FireEye

The Emerging Threat Matrix

Greg Day
VP & Chief Technology Officer, EMEA
FireEye

1. Cyber – what's changing
2. What does it means to me
3. Aren’t I stopping it already
4. What should good look like

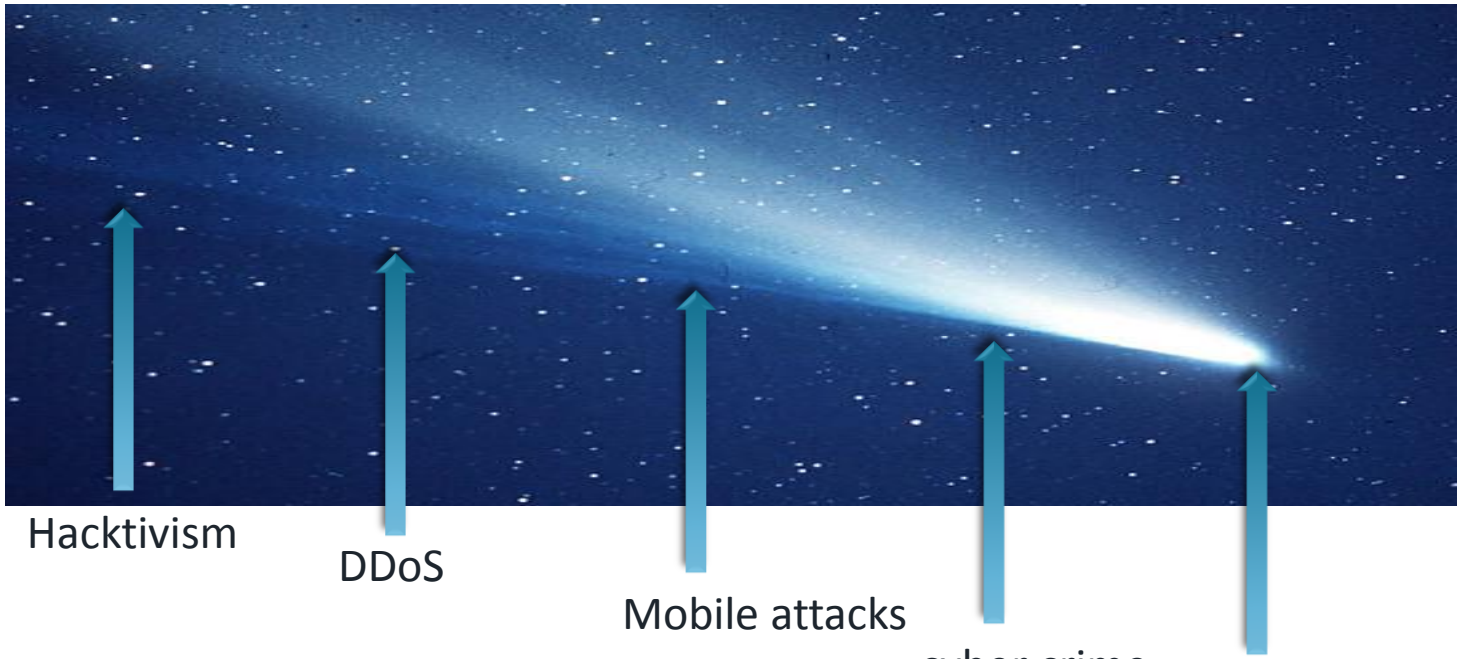
Cyber…so what's the problem?

In Top 3 Risk register for numerous European countries…..why…..why NOW?

- 1990's – PoC - Discover and Recover
- 2000's – cybercrime – target the masses
  - Protect the users IP and the infrastructure
- 2010+ - Targeted attack - Business IP
  - Information = 40% business value (Symantec State of Information EMEA 2012)
- Impacts profitability
- Impacts Gross Domestic Produce (GDP)

FireEye

Cyber Evolution – Isn't this just Nation state?



