ACI Threat Trends and Predictions 2017 Report

-Mrs. Quincey Rhoades

-MAJ Jim Twist

“The expanding attack surface enabled by technology innovations such as cloud computing and IoT devices, a global shortage of cyber-security talent, and regulatory pressures continue to be significant drivers of cyber-threats. The pace of these changes is unprecedented, resulting in a critical tipping point as the impact of cyber-attacks are felt well beyond their intended victims in personal, political, and business consequences. Going forward, the need for accountability at multiple levels is urgent and real affecting vendors, governments, and consumers alike. Without swift action, there is a real risk of disrupting the progress of the global digital economy.”

– *Derek Manky, Global Security Strategist at Fortinet*

Most Compelling Predictions

Cloud Computing

- Ransomware will Attack the Cloud. (Symantec)
- The Cloud As an Expanding Attack Vector. (Forcepoint)

Defensive Cyberspace Operations

- Hacking for Political Leverage will Become Commonplace. (CSOonline)
- Nation state Cyber attacks will increase sharply resulting in escalating responses from the West. (Possibly War) (SC Magazine.com)
- Cyber Threats will attack soft underbelly of data centers by gaining control of physical infrastructure. (firewalls, routers, switches). (SCMagazine.com)

Malware

- Ransomworm. Ransomware with worm-like propagation capabilities. (Watchguard)
- Exploit Kits will give way to “Human Kits”. (Relying on social engineering to trick users to infect own machines). (Proofpoint)
- Automated phishing attacks Social Media Platforms. (Proofpoint).

Cyber Crime

- Rise of Autonomous Machine Hacking for Criminal Purposes (Forcepoint)
- Cars Will Be a Key Target for Hackers. (White Hat Security)
- Mobile Payments will Become a Liability. (Poor security combined with biometrics and financial data expand vulnerabilities). (CIO.com)
- Data Integrity Attacks Will Increase Dramatically. (Weaponization of Data). (SCMagazine.com)

Insider Threats

- Rise of the Corporate-Incentivized Insider Threat. (Forcepoint)

Others of Note

- Expect APTs to Target Religious Institutions. Low cyber security and high value PII. (Fireye)
- Privacy Deteriorates Rapidly with Increased Government Surveillance. (CSOonline)
- Companies will fight back. (Above Security).

Defensive Cyber Operations

Prediction: 3-5 years will see increased migration towards active defense.

Trend: Vulnerabilities in middleware

- software that serves as a bridge or connector between platforms or applications—are becoming more apparent, raising concerns that middleware is becoming a popular threat vector. (CISCO)

Trend: Operationalizing Cyber Threat Intelligence.

- For the purpose of strengthening baseline profile. (Cyber Hygiene)

Observation: Most companies use more than five security vendors and more than five security products in their environment.

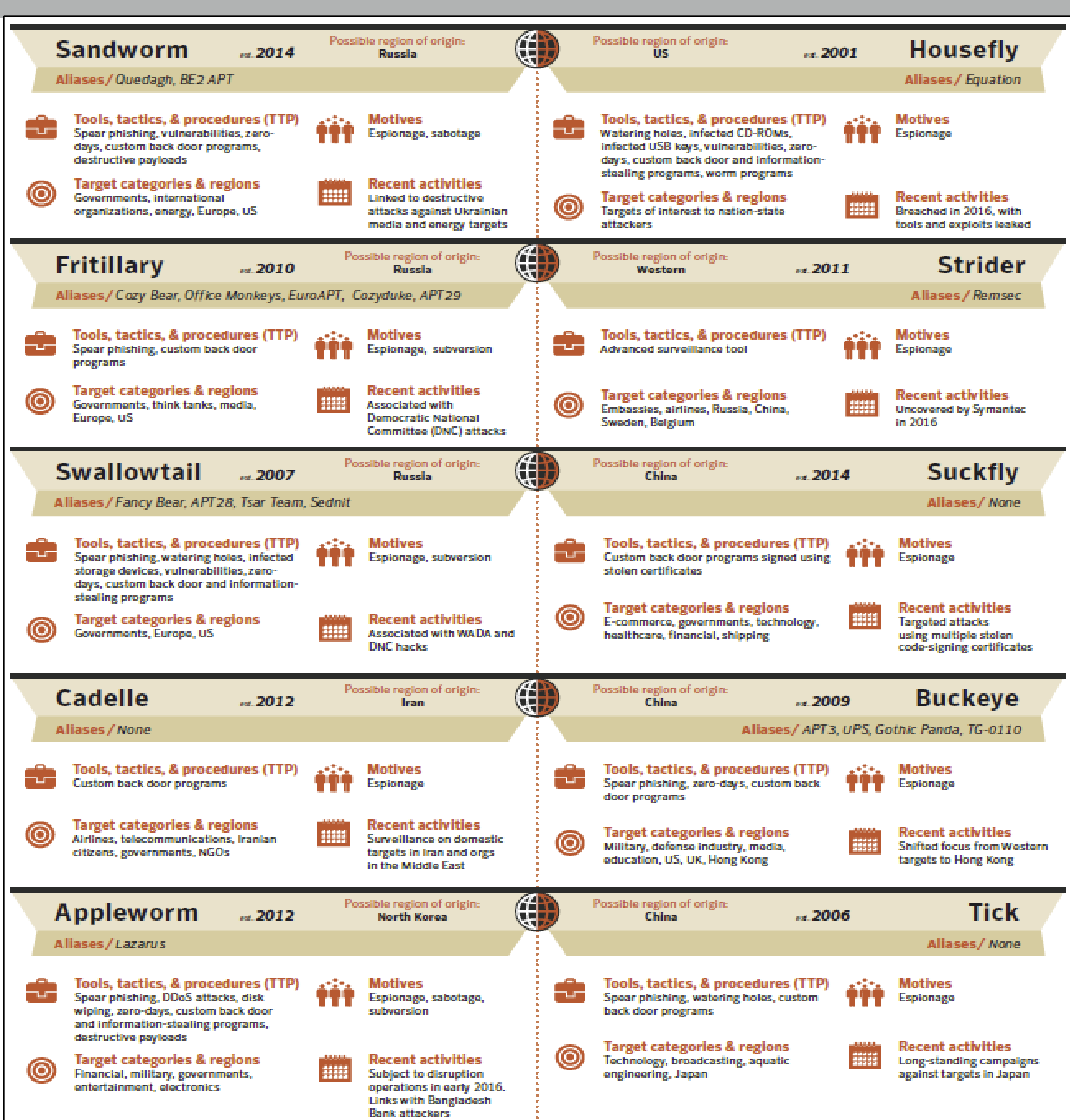
(CISCO, 2017 Annual Cybersecurity Report)

Observation: The Talent shortfall will continue and the cyber security industry will respond with more innovation in automation. (Fireye, pg. 5)

STATISTICS:

- Due to various constraints, organizations can investigate only 56 percent of the security alerts they receive on a given day. **Half of the investigated alerts (28 percent) are deemed legitimate; less than half (46 percent) of legitimate alerts are remediated.** In addition, 44 percent of security operations managers see more than 5000 security alerts per day. - Cisco 2017 Security Capabilities Benchmark Study

- **Security patches were not yet available for more than 30 percent of identified vulnerabilities** in SCADA-ICS environments. (Fireye, pg. 10)



Sandworm est. 2014
Possible region of origin: Russia
Aliases / *Quedagh, BE2 APT*
Tools, tactics, & procedures (TTP): Spear phishing, vulnerabilities, zero-days, custom back door programs, destructive payloads
Motives: Espionage, sabotage
Target categories & regions: Governments, international organizations, energy, Europe, US
Recent activities: Linked to destructive attacks against Ukrainian media and energy targets

Fritillary est. 2010
Possible region of origin: Russia
Aliases / *Cozy Bear, Office Monkeys, EuroAPT, Cozyduke, APT29*
Tools, tactics, & procedures (TTP): Spear phishing, custom back door programs
Motives: Espionage, subversion
Target categories & regions: Governments, think tanks, media, Europe, US
Recent activities: Associated with Democratic National Committee (DNC) attacks

