FUNG GLOBAL RETAIL & TECHNOLOGY

June 6, 2017

Deep Dive: An Introduction to Cybersecurity—Part Two

Deborah Weinswig

Managing Director
Fung Global Retail & Technology
deborahweinswig@fung1937.com
US: 917.655.6790
HK: 852.6119.1779
CN: 86.186.1420.3016

1) In Part One of this *Deep Dive* report, we provided a summary of the current cybersecurity environment and discussed its components.
2) Here in Part Two, we discuss the components and characteristics of an advanced attack, the different types of attacks and vulnerabilities, and the different types of hackers.
3) An advanced attack comprises four stages: infection, persistence, communication, and command and control.
4) Advanced persistent threats are designed to remain undetected and to operate over a long period, slowly accumulating data from servers and databases, aggregating it, and then sending it in a burst to a remote server.
5) Types of attacks include malware, spam, botnets and ransomware, and hackers can take advantage of vulnerabilities in systems, such as the use of weak or common passwords, in order to wage attacks.
6) The typical hacker is not some 15-year-old working at his bedroom desk, as we might imagine. Rather, there are a variety of hackers, who are categorized by the color of "hat" they wear, which corresponds with their presumed motivation. There are also organized crime and state-sponsored hackers. The dark web has emerged as a marketplace for stolen personal information.
7) Fortunately, a powerful cybersecurity industry has emerged, and many private and public companies now specialize in providing targeted hardware and software solutions to thwart and minimize the impact of cyberattacks. Venture capital investment in the space is also healthy, keeping the level of innovation high.

Table of Contents

Executive Summary

Ever since humans began treasuring objects of value, there have been individuals who have wanted to steal or damage those objects. In our current era, the Information Age, data represent many of our objects of value. PC viruses have existed essentially since the advent of the PC. And as the PC's capabilities have increased over time, following Moore's law, so, too, has the value of the data residing on them, making them an attractive target for criminals.

The invention of the Internet has made the world flat, enabling us to shop and make purchases from faraway countries. At the same time, it has enabled invisible criminals at home and abroad to sometimes break into our PCs and take our data, lock up our devices in exchange for ransom, or cause other types of havoc.

At one time, cybersecurity simply consisted of protecting computers from viruses and malware that could be hidden on a floppy disk. Now, computer users are vulnerable to picking up such maladies while browsing the web, using a mobile phone, logging into a free Wi-Fi service or even plugging in a USB stick they might have found.

Unfortunately, the Internet has become a darker place. Organized criminal gangs are colluding with state-sponsored hacking groups to engage in larceny, extortion, and corporate and private espionage and miscreants are encrypting hard drives and demanding the payment of ransomware.

Unfortunately, the Internet has become a darker place. In the past, teenage hackers might have broken into computer systems in order to demonstrate their abilities and cause minor chaos, but now, organized criminal gangs are colluding with state-sponsored hacking groups to engage in larceny, extortion, and corporate and private espionage. Moreover, some miscreants are now invading computers and encrypting the hard drive, threatening to release it only in exchange for a hefty ransom payment made in untraceable bitcoin.

For both individuals and enterprises, it is a struggle to keep the bad actors at bay. They are relentless and tireless, and all it takes is one person clicking on the wrong email link to let them in. Cyberattacks are largely enabled by the human element—by our own apathy, inattention to detail or lack of vigilance. Hackers often get in when IT managers do not apply software updates or patches or do not heed the yellow and red flags generated by security monitors. And many IT teams do not have a plan in place to deal with break-ins, which are almost inevitable. The burden of cybersecurity falls on all of us: to keep cybercriminals out, we must stay on top of our game and not doze off.

Enter the good guys, offering cybersecurity solutions. Just as we have to buy locks to protect our homes, IT managers have to arm themselves with a suite of tools to fend off network invasions, or at least minimize their effects. The negative PR and business consequences that can result from a network incursion are just too great a risk to not deal with the cybersecurity threat proactively, as many retailers and government agencies have painfully learned.

In this report, we provide a general overview of cybersecurity, the different types and methods of cyberattacks, and many details about the industry and the companies that are working to keep our devices and networks safe from cybercriminals.

About This *Deep Dive*

Fung Global Retail & Technology is publishing its *Deep Dive: An Introduction to Cybersecurity* in three installments.

The Executive Summary outlines the growth of the Information Age and the advent of the Internet, the benefits of which have been tested often by corresponding developments in computer viruses and malware. Recently, though, the Internet has become a significantly darker place. The bad actors online used to be mostly teenage hackers, but they are being replaced by organized crime syndicates and state-sponsored hackers with much bigger criminal ambitions. The good guys have labored to keep pace with the cybercriminals, and a rich cybersecurity industry has emerged, with a large number of companies specializing in the various aspects of online security.

Part One: Introduction and Components of Cybersecurity

The growing interconnectedness of computers and increasing use of the Internet make computers an irresistible target for cybercriminals. As Internet usage has increased and hacking tools have become more accessible, the number of reported cyberattacks has risen. The cat-and-mouse game between virus developers and antivirus software makers continued relatively peacefully until about 2010, when the balance between hackers and defenders was severely altered.

In 2013, the National Institute of Standards and Technology defined five categories in a framework for reducing cyber-risks to infrastructure: identification, protection, detection, response and recovery.

Part Two: Components of an Advanced Attack, Characteristics of an Advanced Persistent Threat, and Types of Attacks and Hackers

The term “APT” refers to an advanced persistent threat, a cyberattack in which an unauthorized person gains and maintains access to a network for an extended period of time. Recent APTs have targeted enterprises.

APTs can take a number of forms, including malware, spam, botnet and ransomware attacks, and hackers can take advantage of vulnerabilities in systems, such as the use of weak or common passwords.

Types of hackers include script kiddies and white, black, gray, green, red and blue hats.

Part Three: New Threats/Threat Vectors, Markets and Cybersecurity Companies

The number and kinds of cyberthreats continue to grow and evolve due to advances in technology that benefit both attackers and defenders.

