2001-2013: Survey and Analysis of Major Cyberattacks

Tavish Vaidya
Georgetown University

Abstract

Widespread and extensive use of computers and their interconnections in almost all sectors like communications, finance, transportation, military, governance, education, energy etc., they have become attractive targets for adversaries to spy, disrupt or steal information by presses of keystrokes from any part of the world. This paper presents a survey of major cyberattacks from 2001 to 2013 and analyzes these attacks to understand the motivation, targets and technique(s) employed by the attackers. Observed trends in cyberattacks have also been discussed in the paper.

1 Introduction

Cyberattacks are computer-to-computer attacks undermining the confidentiality, integrity, and/or availability of computers and/or the information they hold[1]. Computer networks have no geographical borders that need to be crossed for an attacker to steal information. This grants freedom to any attacker to pick his target anywhere in the world and carry out a cyberattack. Therefore, securing computer systems is as important as securing physical entities from being attacked. In terms of money, Ponemon Institute[2] estimated the average cost of cyberattacks to be $11.6 million per organization for 2013, which was 26 percent more than 2012.

Cyberattacks have not only caused losses in billions of dollars[3], but also had psychological impact on human psyche. As an example, in August 2004, fear of cyberattacks during Olympic games in Greece kept people from attending the Olympic events[4]. With Internet of Things[1] already here, securing computer networks and end devices becomes a paramount concern to prevent cyberattacks from disrupting and hijacking them for malicious purposes. Hence, it imperative and necessary to understand the motivations, attack vectors and weaknesses exploited by past cyberattacks. Lessons must be learned from past experiences to improve upon all aspects necessary for defending against cyberattacks in future.

[1] http://en.wikipedia.org/wiki/Internet_of_Things

This paper covers major cyberattacks starting from 2001 till 2013. The scope of this paper is limited to cyberattacks that caused significant monetary losses, threatened critical infrastructure or national security, had potential to cause loss of life and damage to physical property or involved data-leaks exposing personal information of users. This paper also covers cyber-espionage campaigns and cyberattacks with political motivations or agenda as well as some acts of hacktivism. It then examines the trend in attack methodology, frequency, motivation behind the attacks, damage caused, attribution and if any lessons were learned from past cyberattacks to improve security of computer systems.

(The source of the cyberattacks have been mentioned when the attackers were identified or suspected. In attacks where the source was unknown, we omit mentioning this fact explicitly throughout the text of this paper. The term attack(s) will be used interchangeably with cyberattack(s), unless explicitly mentioned otherwise.)

2 Revisiting past Cyberattacks

This sections surveys past cyberattacks to put the facts together and help support the analysis and uncover trends. Looking at each attack in isolation only provides limited information, however, cyberattacks can also be related to one another and therefore, can provide a lot more understanding when analyzed together.

This paper classifies cyberattacks based on their targeting, i.e. undirected or directed/targeted. Undirected cyberattacks are not directed towards a specific target but attack any vulnerable host. Directed/targeted attacks are carried out against specific targets and are designed to exploit specific weaknesses of the targeted systems.

2.1 Undirected Cyberattacks

The first undirected attack within the scope of this paper was the Anna Kournikova virus identified in February, 2001[5]. It exploited multiple vulnerabilities in Windows operating system and Microsoft Outlook to spread to other systems[6]. Dutch programmer Jan de Wit created the virus to see if lessons were learned from the ILOVEYOU[7] virus from last year[8]. In July 2001, self-propagating *Code Red* worm[9] infected 359,000 computers in less than 14 hours by exploiting a buffer overflow vulnerability in Microsoft IIS Server, disrupting hosted websites[10]. The estimated losses were put close to $2.6 billion[11].