Swallowtail est. 2007
Possible region of origin: Russia
Aliases / *Fancy Bear, APT28, Tsar Team, Sednit*
Tools, tactics, & procedures (TTP): Spear phishing, watering holes, infected storage devices, vulnerabilities, zero-days, custom back door and information-stealing programs
Motives: Espionage, subversion
Target categories & regions: Governments, Europe, US
Recent activities: Associated with WADA and DNC hacks

Cadelle est. 2012
Possible region of origin: Iran
Aliases / *None*
Tools, tactics, & procedures (TTP): Custom back door programs
Motives: Espionage
Target categories & regions: Airlines, telecommunications, Iranian citizens, governments, NGOs
Recent activities: Surveillance on domestic targets in Iran and orgs in the Middle East

Appleworm est. 2012
Possible region of origin: North Korea
Aliases / *Lazarus*
Tools, tactics, & procedures (TTP): Spear phishing, DDoS attacks, disk wiping, zero-days, custom back door and information-stealing programs, destructive payloads
Motives: Espionage, sabotage, subversion
Target categories & regions: Financial, military, governments, entertainment, electronics
Recent activities: Subject to disruption operations in early 2016. Links with Bangladesh Bank attackers

Housefly est. 2001
Possible region of origin: US
Aliases / *Equation*
Tools, tactics, & procedures (TTP): Watering holes, infected CD-ROMs, infected USB keys, vulnerabilities, zero-days, custom back door and information-stealing programs, worm programs
Motives: Espionage
Target categories & regions: Targets of interest to nation-state attackers
Recent activities: Breached in 2016, with tools and exploits leaked

Strider est. 2011
Possible region of origin: Western
Aliases / *Remsec*
Tools, tactics, & procedures (TTP): Advanced surveillance tool
Motives: Espionage
Target categories & regions: Embassies, airlines, Russia, China, Sweden, Belgium
Recent activities: Uncovered by Symantec in 2016

Suckfly est. 2014
Possible region of origin: China
Aliases / *None*
Tools, tactics, & procedures (TTP): Custom back door programs signed using stolen certificates
Motives: Espionage
Target categories & regions: E-commerce, governments, technology, healthcare, financial, shipping
Recent activities: Targeted attacks using multiple stolen code-signing certificates

Buckeye est. 2009
Possible region of origin: China
Aliases / *APT3, UPS, Gothic Panda, TG-0110*
Tools, tactics, & procedures (TTP): Spear phishing, zero-days, custom back door programs
Motives: Espionage
Target categories & regions: Military, defense industry, media, education, US, UK, Hong Kong
Recent activities: Shifted focus from Western targets to Hong Kong

Tick est. 2006
Possible region of origin: China
Aliases / *None*
Tools, tactics, & procedures (TTP): Spear phishing, watering holes, custom back door programs
Motives: Espionage
Target categories & regions: Technology, broadcasting, aquatic engineering, Japan
Recent activities: Long-standing campaigns against targets in Japan

Synmantec, Internet Security Threat Report, 2017, pg. 15

Offensive Cyberspace Operations

Prediction: Rise of Hypervisor Hacking.

- With governments moving to the Cloud, the underlying foundation that runs virtual machines there may be increasingly subject to attack. If a hypervisor gets compromised attackers will have full control of any and all systems running there. (Forcepoint, pg. 10)

Prediction: Government Sponsored Hacking of Politicians, Campaigns, and Elections.

- Expect more Wikileaks-style releases of embarrassing photos and corporate documents, through hacking of SS7 and diameter networks that will allow exploitation of mobile phone location and conversation data. Hacking will become a common technique for opposition research that will trickle down from the presidential election to House, Senate and state contests. The damage to public figures could range from embarrassment, like the hack of the Democratic National Committee, to physical danger from the use of location data to launch a physical attack. (CSOonline, 2017 Security Predictions)

Prediction: Open Season on Open Source.

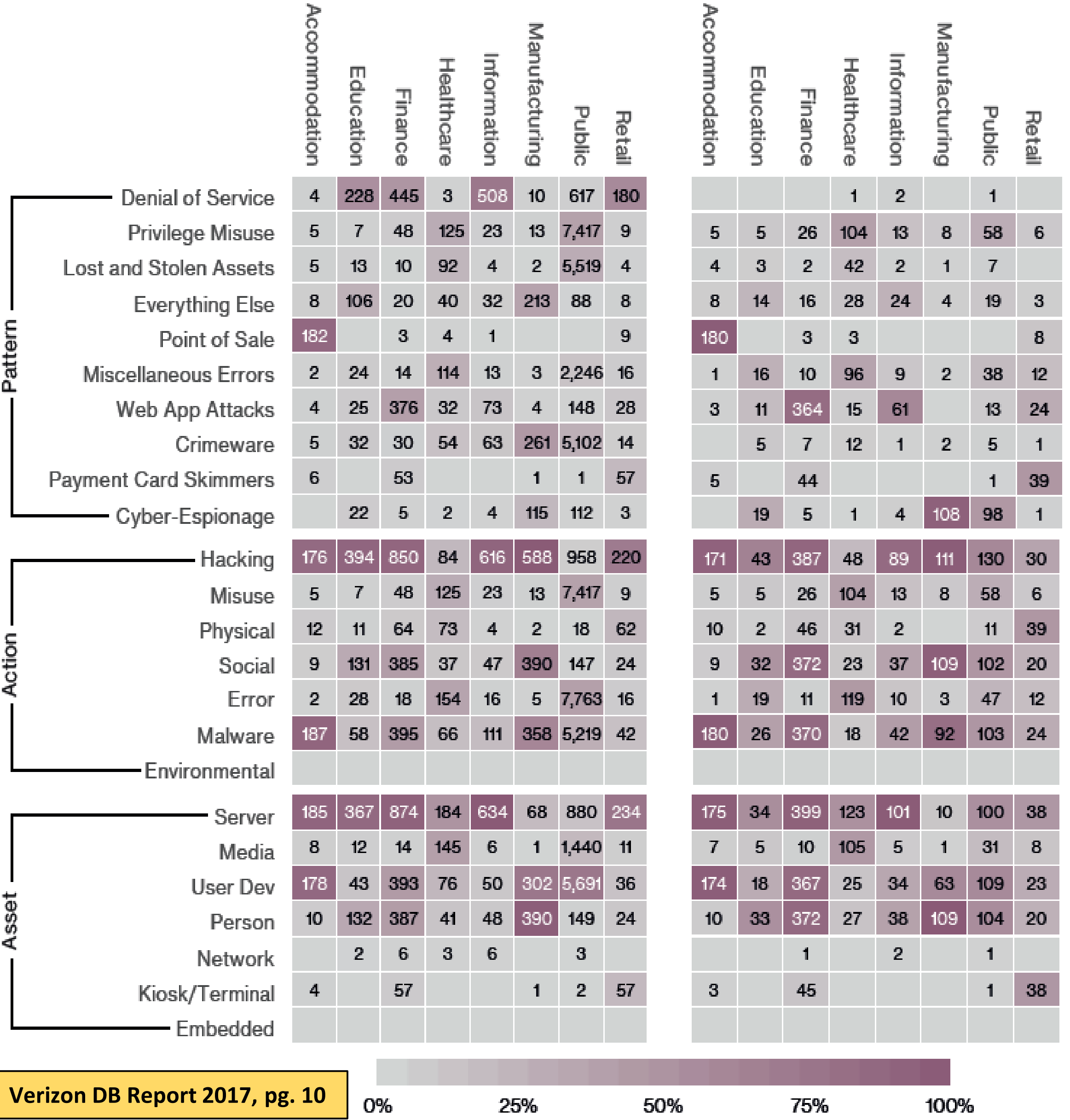
- Open source has become the foundation of global app development because it reduces developmen costs, promotes innovation, speeds time to market and increases productivity. But hackers have learned that applications are the weak spot in most organizations' cyber security defenses, and that companies are doing an abysmal job of securing and managing their code, even when patches are available. That means open-source vulnerability exploits deliver a high ROI. And those exploits will increase in 2017 against sites, applications, and IoT devices. (CSOonline, 2017 Security Predictions)

Prediction: Targeted Attacks.

