Persistent Threats
  - Zero-day
  - Targeted attacks
  - Dynamic Trojans
  - Stealth Bots
- Cyber-espionage & Cybercrime

Damage of Attacks

2004  2006  2008  2010
Why did this happen?

1970s

Security

... ... ...

Usability

2010s

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

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

We could detect and block these attacks before they succeed.
New Assumption

Assume the attackers *succeed* and the infrastructure is already *compromised.*

• Learn more about who is attacking us
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
What is Threat Intelligence?

A mix of:
– Computer science
– Software engineering
– Information security
– Intelligence analysis
– Malware analysis
– Reverse engineering
– Risk analysis
– Statistics
– Criminal Psychology
Advanced Persistent Threat (APT) Actors
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"
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.


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"
Crux: Classic Asymmetric Warfare

• Can’t defend everything, all the time
• Defenders need to succeed every time
• Attackers only need to succeed once
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?
• 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?
Example Attacker/APT Playbook

1. Phishing and Zero Day Attack
   A handful of users are targeted by two phishing attacks; one user opens Zero day payload (CVE-02011-0609)

2. Back Door
   The user machine is accessed remotely by Poison Ivy tool

3. Lateral Movement
   Attacker elevates access to important user, service and admin accounts, and specific systems

4. Data Gathering
   Data is acquired from target servers and staged for exfiltration

5. Exfiltrate
   Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider

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)
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
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
OPERATION EPHEMERAL HYDRA

Watering Hole Attack

Compromised Website

Exploitation

ROP Code

1

Victim

Information Gathering

2

Infiltration

3

Evasion

Diskless 9002 RAT

POST /2 HTTP/1.1
User-Agent: lynx
Host: 111.68.9.93:443
Content-Length: 104
Connection: Keep-Alive
Cache-Control: no-cache

111.68.9.93

CNC
Email Attack
Operation Beebus

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

Timeline of attack – multiple vectors, multiple campaigns

1 – Email/Web with weaponized malware
2 – Backdoor DLL dropped
3 – Encrypted callback over HTTP to C&C
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**.
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*
### Map IOCs to Standard “Kill Chain”/Playbook

<table>
<thead>
<tr>
<th>Phase</th>
<th>Indicators</th>
</tr>
</thead>
</table>
| 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\:\...\IEUped.exe  
C\:\...\EXPLORE.hlp                                                        |
| C2                   | 202.abc.xyz.7  
[HTTP request]                                                            |
| Actions on Objectives| N/A                                                                         |

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

Simplified Methodology

1. Victim discovers malware
2. Malware contains C2 domain
3. C2 Domain resolves to C2 IP address
4. Firewall logs reveal further victims contacting C2 IP address
5. IP address ownership details reveal adversary

Adversary

Infrastructure

Capability

Victim
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
What Actually Matters

Focus on (Actor, TTP) Mappings

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

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

Target: Legal
- Always: TTP6
## Defender’s Playbook
(Custom Per Actor/Group’s Collection of TTPs)

<table>
<thead>
<tr>
<th></th>
<th>Detect</th>
<th>Deny</th>
<th>Disrupt</th>
<th>Degrade</th>
<th>Deceive</th>
<th>Destroy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reconnaissance</strong></td>
<td>Web Analytics</td>
<td>Policy to Prevent Forum Use</td>
<td></td>
<td>Create fake postings</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Weaponization</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Delivery</strong></td>
<td>NIDS, User Education</td>
<td>Email AV Scanning</td>
<td>Email Queuing</td>
<td>Filter but respond with out-of-office message</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Exploitation</strong></td>
<td>HIDS</td>
<td>Patch</td>
<td>DEP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Installation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C2</strong></td>
<td>NIDS</td>
<td>HTTP Whitelist</td>
<td>NIPS</td>
<td>HTTP Throttling</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action on Objectives</strong></td>
<td>Proxy Detection</td>
<td>Firewall ACL</td>
<td>NIPS</td>
<td>HTTP Throttling</td>
<td>Honeypot</td>
<td></td>
</tr>
</tbody>
</table>
Analysts’ Hierarchy of Needs

- Actor ID
- Tools, Techniques Procedures (TTPs)
- Indicators of Compromise (IOCs)
- Raw Indicators
Case Studies
Poison Ivy

Home - Downloads - Screenshots - Development - Customer Portal - Links - Contact

Site/downloads up again
2008-11-20

I have received a tremendous amount of emails from people wanting me to continue the project even though it might take some time until the next release. It’s meant allot to me to see this kind of support for the project. That’s why I’ve decided to bring the site, but I will not promise anything...
I hope to get some time and motivation to finish the new version.

Development
2008-03-30

The next version is well on its way (even though I haven’t updated the dev.log in ages). I decided to redo most of the core code in the client and also implement language support. The new client will use less memory and be somewhat faster. The language file (english) will be uploaded, once the new version is done, for anyone to translate.

Stay tuned for more info.

New plugin: Optix Screen Capture
2008-02-04

The former EES founder, th3 sl3a23, has contributed with an excellent screen capture plugin. Hence the name it has the same style as Optix Pro (which th3 sl3a23 was the author of). Source codes are included (which requires a couple of Delphi Components, they are included as well).

Download it here!
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
• 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)
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
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:
Gathering Intelligence from Poison Ivy

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

Please see attached draft letter to Minister. Please let me have your comments before 9am tomorrow. I intend to send this out first thing in the morning.

Thanks.
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
• Decoy documents
Other passwords used by the admin@338 actor:
- gwx@123
- key@123
- wwwst@Admin
admin@338 TTP Identification
Attacker getting sloppy…
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
admin@338 Target Verticals

- Financial Services: 41%
- Energy: 7%
- Technology: 6%
- Satellite: 6%
- Media: 6%
- Education: 3%
- Government: 3%
- State and Local Government: 3%
- Think Tank: 3%
- Manufacturing: 3%
- Engineering: 3%
- Consulting: 3%
- Defense: 3%
- ISP/Telco: 3%
admin@338 Cluster Analysis

11 seemingly distinct APT campaigns…
How the attacker got sloppy...

Sunshop vs DTL

We discovered 64 total samples using these two PE resources. These samples were linked used in 11 different campaigns.
Shared builder used across campaigns
It’s actually all related…Sunshop DQ
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
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?
Questions?

Visit [http://fireeye.jobs](http://fireeye.jobs)
UR@FireEye.com

“The spark starts here”