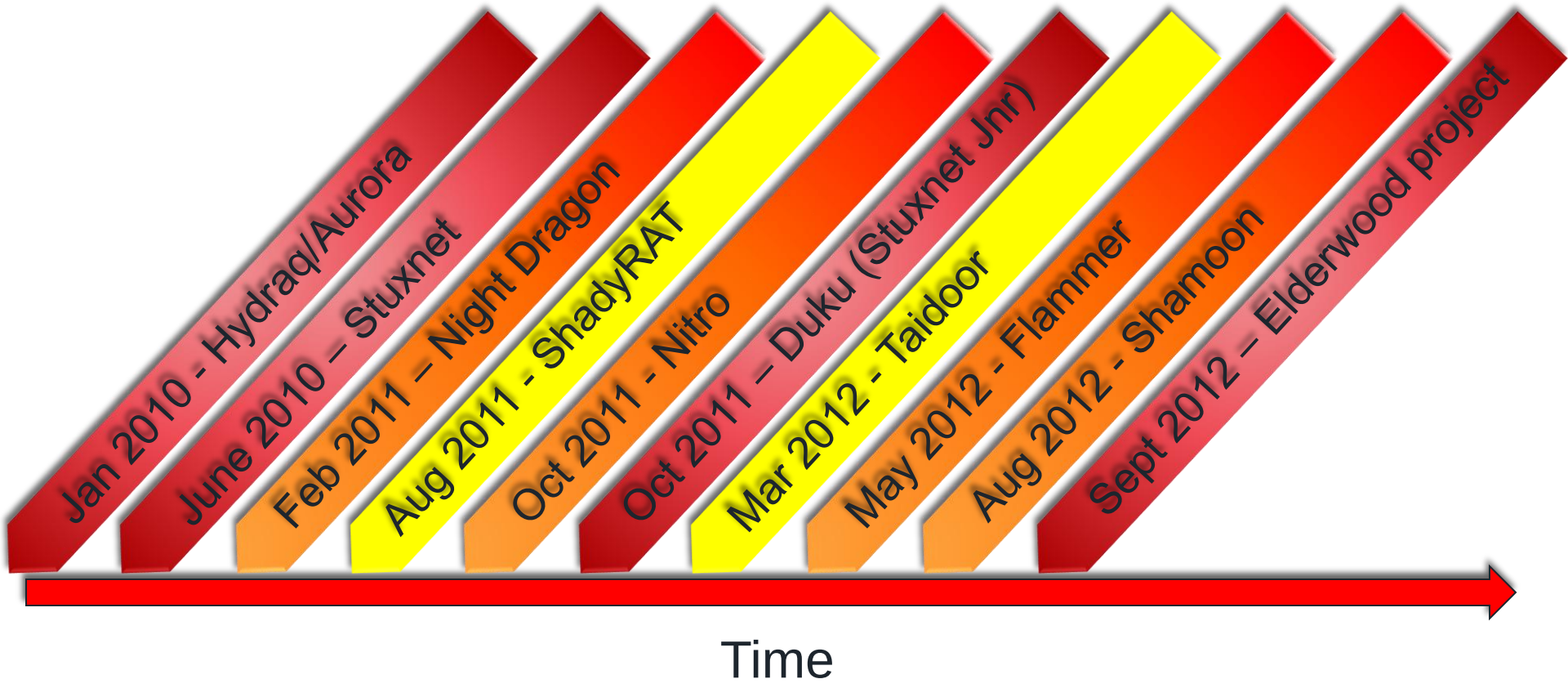
Hobbyists
Personal motive

Organized crime
Skilled individuals

State sponsored?
Sophisticated groups

FireEye

Levels of sophitication



FireEye

5

Business Impact: examples from the field

FireEye

How do we measure Cyber success?

FireEye

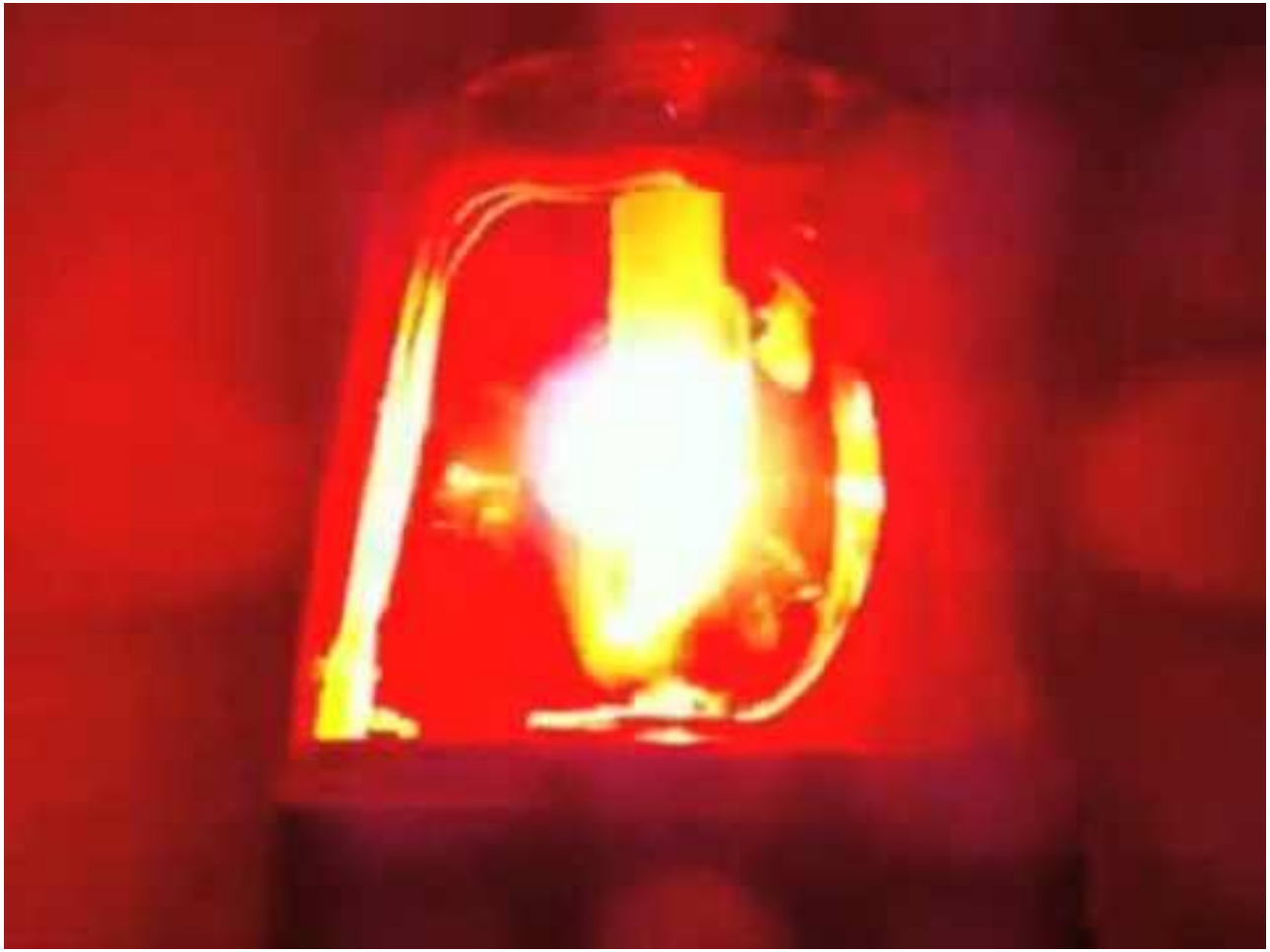
What does it mean???

- 71.5% thought there security was between good to excellent
- 45% said "NO" when asked if their budget is achieving a strong security posture
- 51% either unsure or said NO when asked if the technology they use would block a modern day attack
- 72% had a data breach in the last year!

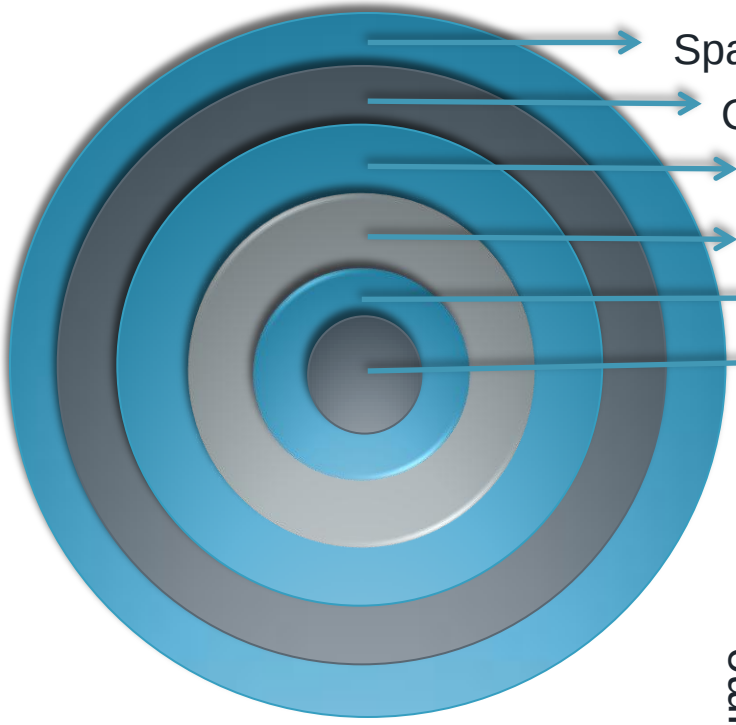
Ponemon Research: UK data 2103
Cyber Security in the Trenches

FireEye

So we wait…..