- Cyber-attacks will be targeted against victims for maximum effect based on business cycle and an understanding of the business operations. (ie during holidays, Thanksgiving Weekend, and Cyber Monday, and Sales Events) (Akamai, 2017 Cybersecurity Report)

Prediction: High Profile Attack on U.S. Industrial Control Systems.

- Likely intent to encourage feelings of fear and insecurity in U.S. population. Targets are likely to be large-scale municipal systems, such as water or electric, or metropolitan transportation systems. Attack is likely to be organized by sophisticated state actors using a cover group (such as an Islamic extremist organization).



		Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail
Pattern	Denial of Service	4	228	445	3	508	10	617	180
	Privilege Misuse	5	7	48	125	23	13	7,417	9
	Lost and Stolen Assets	5	13	10	92	4	2	5,519	4
	Everything Else	8	106	20	40	32	213	88	8
	Point of Sale	182		3	4	1			9
	Miscellaneous Errors	2	24	14	114	13	3	2,246	16
	Web App Attacks	4	25	376	32	73	4	148	28
	Crimeware	5	32	30	54	63	261	5,102	14
	Payment Card Skimmers	6		53			1	1	57
	Cyber-Espionage		22	5	2	4	115	112	3
Action	Hacking	176	394	850	84	616	588	958	220
	Misuse	5	7	48	125	23	13	7,417	9
	Physical	12	11	64	73	4	2	18	62
	Social	9	131	385	37	47	390	147	24
	Error	2	28	18	154	16	5	7,763	16
	Malware	187	58	395	66	111	358	5,219	42
	Environmental								
Asset	Server	185	367	874	184	634	68	880	234
	Media	8	12	14	145	6	1	1,440	11
	User Dev	178	43	393	76	50	302	5,691	36
	Person	10	132	387	41	48	390	149	24
	Network		2	6	3	6		3	
	Kiosk/Terminal	4		57			1	2	57
	Embedded								

		Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail
Pattern	Denial of Service				1	2		1	
	Privilege Misuse	5	5	26	104	13	8	58	6
	Lost and Stolen Assets	4	3	2	42	2	1	7	
	Everything Else	8	14	16	28	24	4	19	3
	Point of Sale	180		3	3				8
	Miscellaneous Errors	1	16	10	96	9	2	38	12
	Web App Attacks	3	11	364	15	61		13	24
	Crimeware		5	7	12	1	2	5	1
	Payment Card Skimmers	5		44				1	39
	Cyber-Espionage		19	5	1	4	108	98	1
Action	Hacking	171	43	387	48	89	111	130	30
	Misuse	5	5	26	104	13	8	58	6
	Physical	10	2	46	31	2		11	39
	Social	9	32	372	23	37	109	102	20
	Error	1	19	11	119	10	3	47	12
	Malware	180	26	370	18	42	92	103	24
	Environmental								
Asset	Server	175	34	399	123	101	10	100	38
	Media	7	5	10	105	5	1	31	8
	User Dev	174	18	367	25	34	63	109	23
	Person	10	33	372	27	38	109	104	20
	Network			1		2		1	
	Kiosk/Terminal	3		45				1	38
	Embedded								

Verizon DB Report 2017, pg. 10

ARMY CYBER INSTITUTE

Internet of Things

Prediction: Vehicles Become High Value Targets.

Modern cars, typically containing more than 100 million lines of code, are increasingly intelligent, automated, and most importantly, Internet-connected. But carmakers don't know exactly what software is inside their vehicles because it comes from third parties and almost certainly contains open-source components with security vulnerabilities – a target-rich environment for hackers. (CSOonline).

Prediction: Expanding Pool of Attack Resources.

o An increase in internet-capable products will lead to an increase in vulnerabilities. Expect to see a rise in issues related to unsecured products. (Palo Alto Networks, 2017 Cybersecurity Predictions)

o Source code adaptation of Botnets (Mirai) will drive increased frequency of very large DDoS attacks.

(Akamai, 2016, Cybersecurity Report)

o Increased Penetration of IoT into Business Enterprises. (Symantec)

o Observation: LG (Life's Good) Industries presented idea at Consumer Electronics Show in Las Vegas that every device they build will have an IP address. This will generate competition at low end manufacturers to compete, generating new types of smart home appliances.

Prediction: Larger DDoS Attacks Will Become More Common.

o Seven DDoS attacks in greater than 300gps speeds occurred in 2016. (Akamai, 2017, Cybersecurity Report)

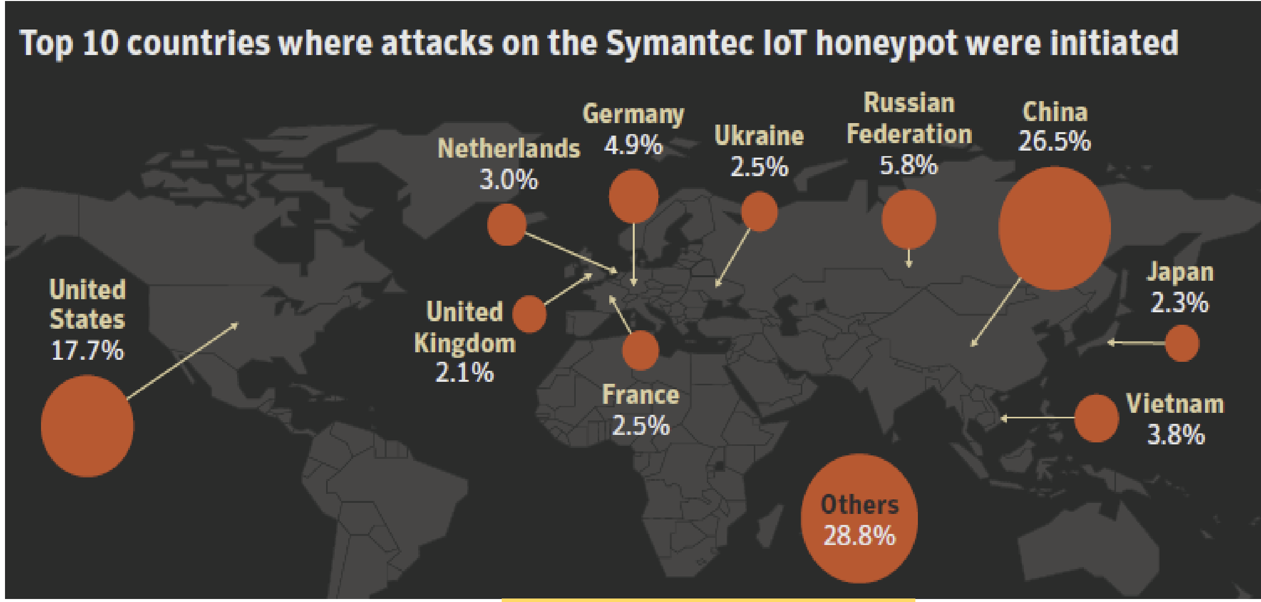
Prediction: Ransomware Attacks Against IoT

o Many concerns have arisen that Internet-connected devices will lend themselves to ransomware attacks, especially those controlling or connected to municipal agencies, such as water, power, nuclear, etc. Researchers are especially concerned about compromised security cameras:

o Potentially used to facilitate expanded access to an organization's networks, including physical address.

