FireEye

The Execution List

Day-Con VII

If you don't understand WHY they (are attacking), it makes it very difficult to stop - General Stanley McChrystal

Road map

- Bio
- Whitelist
- Intel from existing data
- Case Study
- Contact Info and Questions

FireEye

Whoami

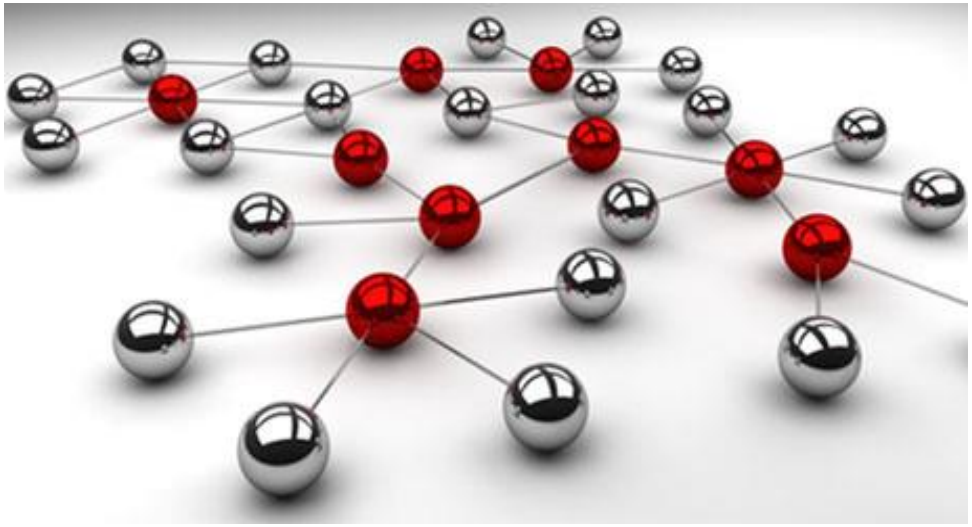
- FireEye Incident Response/Researcher/

- Cyber Analyst for CIA
  - Educated US Govt on cyber threats
  - Wrote for President's Daily Briefing
  - Presented at workshops and cyber conferences