In January 2003, *Slammer* worm wrecked havoc on the Internet by flooding networks with queries causing the routers to collapse[12]. *Slammer* worm also exploited a buffer overflow bug in Microsoft SQL Server[13], for which a patch was already available 6 months before the worm was launched. Same year in August, *Blaster* worm infected more than 48,000 computers worldwide and caused a distributed denial-of-service(DDoS) attack on windowsupdate.com[14]. Author of the *Blaster* worm, Jeffrey Lee Parson[15], exploited vulnerabilities in the Microsoft Remote Procedure Call Interface to infect vulnerable hosts[16] even though patches were released a month

before the attack. Also in August 2003, *Sober* email worm[17] was used to send political spam[18] and in 2005, its variants were circulated with fake emails impersonating the FBI and the CIA[19].

In 2004, *Mydoom* worm[20] caused an estimated loss of $38.5 billion[21]. Believed to have originated in Russia[22], the worm infected more than 500,000 machines and was sent out as email attachments[21], with later version exploiting a zero-day vulnerability in Internet Explorer browser[23]. Sasser worm[24] disrupted services of many companies in 2004[25], that claimed losses totaling $155,000 in civil lawsuits[26]. *Sasser* exploited a known buffer overflow vulnerability in Microsoft's Local Security Authority Subsystem Service[27] and was attributed to Sven Jaschan[25]. Just before the Christmas holidays of 2004, *Santy* worm was seen using search engines to find servers running vulnerable phpBB software and was able to deface over 40,000 websites[28, 29].

In August 2005, with monetary benefit being the primary motive, Farid Essebar and Atilla Ekici[30] launched the *Zotob* worm[31] that exploited known vulnerabilities in Windows 2000 operating system[32]. *Zotob* slowed down computers of more than 100 companies causing them to continually crash and reboot while also opening a backdoor[33]. The worm caused an estimated average loss of $97,000 and 80 hours of cleanup per affected company[34].

In November 2008, *Conficker* worm was detected exploiting a vulnerability present in multiple Microsoft operating systems that allowed arbitrary remote code execution, for which Microsoft had issued a critical security bulletin on 23rd October, 2008[35]. *Conficker* infected 11 million hosts globally[36] with an estimated economic cost of $9.1 billion[37]. *Conficker* is believed to have originated in Ukraine[38].

Undirected cyberattacks, exploiting vulnerabilities in widely deployed software, remain to be major threats. *Heart Bleed* vulnerability is a recent witness[39, 40].

2.2 Targeted/Directed Cyberattacks

Targeted cyberattacks have been further categorized according to their targets and potential motivations.

2.2.1 Cyberattacks directed towards Nations

Cyberattacks have targeted nations by specifically going after targets within a particular nation and disrupting normal operations of computers and networks.

The US-China spy plane incident in April, 2001 led to a month long online battle between US and Chinese hackers, both causing defacements and posting messages on government related websites while accusing each other of the incident[41].

April 2007 witnessed the first series of cyberattacks targeting a particular nation, Estonia[42]. Botnets from all around the world were directed towards Estonia in a Distributed Denial-of-Service(DDoS) attack and also posted messages on various defaced websites. The main targets were the websites of Estonian President and parliament, government ministries, political parties,

news organizations, the two biggest banks and telecommunication firms[42]. Consequently, Estonia had to cut off its networks from the outside internet to protect against these attacks. Only one bank reported an estimated loss of 1 million dollars[43]. The attacks were seen as patriotic response and blunt payback from Russia against the Estonian government's decision to relocate the statue of Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn. Some reports alleged Russian government involvement, given the money and technical skills required to carry out such a sophisticated and co-ordinated attack on a country[44, 45]. Other experts doubted Russian involvement[46][47]. In 2009, a Kremlin-backed youth group claimed to have carried out these cyberattacks[48].

In September 2007, Israel disrupted Syrian air defense systems during Operation Orchard allowing Israeli F-15s and F-16s to enter Syrian airspace without detection[49, 50].

August 2008, Georgia suffered massive DDoS attacks and traffic re-routing that crippled its limited Internet infrastructure[51, 52]. The attacks started before the beginning of conventional war between Russia and Georgia and continued alongside the military engagement. Georgia blamed Russia for the cyberattacks, though the attacks originated from infected computers in various countries[53].