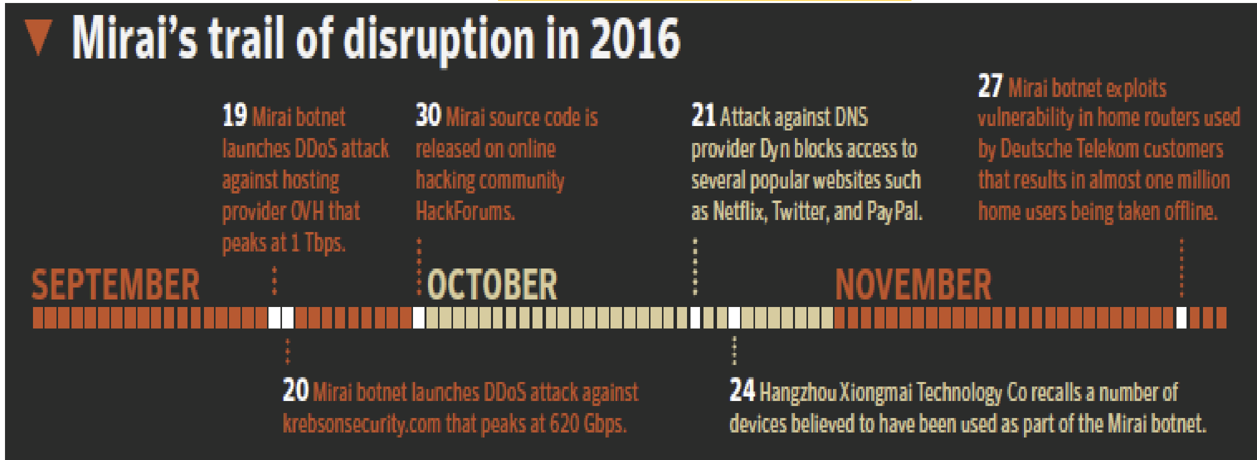
o Of special concern are strategically places cameras in banks, ATMs, Trade

o Malicious actors could built a trade in compromised IoT devices. (BoozAllenHamilton, 2017, Cyber4sights)


Top 10 countries where attacks on the Symantec IoT honeypot were initiated

Symantec, ISTR 2017, pg. 65

Symantec, ISTR 2017, pg. 67


Mirai's trail of disruption in 2016

19 Mirai botnet launches DDoS attack against hosting provider OVH that peaks at 1 Tbps.

20 Mirai botnet launches DDoS attack against krebsonsecurity.com that peaks at 620 Gbps.

30 Mirai source code is released on online hacking community HackForums.

21 Attack against DNS provider Dyn blocks access to several popular websites such as Netflix, Twitter, and PayPal.

24 Hangzhou Xiongmai Technology Co recalls a number of devices believed to have been used as part of the Mirai botnet.

27 Mirai botnet exploits vulnerability in home routers used by Deutsche Telekom customers that results in almost one million home users being taken offline.

Cyber Crime

Prediction: Autonomous Machine Hacking for Crime.

- Automated—and autonomous—hacking machines designed to rapidly seek out vulnerabilities and potential breaches in networks are here. The capabilities of AI cyber defense machines to search, surface, interpret and remediate attacks and potential breaches far outpaces human Security Operations (SecOps) teams' abilities. (Forcepoint, pg. 12)

Prediction: Crimeware as a Service Generates Script Kiddie Explosion.

- Rookie hacktivists and hobby hackers, driven by pop-culture references and increased media attention, will increasingly get into the cybercrime game. They will use off-the-shelf tools for nuisance attacks like web defacement and port scans, plus more damaging attacks through DDoS as a service and Ransomware as a Service (RaaS). While these adversaries won't have the skills for lateral movement, their attacks could be costly and cause reputational damage to the company brand. (HP Enterprise.)

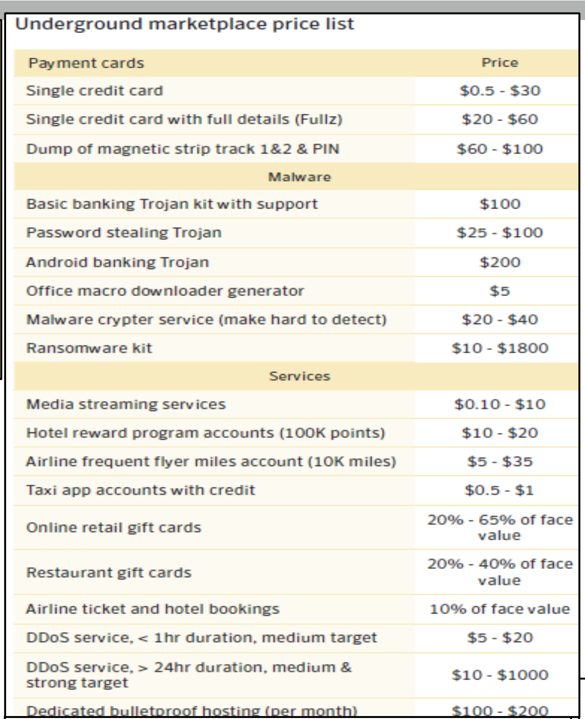
Trend: Business Email Compromise.

- BEC, specifically CEO fraud, a more attractive mode of attack for cybercriminals. The scam is easy and cost-effective. The average payout for a successful BEC attack is US$140,000. The total estimated loss from BEC in two years is US$3 billion. In comparison, the average payout for a ransomware attack is US$722 (currently 1 Bitcoin), which could reach up to US $30,000 if an enterprise network is hit. (Trend Micro)

Trend: Business Process Compromise.

- BPC fund transfers will remain its most typical endgame. Possible scenarios include hacking into a purchase order system so cybercriminals can receive payment intended for actual vendors. Hacking into a payment delivery system can likewise lead to unauthorized fund transfers. Cybercriminals can hack into a delivery center and reroute valuable goods to a different address. This already happened in an isolated incident in 2013, where the Antwerp Seaport shipping container system was hacked in order to smuggle drugs. (Trend Micro)

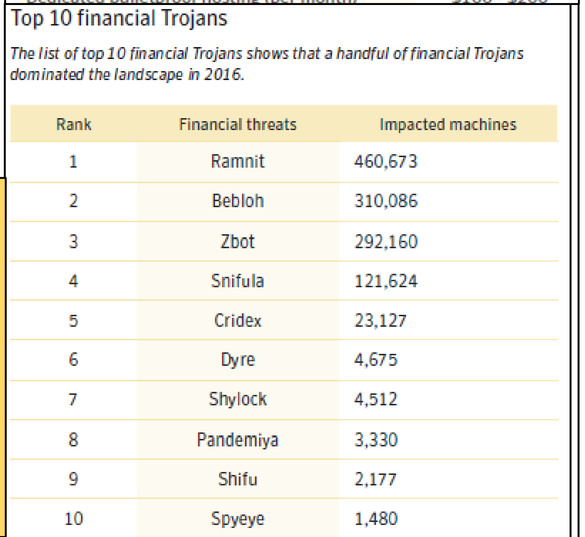
Symantec, ISTR, 2017, pg. 51



Underground marketplace price list

Payment cards	Price
Single credit card	$0.5 - $30
Single credit card with full details (Fullz)	$20 - $60
Dump of magnetic strip track 1&2 & PIN	$60 - $100
Malware	
Basic banking Trojan kit with support	$100
Password stealing Trojan	$25 - $100
Android banking Trojan	$200
Office macro downloader generator	$5
Malware crypter service (make hard to detect)	$20 - $40
Ransomware kit	$10 - $1800
Services	
Media streaming services	$0.10 - $10
Hotel reward program accounts (100K points)	$10 - $20
Airline frequent flyer miles account (10K miles)	$5 - $35
Taxi app accounts with credit	$0.5 - $1
Online retail gift cards	20% - 65% of face value
Restaurant gift cards	20% - 40% of face value
Airline ticket and hotel bookings	10% of face value
DDoS service, < 1hr duration, medium target	$5 - $20
DDoS service, > 24hr duration, medium & strong target	$10 - $1000
Dedicated bulletproof hosting (per month)	$100 - $200