Market intelligence firm IDC forecasts that global spending on cybersecurity will increase at an 8.3% CAGR between 2016 and 2020, growing from $73.6 billion to $101.6 billion. This growth rate is more than double the 3.3% CAGR that IDC forecasts for worldwide IT product revenue from 2015 through 2020.

The Fung Global Retail & Technology team hopes that you will find this *Deep Dive* interesting and informative and that it will help you protect your enterprise against cybersecurity threats!

Components of an Advanced Attack

An advanced attack comprises four stages, according to *Cybersecurity For Dummies, Palo Alto Networks Edition*: infection, persistence, communication, and command and control.

Infection

Cyberattack exploits generally seek to cause a buffer overflow in the target's software, which makes the program quit and transfers the attacker to the shell (or command line), thereby enabling the attacker to enter commands and gain access. The malware enters the target system via one of the following means:

- Phishing/social engineering
- Hiding in a transmission in the secure sockets layer, instant messaging or peer-to-peer traffic
- Via remote shell access
- Drive-by download (the unintentional downloading of a virus or malware onto a device)

Persistence

Persistence refers to malware remaining within a network until activated. It can make use of a rootkit (using privileged, root-level access) or a bootkit (modifying the kernel or boot code), or it can install a backdoor.

Communication

In this stage of an attack, the malware establishes a communication channel with the attacker. Such channels can use encryption or unusual routes, be embedded in other protocols, use several or nonstandard ports, or route communications via several infected hosts.

Command and Control

The command and control component ensures that the attack can be controlled, managed and updated over time.

Characteristics of an Advanced Persistent Threat (APT)

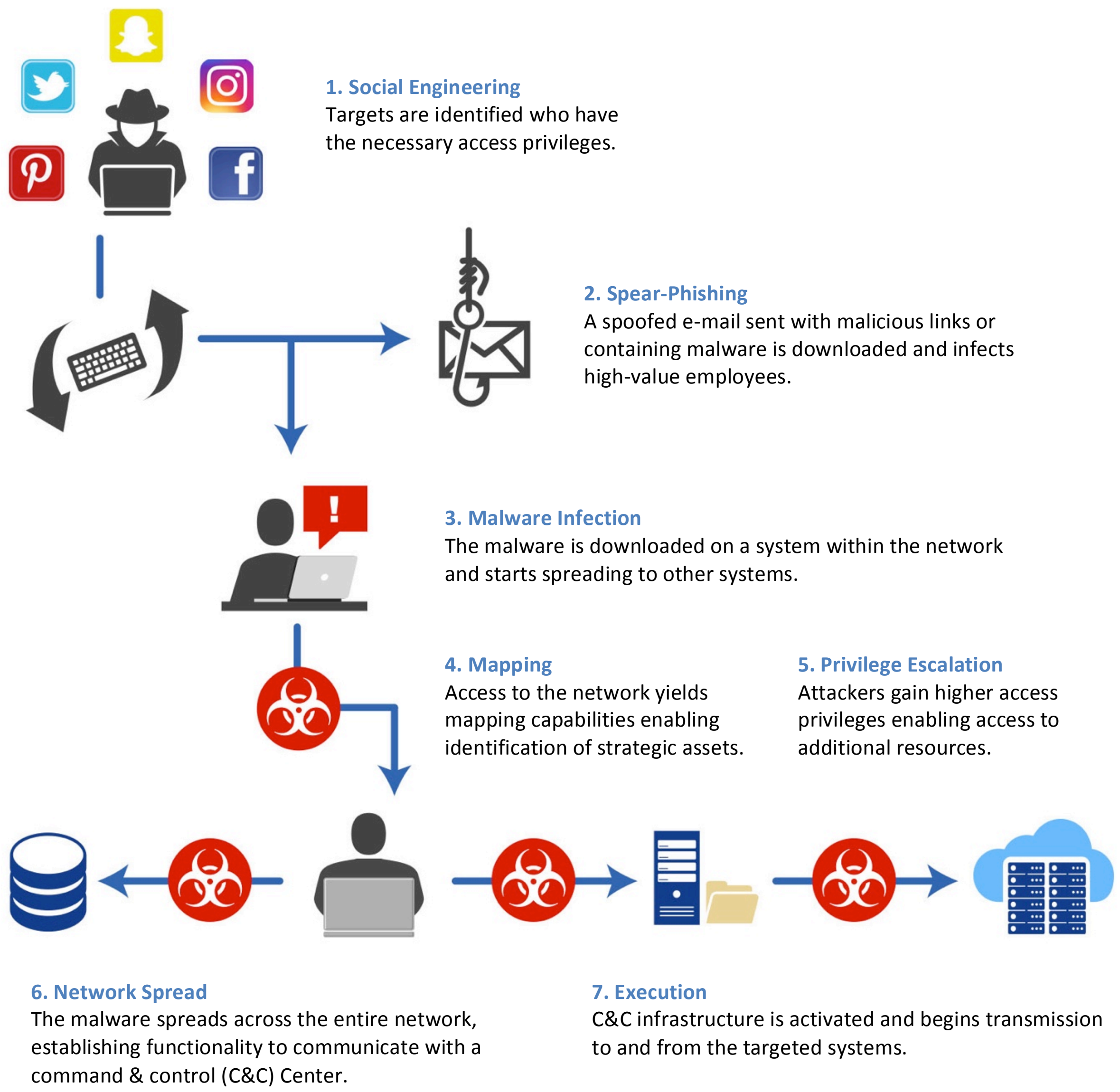
The term "APT" was coined by US military and defense agencies. It refers to an attack in which an unauthorized person gains and maintains access to a network for an extended period of time. While early APTs were primarily aimed at political targets and government agencies, recent APTs have targeted enterprises. Sony Pictures, Home Depot and Target are three high-profile examples of companies that have suffered APT attacks in recent years.

The term "APT" was coined by US military and defense agencies. It refers to an attack in which an unauthorized person gains and maintains access to a network for an extended period of time. While early APTs were primarily aimed at political targets and government agencies, recent APTs have targeted enterprises.