We focus on the volume problem.



Spam – 80%+ emails globally on Internet

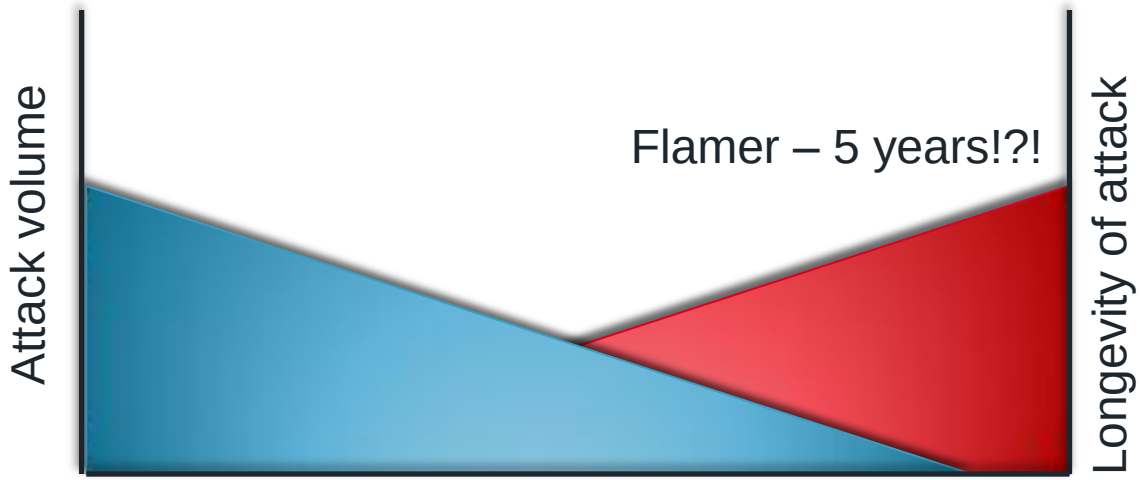
Cybercrime – 13+ new threats per sec

Phishing

Vulnerabilities – 1000's per year

Targeted attacks

APTs



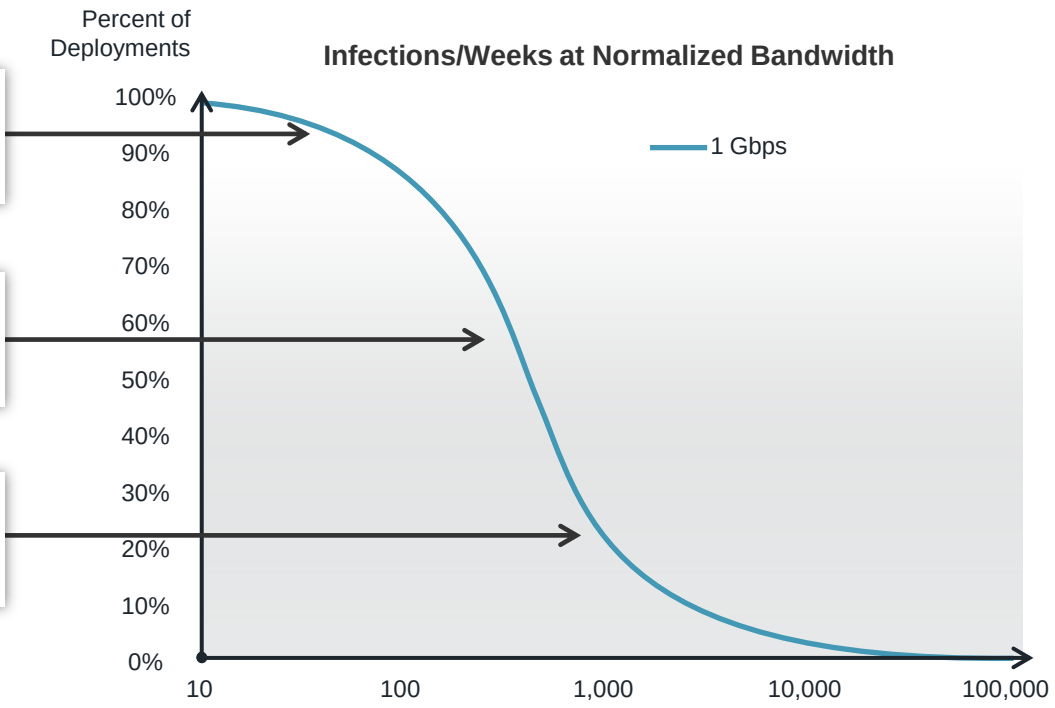
FireEye

Significant Compromise Still Exists!

