Rapidly Evolving Security Connected

"Participating in Your Own Survival: FirstNet - The New World"

David O'Berry CCSP, CISSP-ISSAP, ISSMP, CSSLP, CRISC
Worldwide Technical Strategist
Office of the CTO
Intel Security Group

Intel Security Group

FirstNet: The New World

Alternatively Subtitled:

"It Is VERY VERY Different From The Old One"

AND/OR

"God Help Us ALL...I Want The Old One Back"

- David O'Berry, Previously Director of Strategic Development and ITS for SC Probation, Parole, & Pardon Services
  - During my 19+ years with South Carolina
  - MS-ISAC Executive Board
  - SC Security Domain Chairman and Collaboration TL
  - Midland's ISSA Chapter Founder and President
  - Trusted Computing Group's Customer Advisory Council (TNC-CAC)
  - Chairman, TOG's "Improving The Digital EcoSytem Workgroup"
  - Chapters Published on IF-MAP, SCAP, TNC and Standard's Based Defense/Mitigation (ISMH 09,10,11)

- My Previous Life's Work and the IT Environment
  - 800+ users, rapidly growing external user-base (1000s)
  - 100% Mobile capable – Plan started in 2002
  - 26 – 30+ Full-time IT including development , engineering, help desk, & remote support
  - Decentralized work force

- Heterogeneous and Open Standards Deployments
  - Core: McAfee, Dell, Juniper, APC
  - Network: Juniper, BlueCoat, Citrix, Imprivata
  - Data: McAfee EEPC, Device Control, Host DLP
  - Endpoint: McAfee AV, HIPS, Policy Auditor
  - Management: McAfee's ePolicy Platform, STRM, NSM Manager, Cacti & other "Open Source" products

The “Art of Security”

The Techno-Industrial Revolution 2.x is…

“The ULTIMATE outcome of the application of human creative skills and imagination”

We're NOT Winning…

White Lodging - Attack

Mar 30, 2013 – Dec 16, 2013

Marriott International, Starwood Hotels and Resorts Worldwide Inc., Radisson Hotels & Resorts, InterContinental Hotels Group, White Lodging Services, Corporation

'Wichcraft - Attack

Aug 11, 2013 – Oct 2, 2013

'wichcraft Notice to Our Customers

'wichcraft Operating, LLC recently learned that an unauthorized party gained access to our systems, compromising the payment card information of certain customers who made purchases at a 'wichcraft location in New York or San Francisco using a payment card from approximately August 11, 2013 to October 2, 2013.

Harbor Freight - Attack

May 6, 2013 – Jun 30, 2013

HARBOR FREIGHT TOOLS Quality Tools at Ridiculously Low Prices

" The attack was similar to attacks reported by other national retailers. In response, we immediately engaged a leading cyber-security company to investigate and notices were posted in every store and on our website. "

Neiman Marcus - Attack Wave

Jul 16, 2013 – Oct 30, 2013

Confirmed January 22, 2013

Neiman Marcus

Target - Attack

Nov 27, 2013 – Dec 15, 2013

TARGET

Easton-Bell - Attack

Dec 1, 2013 – Dec 31, 2013

EASTON-BELL SPORTS

Easton-Bell Sports, Inc. ("Easton-Bell"), which includes Easton, Bell, Riddell, Giro, Blackburn and Easton Cycling, recently discovered that vendor servers were subject to a malicious software ("malware") computer intrusion.

*"…the company said earnings were down 46 percent from the same period a year earlier, **including an expenditure of 61M USD for the breach itself.** Earnings per share were 81 cents, down from $1.47 the year before. Target executives repeatedly called 2013 a "challenging" year on Wednesday."*

http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html?_r=0

May 1, 2013 | Jul 1, 2013 | Sep 1, 2013 | Nov 1, 2013 | Jan 1, 2014 | Mar 1, 2014

Retail POS Attack Waves

How Big is the Emerging Attack Surface?

The Average Day in the Average Enterprise

Every **1min** a host accesses a malicious website

Every **3mins** a bot is communicating with its command and control center

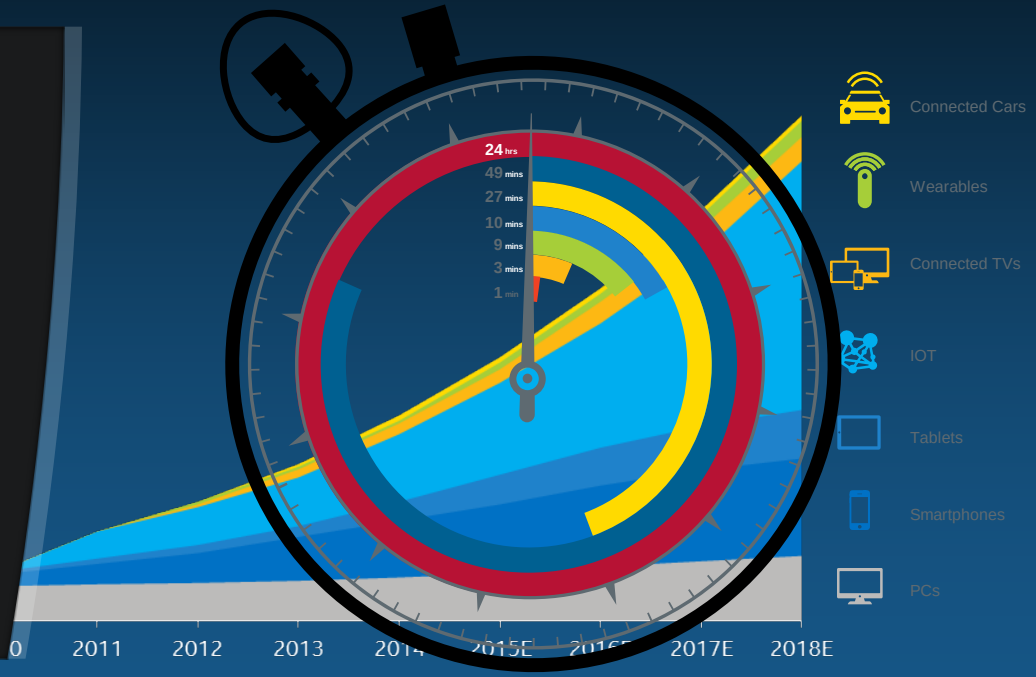
Every **9mins** a High Risk application is being used

Every **10mins** a known malware is being downloaded

Every **27mins** an unknown malware is being downloaded

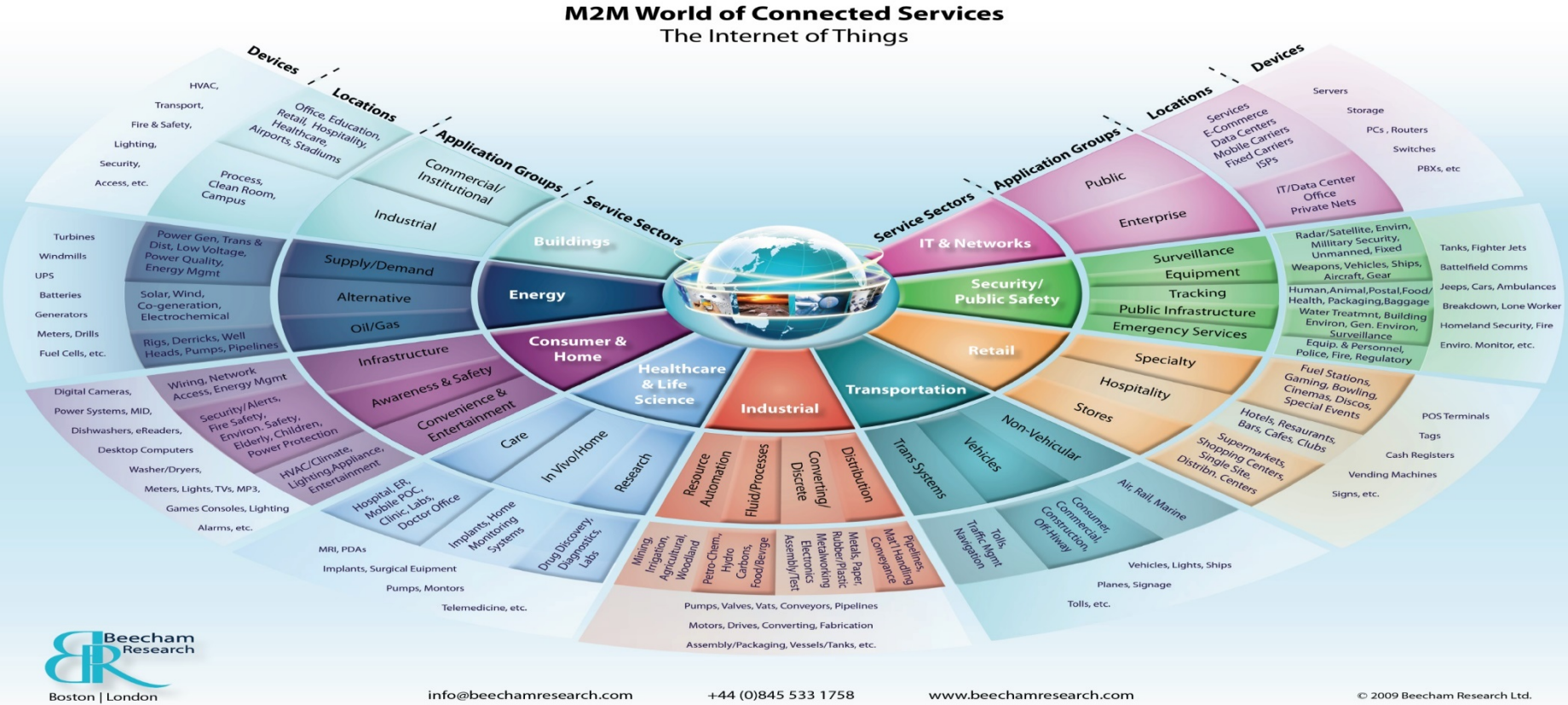
Every **49mins** sensitive data is sent outside the organization