FireEye

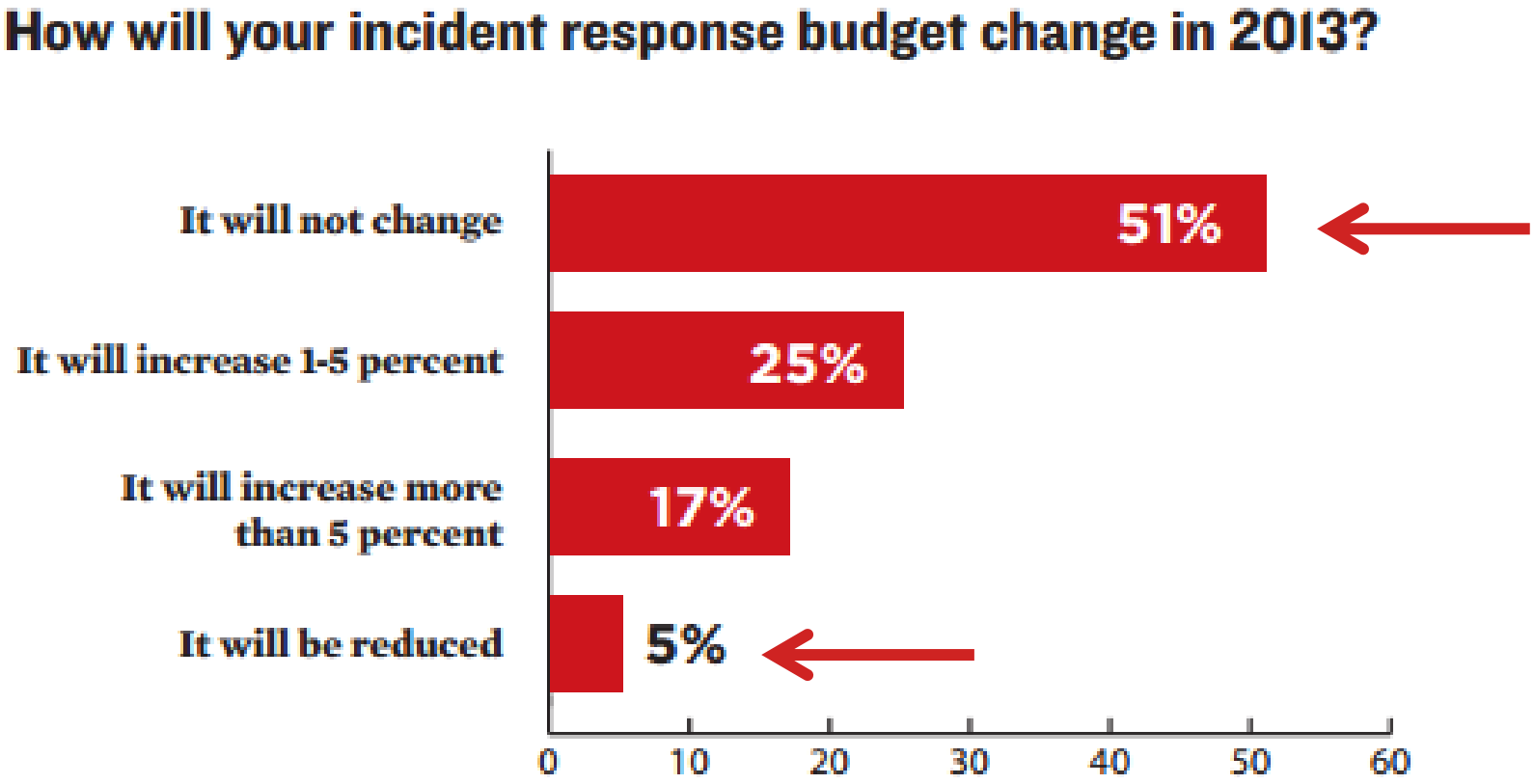
Two topics, one goal: limit attacks

1. Whitelist and monitor
2. Land and expand



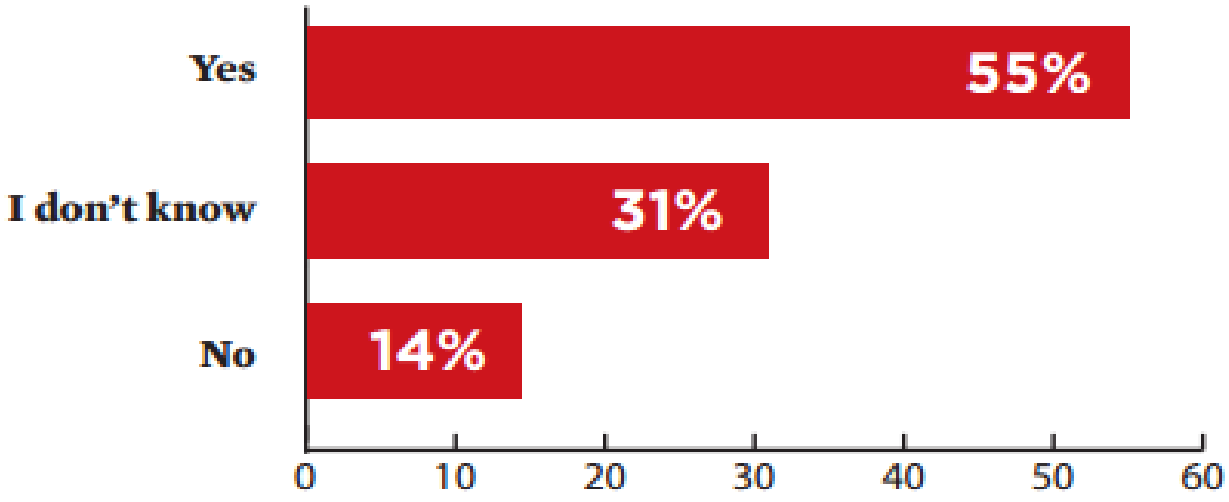
FireEye

Well, there's this…



…and this.

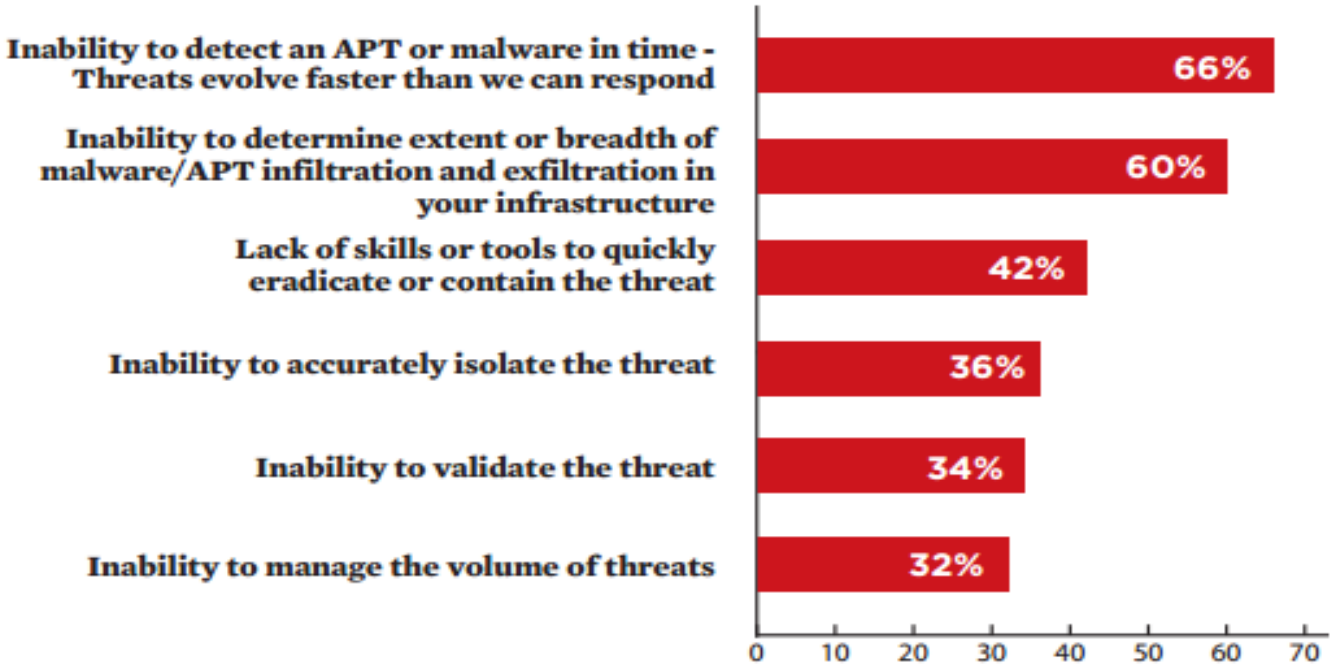
Can you detect the exact location of malware in your environment?