APTs are designed to remain undetected, allowing attackers to steal as much data as possible. The malware is designed to operate over a long period, slowly accumulating data from servers and databases, aggregating it, and then sending it in a burst to a remote server.

APTs also seek to move from one server to the next without being detected by generating recognizable network traffic. Once the malware resides on the target server and other criteria are met, the attack either takes down the system or begins to control operations. The diagram below illustrates the seven steps of an APT attack, according to cybersecurity firm Netswitch.

Figure 1. The Seven Steps of an APT Attack



1. Social Engineering
Targets are identified who have the necessary access privileges.

2. Spear-Phishing
A spoofed e-mail sent with malicious links or containing malware is downloaded and infects high-value employees.

3. Malware Infection
The malware is downloaded on a system within the network and starts spreading to other systems.

4. Mapping
Access to the network yields mapping capabilities enabling identification of strategic assets.

5. Privilege Escalation
Attackers gain higher access privileges enabling access to additional resources.

6. Network Spread
The malware spreads across the entire network, establishing functionality to communicate with a command & control (C&C) Center.

7. Execution
C&C infrastructure is activated and begins transmission to and from the targeted systems.

Source: Netswitch.net

In these seven steps:

1. **Social engineering** is used to identify those individuals possessing the needed access privileges.
2. **Spearphishing** is used to send spoofed emails or malicious links to those individuals in order to gain access.
3. **Malware infection** occurs on the network and the malware begins spreading to other systems.

4. **Mapping** locates the key assets within the network.
5. **Privilege escalation** grants higher privileges and access to higher-level resources.
6. **Network spread** occurs within the entire network, enabling communication with a command-and-control center.
7. **Execution** of the transmission of the desired data is activated by the command-and-control center.

Types of Attacks/Vulnerabilities

APTs can take a number of forms, including malware, spam, botnet and ransomware attacks, and hackers can take advantage of vulnerabilities in systems, such as the use of weak or common passwords.

Malware

Malware, derived from the phrase “malicious software,” is software designed to invade others’ computers and inflict harm. Examples include viruses and worms (the two most common types of malware), in addition to bots and Trojans, as described below.

Malware, derived from the phrase “malicious software,” is software designed to invade others’ computers and inflict harm. Examples include viruses and worms (the two most common types of malware), in addition to bots and Trojans.

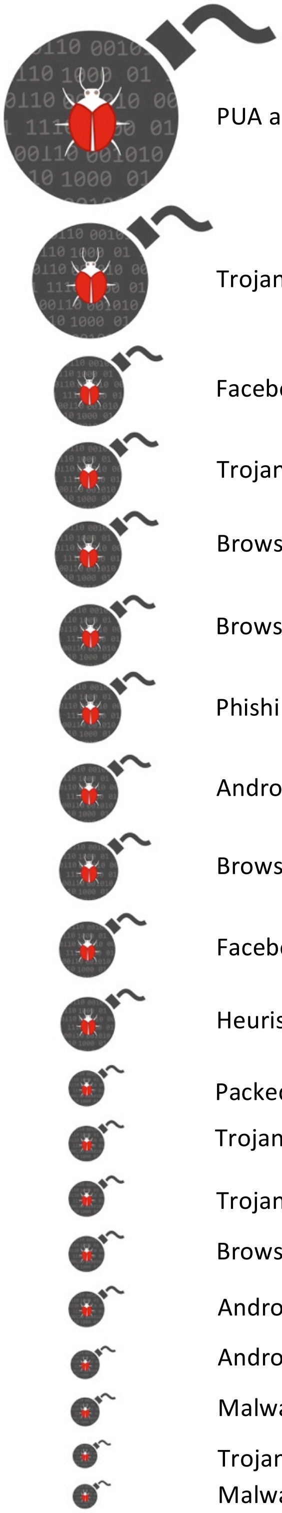
Figure 2. Types of Malware

Type	Characteristics
Bot	Derived from “robot,” a bot represents an automated process that interacts with network services. Bots can collect information (as “web crawlers”) or interact with instant-messaging or web interfaces and/or websites.
Trojan	Like the Trojan horse in ancient Greek literature, a Trojan looks legitimate but contains something harmful, in the form of software. Trojans can also create backdoors, but, unlike viruses and worms, they do not replicate.
Virus	Like a human virus, a computer virus replicates by inserting a copy of itself into another program. Viruses can cause data damage through distributed-denial-of-service (DDoS) attacks. They are typically attached to an executable (.exe) file and they spread from one computer to the next via networks, external disks, file sharing or e-mail attachments.
Worm	Worms work like viruses, but are stand-alone software that requires human assistance to spread. A worm enters a system via a vulnerability or social engineering and travels within the network via the system’s file- or information-transport features.

Source: Cisco

There is a wide variety of malware that has been found in cyberspace, as depicted below.