Every **24h** a given host is infected with a bot



Source: Bi Intelligence Investments

Firm or Fixed Function Devices and the “IoT”



Beecham Research

Boston | London

info@beechamresearch.com +44 (0)845 533 1758 www.beechamresearch.com

Vulnerabilities

#	Affected	Contra Indications – KB	Known Exploits	Microsoft rating(**)	ISC rating(*) clients	ISC rating(*) servers
MS15-032	Cumulative Security Update for Internet Explorer (ReplacesMS15-018)					
	CVE-2015-1652, CVE-2015-1657, CVE-2015-1659, CVE-2015-1660, CVE-2015-1661, CVE-2015-1662, CVE-2015-1665, CVE-2015-1666, CVE-2015-1667, CVE-2015-1668	KB 3038314	No	Severity:Critical Exploitability:	Critical	Important
MS15-033	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (ReplacesMS14-081 MS15-022)					
	CVE-2015-1639 CVE-2015-1641 CVE-2015-1649 CVE-2015-1650 CVE-2015-1651	KB 3048019	vuln. public.	Severity:Critical Exploitability:	Critical	Important
MS15-034	Vulnerability in HTTP.sys Could Allow Remote Code Execution					
	CVE-2015-1635	KB 3042553	No	Severity:Critical Exploitability:	Critical	Critical
MS15-035	Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution					
	CVE-2015-1645	KB 3046306	No	Severity:Critical Exploitability:	Critical	Critical
MS15-036	Vulnerabilities in Microsoft SharePoint Server Could Allow Elevation of Privilege (ReplacesMS15-022)					
	CVE-2015-1640 CVE-2015-1653	KB 3052044	No	Severity:Important Exploitability:	N/A	Important

Source: https://isc.sans.edu/forums/diary/Microsoft+Patch+Tuesday+April+2015/19577/

Vulnerabilities

Security Update	For…	CVE numbers
APSB15-06	Adobe Flash Player	CVE-2015-0346, CVE-2015-0347, CVE-2015-0348, CVE-2015-0349, CVE-2015-0350, CVE-2015-0351, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0356, CVE-2015-0357, CVE-2015-0358, CVE-2015-0359, CVE-2015-0360, CVE-2015-3038, CVE-2015-3039, CVE-2015-3040, CVE-2015-3041, CVE-2015-3042, CVE-2015-3043, CVE-2015-3044
APSB15-07	ColdFusion	CVE-2015-0345
APSB15-08	Adobe Flex	CVE-2015-1773

Source: http://helpx.adobe.com/security.html

Vulnerabilities

April 2015 Apple Security Updates 1/4

Name	For…	CVE numbers		
OS X Server 4.1	OS X Yosemite v10.10 or later	CVE-2014-3566	CVE-2015-1150	CVE-2015-1151
Xcode 6.3	OS X Yosemite v10.10 or later	CVE-2015-1149		
Apple TV 7.2	Apple TV 3rd generation and later	CVE-2015-1068 CVE-2015-1069 CVE-2015-1070 CVE-2015-1071 CVE-2015-1072 CVE-2015-1073 CVE-2015-1074 CVE-2015-1076 CVE-2015-1077 CVE-2015-1078 CVE-2015-1079 CVE-2015-1080 CVE-2015-1081	CVE-2015-1082 CVE-2015-1083 CVE-2015-1086 CVE-2015-1092 CVE-2015-1094 CVE-2015-1095 CVE-2015-1096 CVE-2015-1097 CVE-2015-1099 CVE-2015-1100 CVE-2015-1101 CVE-2015-1102 CVE-2015-1103	CVE-2015-1104 CVE-2015-1105 CVE-2015-1110 CVE-2015-1114 CVE-2015-1117 CVE-2015-1118 CVE-2015-1119 CVE-2015-1120 CVE-2015-1121 CVE-2015-1122 CVE-2015-1123 CVE-2015-1124

Source: https://support.apple.com/en-us/HT201222

Vulnerabilities

Name	For…	CVE numbers		
iOS 8.3	iPhone 4s and later, iPod touch (5th generation) and later, iPad 2 and later	CVE-2015-1068 CVE-2015-1069 CVE-2015-1070 CVE-2015-1071 CVE-2015-1072 CVE-2015-1073 CVE-2015-1074 CVE-2015-1076 CVE-2015-1077 CVE-2015-1078 CVE-2015-1079 CVE-2015-1080 CVE-2015-1081 CVE-2015-1082 CVE-2015-1083 CVE-2015-1084 CVE-2015-1085 CVE-2015-1086 CVE-2015-1087 CVE-2015-1088	CVE-2015-1089 CVE-2015-1090 CVE-2015-1091 CVE-2015-1092 CVE-2015-1093 CVE-2015-1094 CVE-2015-1095 CVE-2015-1096 CVE-2015-1097 CVE-2015-1098 CVE-2015-1099 CVE-2015-1100 CVE-2015-1101 CVE-2015-1102 CVE-2015-1103 CVE-2015-1104 CVE-2015-1105 CVE-2015-1106 CVE-2015-1107 CVE-2015-1108	CVE-2015-1109 CVE-2015-1110 CVE-2015-1111 CVE-2015-1112 CVE-2015-1113 CVE-2015-1114 CVE-2015-1115 CVE-2015-1116 CVE-2015-1117 CVE-2015-1118 CVE-2015-1119 CVE-2015-1120 CVE-2015-1121 CVE-2015-1122 CVE-2015-1123 CVE-2015-1124 CVE-2015-1125 CVE-2015-1126

Source: https://support.apple.com/en-us/HT201222

Vulnerabilities

April 2015 Apple Security Updates 3/4

Name	For…	CVE numbers		
OS X Yosemite 10.10.3 and Security Update 2015-004	OS X Mountain Lion v10.8.5, OS X Mavericks v10.9.5, OS X Yosemite v10.10 to v10.10.2	CVE-2013-5704 CVE-2013-6438 CVE-2013-6712 CVE-2014-0098 CVE-2014-0117 CVE-2014-0118 CVE-2014-0207 CVE-2014-0226 CVE-2014-0231 CVE-2014-0237 CVE-2014-0238 CVE-2014-2497 CVE-2014-3478 CVE-2014-3479 CVE-2014-3480 CVE-2014-3487 CVE-2014-3538 CVE-2014-3569 CVE-2014-3570 CVE-2014-3571 CVE-2014-3572 CVE-2014-3587 CVE-2014-3597 CVE-2014-3668 CVE-2014-3669 CVE-2014-3670	CVE-2014-3710 CVE-2014-3981 CVE-2014-4049 CVE-2014-4380 CVE-2014-4404 CVE-2014-4405 CVE-2014-4670 CVE-2014-4698 CVE-2014-5120 CVE-2014-8275 CVE-2014-8830 CVE-2014-9298 CVE-2015-0204 CVE-2015-1069 CVE-2015-1088 CVE-2015-1089 CVE-2015-1091 CVE-2015-1093 CVE-2015-1095 CVE-2015-1096 CVE-2015-1098 CVE-2015-1099 CVE-2015-1100 CVE-2015-1101 CVE-2015-1102 CVE-2015-1103	CVE-2015-1104 CVE-2015-1105 CVE-2015-1117 CVE-2015-1118 CVE-2015-1130 CVE-2015-1131 CVE-2015-1132 CVE-2015-1133 CVE-2015-1134 CVE-2015-1135 CVE-2015-1136 CVE-2015-1137 CVE-2015-1138 CVE-2015-1139 CVE-2015-1140 CVE-2015-1141 CVE-2015-1142 CVE-2015-1143 CVE-2015-1144 CVE-2015-1145 CVE-2015-1146 CVE-2015-1147 CVE-2015-1148 CVE-2015-1545 CVE-2015-1546