FireEye

Top Technical Challenges for IR

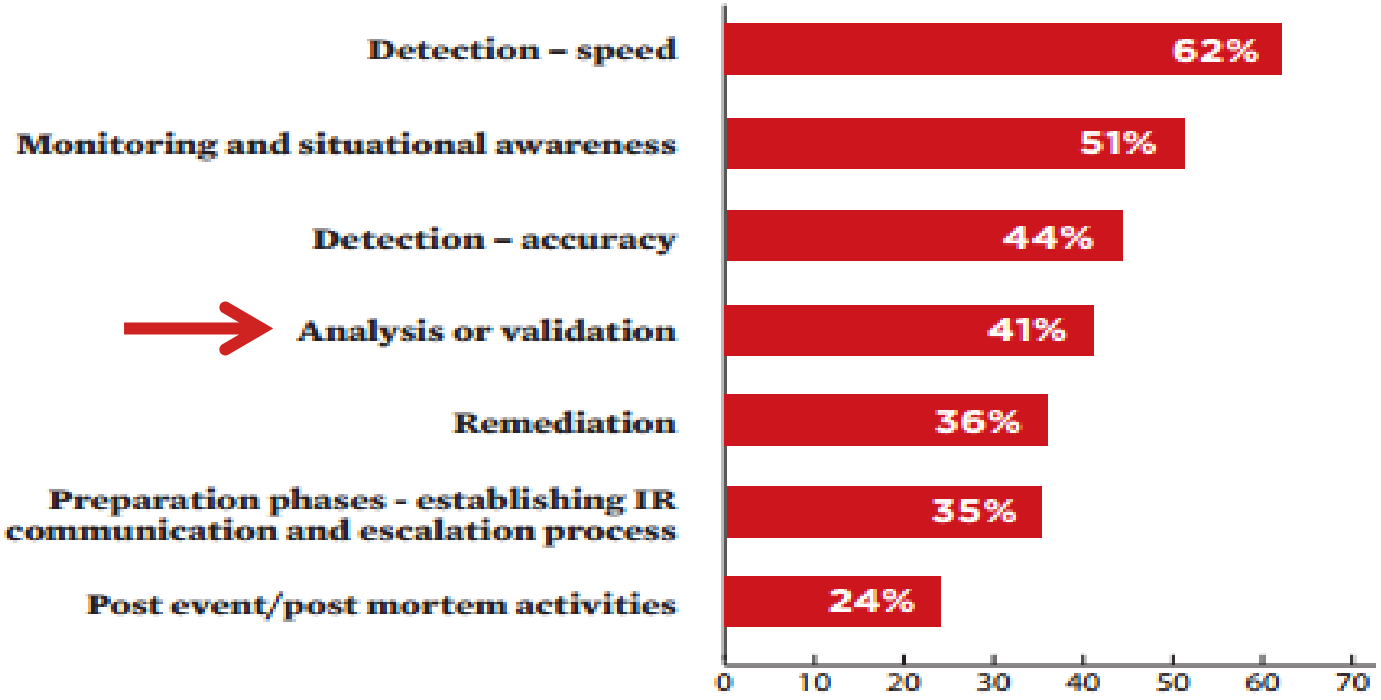
What do you believe are the top 3 technical challenges that impact the ability for effective incident response?