Figure 3. Most Commonly Observed Malware, 2016

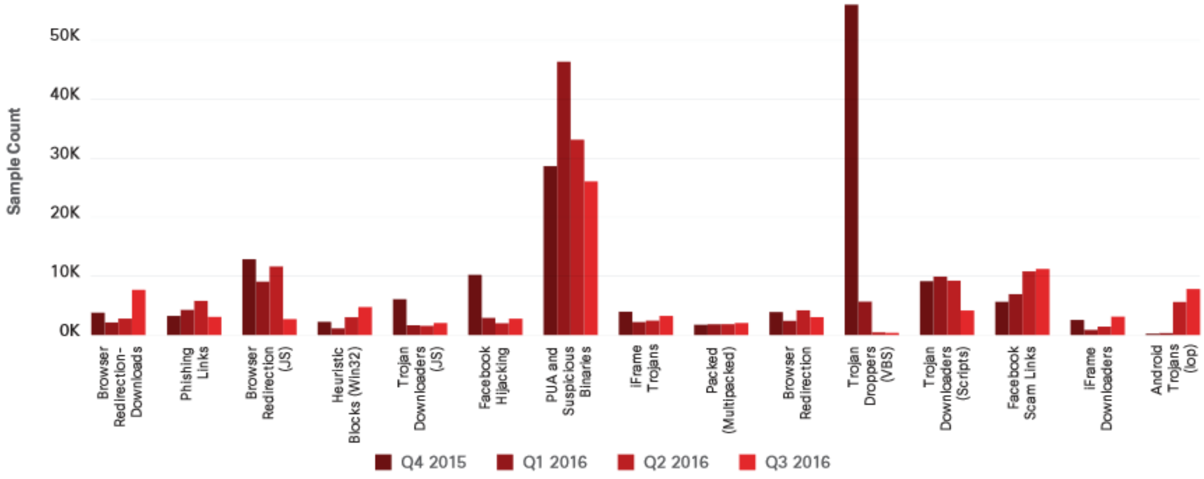


Sample Count	
87,329	PUA and Suspicious Binaries
50,081	Trojan Droppers (VBS)
35,887	Facebook Scam Links
27,627	Trojan Downloaders (Scripts)
24,737	Browser Redirection (JS)
18,505	Browser-Redirection Downloads
15,933	Phishing (Links)
14,020	Android Trojans (Iop)
12,848	Browser Redirection
11,600	Facebook Hijacking
11,506	Heuristic Blocks (Scripts)
7,712	Packed Binaries
5,996	Trojan Downloaders (JS)
5,510	Trojans, Heuristic (Win32)
5,467	Browser iFrame Attacks
4,970	Android (Axent)
4,584	Android Trojans (Loki)
4,398	Malware (FakeAvCn)
3,646	Trojans (HideLink)
3,006	Malware (HappJS)

Source: Cisco, 2017 Annual Cybersecurity Report

The figure below illustrates the most commonly observed types of malware during a four-quarter period spanning 2015–2016. It shows that potentially unwanted applications (PUAs) and suspicious binaries remained a fairly constant threat over the period, whereas the number of Trojan droppers declined sharply.

Figure 4. Most Commonly Observed Malware, 4Q15–3Q16



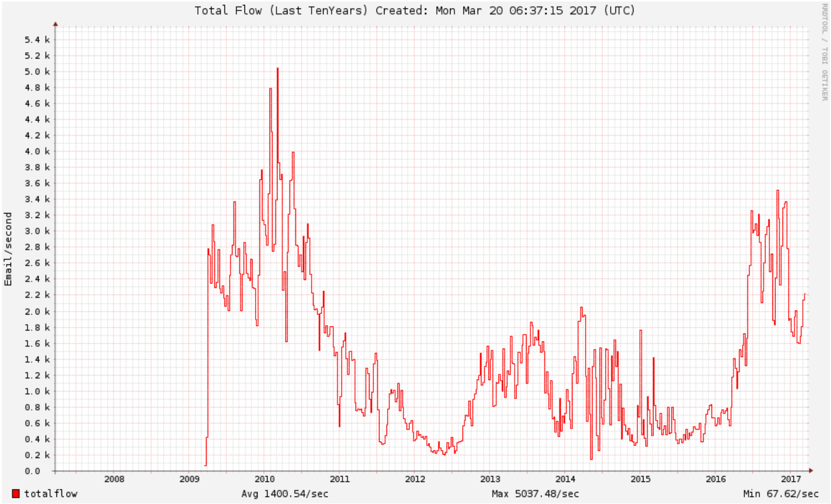
Source: Cisco

Spam

Spam is named after a famous skit by British comedy troupe Monty Python in which the word, which is the name of a Hormel processed-meat product, is repeated in a silly way. It is unwanted and irrelevant email that is sent in bulk to a large number of recipients—the digital version of junk mail. Spam may or may not contain malware. Although many of us may feel like the amount of spam mail we receive is steadily on the rise, the graph below shows that spam volume has varied over the past 10 years.

Spam is named after a famous skit by British comedy troupe Monty Python in which the word, which is the name of a Hormel processed-meat product, is repeated in a silly way. It is unwanted and irrelevant email that is sent in bulk to a large number of recipients.

Figure 5. Spam Trap Flow Statistics (Emails per Second)

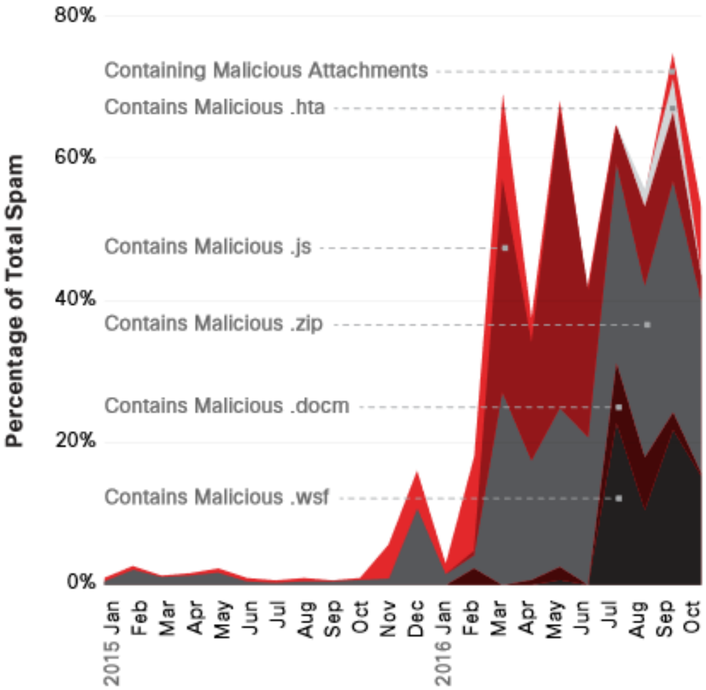


Source: Abuseat.org

In some cases, authorities have been able to stop spammers. Shane Atkinson of New Zealand was exposed as a spammer in 2003 following the publication of a newspaper article about him. He then claimed he would cease his operation, which sent out 100 million emails per day. However, he continued his operation and was fined NZ$100,000 (US$70,474) in 2008.