Source: https://support.apple.com/en-us/HT201222

Past, Present, and Future

2007 (8 years ago)

1M malware samples

2015 (today's estimate)

150M+ malware samples

By **2020** (in 5 years)

40% of data will be generated by IoT

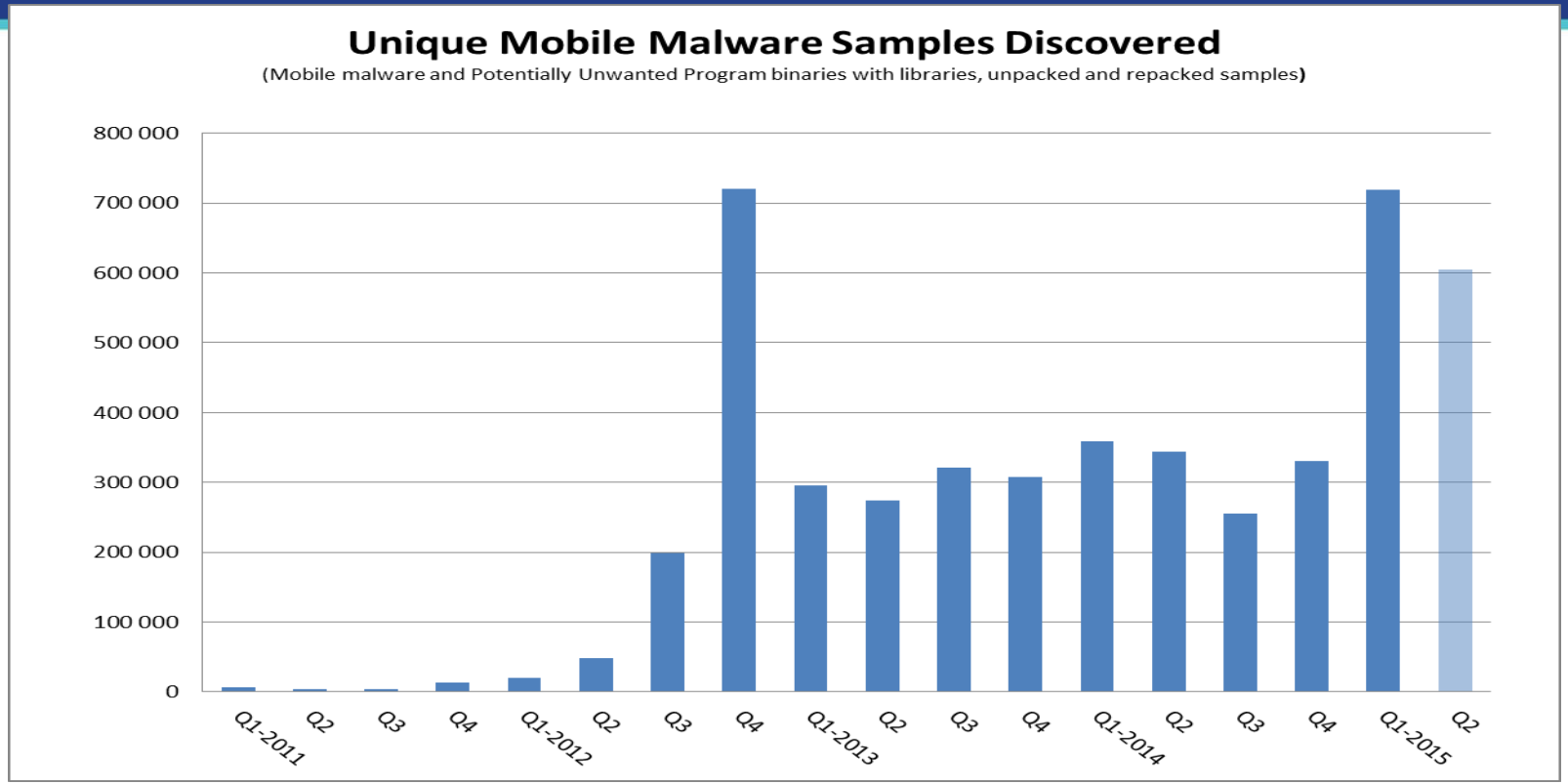
Connected Devices (IoT)

*Will represent 24 Billion

Global Malware Vision

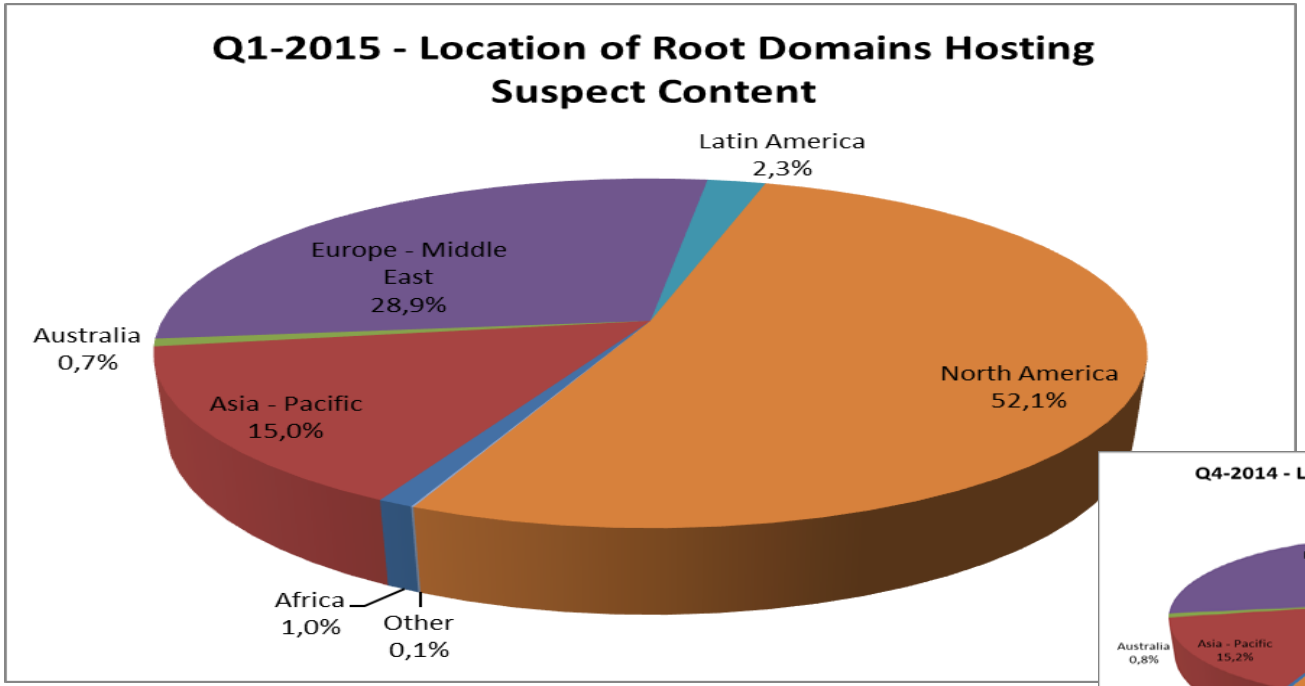
(Collection) "The Zoo"	End of 2012 (cumulative)	End of 2013 (cumulative)	End of 2014 (cumulative)	Added in				
				Q3-2014	Q4-2014	Q1-2015	April 2015	MAR-2015 / APR-2015
Malware Zoo	113,000,000	196,000,000	350,000,000	+40,000,000	+51,000,000	+48,000,000	+17,000,000	↑ (**)
Autorun	5,300,000	8,400,000	14,500,000	+1,800,000	+2,000,000	+1,600,000	+665,000	→
Exploits	3,600,000	6,900,000	9,400,000	+853,000	+672,000	+365,000	+116,000	→
FakeAV	8,500,000	10,400,000	11,100,000	+124,000	+85,000	+155,000	+28,000	↘
Virtual Money	7,200	26,000	46,000	+3,400	+3,700	+5,600	+1,000	↘
Macintosh	3,400	4,600	9,600	+1,500	+2,700	+20,000	+3,300	↘
Mobile (*)	1,000,000	2,200,000	3,500,000	+256,000	+331,000	+719,000	+242,000	→
PWS & Keyloggers	17,800,000	25,800,000	34,200,000	+2,300,000	+2,300,000	+2,600,000	+540,000	↓ ↓
Ransomware	493,000	1,600,000	2,300,000	+105,000	+272,000	+749,000	+103,000	↓ ↓
Rootkits	1,600,000	1,700,000	2,000,000	+35,000	+42,000	+40,000	+28,000	↗
Unix Like	40,000	51,000	61,000	+2,400	+3,400	+3,900	+1,300	↗