FireEye

Top 3 Security Challenges

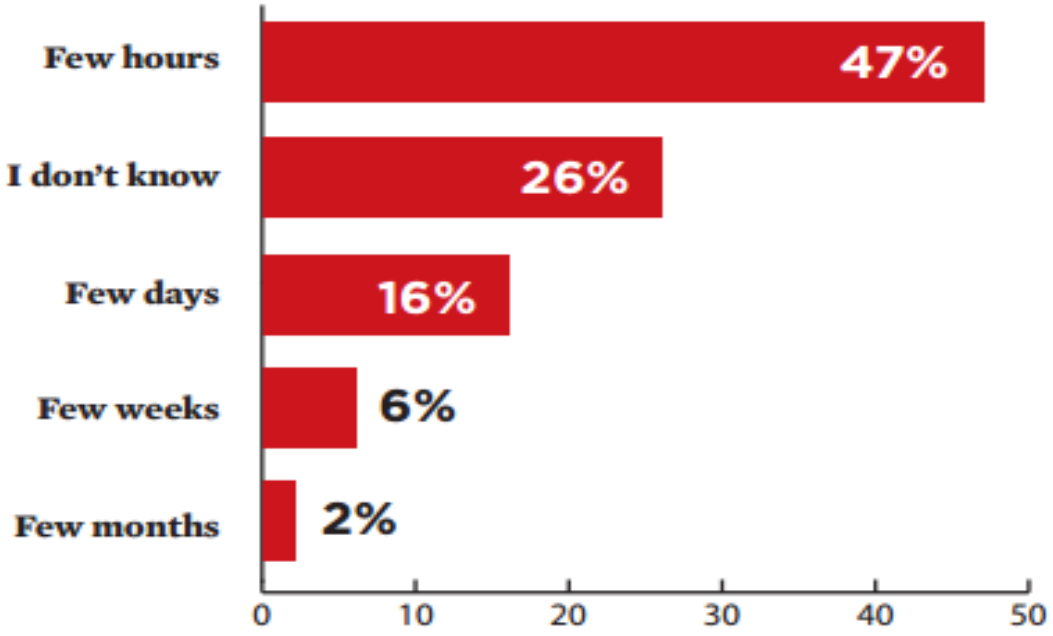
What do you believe are the top 3 security challenges in your IR cycle?



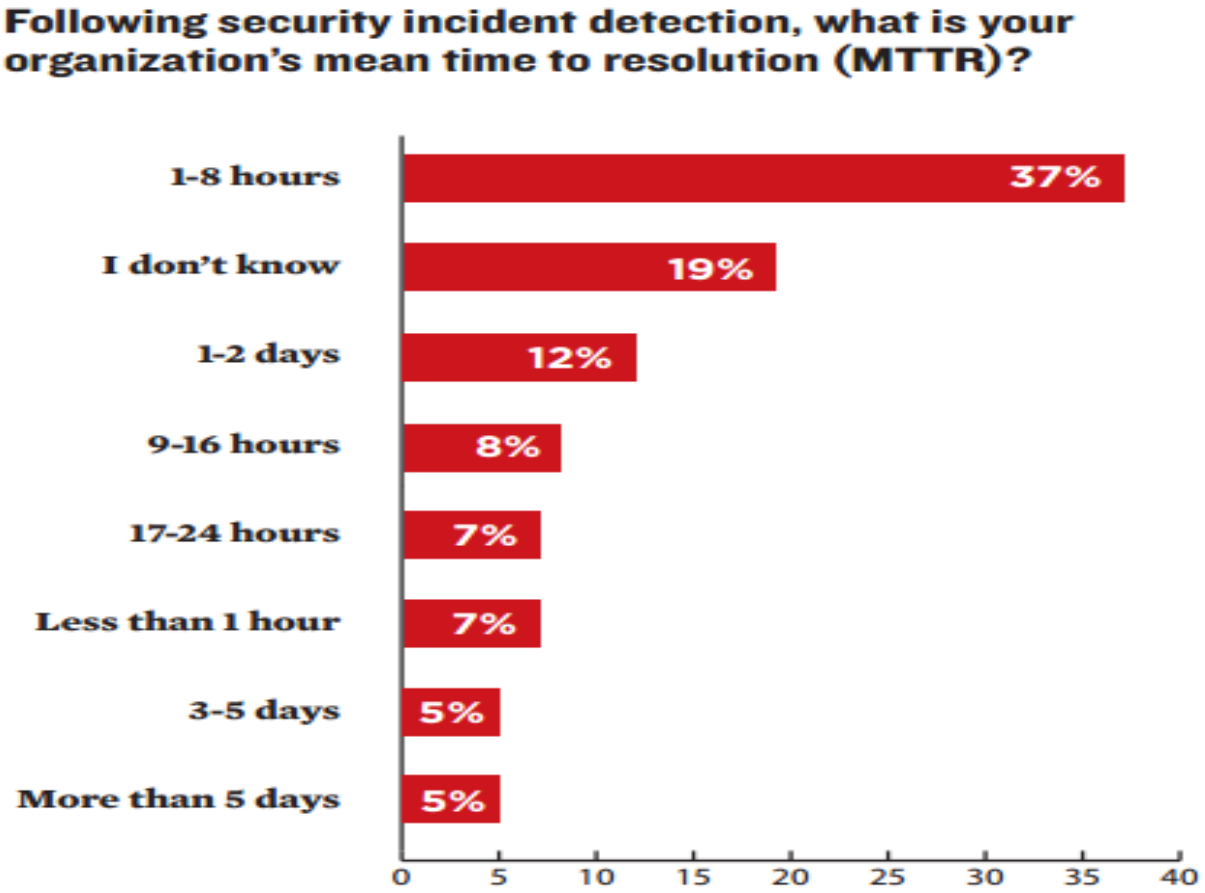
FireEye

Mean Time to Discovery

From early indicator of compromise to actual detection, what is your organization's mean time to discovery?