In January 2009, Israeli websites belonging to small companies and government bodies including the Israeli Defense Forces and the Israel Discount Bank were targeted with DDoS attacks and defacements in protest and retaliation to Israeli military attacks on Gaza[54]. Israel suspected former Soviet Union hackers, paid by Hamas or Hezbollah, for carrying out the attacks[55]. In July 2009, DDoS attacks were directed at major government, news media, and financial websites in South Korea and the US[56, 57]. South Korea, where some websites suffered outages for days, blamed the North Korean telecommunications ministry for the attacks[58].

In October 2012, DDoS attacks on Iran slowed down the Internet throughout the country[59].

2.2.2 Cyberattacks threatening National Security

Government organizations and personnel, military networks, defense contractors and other entities tied to national security have been targets of various cyberattacks worldwide aimed at getting sensitive information on military, political, economic, strategic and government.

Beginning in 2003, several US government agencies, including the departments of State, Energy and Homeland Security, NASA, as well as defense contractors were targeted by a series of coordinated cyberattacks[60, 61]. The attacks, code named *Titan Rain*, breached hundreds of unclassified networks siphoning off any available information. In August 2005, SANS Institute revealed that the attacks originated in Chinese province of Guangdong[62].

In May 2006, hackers targeted US State Department's headquarters and offices dealing with Asia, breaching the unclassified network[63]. The attacks exploited a zero-day vulnerability in Microsoft operating system and the malware exploit was delivered via phishing emails[64]. Sensitive information including passwords were believed to have been stolen.[63, 65]. In August 2006, Maj. Gen. William Lord publicly stated that 10 to 20 terabytes of data has been downloaded by

China from NIPRNet[66]. Also in 2006, spyware was found on computer systems of classified departments at China's China Aerospace Science & Industry Corporation[67].

In June 2007, cyberattacks originating in China targeted the US Department of Defense[68]. Spoofed email with recognizable names and malicious code was sent to the office of the Secretary of Defense. The malicious code exploited a known vulnerability in Microsoft Windows operating system. Sensitive information accessible from the network, like user IDs and passwords that allowed access to the entire unclassified network[69, 70], was exfiltrated, causing 1,500 computers to be taken offline[71]. In October, China accused foreign hackers from Taiwan and the US for stealing information, without providing any other details[67]. In November 2007, about 1,100 employees of nuclear arms lab at Oak Ridge National Laboratory were targeted with phishing emails with attached malware, originating at Internet and web addresses located in China. The attackers were able to obtain visitor information to the lab since 1990[72].

During the summer of 2008, the databases of Republican and Democratic presidential campaigns containing sensitive internal documents and private data were copied in a cyberattack[73]. The attacks were traced back to China by US intelligence agencies[74]. In November 2008, classified and unclassified networks of US Department of Defense and US Central Command were hacked because of a SillyFDC malware variant which was delivered via an infected USB stick at a base in Middle-East[75, 76].

In 2009, *Conficker* worm infection grounded French fighter planes[77] and computers on board Royal Navy warships and submarines were also affected[78]. In March 2009, a global cyber-espionage network named *GhostNet* was revealed, which exploited a known vulnerability in Adobe PDF reader[79]. *GhostNet* spied on multiple high-value targets like ministries of foreign affairs, embassies etc. in 103 countries, international organizations, news media and NGOs[80]. Most attacks under *GhostNet* originated in China, though involvement of the Chinese government was not ascertained[81]. In April 2009, hackers stole terabytes of data related to design and electronics systems of the F-35 Lightning II fighter jet. The sensitive data was encrypted before exfiltration to sources in China, making it impossible to determine precisely what information was stolen[82].

In April 2010, computer systems of the Indian Defense Ministry and Indian embassies in various countries were compromised[83]. Attacks stole classified information including designs of weapon systems, internal security assessments of sensitive regions and emails from Dalai Lama's office[84]. The attacks were traced back to China[85, 83].