The figure below illustrates a recent explosion in the incidence of spam that contains malicious attachments.

Figure 6. Percentage of Total Spam Containing Malicious Attachments



Source: Cisco

Due to the high volume of spam sent, and the high level of irritation it causes, an entire industry has emerged to prevent and detect it.

Due to the high volume of spam sent, and the high level of irritation it causes, an entire industry has emerged to prevent and detect it. But plenty of companies still generate spam email as well as mass mailings for legitimate purposes.

Two particularly difficult types of spam attacks to deal with are **hailstorm attacks** and **snowshoe attacks**, which both employ speed and targeting, and are highly effective. Hailstorms target antispam systems and take advantage of the window of time between the launch of a spam campaign and coverage by antispam scanners; typically, the window is only a few seconds or minutes. Snowshoe spam attacks, by contrast, aim to fly under the radar of volume-based detection tools in a steady but low-volume attack.

Botnets

A large number of infected, controlled computers can be aggregated to form a botnet, which can inflict large-scale attacks on servers and computers. One particularly destructive botnet is Mirai (Japanese for “the future”), which primarily targets IoT devices such as Internet cameras and routers.

Distributed Denial of Service (DDoS)
A denial-of-service (DoS) attack attempts to disrupt an Internet server by flooding it with superfluous requests that are intended to overload it and crowd out the legitimate requests. A DDoS attack is a DoS attack implemented from a large number of computers, e.g., from a botnet.

Ransomware is a type of malware that infects or takes control of the user's machine in an attempt by a hacker to extort a payment from the user. The malware typically locks and/or encrypts the user's computer, files or applications in order to prevent the user from accessing them.

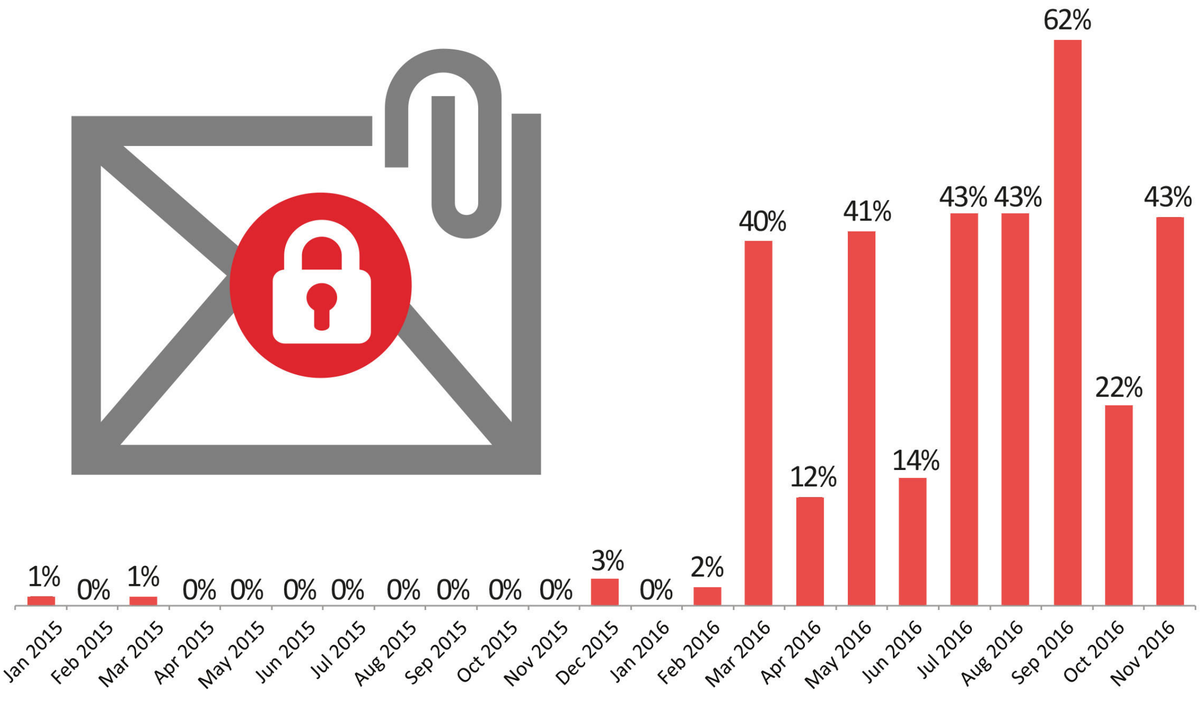
Ransomware
Ransomware is a type of malware that infects or takes control of the user's machine in an attempt by a hacker to extort a payment from the user. The malware typically locks and/or encrypts the user's computer, files or applications in order to prevent the user from accessing them.

Kaspersky Lab called 2016 "the year of ransomware," as malware developers were busy last year transferring resources from less-profitable schemes toward the development of ransomware. Kaspersky Lab noted the following with regard to the explosion of ransomware in 2016:

- The appearance of 62 new families of ransomware
- The number of ransomware modifications increased to 32,091 in the July–September period from 2,900 in the January–March period
- The number of businesses attacked by ransomware increased to one every 40 seconds in September from one every two minutes at the beginning of the year

IBM X-Force Research found that spam volume quadrupled over a period of 23 months from January 2015 through November 2016, including an increase in the attachment rate of ransomware from 0.6% to 40%.

Figure 7. Percentage of Spam with Ransomware Attachments



Source: IBM X-Force Research

There are three main types of ransomware:

1. (B)lockers/lockscreen ransomware, which locks the user's screen, blocks all other windows and prevents the user from accessing the device
2. (En)cryptors, which encrypt data on the user's device and demand the user pay money to release the encryption
3. Master boot record ransomware, which blocks the record on the user's hard drive that enables startup

Skiddie ransomware (created by a "script kiddie," or unskilled individual) is ransomware that is based on programs developed by other individuals. Reaffirming the old adage about there being no honor among thieves, Kaspersky Lab commented in its *Kaspersky Security Bulletin 2016*, "We expect 'skiddie' ransomware to lock away files or system access or simply delete the files, trick the victim into paying the ransom, and provide nothing in return."