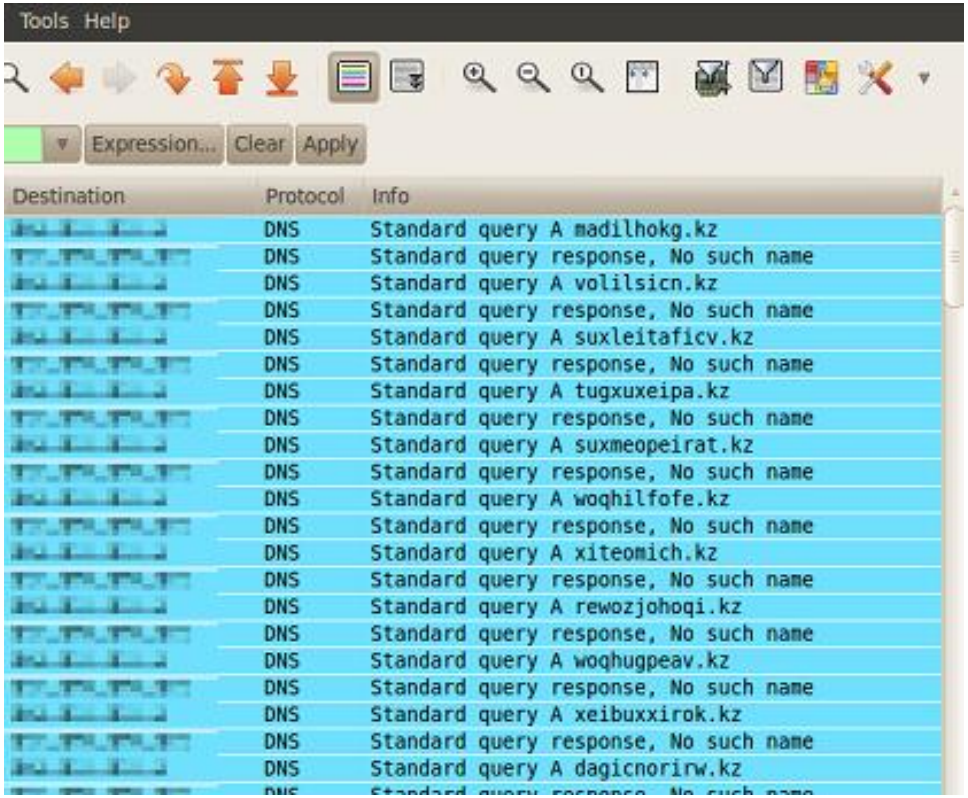


Mean Time to Resolution



Blacklisting is worthless

BAD



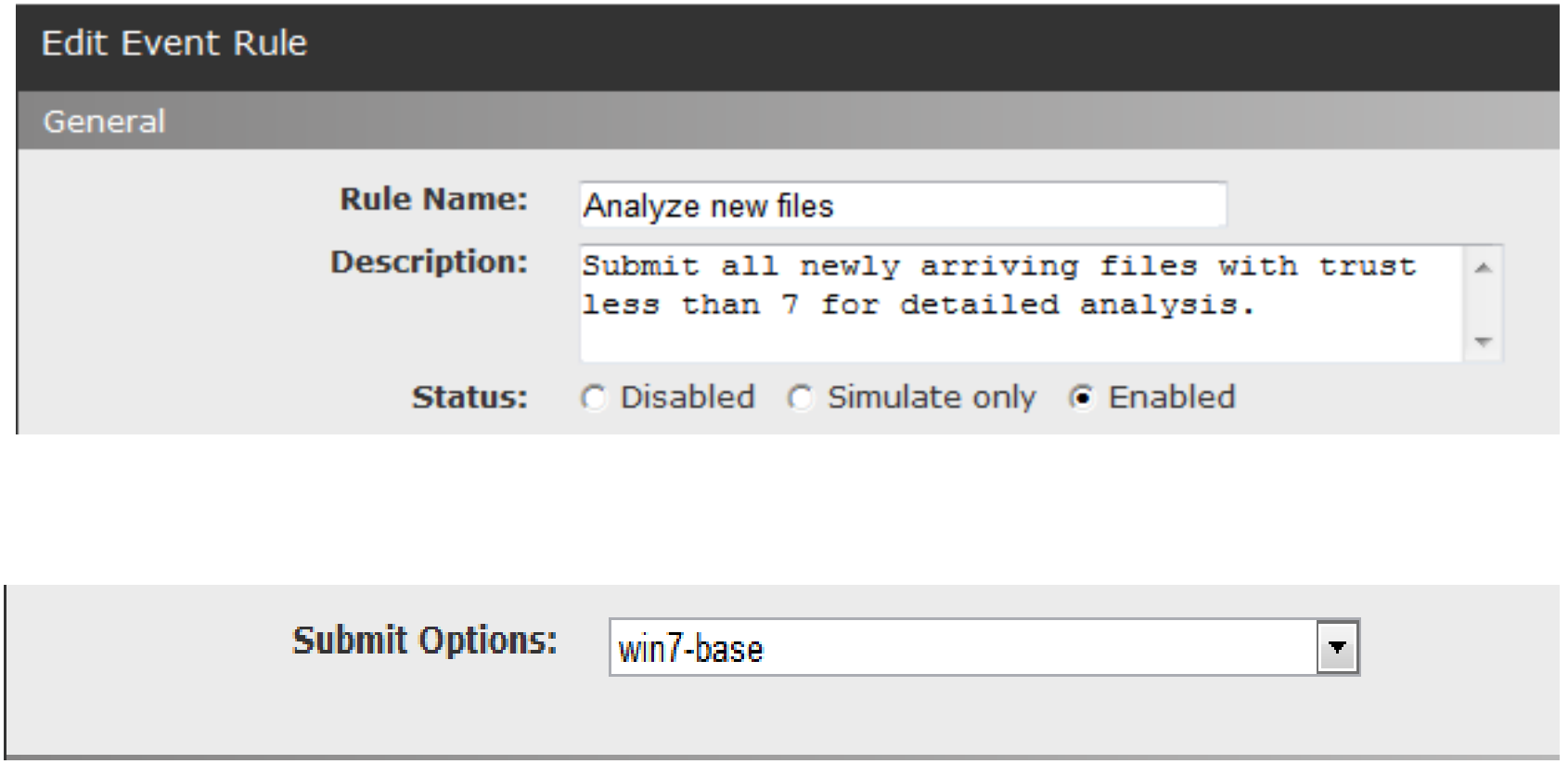
FireEye

Down side of whitelisting

- Timely to manage
- Stolen certs
- Maintaining the list
- Too many files

FireEye

Going forward = Analyze + Whitelist



FireEye

Workflow