In April 2011, within a month of the RSA breach[86], the stolen SecurID tokens were used to hack defense contractor L-3 Communications for theft of sensitive information[87]. In May, Lockheed Martin[88, 89] as well as Northrop Grumman[90, 86] were targeted in a cyber-attack using the stolen RSA SecurID tokens, though the attacks were thwarted. In July 2011, unknown attackers breached Pentagon networks stealing 24,000 files, with the exact damage being undisclosed[91, 92]. In August 2011, operation *Shady Rat* was revealed to have been attacking 70 corporations and government organizations in the US since mid-2006 and other international targets[93, 94]. This cyber-espionage campaign employed spear-phishing with attached files containing malware that exploited a known vulnerability in Microsoft Excel to open a backdoor[95]. In October 2011, 2 US satellites were interfered with for few minutes, allegedly by attackers from China[96].

In September 2012, the White House became a victim of spear-phishing attacks allegedly carried out by hackers in China[97]. In December 2012, computer networks of Indian government were breached, compromising 10,000 email accounts of top government officials and information on troop deployment[98].

In February 2013, a US government report revealed that 23 US gas companies were targeted by cyberattacks that stole potentially security-sensitive information[99]. In May, infiltration of systems at defense contractor QinetiQ by Chinese hackers was discovered. The attackers were in the system since 2007 because of a known security flaw resulting in the compromise and exfiltration of most of the company's research[100]. Also in May, a report by the Defense Science Board reported that designs of US defense systems including the Patriot missile system (PAC-3), Terminal High Altitude Area Defense and Navy's Aegis ballistic-missile defense system had been compromised by persistent, highly-sophisticated cyberattacks carried out by China[101]. In August 2013, hackers gained access to personal information, social security numbers and payroll information of 14,000 current and former employees at the US Department of Energy[102]. In September 2013, *Operation Kimsuky* was revealed to be spying and stealing information from South Korean think-tank organizations using malware, delivered via a spear-phishing campaign. North Korea was blamed for the targeted attack as the malware specifically disabled a particular South Korean antivirus[103].

2.2.3 Cyberattacks on Companies and Organizations

Cyberattacks discussed in this section targeted organizations in banking, finance, oil and energy, communications, technology, news media, retail sectors and other private enterprises.

In January 2001, Microsoft websites were targeted with a DDoS attack for a day due to poor configuration of the network[104].

In 2004, hosts infected with the *Mydoom* worm were used in DDoS attacks on Google, Microsoft and other companies[105].

In January 2007, retail giant TJX suffered a targeted hack due to poor security of their WiFi network that allowed sniffing of information[106] on 45.7 million accounts including credit and debit card numbers[107, 108]. Albert Gonzalez was convicted and sentenced to 20 years in prison for being the primary hacker[109] in the attack that costed $4.5 billion[110].

During the summer of 2008, 3 US oil companies were targeted with phishing emails containing links to spyware to infect their systems. Attackers stole data on discoveries of new oil deposits, e-mails, passwords and other information related to executives who had access to proprietary exploration and discovery information[111, 112]. China's involvement was suspected in the attacks[111].

In December 2009, Citibank lost tens of millions of dollars to a cyberattack, which it denied[113, 114]. Hackers used spyware keylogger in one of the publicly known incidents to gain access to user account[115]. Source IPs used in the attacks had been linked to Russian Business Network hacking group in the past[116].

In January 2010, Google announced that it has been targeted by sophisticated cyberattacks that compromised various user accounts[117]. At least 34 other companies including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical were hit by similar attacks, named *Operation Aurora*. The attacks exploited a zero-day vulnerability in Adobe Reader, known vulnerabilities in Microsoft Internet Explorer and used spear-phishing to deliver malware for stealing data from targeted companies[118, 119]. In October 2010, it was reported that banks in the US lost over $12 million to hackers who used Zeus trojan to infect computers via phishing emails and recorded keystrokes to steal bank account credentials[120]. 100 people were charged as suspects.[121].