98.5% of deployments see at least 10 incidents*/week/Gbps

Average is about **221** incidents*/week

20% of deployments have thousands of incidents*/week



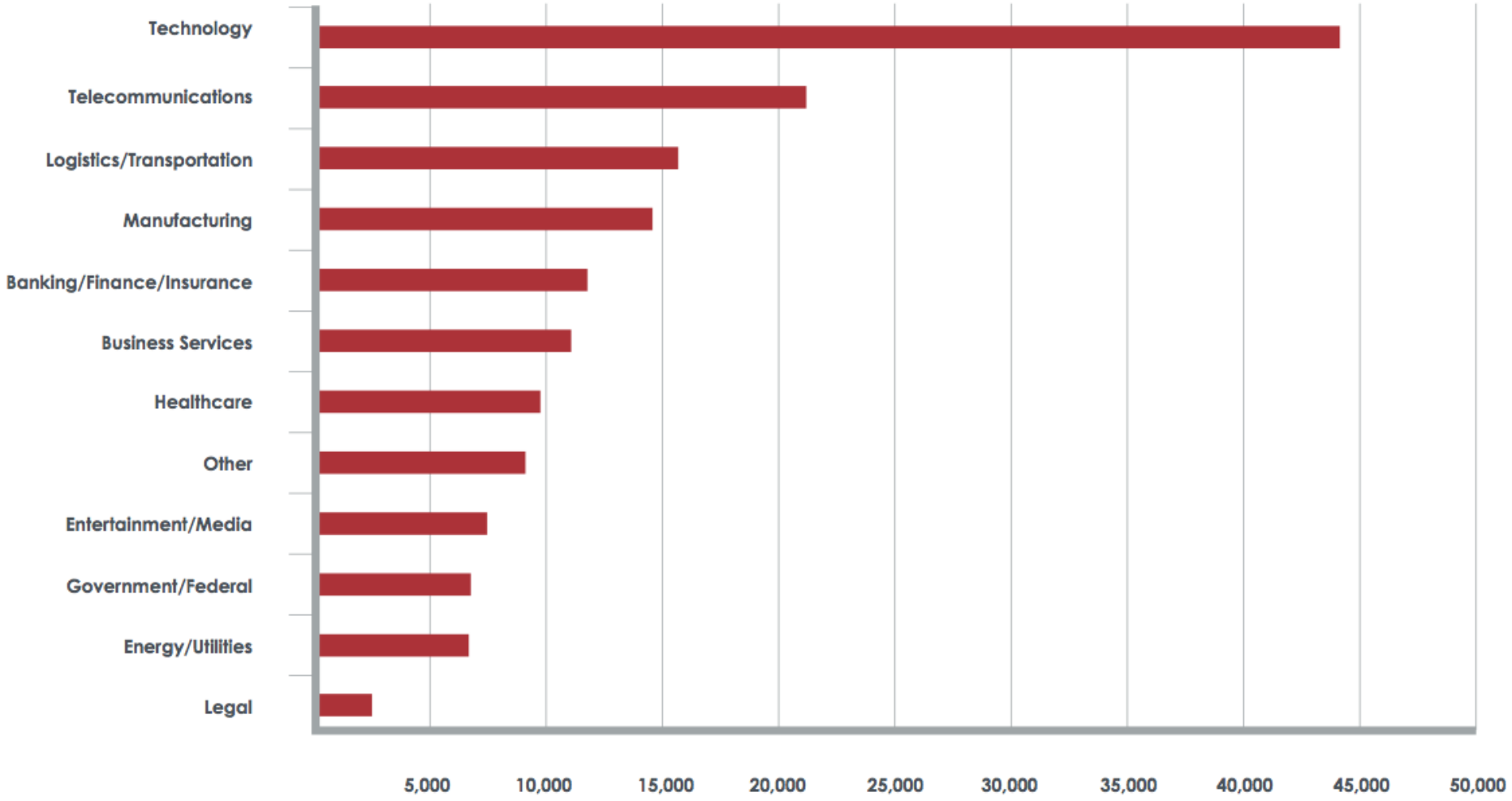
Source: FireEye Advanced Threat Report, March, 2013

221 Average Net New Incidents Per Week at Only 1 Gbps!

*** An incident is beyond inbound malware – it includes an exploit and callback**

FireEye

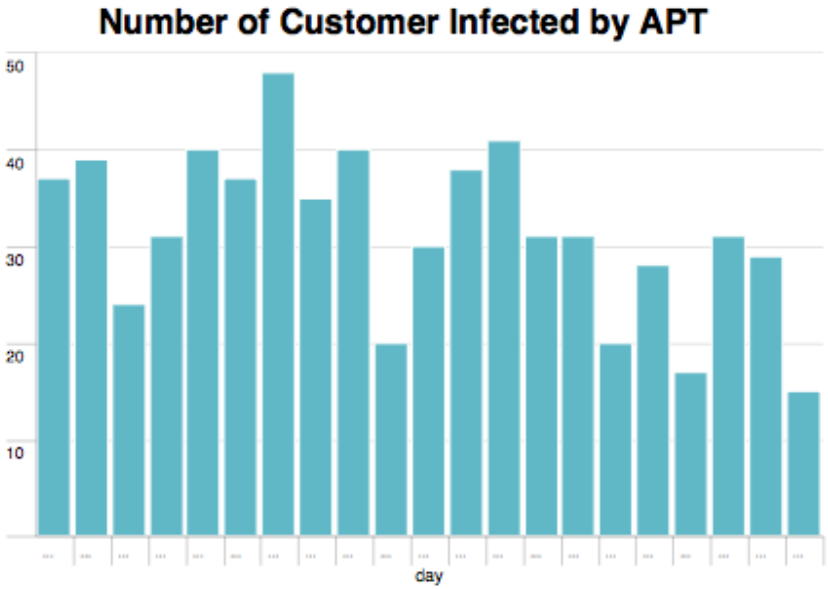
What's the probability of it happening to me?
Industry Average targeted Incidents in 2h 2012

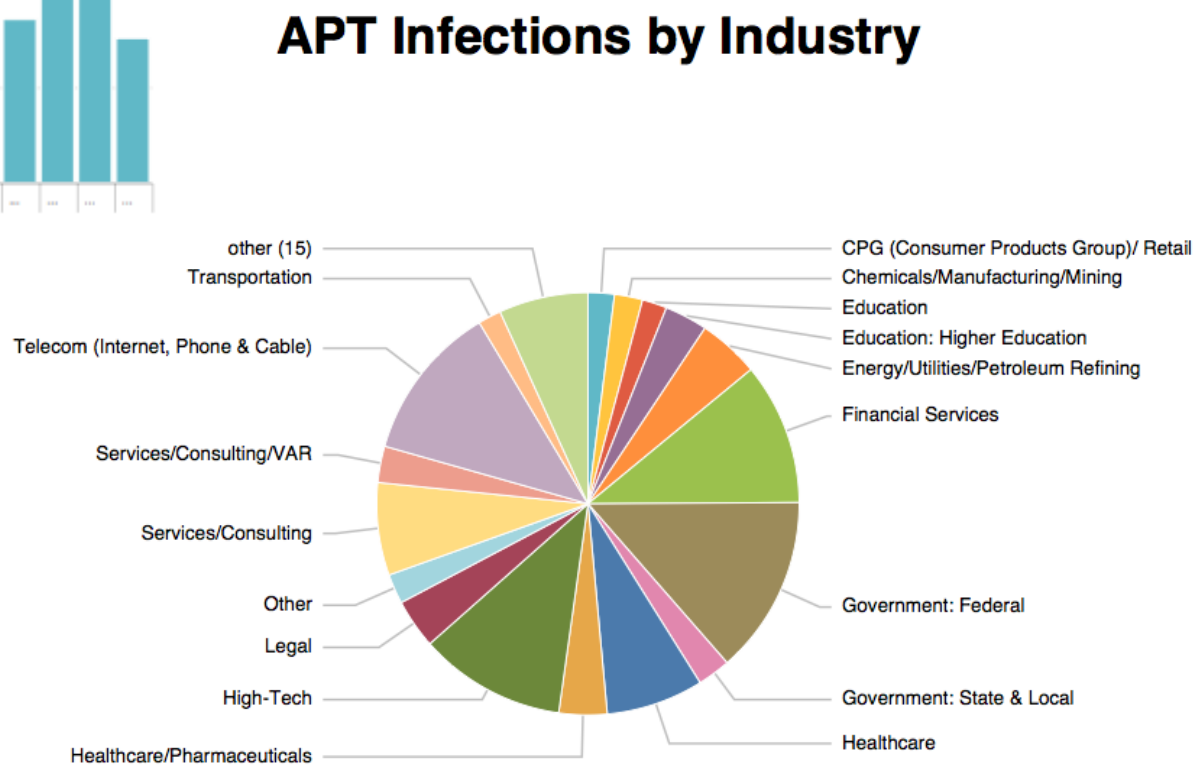


FireEye Advanced Threat Report 2H 2012

FireEye

Just how real is it right now? – 21 days in June





Under the headlines

3 Minutes

184 Countries, 41% Rise

Asia & East Europe (46%)