Symantec, ISTR, 2017, pg. 42

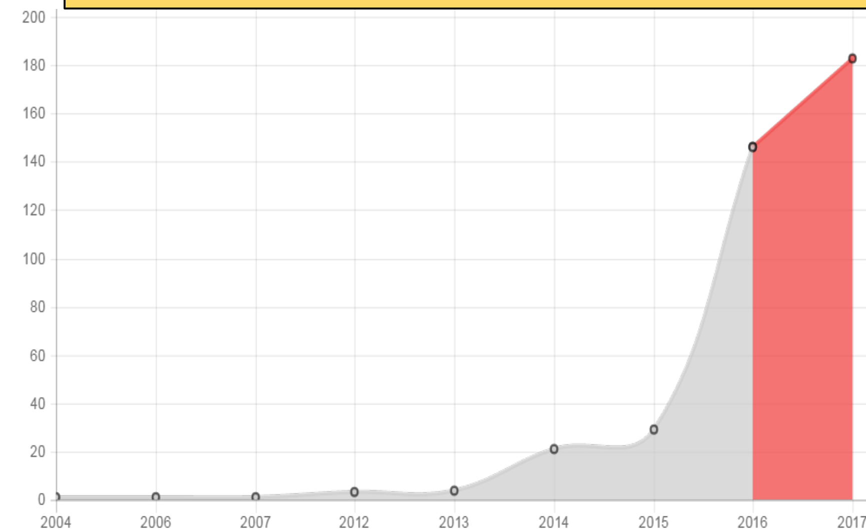


Top 10 financial Trojans

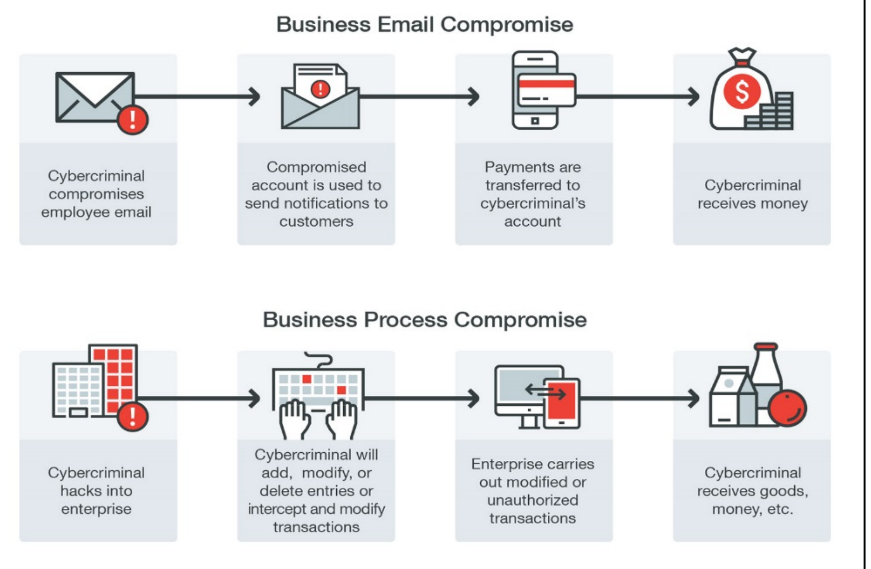
The list of top 10 financial Trojans shows that a handful of financial Trojans dominated the landscape in 2016.

Rank	Financial threats	Impacted machines
1	Ramnit	460,673
2	Bebloh	310,086
3	Zbot	292,160
4	Snifula	121,624
5	Cridex	23,127
6	Dyre	4,675
7	Shylock	4,512
8	Pandemiya	3,330
9	Shifu	2,177
10	Spyeye	1,480

Trend Micro: Annual #of ransomware families, with 2017 projection



Trend Micro: BEC Vs. BPC Process Comparison



Business Email Compromise

Cybercriminal compromises employee email → Compromised account is used to send notifications to customers → Payments are transferred to cybercriminal's account → Cybercriminal receives money

Business Process Compromise

Cybercriminal hacks into enterprise → Cybercriminal will add, modify, or delete entries or intercept and modify transactions → Enterprise carries out modified or unauthorized transactions → Cybercriminal receives goods, money, etc.

ARMY CYBER INSTITUTE

Data Breaches

Prediction: More World Changing Leaks.

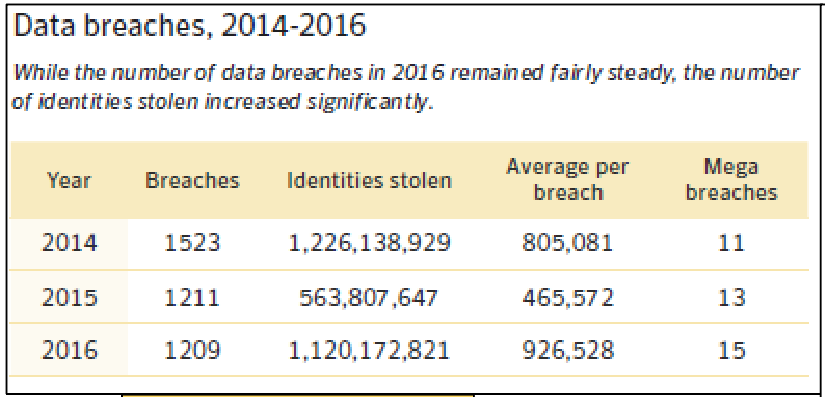
Events such as Panama Papers, DNC, and Yahoo had an unmistakable world wide impact. Expect this trend to continue. (IBM X-Force, Threat Index 2017, pg. 5)

Trend: Lost Business Opportunities.

Nearly a quarter of the organizations that have suffered an attack lost business opportunities. Four in 10 said those losses are substantial. One in five organizations lost customers due to an attack, and nearly 30 percent lost revenue. (Cisco 2017 Security Capabilities Benchmark Study)

STATISTIC: **The average price of a data breach now stands at $4 Million**. (BMC, Re-engineering Security, 2017)

Symantec, ISTR 2017, pg. 45

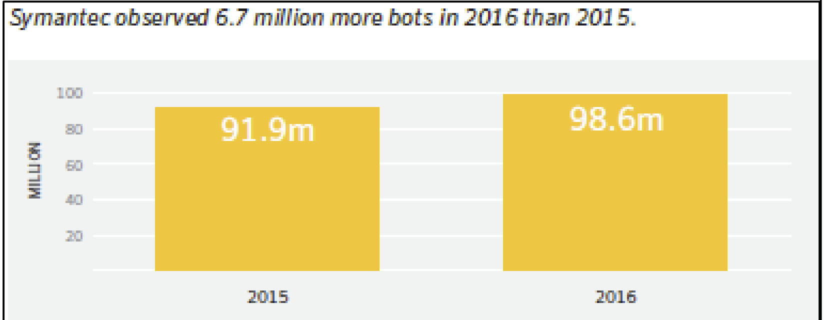


Data breaches, 2014-2016

While the number of data breaches in 2016 remained fairly steady, the number of identities stolen increased significantly.

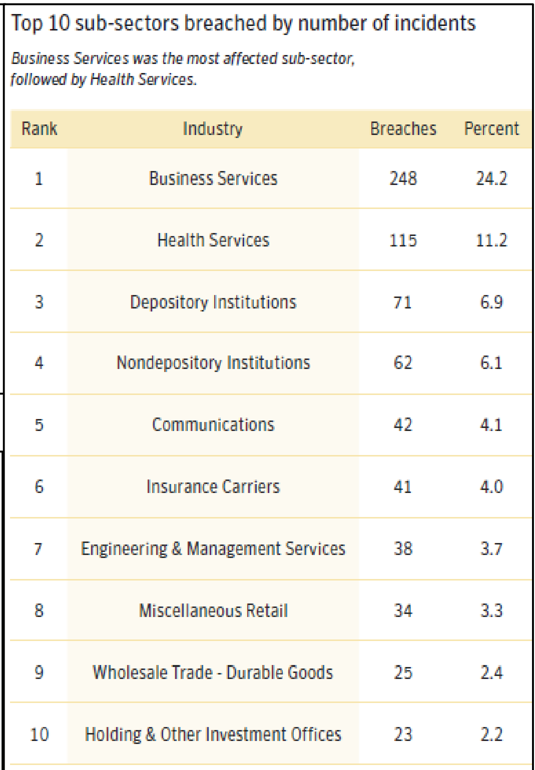
Year	Breaches	Identities stolen	Average per breach	Mega breaches
2014	1523	1,226,138,929	805,081	11
2015	1211	563,807,647	465,572	13
2016	1209	1,120,172,821	926,528	15

Symantec, ISTR 2017, pg. 41



Symantec observed 6.7 million more bots in 2016 than 2015.