In March 2011, Epsilon suffered a data breach due malware delivered via spear-phishing campaign[122, 123, 124]. The breach cost $225 million in damages plus additional costs to clients with the total running in billions[125]. Also in March, security firm RSA suffered a massive breach in its network[86] due to malware exploiting a zero-day and an existing Adobe Flash vulnerability to install a backdoor[126]. Source code of company's SecurID two-factor authentication product was stolen[127] with resulting cost of $66 million for replacing the SecurID tokens[128]. In April 2011, malware introduced months ago caused a three-day service outage at Nonghyup agricultural bank in South Korea[129, 130]. North Korea was blamed for the disruption that prevented 300 million bank customers from using bank ATM's and credit cards[130]. In April 2011, Sony Playstation Network lost personal information of about 77 million users, including credit card numbers which were stored unencrypted costing Sony $171 million[131, 132, 133, 134]. During May-June 2011, Sony BMG lost billions of dollars[135] after it was hacked due to SQL-injection by hacker group LulzSec that posted plaintext data of 50,000 users online to expose weaknesses in the company's security[136, 137] In May 2011, 360,083 credit card account details were stolen in a data breach at Citigroup Inc.[138, 139]. The hack exploited insecure direct object reference, SQL-injection and XSS vulnerabilities[140]. Attackers stole $2.7 million[141] and it cost additional $77 million to the company[142]. During October 2011, multiple chemical and defense sector companies worldwide came under "Nitro-attacks" allegedly carried out by China[143, 144]. Phishing emails with attached malware and remote administration tools were used in these cyberattacks[144]. In June 2011, International Monetary Fund suffered a cyberattack aimed at stealing confidential information using spear-phishing to install malware. The exact damage caused by the attack remains undisclosed[145, 146]. In November 2011, a cyberattack employing phishing on Norway's oil, gas and energy systems stole industrial drawings, industrial secrets and user credentials[147].

In January 2012, Zappos lost the data of 24 million customers including emails, phone numbers and billing addresses[148]. Reported in June 2012, Gmail accounts of various users were hijacked by unknown state-sponsored attackers that exploited a zero-day vulnerability in Internet Explorer allowing remote code execution[149, 150]. In September 2012, an industrial espionage campaign called *The Mirage Campaign* as it used Mirage remote exploit tool, targeted computers with IP addresses owned by oil, energy and military organizations primarily in Taiwan or the Philippines, with some IPs located in Nigeria, Brazil, Israel, Canada and Egypt[151].

In February 2013, water-holing cyberattacks exploiting a zero-day vulnerability in Java targeted Facebook, Apple and Microsoft[152, 153, 154]. The zero-day exploit was used to automatically download malware. In March, a virus from phishing emails caused sudden shutdown of 2 South Korean banks and 3 TV broadcasters, severely affecting broadcasting and ATM

services[155]. Also in March, *TeamSpy* espionage operation was discovered changing TeamViewer's[2] DLL files to spy and control targeted computers. The list of victims included high profile industrial, research and diplomatic targets in Hungary and Embassy of NATO/EU state in Russia[156]. The Reserve Bank of Australia was also hacked in March and malware was installed to gather intelligence on sensitive G20 negotiations[157]. The exact extent of damage remains undisclosed, with China being the alleged attacker[157]. In April, Japan's Goo and Yahoo Internet portals were hacked. 100,000 records of user data including financial details like credit card numbers were leaked from Goo.[158]. In July 2013, a Ubisoft website was hacked exposing user emails and passwords[159], potentially affecting up to 58 million accounts[160]. JPMorgan Chase bank also suffered a massive data breach in July 2013. 465,000 holders of bank's prepaid cash cards had their personal information accessed by the attackers[161]. In November 2013, Ireland-based Loyalty Build lost 376,000 credit card numbers and personal information of 1.12 million customers[162]. In December 2013, retail chain Target suffered a massive network breach[163]. Attackers installed memory-scraping malware on point-of-sale (POS) devices by gaining entry access to the network using stolen credentials from HVAC service[164, 165]. Personal information of up to 70 million people and information on 40 million credit and debit card accounts was compromised. The reported cost of the breach was $148 million[166]. In December 2013, Chinese hackers spied on computers of G20 members from Europe before the G20 meeting[167]. Hackers employed spear-phishing for infecting the targets with malware to gather intelligence on summit negotiations.