Across Verticals

Chinese Linkage (89%)

3 Emails to Compromise

Source: FireEye Advanced Threat Report, March 2013
Verizon Data Breach Investigations Report, 2013

FireEye

What have you seen more of (last 12mth)?

- 48% DDoS & Botnets
- 44% advanced/zero day attacks
- 32% Spear phishing/social engineering
- 11% traditional malware

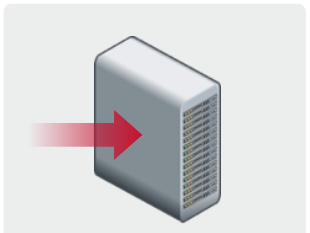
Ponemon Research: UK data 2103
Cyber Security in the Trenches

FireEye

What is the gap in our strategies?

Advanced threat lifecycle

Exploit an application or OS vulnerability



Callback to Command & Control

Malware Download

Data Exfiltration

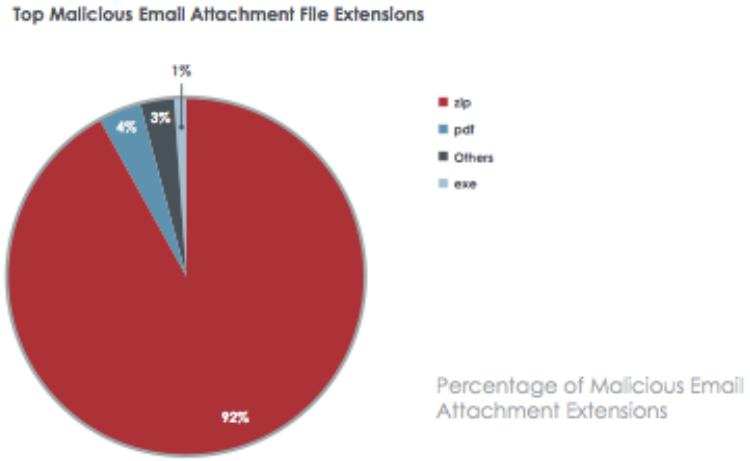
Lateral Spread

Exploit detection is critical

Every stage after it can be hidden or obfuscated

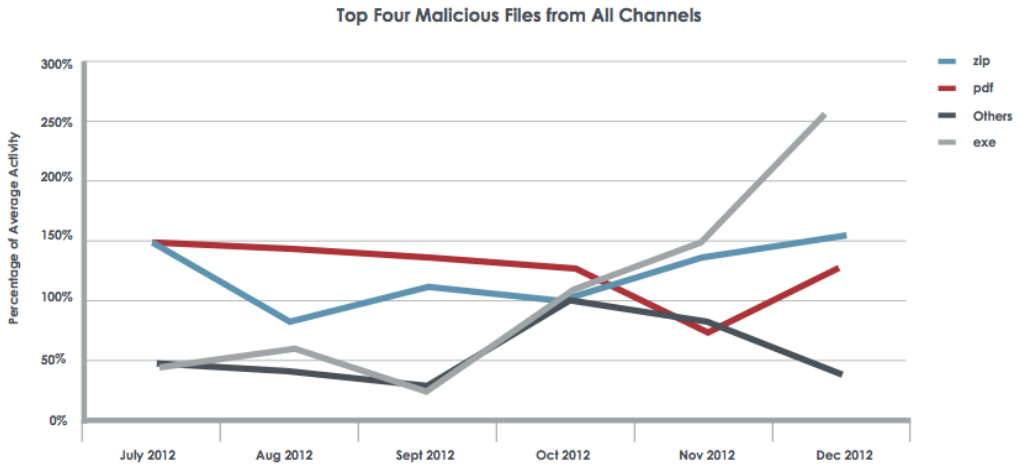
FireEye