- Set a baseline of your network
  1. Check if any malicious files on end point
  2. Prioritize IR teams
  3. Block malware after patient zero
  4. BCC email results to whitelist container

FireEye

What About Valid Certs?

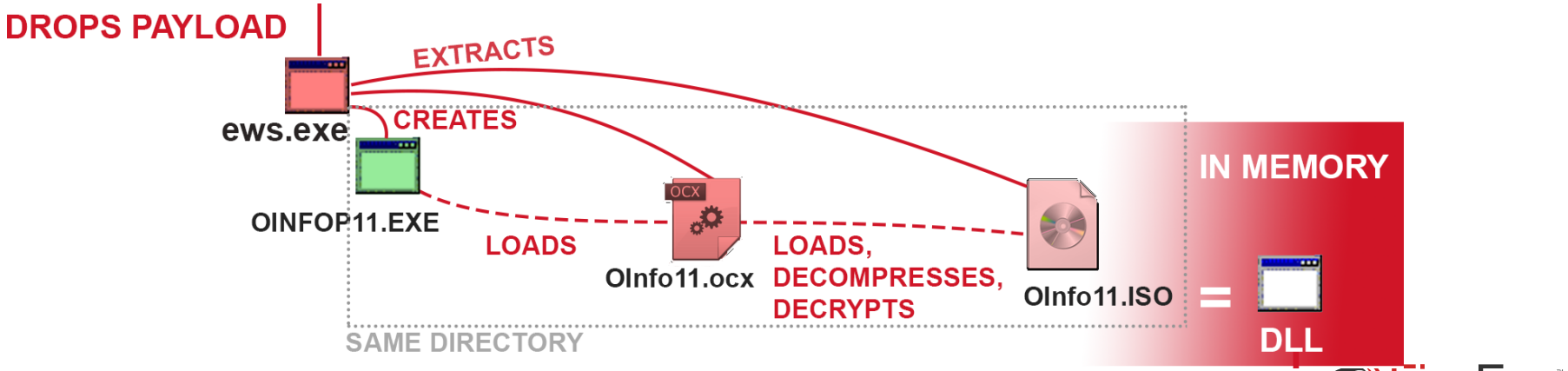
Monitor what the file does instead of who it's from