Mobile Detection

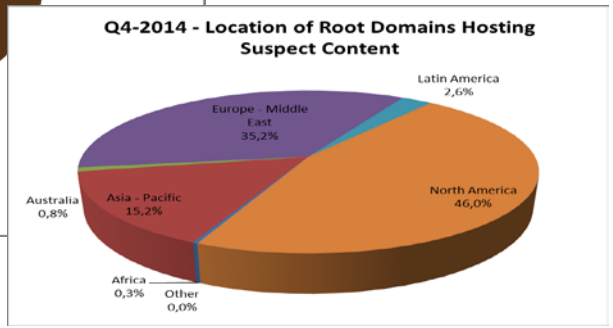


Web Threats

Location of servers hosting suspect content

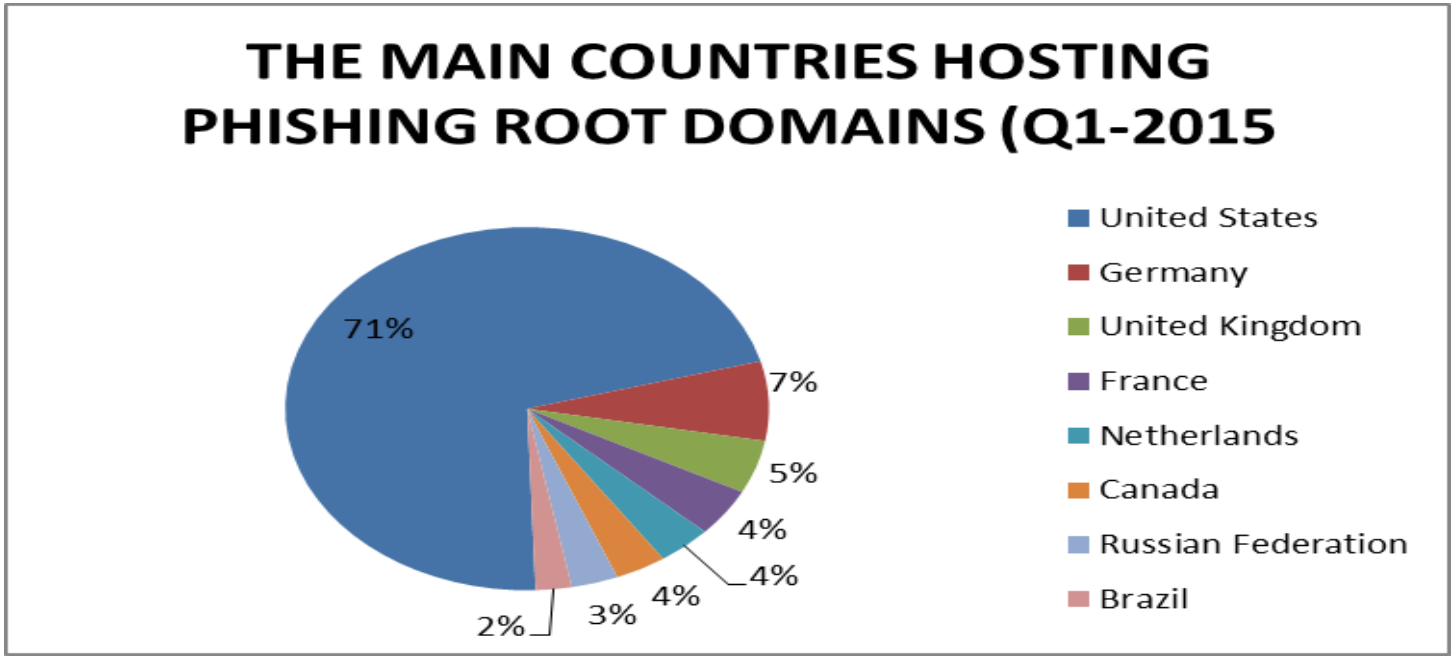


These charts are updated on a quarterly basis.



Web Threats

Top countries hosting phishing domains

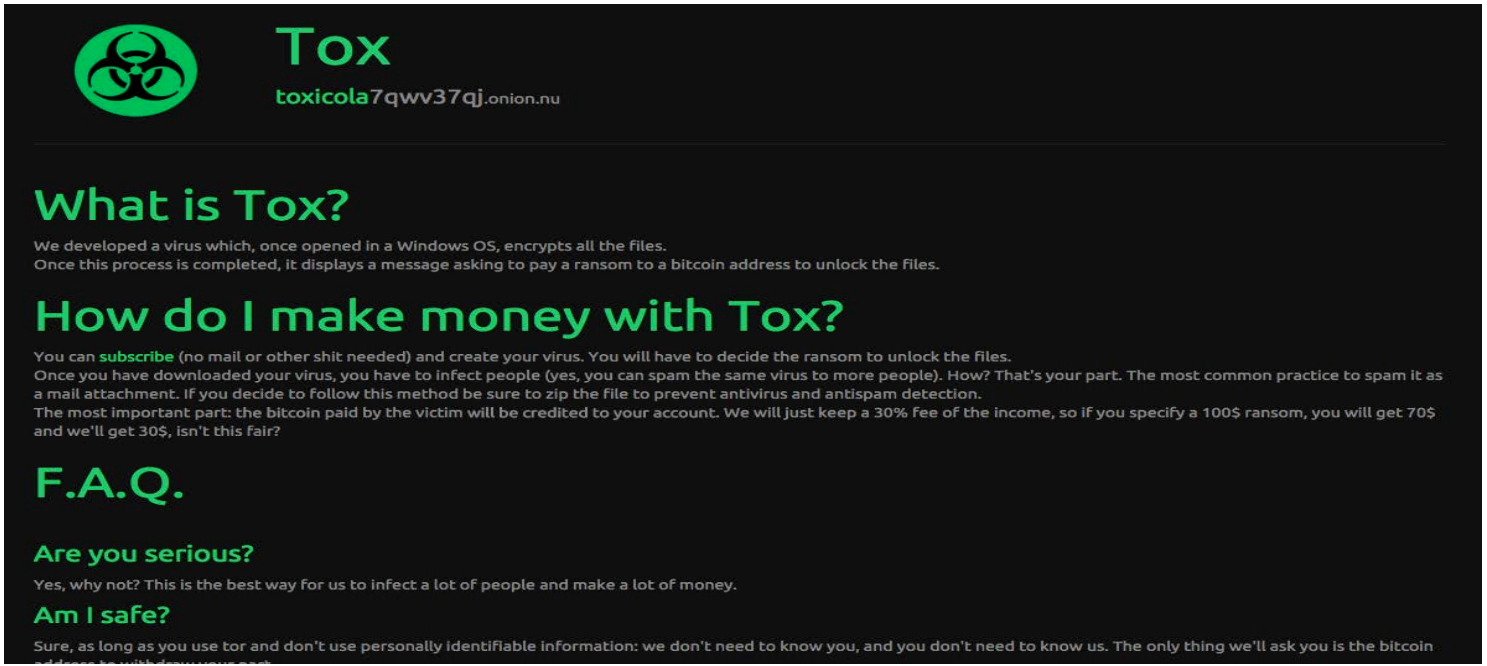


These charts are updated on a quarterly basis.

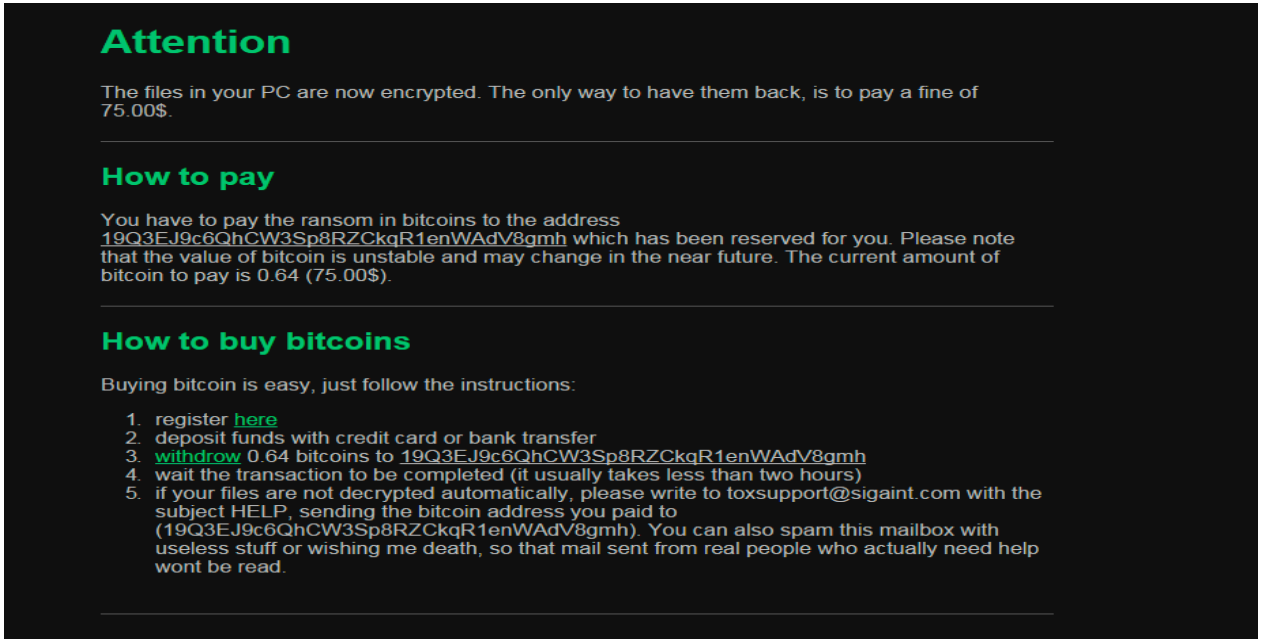

Tox - Viruses
toxicola7qwv37qj.onion


Create a virus
Ransom - $
Ransom in dollars (min. 50)
Notes

Meet “Tox”