Symantec, ISTR 2017, pg. 48

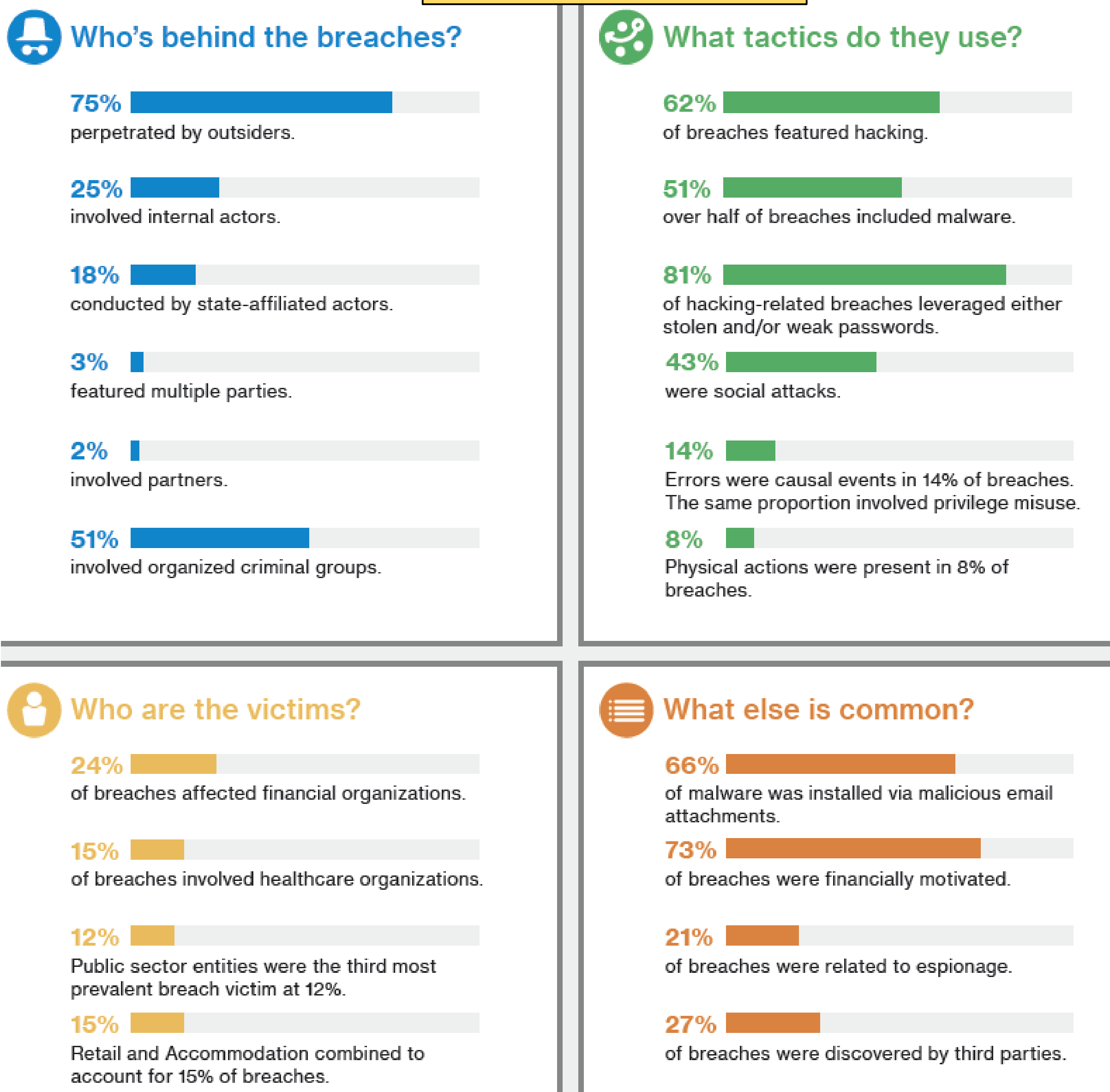


Top 10 sub-sectors breached by number of incidents

Business Services was the most affected sub-sector, followed by Health Services.

Rank	Industry	Breaches	Percent
1	Business Services	248	24.2
2	Health Services	115	11.2
3	Depository Institutions	71	6.9
4	Nondepository Institutions	62	6.1
5	Communications	42	4.1
6	Insurance Carriers	41	4.0
7	Engineering & Management Services	38	3.7
8	Miscellaneous Retail	34	3.3
9	Wholesale Trade - Durable Goods	25	2.4
10	Holding & Other Investment Offices	23	2.2

Verizon Data Breach Report, 2017



Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

21% of breaches were related to espionage.

27% of breaches were discovered by third parties.

ARMY CYBER INSTITUTE

Cyber Espionage

RUSSIA

- o FANCY BEAR AND COZY BEAR
  - oSeparately working at nation-state capability and engaged in political espionage of DNC and previously infiltrated White House, State Department, and others
  - oBoth groups have ties to Russian government, and are likely engaging in political and economic espionage for Russian Intelligence
  - oSpear phishing is a commonly relied-upon technique, especially for COZY BEAR
  - oFANCY BEAR is known to establish phishing sites on registered domains that resemble other, legitimate domains they plan to target.
  - o Cyber espionage will increase in private sector and criminal underworld.

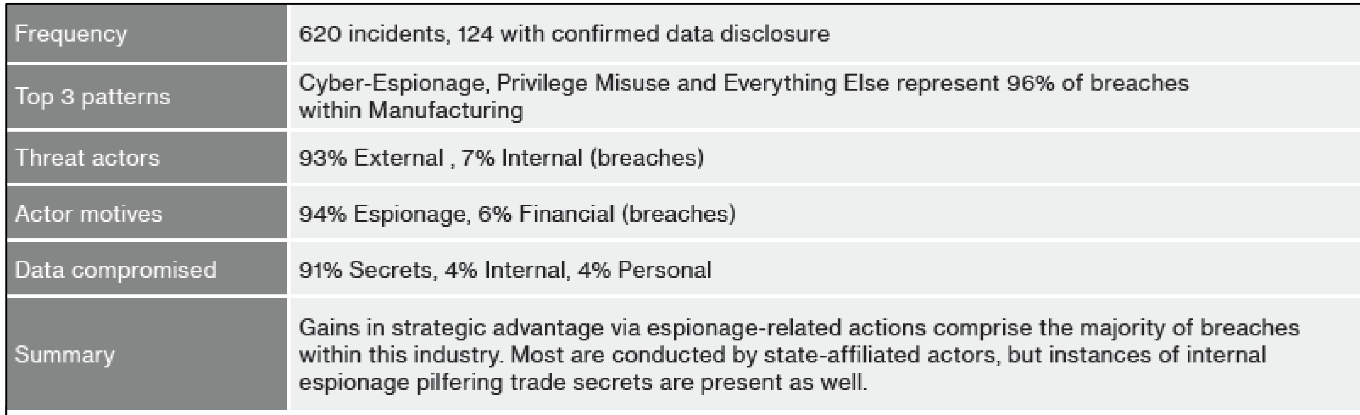
CHINA.