- Network callbacks
- Drop other files
- File/Registry changes

FireEye

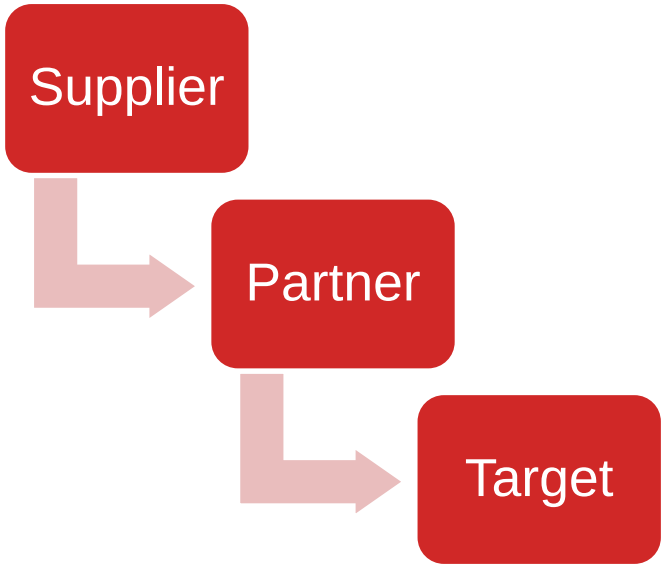
Intel from past infections

- Don’t rely on MD5 only
- Search via file name – be careful
  - Sever.exe – Gh0st RAT, njRAT, Xtreme RAT
- Search via location
  - File should not be stored here
  - Prevent .dll sidejacking
  - Timeline analysis, how/when did it move through a network
- Search via registry
  - Location
  - HKLM\System\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\
  - HKCU\Software\Microsoft\Windows\CurrenVersion\Run and RunOnce



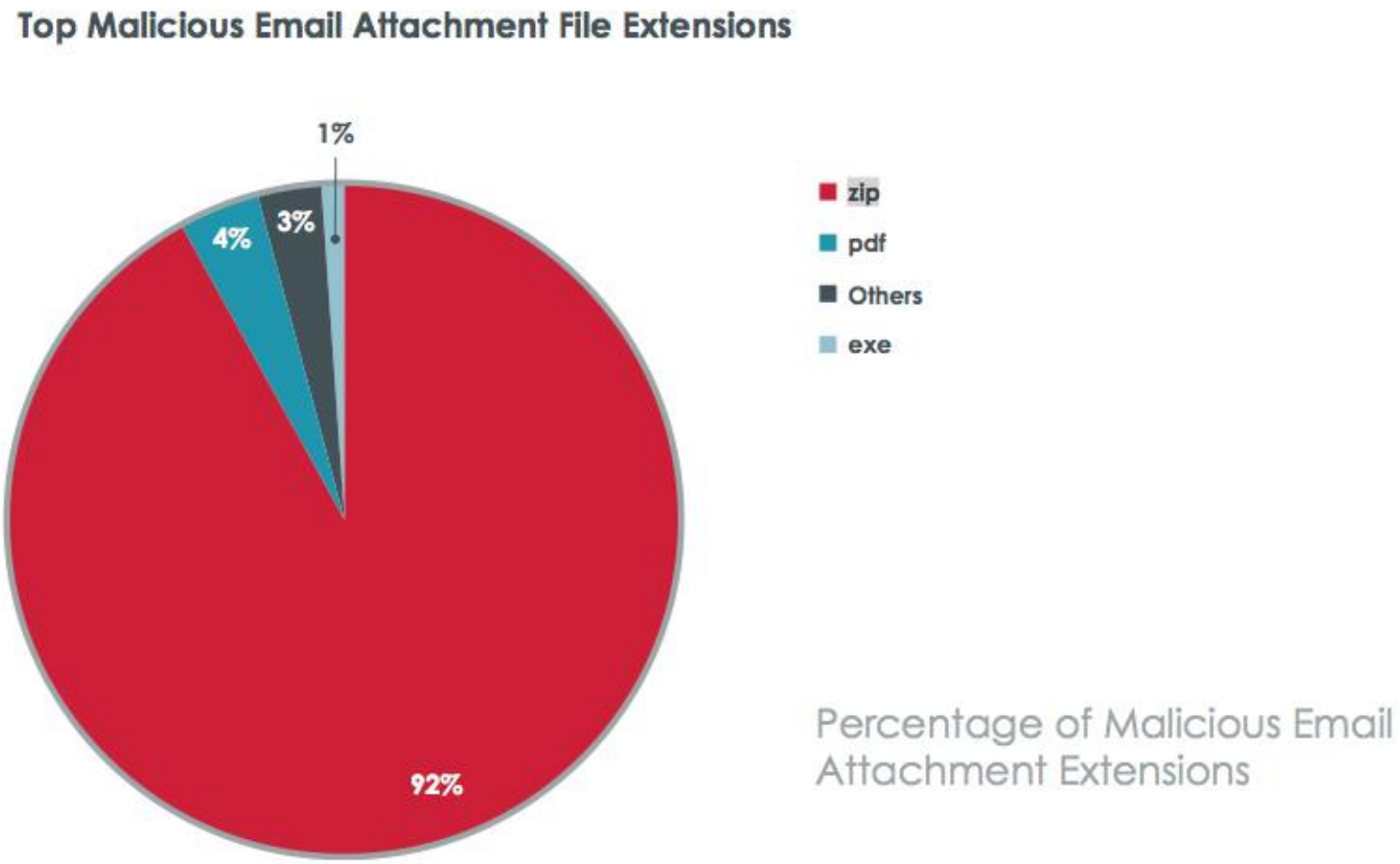
Case Study

- Large Company noticing partner traffic
- Identify malicious attempts
- Inform partner
  - Look for other incidents/remediate
  - Months later partner notifies of a breach