Tox
toxicola7qwv37qj.onion.nu
What is Tox?
We developed a virus which, once opened in a Windows OS, encrypts all the files.
Once this process is completed, it displays a message asking to pay a ransom to a bitcoin address to unlock the files.
How do I make money with Tox?
You can subscribe (no mail or other shit needed) and create your virus. You will have to decide the ransom to unlock the files.
Once you have downloaded your virus, you have to infect people (yes, you can spam the same virus to more people). How? That's your part. The most common practice to spam it as a mail attachment. If you decide to follow this method be sure to zip the file to prevent antivirus and antispam detection.
The most important part: the bitcoin paid by the victim will be credited to your account. We will just keep a 30% fee of the income, so if you specify a 100$ ransom, you will get 70$ and we'll get 30$, isn't this fair?
F.A.Q.
Are you serious?
Yes, why not? This is the best way for us to infect a lot of people and make a lot of money.
Am I safe?
Sure, as long as you use tor and don't use personally identifiable information: we don't need to know you, and you don't need to know us. The only thing we'll ask you is the bitcoin

Meet “Tox”


Attention
The files in your PC are now encrypted. The only way to have them back, is to pay a fine of 75.00$.
How to pay
You have to pay the ransom in bitcoins to the address 19Q3EJ9c6QhCW3Sp8RZCkqR1enWAdV8gmh which has been reserved for you. Please note that the value of bitcoin is unstable and may change in the near future. The current amount of bitcoin to pay is 0.64 (75.00$).
How to buy bitcoins
Buying bitcoin is easy, just follow the instructions:
1. register here
2. deposit funds with credit card or bank transfer
3. withdrow 0.64 bitcoins to 19Q3EJ9c6QhCW3Sp8RZCkqR1enWAdV8gmh
4. wait the transaction to be completed (it usually takes less than two hours)
5. if your files are not decrypted automatically, please write to toxsupport@sigaint.com with the subject HELP, sending the bitcoin address you paid to (19Q3EJ9c6QhCW3Sp8RZCkqR1enWAdV8gmh). You can also spam this mailbox with useless stuff or wishing me death, so that mail sent from real people who actually need help wont be read.

Around the world

US Police Department paid the ransom

Lincoln County Sheriff Todd Brackett said four towns and the county have a special computer network to share files and records. Someone accidentally downloaded a virus, called "megacode", that put an encryption code on all the computer data.
The Sheriff said it basically made the system unusable, until they paid a ransom fee of about $300 to the creator of the virus. After the fee was received, the department was given a special code to unlock the encryption and restore the files.

The Sheriff and Damariscotta Police Chief Ron Young said no one liked having to pay off the bad guy, but it was the only way to get their information back.

"We needed our programs to get back online," said Young, "and that was a choice we all discussed and took to get back on line to get our information."

Source: http://www.wcsh6.com/story/news/local/2015/04/10/police-departments-hit-by-ransomware-virus/25593777/

Attacks

National power grids hit by cyber terrorist onslaught

An analysis of federal energy records has revealed that parts of the US power grid are attacked online or in person every few days. This threat is now also looming over major cities outside the US such as London.

After analyzing federal data and surveying more than 50 electric utilities, USA Today described the power grid as vulnerable to a major outage that could affect millions. Although a cyberattack has not yet caused a major loss of power, the mechanisms guarding the grid undergo small hacks multiple times a week. The Department of Homeland Security was alerted to 151 energy-related “cyber incidents” in 2013, up from 111 in 2012.

But, since 2013, the attacks have escalated hugely with probes now continuously taking place, according to the Edison Electric Institute."

A group of terrorist hackers located in Iran called Parastoo is already known to be actively recruiting software engineers with precisely those skills needed to bring down the power supply in a major city such as New York or London. Parastoo has already been linked to a military-style attack on an electric power station, the PG&E Metcalf substation in California on 16 April 2013. Parastoo now claims it has been testing national critical infrastructure using cyber vectors.

Source: http://www.itproportal.com/2015/04/07/cyber-terrorists-target-national-power-grids/

Malware of Note

Trojan Laziok targets the energy sector

Symantec detected a Trojan.Laziok, which acts as a reconnaissance tool allowing the attackers to gather data about the compromised computers.

Between January and February, researchers observed a 'multi-staged, targeted attack campaign' against energy companies around the world, and the focus was on the Middle East Countries.
The attack started with spam emails from the moneytrans[.]eu domain, which acted as an open relay Simple Mail Transfer Protocol (SMTP) server. These mails included a malicious attachment that contained an exploit for the Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability (CVE-2012-0158).

Source: http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

APT, Precision Equals Power

Operation CozyDuke

CozyDuke (aka CozyBear, CozyCar or "Office Monkeys") is a precise attacker. Kaspersky Lab has observed signs of attacks against government organizations and commercial entities in the US, Germany, South Korea and Uzbekistan. In 2014, targets included the White House and the US Department of State, as believed.

The operation presents several interesting aspects

- extremely sensitive high profile victims and targets
- evolving crypto and anti-detection capabilities
- strong malware functional and structural similarities mating this toolset to early MiniDuke second stage components, along with more recent CosmicDuke and OnionDuke components

Source: https://securelist.com/blog/research/69731/the-cozyduke-apt/

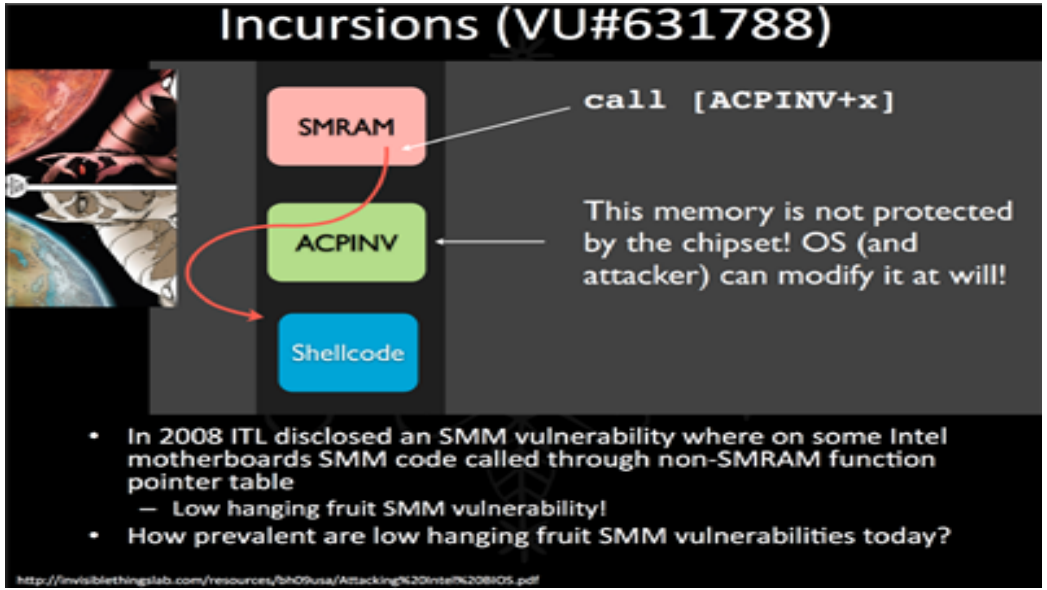
Around the world

Millions of flawed BIOSes can be infected

Millions of flawed BIOSes can be infected using simple two-minute attacks that don't require technical skills and require only access to a PC to execute.

Basic Input/Output Systems (BIOS) have been the target of much hacking research in recent years since low-level p0wnage can grant attackers the highest privileges, persistence and stealth.

LegbaCore researchers Xeno Kovah and Corey Kallenberg revealed the threat at CanSecWest.