Cybercriminals typically demand ransom of $200–$10,000, according to the FBI. IBM conducted a ransomware study and found that 54% of consumers said they would pay $100 for the return of their financial data. It also found that 55% of parents, and 39% of nonparents, said they would pay for the return of precious photos.

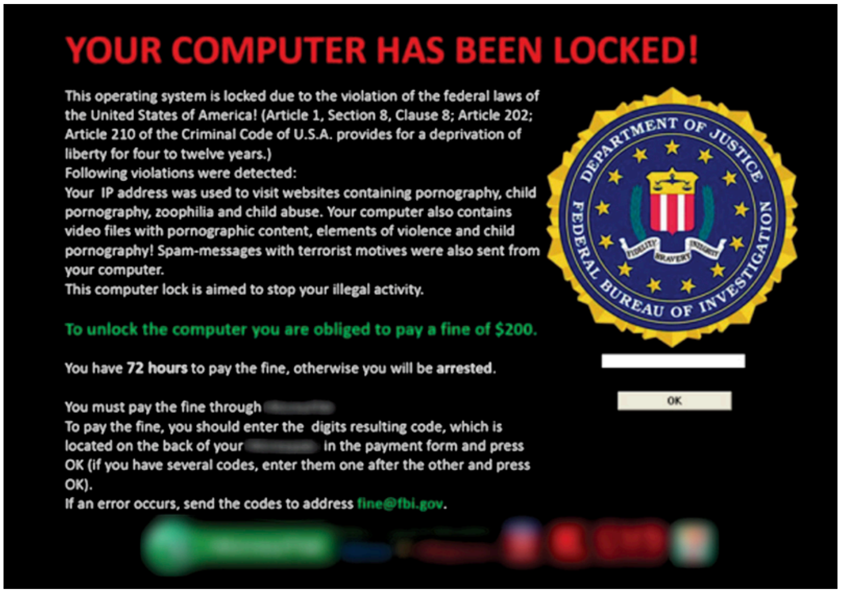
Ransomware is surprisingly lucrative for cybercriminals targeting the corporate sphere. The CryptoWall ransomware has generated total ransom payments of $325 million, and the criminals behind CryptoLocker claim a 41% success rate.

Ransomware is surprisingly lucrative for cybercriminals targeting the corporate sphere. The CryptoWall ransomware has generated total ransom payments of $325 million, and the criminals behind CryptoLocker claim a 41% success rate, with total proceeds estimated as much as $27 million. An IBM survey found that seven in 10 companies that have been targeted have paid extortionists to get data back. Of those companies:

- 11% paid $10,000–$20,000
- 25% paid $20,000–$40,000
- 20% paid more than $40,000

The graphic below depicts an attack in which a criminal claiming to be acting on behalf of the US Department of Justice has used the agency's logo in order to extort the victim into paying a $200 ransom.

Figure 8. Example of Ransomware



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Source: Wired

Scareware is a less harmful type of attack in which the attacker attempts to induce the victim to pay in order to prevent or remedy a nonexistent attack.

Privilege Escalation

Privilege escalation refers to exploiting a bug or weakness in an operating system in order to gain access to resources that were not assigned to the user. Examples of privileges normally reserved for a developer or system administrator include viewing, editing or modifying system files. Vertical privilege escalation, or privilege elevation, refers to a user gaining a higher privilege level, such as that normally reserved for a system administrator.

Zero-day exploits make use of undisclosed vulnerabilities to affect computer systems. Exploits operate within the "window of vulnerability," which is the period between the activation of the exploit and the patching of the vast majority of vulnerable systems.

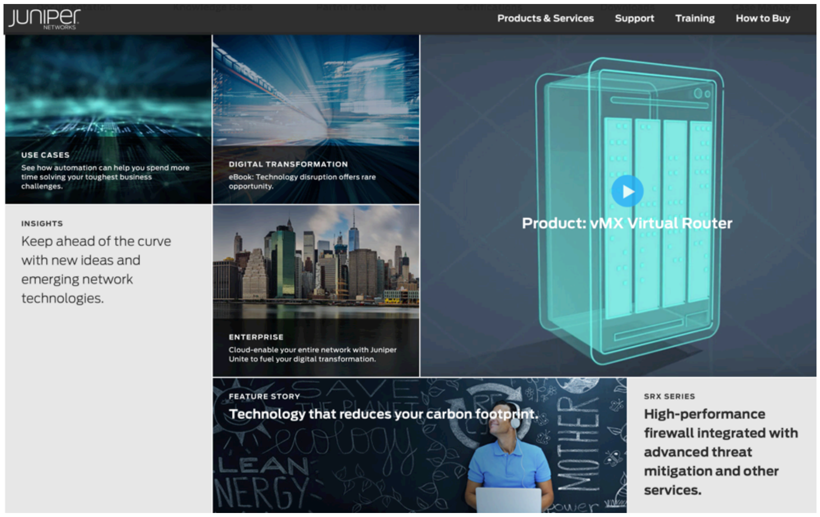
Exploits

Exploits make use of a command, methodology or routine in software that can be used to take advantage of security vulnerabilities. **Zero-day exploits** make use of undisclosed vulnerabilities to affect computer systems. Exploits operate within the "window of vulnerability," which is the period between the activation of the exploit and the patching of the vast majority of vulnerable systems. German computer magazine *C't* determined that antivirus software was able to detect 20%–68% of zero-day viruses, and an Internet security report from Symantec estimated that the average window of vulnerability is 28 days.

Backdoors

Backdoors refer to secret, undocumented ways of accessing a system, possibly using high-level privileges. Backdoors can be implemented in a hidden part of a program, an external program or through hardware, and they can take the form of hardcoded passwords. They differ from Easter eggs, which are unauthorized functions in programs that often pay tribute to the programmers. Backdoors and Easter eggs can offer opportunities for hackers or cybercriminals to find weaknesses and gain entry into a computer or network.