- o Expect economic espionage against U.S. and Western targets to rebound and increase
- o China will target cutting-edge industrial manufacturers, e-commerce, mobile, and IT companies

European Elections.

- o EU should expect foreign influence in upcoming elections
- o Cyber experts should be prepared to share information across EU to combat misinformation and disinformation
- o Declare political figures and organizations as critical infrastructure for defense
- o Hacktivists may violate privacy laws to expose individual information or business information

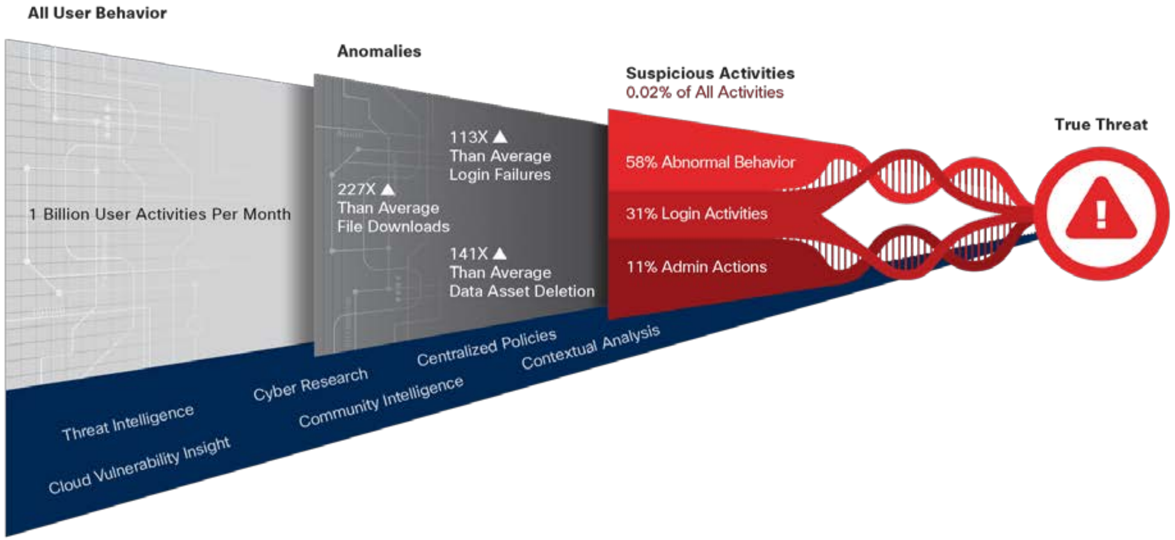
Snapshot of U.S. Manufacturing Sector: Verizon DB Report, 2017, pg. 26



Frequency	620 incidents, 124 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Privilege Misuse and Everything Else represent 96% of breaches within Manufacturing
Threat actors	93% External , 7% Internal (breaches)
Actor motives	94% Espionage, 6% Financial (breaches)
Data compromised	91% Secrets, 4% Internal, 4% Personal
Summary	Gains in strategic advantage via espionage-related actions comprise the majority of breaches within this industry. Most are conducted by state-affiliated actors, but instances of internal espionage pilfering trade secrets are present as well.

Figure 9 Identifying User Behavior Patterns with Automation (Process)

Source: Cisco CloudLock



For more info visit: www.cisco.com/go/acr2017

CISCO: Annual Cybersecurity Report, 2017

Malware

Increased Stealth.

o Expect attackers to continue making their malware more stealthy and effective. For example, threat actors are hiding malicious code in unused sectors, and maliciously modifying master file tables (MFT) and volume boot records (VBR) to load malware before security software loads is becoming more prevalent. (Fireye, pg. 14)

oFile less Malware will Increase in Frequency. (Symantec)

oMalware and Money

- o E-commerce-focused malware will be developed over POS malware
- oCompromised EMV cards will be increasingly difficult to use

Ransomware

o (Trend) Ransomware attacks have been steadily increasing in enterprising environments

Doxware

oVictims are locked out of computers, and a ransom is demanded; if unpaid, doxware threatens to expose user's personal data

oMobile devices could be particularly vulnerable

oPreventative measures: training employees to recognize malicious email, utilizing anti-virus packages, maintaining regular system back-ups.

Key Ransomware Developments in 2016 (VZ DV Report, 2017, pg. 36)

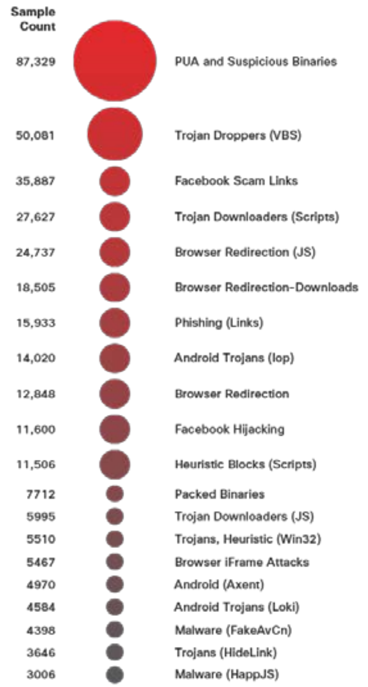
- Master boot record locking
- Full disk encryption
- Execution time differences between real and virtual machines.
- Extensive use of exploit kits (Angler, Neutrino, RIG)
- Ransomware as a service.
- Point and Pwn Tools for Non –expert criminals.

Nomoreransom.org

57+ members host 27 decryption tools which can recover from a wide range of ransomware families.

Figure 2 Most Commonly Observed Malware

Source: Cisco Security Research



For more info visit: www.cisco.com/go/acr2017

CISCO

STATS:

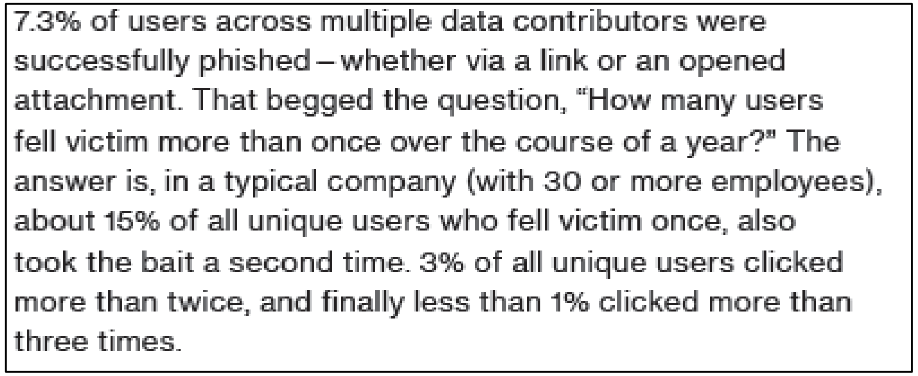
- An investigation by Cisco that included 130 organizations across verticals found that **75 percent of those companies are affected by adware infections**. Adversaries can potentially use these infections to facilitate other malware attacks.
- Since January 1, 2016, Symantec's Security Response group has seen an average of more than **4,000 ransomware attacks per day: a 300 percent increase over 2015**. (Symantec 2016 Internet Security Threat Report).

Phishing

Trend: Increased Spam Volume.

- Spam accounts for nearly two-thirds (65 percent) of total email volume, and our research suggests that global spam volume is growing due to large and thriving spam-sending botnets. According to Cisco threat researchers, about 8 percent to 10 percent of the global spam observed in 2016 could be classified as malicious.