Source: http://legbacore.com/Research_files/HowManyMillionBIOSWouldYouLikeToInfect_Full2.pdf

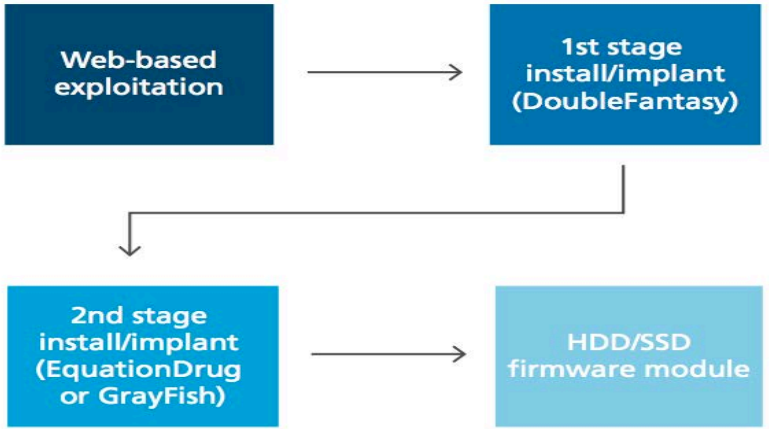
Real Advanced Threats

BIOS / Firmware / PDoS

The Equation Group: exploiting hard disk and solid state drive firmware

James Walter and Alexander Matrosov

Equation Group HDD/SSD Attack Steps



Real Advanced Threats

BIOS / Firmware / PDoS

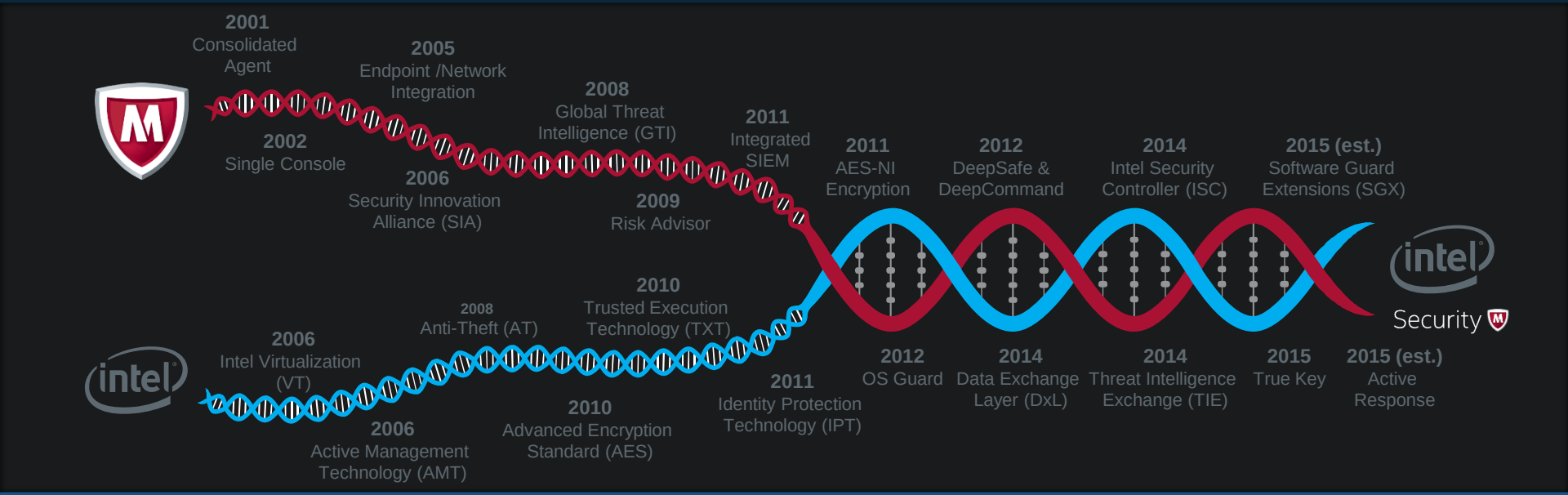
LightEater

- Because almost no one applies BIOS patches, almost every BIOS in the wild is affected by *at least* one vulnerability, and can be infected
- The high amount of code reuse across UEFI BIOSes means that BIOS infection is automatable and reliable

I am **not** *tense. Just terribly, terribly alert.*

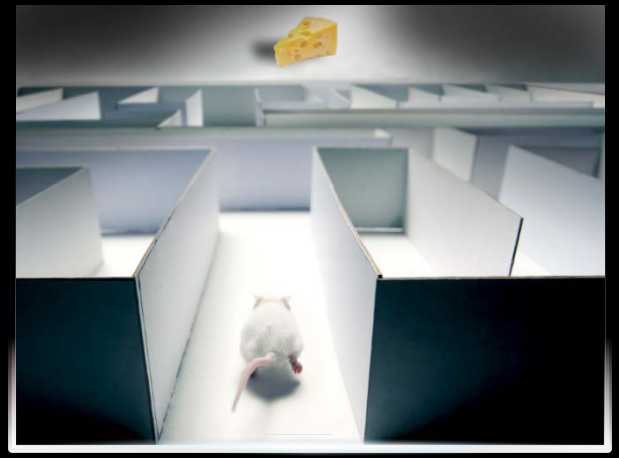
Innovating the Security Connected Concept

A Culture of Security Innovation



“Technological Evolution”

The Approach Must Change…



TRIAL & ERROR

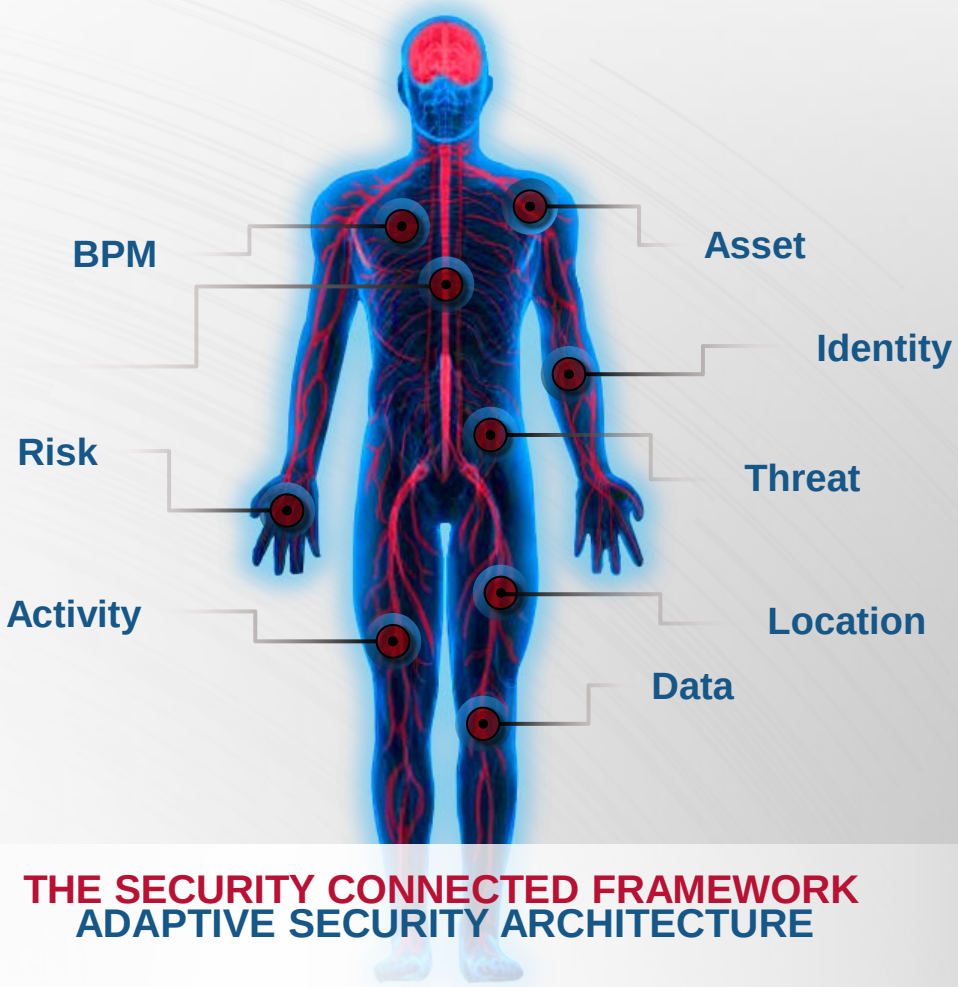
VS.

ORCHESTRATED DEFENSE

Data Exchange Layer

An innovative, real-time, bi-directional communications fabric providing with product integration simplicity.

Security components operate as one to **immediately share** relevant data between endpoint, gateway, and other security products enabling **security intelligence** and **adaptive security**.