In 2015, network hardware maker Juniper Networks disclosed that it had found unauthorized code in an operating system running on some of its firewalls (existing since 2012). The code would have allowed attackers to take complete control of its enterprise firewalls running the affected software. Attackers would also have been able to decrypt encrypted traffic running through the VPN on its firewalls.



USE CASES
See how automation can help you spend more time solving your toughest business challenges.

DIGITAL TRANSFORMATION
eBook: Technology disruption offers rare opportunity.

INSIGHTS
Keep ahead of the curve with new ideas and emerging network technologies.

ENTERPRISE
Cloud-enable your entire network with Juniper Unite to fuel your digital transformation.

FEATURE STORY
Technology that reduces your carbon footprint.

SRX SERIES
High-performance firewall integrated with advanced threat mitigation and other services.

Source: Juniper.net

The advent of backdoors has made telecommunications equipment politically sensitive. Former National Security Agency (NSA) contractor Edward Snowden revealed that the NSA routinely intercepted routers manufactured by Cisco—without Cisco's knowledge—and installed hidden surveillance software on them prior to export. To prevent importation of such hidden surveillance software, the US government banned certain foreign telecommunications equipment providers from bidding on government contracts.

Bad Passwords

In early versions of the UNIX operating system, all users' passwords were hashed (mathematically transformed into an unintelligible series of characters) and stored in a publicly accessible directory called /etc/passwd. It was simple for hackers to run the English dictionary through the hashing algorithm and find passwords in the common directory that were simple English words. Since then, the password file has been moved to /etc/shadow, which is accessible only by privileged users, and more sophisticated hashing algorithms have been developed.

Many computer users, overwhelmed by the number of passwords they need to memorize, resort to simple passwords that can be typed easily with a traditional QWERTY computer keyboard. These passwords, however, are easily guessed by hackers.

Figure 9. The 25 Most Common Passwords, 2016

123456
123456789
qwerty
12345678
111111
1234567890
1234567
password
123123
987654321
qwertyuiop
mynoob
123321
666666
18atcskd2w*
7777777
1q2w3e4r
654321
555555
3rjs1la7qe*
google
1q2w3e4r5t
123qwe
zxcvbnm
1q2w3e

**These passwords were likely created by bots.*
Source: HuffingtonPost.com

Passwords containing a mixture of capital and lowercase letters, numbers and punctuation (and not corresponding to dictionary entries) take a much longer amount of time to be generated by hackers' programs.

Hacktivism/Vigilantism/Cyberdissidents/Shaming

Some individuals turn to hacking in order to, in their view, do good. Hacktivism (derived from "hacking" plus "activism") is the act of breaking into a computer system to further a political or social goal. Internet vigilantism is the use of the Internet, including social media, to expose scams, crimes or unwanted behavior.

Cyberdissidents are professional journalists or activists or citizens who post news, information or commentary on the Internet that criticizes a particular government or regime.

Online shaming is the use of the Internet or social media to publicly humiliate those perceived as wrongdoers in order to counter injustice. Shaming can involve doxing—disclosing a person's private information such as their address and phone number online—which can make the subject a target of threats or harassment.

Internet-Powered Bank Heists

In an apocryphal story, when infamous bank robber Willie Sutton was asked why he robbed banks, he replied, "That's where the money is." By that logic, it is easy to see why cybercriminals have turned their attention to attacking financial institutions on the Internet.

In its Kaspersky Security Bulletin 2016, Kaspersky Lab noted an increase in "bank heists" in 2016, including attacks on stock exchanges and, notably, a successful malware attack on the SWIFT global financial messaging network.

In its *Kaspersky Security Bulletin 2016*, Kaspersky Lab noted an increase in "bank heists" in 2016, including attacks on stock exchanges and, notably, a successful malware attack on the SWIFT global financial messaging network.

In an article published March 25, 2017, *The New York Times* noted that North Korean hacking teams have turned their efforts toward banks. The article asserts that the country maintains an army of 1,700 hackers and 5,000 trainers, supervisors and support staff located in China, Southeast Asia and Europe. The group is allegedly behind a thwarted attack on a Polish bank, the theft of $81 million from Bangladesh’s central bank and the attack on Sony Pictures in 2014.

Types of Hackers

According to cybersecurity education group Cybrary, the typical hacker is not the 15-year-old boy working at his bedroom desk that we might imagine based on what we have seen in movies. The group defines seven distinct types of hackers:

Free and Open Source Cyber Security Learning

Free Training | Certification | Hands on Labs

Source: Cybrary.it

1. **Script kiddie:** As mentioned previously, script kiddies copy others’ code to repurpose it as a virus or as a structured-programming language injection, which is used to attack databases.
2. **White hat:** These hackers, also known as ethical hackers, use their computer skills to help others. For example, they might help companies test their resilience to outside attacks.
3. **Black hat:** These are the bad actors who attempt to find banks or companies with weak defenses in order to steal information. These types of hackers can be members of organized crime syndicates or state-sponsored infiltrators.
4. **Gray hat:** These hackers are more ambiguous in their hacking aims (they operate in a gray area). They do not generally steal from their victims, although they may deface websites. They tend not to use their hacking skills for good, although they could if they chose to.
5. **Green hat:** These are hackers in training, or “n00bz” (“newbies”), who seek to learn hacking secrets from more experienced hackers.
6. **Red hat:** This group represents the vigilantes within the hacker world. They use hacking techniques to disable or hinder other hackers, such as by uploading viruses to the hackers’ own systems.
7. **Blue hat:** These are also fairly inexperienced hackers, who are known to purely seek to enact revenge on those who have angered them.

Organized Crime

Cybercrime is a billion-dollar industry, according to the United Nations Interregional Crime and Justice Research Institute, and the high rewards and low risk associated with cybercrime have attracted criminal groups that plan, organize and commit all forms of online crime, including fraud, theft, extortion, and child abuse. The decentralized structure and anonymity of the Internet make it difficult for law enforcement agencies to locate cybercriminals.