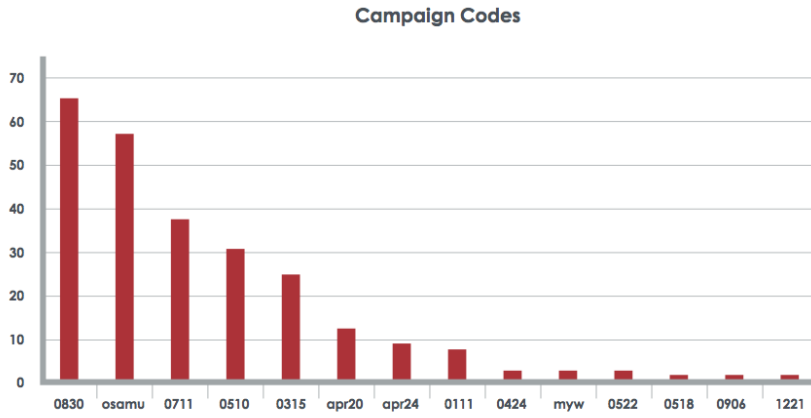
Todays tactics



Initiated by: Spear phishing emails using common terms

1. Shipping and delivery (UPS)
2. Finance
3. General Business





FireEye Advanced Threat Report 2H 2012

Looking at the end state will fail with todays attacks

1 System gets exploited

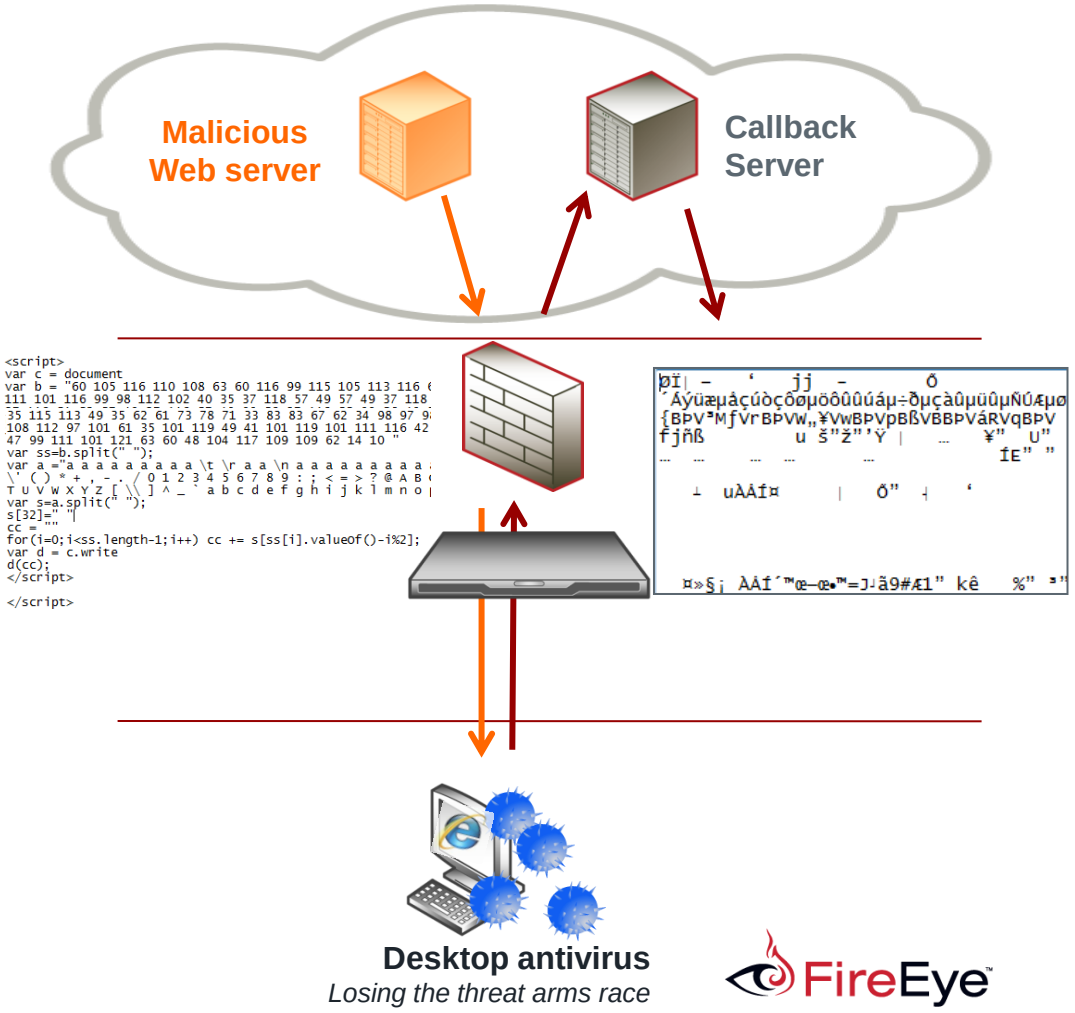
- Social engineering
- Obfuscated JavaScript code
- Exploited IE 6 zero-day vulnerability

2 Web server delivers malware

- Servers mapped by dynamic DNS
- XOR encoded malware EXE delivered
- No Signatures

3 Malware calls home & long-term control established

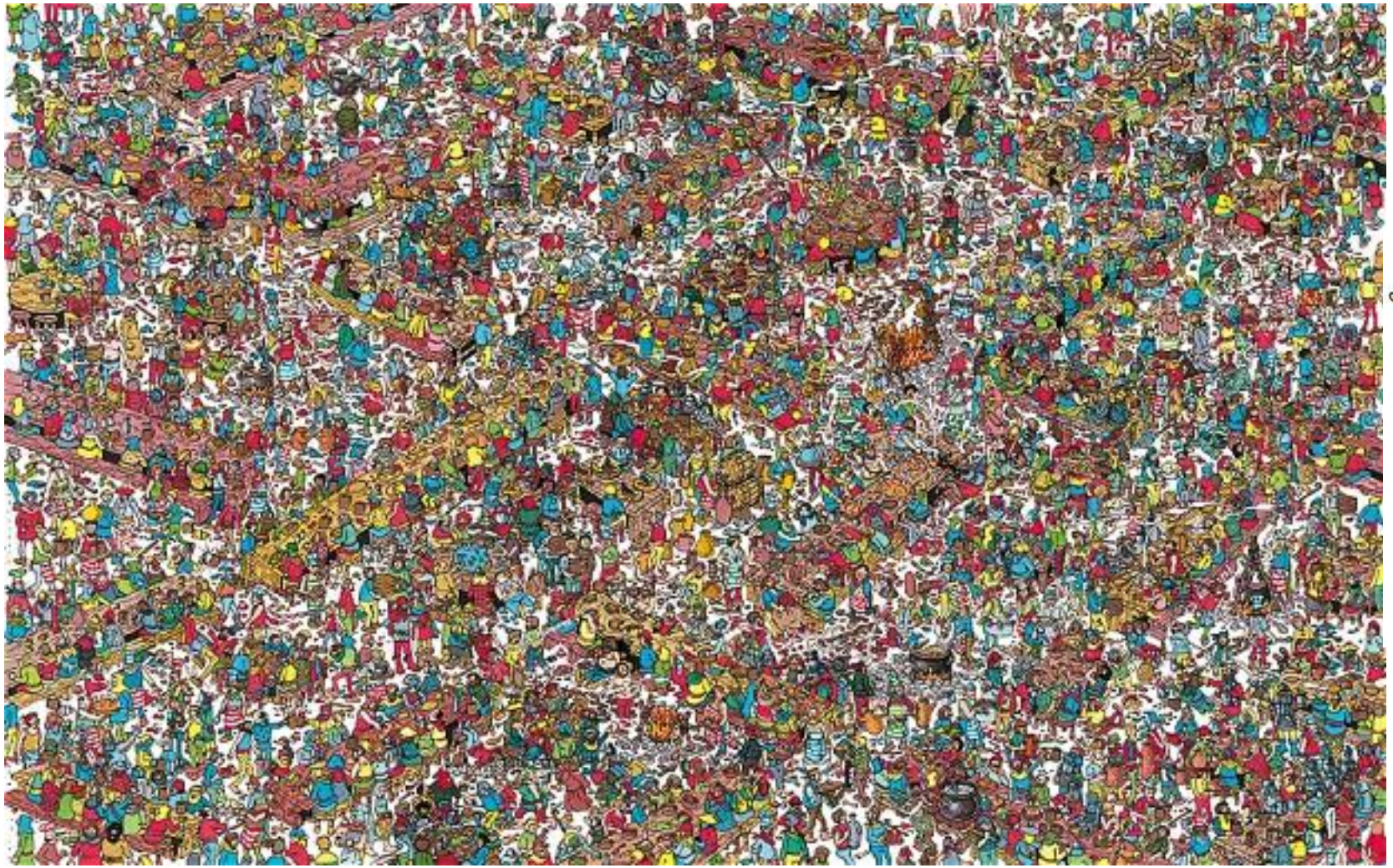
- Complete control of infected system
- Further payloads downloaded
- C&C located here in Taiwan!
- Using outbound port 443 (SSL)



19

How do we solve the Cyber gap problem?