THE SECURITY CONNECTED FRAMEWORK
ADAPTIVE SECURITY ARCHITECTURE

The Security Connected Experience

Security is About Outcomes, Not Features and Functions

PROTECT

your systems and data from exploits

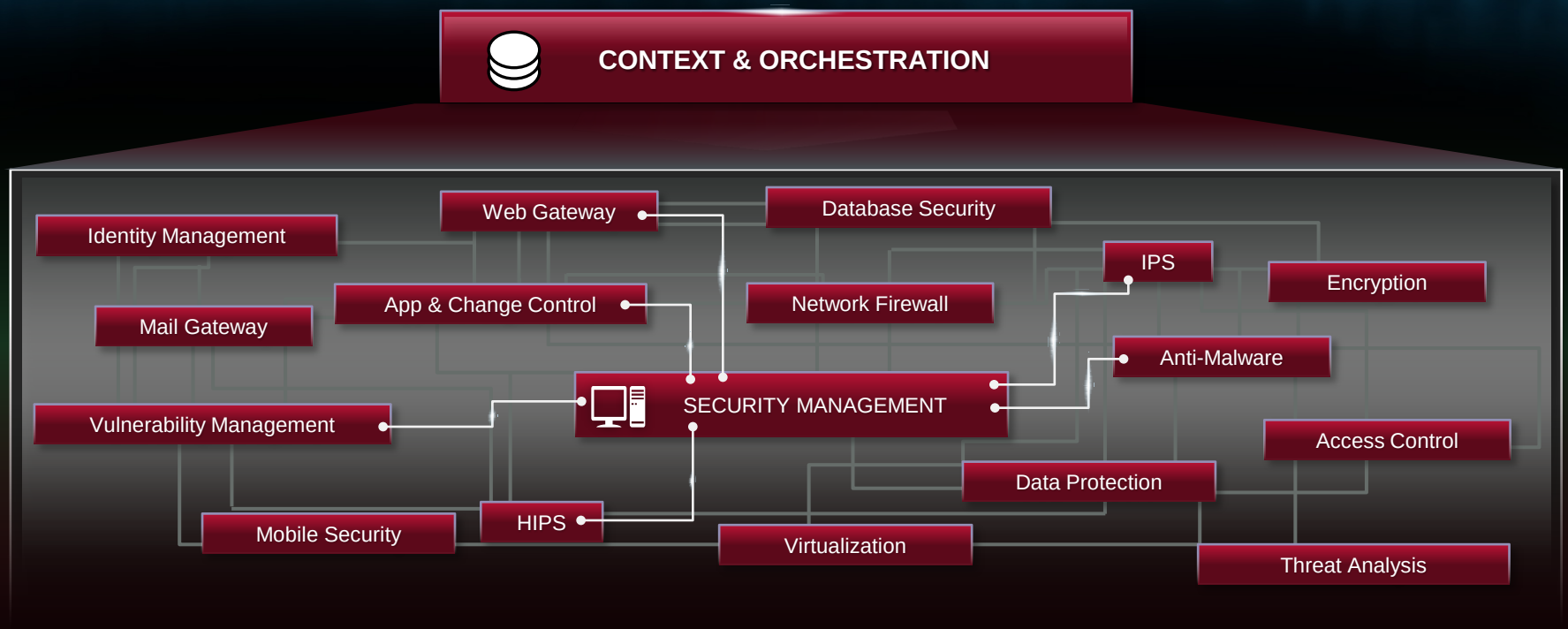
DETECT

exploits of your systems and data

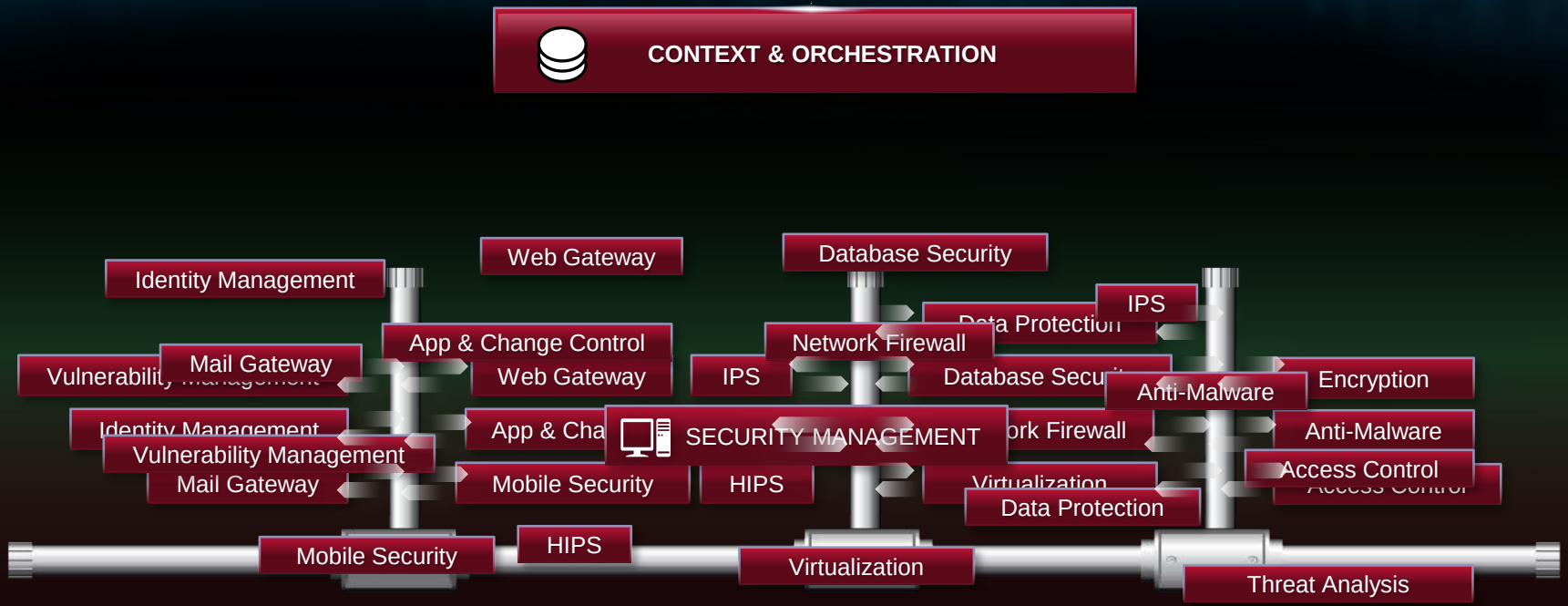
CORRECT

exploits, damage to systems, and lost or stolen data

The Need for Context & Orchestration



Data Exchange Layer



Data Exchange Layer

Delivering Real-Time Risk Mitigation

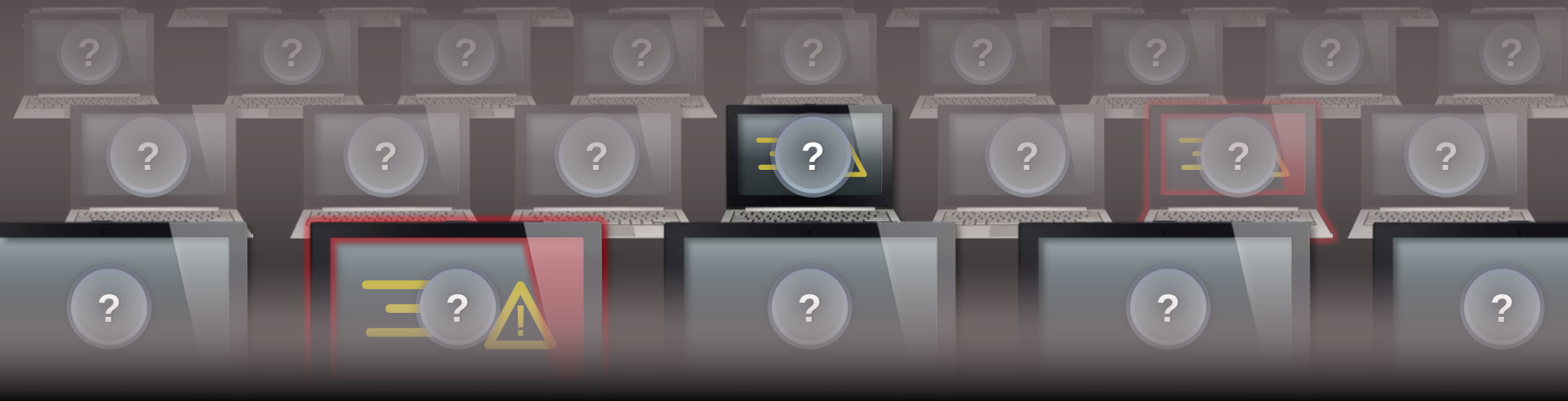
Unknown Event/Process

- System Alerts on New Event or Process
- File Offloaded For Inspection
- Hunt File Behavior In Environment
- Kill Malicious Processes