Cybercrime is a billion-dollar industry, according to the United Nations Interregional Crime and Justice Research Institute, and the high rewards and low risk associated with cybercrime have attracted criminal groups that plan, organize and commit all forms of online crime, including fraud, theft, extortion, and child abuse.

Source: iStockphoto

The Dark Web as Marketplace

The anonymity of the dark web (or deep web) has made it an ideal meeting place for criminals, hackers, drug peddlers, gamblers and child abusers, among others. As previously mentioned, nation-state-grade hacking tools are now available for a small sum, payable in untraceable bitcoin, making it possible for a larger number of individuals to commit high-level attacks.

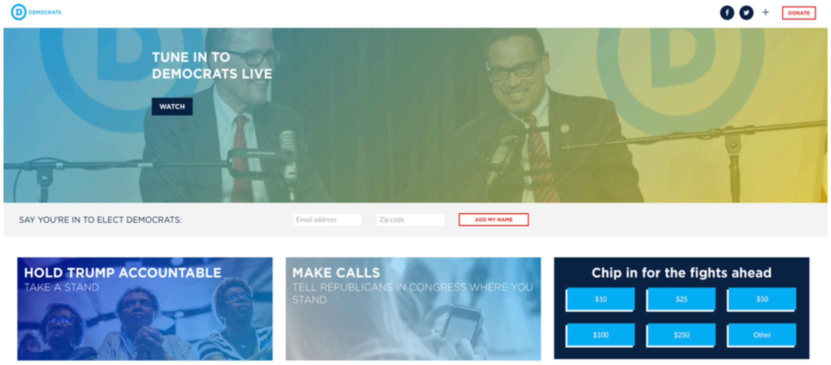
A March 20, 2017, article in the *International Business Times* reported that a dark web vendor named "SunTzu583" had offered 21,800,969 Gmail accounts for $450 (0.4673 bitcoins) in addition to 5,741,802 Yahoo accounts for $250 (0.2532 bitcoins). Some of the accounts include passwords or hashed passwords, many of which were stolen as a result of data breaches of MySpace, Adobe and LinkedIn, and were already disabled.

State-Sponsored Hackers

Many attacks today are reportedly sponsored by nondemocratic states such as Russia, China and North Korea. The countries are reported to sometimes act alone and sometimes in cooperation with organized crime syndicates. The US, too, has used hacking and cyberwarfare to achieve military and foreign-policy objectives. For example, the US used the Stuxnet worm to disable Iranian centrifuges engaged in turning uranium nuclear fuel into weapons-grade material.

Examples of hacking by Russia, China and North Korea include:

- The infiltration of the **US Democratic National Committee** network by Guccifer 2.0, and the subsequent leak of the documents to WikiLeaks. Guccifer 2.0 claimed in an interview to be Romanian, but cybersecurity experts believe that the entity is a Russian state-sponsored hacking group.



Source: Democrats.org

Unfortunately, many information systems are infiltrated by disgruntled employees or former employees. Current employees can sometimes obtain supervisor credentials and use them to grant themselves or their cohorts certain privileges (privilege escalation).

- The hacking and release of emails residing on **Sony Pictures’** servers. The hack was attributed to North Korea as revenge for Sony releasing the film *The Interview*, which satirized North Korea’s leader, Kim Jong Un.
- The theft of as many as 21.5 million records from the **US Office of Personnel Management**. The records included security clearance information, personal details and biometric information. China is the suspected perpetrator of the attack.
- The infiltration of **Ukraine’s electrical power grid**, resulting in three energy distribution companies being invaded, 30 electrical substations being switched off, and about 230,000 people being left without power for several hours. According to company representatives, the attack derived from computers with Russian IP addresses.

Current and Former Employees

Unfortunately, many information systems are infiltrated by disgruntled employees or former employees. Current employees can sometimes obtain supervisor credentials and use them to grant themselves or their cohorts certain privileges (privilege escalation). These privileges allow them to snoop on off-limits servers, data and services, which can be viewed for entertainment, data theft or sabotage.

In addition, employees in some industries (such as financial services) may seek to transfer sensitive company information, including client lists and other data. They may transfer the information by email, by uploading it to cloud-based servers or by saving it to an external storage device before leaving to work for a competitor.

Notable Cases of Hacking

There have been a number of high-profile hacks of large corporations in recent years, including:

- **Home Depot:** An individual who stole a vendor's password and used vulnerabilities in the Windows operating system to move to a more secure system stole information on 56 million credit card accounts, as well as 53 million email addresses, from Home Depot. A Windows patch was installed, but not until after the infiltrator had already entered the system.
- **RSA:** Ironically, this cybersecurity company (now a division of Dell) was invaded in March 2011 via a phishing email embedded in a Microsoft Excel worksheet. The email allowed a hacker to take advantage of a vulnerability in Adobe Flash software to install a backdoor, which was then used to steal passwords and company data.
- **Target:** In December 2013, Target disclosed that hackers had stolen credit and debit card data on as many as 40 million accounts via malware installed in the company's payment system. The company's FireEye malware detection software had issued an alert, but it was not heeded.
- **TJX Companies:** Over an 18-month period through 2007, 46.5 million credit and debit card numbers were stolen from TJX Companies. At the time, it was the largest data breach ever.
- **Yahoo:** In February 2017, Yahoo disclosed that it had been hacked a third time. A breach in August 2013 allowed hackers to steal details for 1 billion user accounts.

Deborah Weinswig, CPA
Managing Director
Fung Global Retail & Technology
New York: 917.655.6790
Hong Kong: 852.6119.1779
China: 86.186.1420.3016
deborahweinswig@fung1937.com

John Harmon, CFA
Senior Analyst

Hong Kong:
8th Floor, LiFung Tower
888 Cheung Sha Wan Road, Kowloon
Hong Kong
Tel: 852 2300 4406

London:
242-246 Marylebone Road
London, NW1 6JQ
United Kingdom
Tel: 44 (0)20 7616 8988

New York:
1359 Broadway, 9th Floor
New York, NY 10018
Tel: 646 839 7017

FungGlobalRetailTech.com