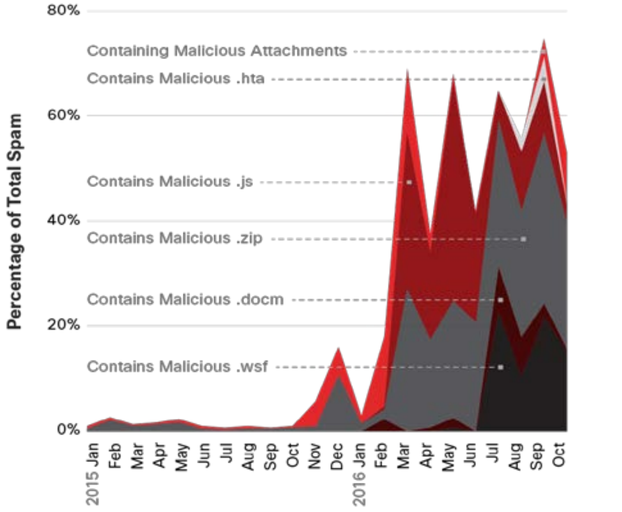
Stat to think about: (VZ DB Report, 2017, pg. 34)



7.3% of users across multiple data contributors were successfully phished – whether via a link or an opened attachment. That begged the question, "How many users fell victim more than once over the course of a year?" The answer is, in a typical company (with 30 or more employees), about 15% of all unique users who fell victim once, also took the bait a second time. 3% of all unique users clicked more than twice, and finally less than 1% clicked more than three times.

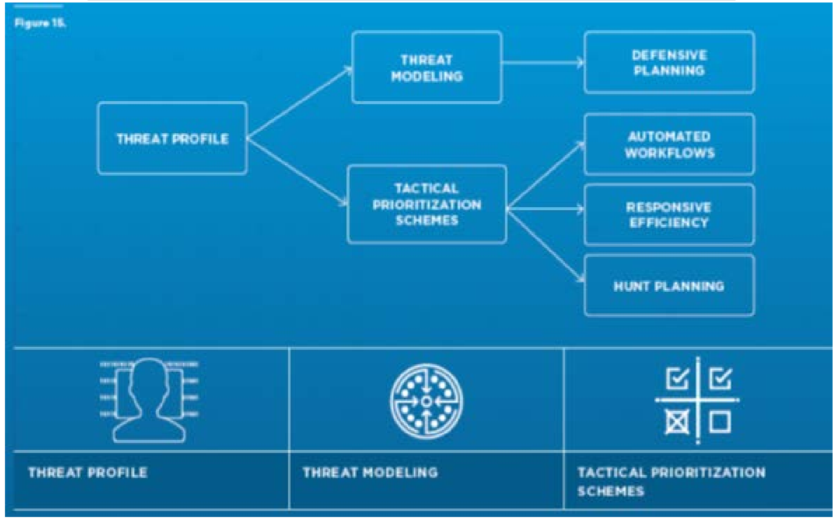
Figure 17 Percentage of Total Spam Containing Malicious Attachments

Source: Cisco Security Research

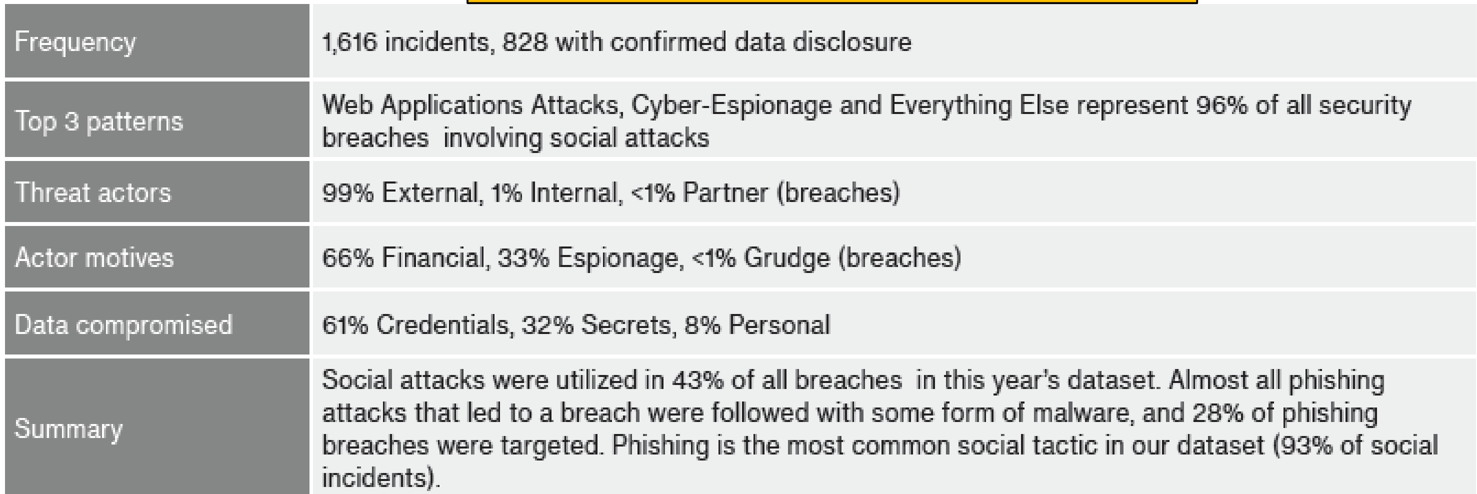


For more info visit: **www.cisco.com/go/acr2017**

Fireye: Intel Driven Defense; Figure, M-Trends, pg. 34)



Attacking the Human Terrain; Verizon DB Report, 2017, pg. 32



Frequency	1,616 incidents, 828 with confirmed data disclosure
Top 3 patterns	Web Applications Attacks, Cyber-Espionage and Everything Else represent 96% of all security breaches involving social attacks
Threat actors	99% External, 1% Internal, <1% Partner (breaches)
Actor motives	66% Financial, 33% Espionage, <1% Grudge (breaches)
Data compromised	61% Credentials, 32% Secrets, 8% Personal
Summary	Social attacks were utilized in 43% of all breaches in this year's dataset. Almost all phishing attacks that led to a breach were followed with some form of malware, and 28% of phishing breaches were targeted. Phishing is the most common social tactic in our dataset (93% of social incidents).

Sources

1. Trend Micro. Security Predictions. Derived from https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017. Accessed 19 April 2017.
2. McAfee Labs. 2017 Threats Predictions. Intelsecurity.com. January, 2017. Accessed 20 April 2017.
3. Forcepoint Security Labs. 2017 Security Predictions. Forcepoint.com. 2016. Accessed 17 April, 2017.
4. Mandiant. M-Trends 2017: A View From the Front Lines. FireEye.com. 2017. Accessed 18 April 2017.
5. FireEye. 2017 Cybersecurity Predictions. FireEye.com, 2017. Accessed 20 April 2017.
6. Watchguard. https://www.watchguard.com/, Derived from https://www.watchguard.com/wgrd-resource-center/2017-security-predictions/2017-security-predictions-infographic, Accessed 29 April 2017.
7. White Hat Security. Derived from https://www.whitehatsec.com/blog/security-predictions-2017/, Accessed April 23 2017.
8. CSO Online. Derived from http://www.csoonline.com/article/3149556/security/top-15-security-predictions-for-2017.html#slide3, Accessed 21 April 2017.
9. Verizon. Verizon Data Breach Report, 2017 (10th Edition). Verizon Enterprise.com. Accessed 21 April, 2017.
10. Symantec. 2016 Internet Security Threat Report. 2016. Accessed 21 April, 2017.
11. CIO.com. Derived from http://www.cio.com/article/3145879/hiring/2017-security-predictions.html. Accessed 28 April 2017.
12. BMC, Re-engineering Security in Age of Digital Transformation, 2017. Accessed 17 April, 2017.
13. SC Magazine. Derived from https://www.scmagazineuk.com/cyber-security-industry-2017-predictions-reaching-the-tipping-point/article/628904/. Accessed 28 April 2017.
14. Proofpoint. Derived from https://www.proofpoint.com/us/corporate-blog/post/eight-cybersecurity-predictions-recommendations-for-2017. Accessed 28 April 2017.
15. Above Security. Derived from http://www.datacenterjournal.com/cybersecurity-trends-2017-companies-fight-back/. Accessed 28 April 2017.
16. CISCO. 2017 Annual Cybersecurity Report. Cisco.com. January 2017. Accessed April 23rd, 2017.