Advanced Threat Defense

File Attributes

- File Path
- Registry Keys
- DNS Lookups
- Network Sockets
- Process Chain

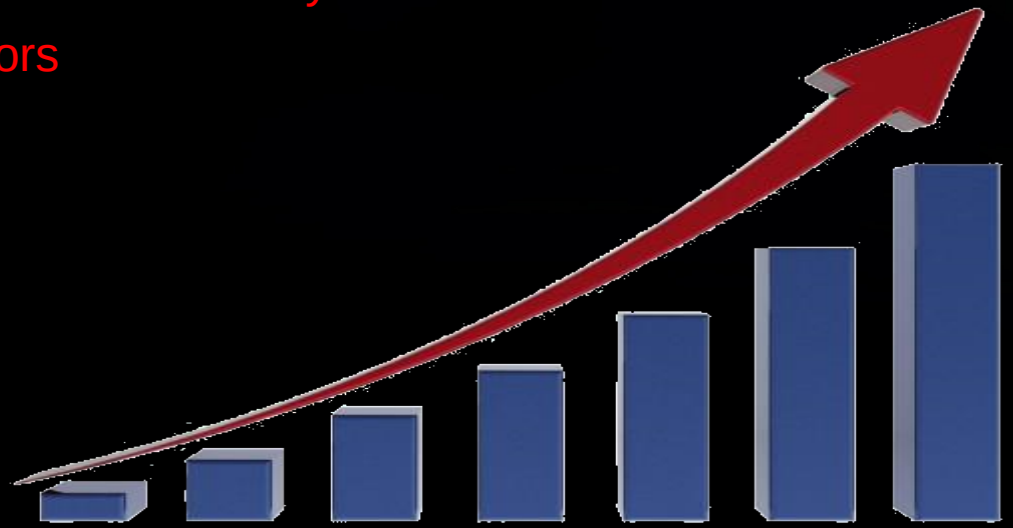


Common Language(s)

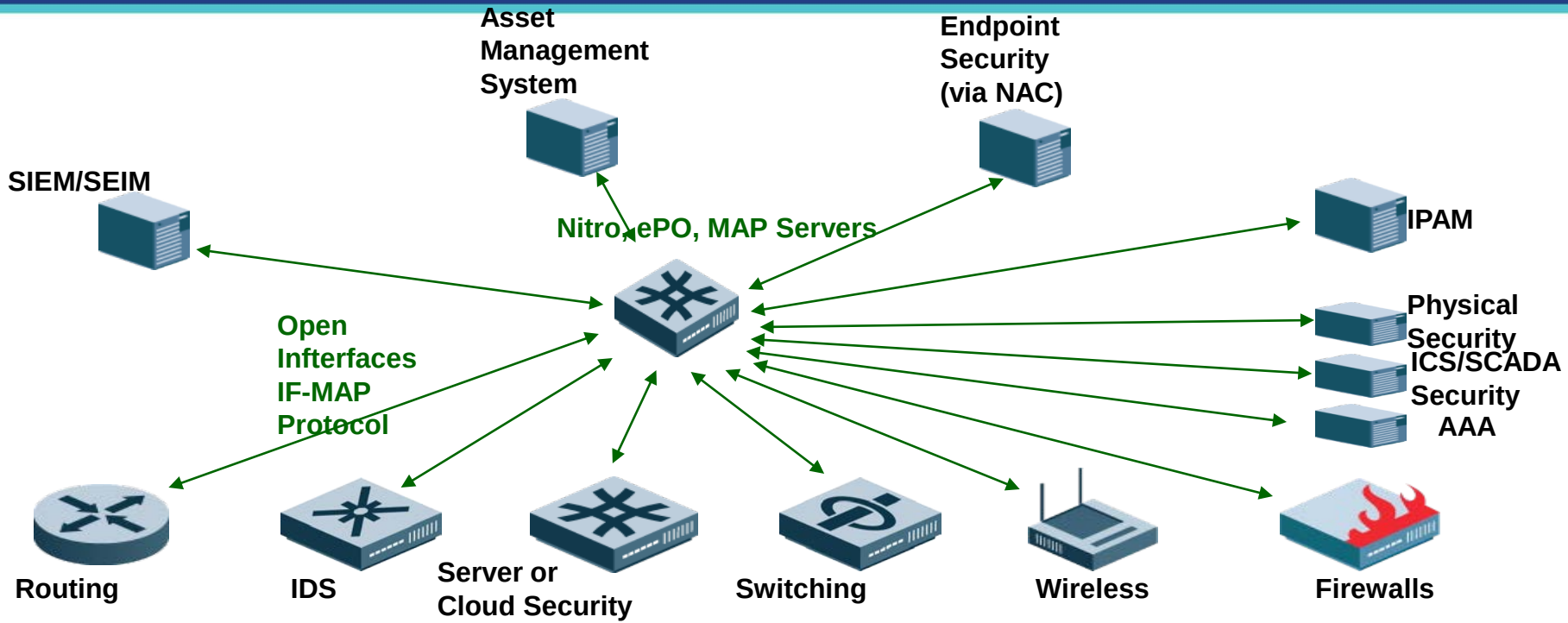
- MITRE has been working with Industry to develop common structures
  - STIX
  - CYBOX
  - TAXII
  - CAPEC
  - MAEC
  - OVAL
- Implementations are still immature but there is a gathering storm…
- Analysts must have a firm grasp of this entire space…

FS_ISAC MISSION:
Sharing Timely, Relevant, Actionable Cyber and Physical Security Information & Analysis

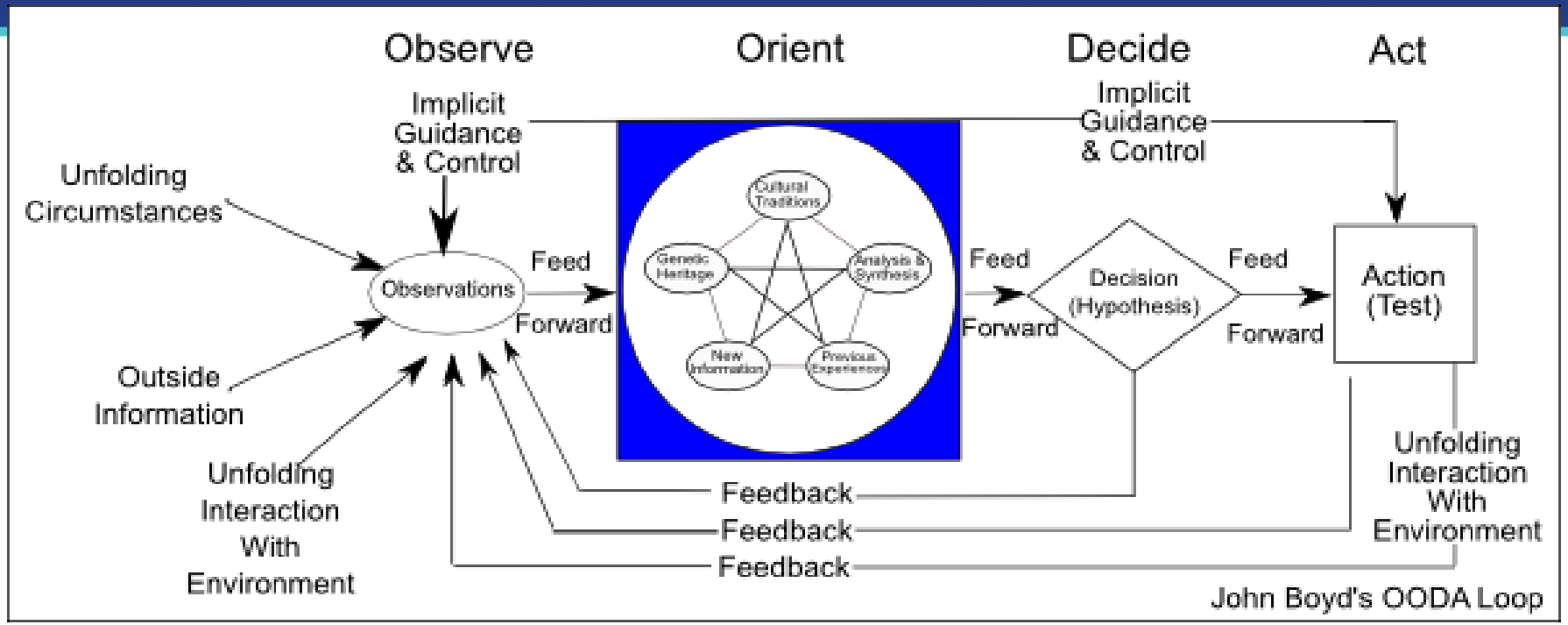
- A nonprofit private sector initiative formed in 1999
- Designed/developed/owned by financial services industry
- Assist to mitigate recent cybercrime & fraud activity
- Process thousands of threat indicators per month
- 2004: 68 members;
- 2014: 5,000+ members
- Sharing information globally



Coordinated Security : Pub/Sub Rules the New World



Iterative Real Time Loops – OODA Matters



The ability to make this world happen exists now…
It is not futures or fiction.


intel
Security