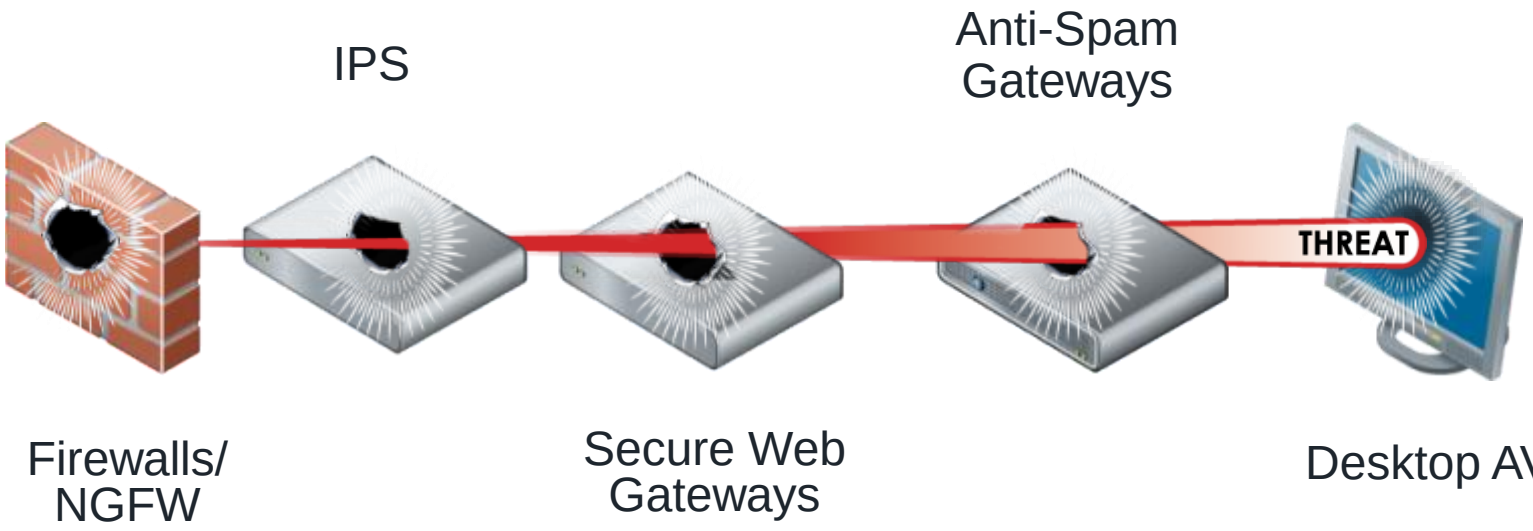
Todays IT environments - Where's Wally?



FireEye

Traditional Defenses Don’t Work

The new breed of attacks evade signature-based defenses



FireEye

We keep responding in the same old ways

- blocked Windows protocols on external firewalls
- enforced auth. tokens and VPN usage
- bolstered patching regimens
- installed IDS/IPS @ gateway/desktop
- segmented networks to contain worm damage

FireEye

Attacks by the APT are human driven; not generally polymorphic

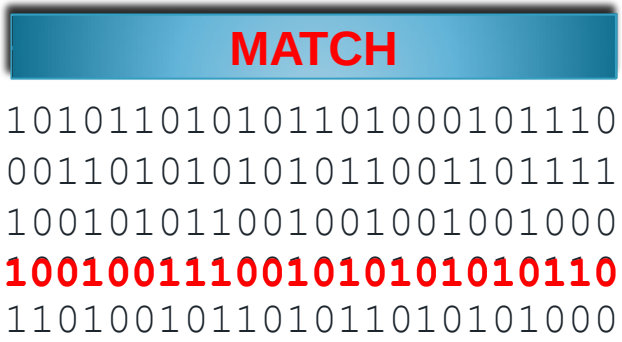
CISO view of the Problem

- Targeted = you're first to see = means there is no signature or behavioral block
- Most environments to complex to see the anomalies
- Compromise time typically months if not years
- Understanding the attackers motives & actions
- Need to see the entire attack stream & gather the forensics