FireEye

Data Example: Email Attack Trends



Email Attack Trends – File Names

Rank	File Name	Percent of Email Attachments
1	Details.zip	6.9%
2	UPS_document.zip	4.0%
3	DCIM.zip	2.7%
4	HP_Document.zip	2.6%
5	Report.zip	1.9%
6	Scan.zip	1.8%
7	UPSDocument.zip	1.5%
8	Amazon_Report.zip	1.2%
9	postcard.zip	1.1%
10	UPSdocument.zip	0.8%
11	UK-Vodafone_MMS.zip	0.6%
12	HP_Scan.zip	0.5%
13	log_2012.zip	0.4%
14	SnowFairy.zip	0.3%
15	Changelog_10172012.zip	0.3%
16	Change_2012.zip	0.3%
17	Vodafone_MMS.zip	0.3%
18	Changelog_2012.zip	0.3%
19	changelog_2012.zip	0.3%
20	RoyalMailTrackingService.zip	0.3%

FireEye

Email Attack Trends – Words

Rank	Word	Percent of Email Attachments
1	ups	17.0%
2	details	13.9%
3	documents	10.6%
4	fedex	7.4%
5	myups	7.1%
6	amazon	5.4%
7	tracking	5.1%
8	invoice	5.0%
9	report	4.7%
10	order	4.4%
11	notification	3.8%
12	scan	3.4%
13	08	3.2%
14	hp	3.1%
15	IRS	2.9%
16	booking	2.8%
17	xerox	2.7%
18	dcim	2.7%
19	2012	2.7%
20	label	2.3%

FireEye

So What?

1. Gets through spam filters
2. Users open them
3. APT's use them:

Backdoor.APT.Gh0stRAT
- .zip files

Backdoor.APT.LV
- CV_English***.exe

Backdoor.APT.SpyNet
- xlsx.exe
- _pdf.exe
- .xlsx.scr

WSJ And NY Times Victims Of Spearphishing

Friday, February 01, 2013 20:28

RSA Blames Phishing Attack for March Security Breach

Spear Phishing Targets Bank Employees

13 Aug, 2013 14:17

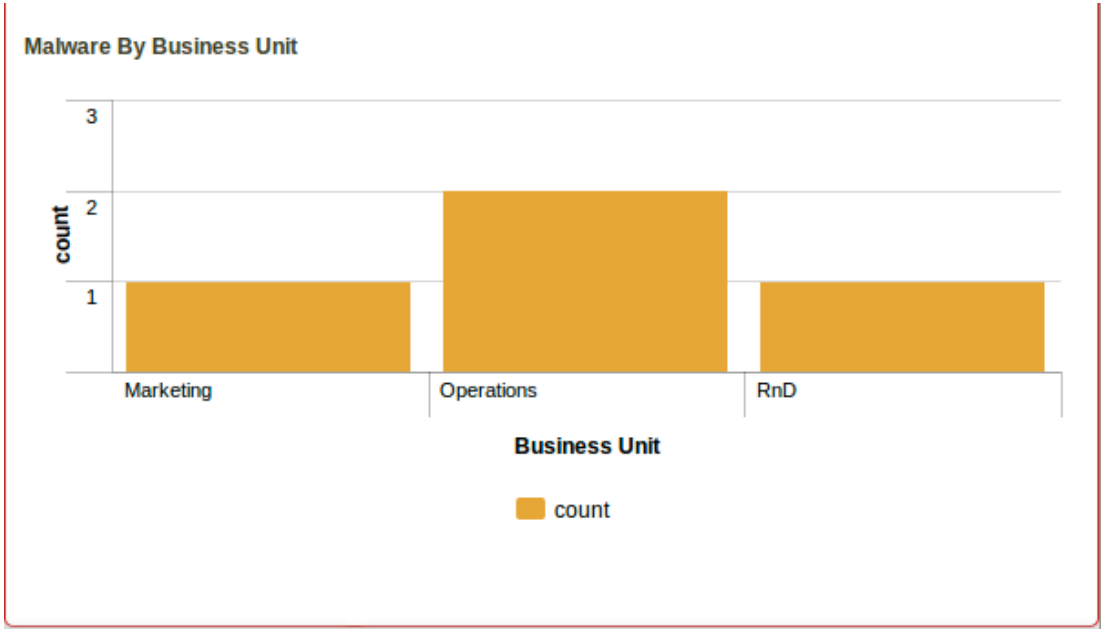
FireEye

Tailor your defenses

Most Exploited App: acrobat.exe

Most Occurring Severity: Critical

Build your case for installing updates/patches



Focus user training with evidence and adjust defense

Identifying Advanced Attacks

- Are they coming back?
- How hard are they trying?
- Is this a targeted attack?
- DNS or DHCP logs + malware ID = Faster response time by IR
  - Helps with VPN/Offsite users

FireEye

The Value of Data

- Latest exploits
  - Identify patterns in traffic
- Big picture
- Train the trainers
- Threats against providers
- Personalize the threat
  - This is why WE are being targeted

FireEye

Road map

- Bio
- Whitelist
- Intel from existing data
- Case Study
- Contact Info and Questions

FireEye

Contact Info

Kevin Thompson – FireEye

Email: kevin.thompson@fireeye.com

Questions?

FireEye