FireEye

Targeted – We can't wait to learn from others

Legacy Pattern-Matching Detection Model



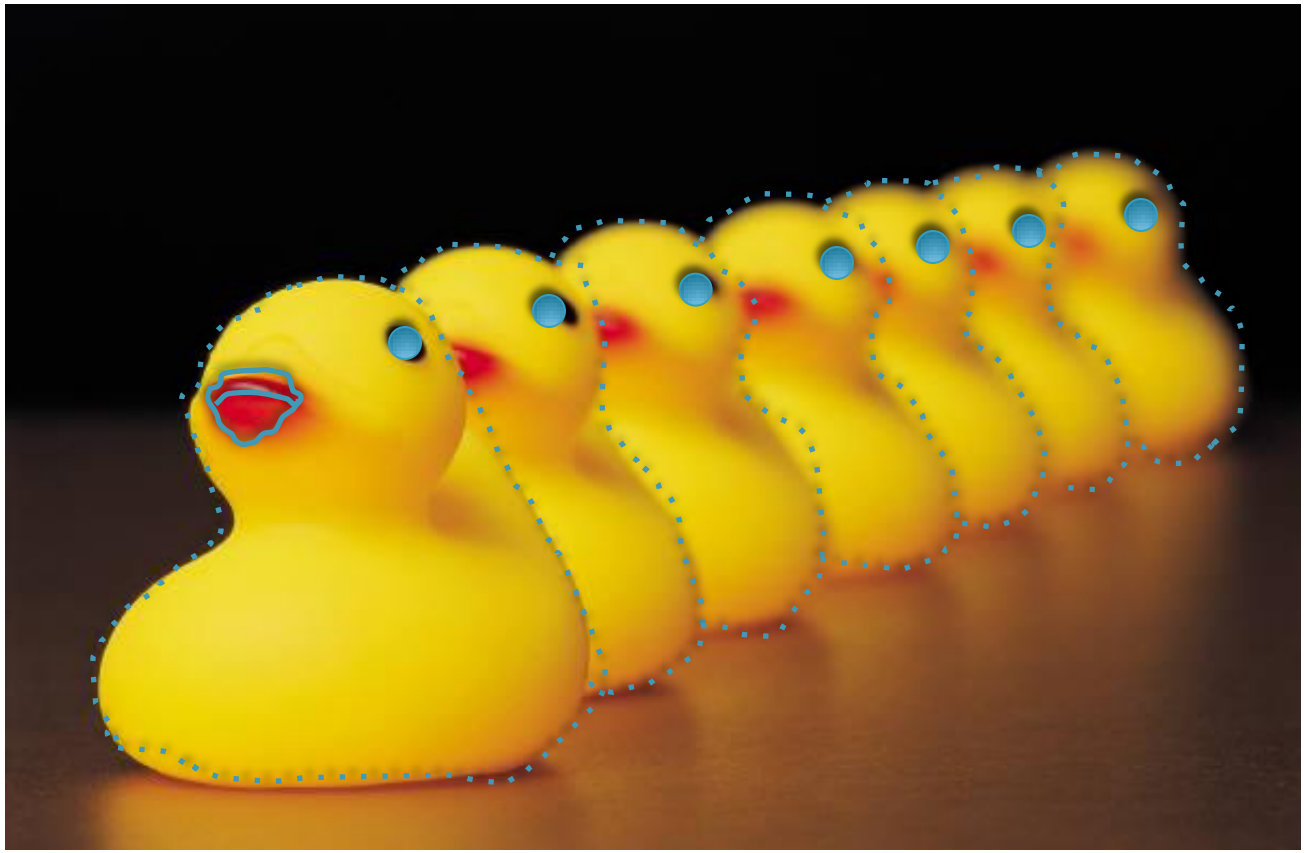
- Signature-Based
- Reactive
- Only known threats
- Many false negatives

New Virtual Execution Model

- Signature-less
- Dynamic, real-time
- Known/unknown threats
- Minimal false positives

FireEye

We need to be able to join the DOTs to comprehend the attack



FireEye Captured Aurora on Day Zero

Exploitcode	Kernel32	*API Name*: WriteFile *Address*: 202964316	900		
Exploitcode	Kernel32	*API Name*: ReadFile *Address*: 202964254	900		
Exploitcode	Kernel32	*API Name*: WriteFile *Address*: 202964316	900		
Exploitcode	Kernel32	*API Name*: VirtualProtect *Address*: 202964803	900		
Exploitcode	Kernel32	*API Name*: LoadLibraryA *Address*: 202964499 *Params*: [shdocvw]	900		
File	Created	C:\Documents and Settings\Administrator\Application Data\a.exe	900		
File	Created	C:\Documents and Settings\Administrator\Application Data\b.exe	900		
File	Delete	C:\Documents and Settings\Administrator\Application Data\a.exe	900		
Process	Started	C:\Documents and Settings\Administrator\Application Data\b.exe *Packed*: yes *GUI*: no MD5: 9f880ac607cbd7cdfffa609c5883c708 SHA1: 08b33a64a85b93530d07ec3ea611e4875ee6c169	1304	900	34816
Malicious Alert	Misc Anomaly	*Detail*: Process started from a packed binary			
Malicious Alert	Anomaly Tag	*Message*: Startup behavior anomalies observed *Detail*: Browser started an unknown process			
File	Date Change	C:\WINDOWS\system32\Rasmon.dll MD5: 0f9c5408335833e72fe73e6166b5a01b SHA1: cfa826c339898e882a1276b694fc935d56b83093	1304		90112
Regkey	Added	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\UpsXZE	544		
Malicious Alert	Misc Anomaly	*Message*: System services modified *Detail*: service loaded through windows			
Regkey	Deleted	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\UpsXZE	1320		
Regkey	Added	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\RaSXkNk	1320		
Network	Dns Query	*Protocol Type*: udp *Qtype*: Host Address *Hostname*: 360.homeunix.com	1320		
Network	Connected	*Protocol Type*: tcp *IP Address*: [redacted] *Destination Port*: 443	1320		
Malicious Alert	Misc Anomaly	*Message*: Malware communication observed			
File	Created	C:\WINDOWS\DFS.bat	1304		
Process	Started	C:\WINDOWS\system32\cmd.exe /c "C:\WINDOWS\DFS.bat" *Packed*: no *GUI*: no MD5: 84ddf54db542b2eb9ef08144fb6e3645 SHA1: 43c3eeadfd2c3aadd32f9a7c750e4b1465d3bc9a	1280	1304	375808
Process	Terminated	C:\Documents and Settings\Administrator\Application Data\b.exe	1304	900	
File	Delete	C:\Documents and Settings\Administrator\Application Data\b.exe	1280		
File	Delete	C:\WINDOWS\DFS.bat	1280		
Appexception		*Exception Faulting Address*: 0x65 *Exception Code*: 0xC0000005 *Exception Level*: SECOND_CHANCE *Exception Type*: STATUS_ACCESS_VIOLATION *Instruction Address*: 0x00000000781444dc *Description*: Data from Faulting Address controls Branch Selection *Classification*: UNKNOWN	900		
Malicious Alert	Misc Anomaly	*Detail*: Crash detected due to second chance			
File	Created	C:\Program Files\Debugging Tools for Windows (x86)\DBG0.tmp	1312		
Uac	Service	UpsXZE			
Malicious Alert	Misc Anomaly	*Detail*: System service running/stopped			

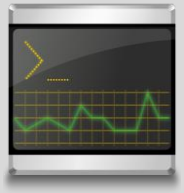
1	VM-verified Outbound Comm.	Exploit.Browser		[redacted]	[redacted]

Decryption complete. MD5 of Trojan.Hydraq

Encrypted callback captured

What should you seek in the solution?

Signature-less detection



Exploit detection

Command and control tracking

Accurate detection

Near real-time analysis

Scalable detection across real-world traffic patterns

Sharing threat intelligence for proactive security

FireEye

Summary

- Targeted attacks ARE personal – NO signature!
  - Often multi vectored and very specific
  - Assume the attackers will know your weak points
- Todays IT is complex, hard to maintain complex standards (SANS20, etc…)
  - Anomalies are hard to spot, can you join the DOTs!
- Often the subtler the breach the bigger the impact
  - If you look just at the end state you miss the attack detail
- Breaches will occur
  - Can you mitigate or marginalize
  - Can you gather the forensic evidence to understand the attack

FireEye

Email: Greg.Day@FireEye.com
Twitter: @GregDaySecurity

FireEye

31