2.2.4 Cyberattacks on Critical Infrastructure

Critical infrastructure[3] is an attractive target for cyberattacks, given its importance in sustaining normal daily operations. Vulnerabilities in computers supporting critical infrastructure can be equally exploited by cyberattacks as in any other vulnerable system.

In 2003, *Slammer* worm disabled the safety monitoring system at Ohio nuclear plant for 5 hours[168]. In 2004, two Romanian hackers penetrated the network of National Science Foundation's Amundsen-Scott South Pole Station and gained control of the critical life support system, potentially endangering the lives of 58 scientists and contractors[169].

In May 2009, FAA's Air-Traffic Network, used to guide and control civilian air traffic is the US, was hacked multiple times because of known vulnerabilities in the system[170, 171].

In June 2010, a highly-sophisticated and targeted cyberattack disrupted centrifuges at Iran's Natanz Uranium enrichment plant[172]. The virus, called *Stuxnet*, exploited 4 zero-day vulnerabilities in Windows operating system[173]. Given the sophistication and complexity of targeting a specific system, *Stuxnet* was believed to have been created by Israel and the US to disrupt Iran's nuclear ambitions[174, 175, 176].

In October 2011, a malware with similarities to *Stuxnet* known as *Duqu* was discovered[177, 178]. *Duqu* created back doors which could be exploited to destroy the network at an arbitrary time and also had a keylogger built in to it. A zero-day vulnerability was exploited to distribute

[2] http://www.teamviewer.com/en/index.aspx
[3] http://www.dhs.gov/what-critical-infrastructure

Duqu trojan[179]. A month later, Iran admitted that its nuclear sites had been hit by *Duqu*[180]. In December 2011, cyberattacks on Northwest rail company disrupted railway signals for two days[181].

In May 2012, *Flame* malware allegedly created by Israel and the US, aimed at slowing down Iran's ability to develop a nuclear weapon was discovered[182, 183]. *Flame* exploited existing bugs and a zero-day vulnerability in Windows operating system[183, 184] to infect systems in Iran, Lebanon, Syria, Sudan, the Israeli Occupied Territories and other countries in the Middle East and North Africa two years ago[185]. In August 2012, oil producer Saudi Aramco was targeted with *Shamoon* malware to disrupt oil production[186, 187]. The malware infected 30,000 workstations without disrupting any production. Cutting Sword of Justice claimed responsibility for the attack[187], though it was attributed to unknown nation-state actor[188].

In May 2013, it was revealed that unauthorized access to databases of National Inventory of Dams allowed attackers to get their hands on sensitive information[189, 190]. In the same month, Israel stated that it had prevented cyberattacks from Syrian Electronic Army targeting computers of water systems for city of Haifa[191].

2.2.5 Hacktivism[4]

Cyberspace has also come under attacks motivated by hactivism leading to disruptions and losses in certain cases. Attacks that caused widespread disruptions have only been mentioned here.

In November 2010, hacker group *Anonymous*[192] under *Operation Payback* launched targeted DDoS attacks on financial organizations like VISA, MasterCard, PayPal etc. in protest and retaliation to the suspension of WikiLeaks accounts[193, 194].

In June 2011, *Anonymous* hacked defense contractor Booz Allen Hamilton to publicly humiliate companies and agencies that fail to protect employee and consumer data[195]. The attacks were carried out using SQL-injection leaking encrypted passwords and 53,000 .mil email addresses online[196, 197].

In February 2013, Bank of America suffered cyberattacks from *Anonymous* with the group claiming that the attacks were in retaliation to bank's online intelligence gathering operation on hacktivists[198]. Poor security mechanism caused over 6 GB of data to be leaked, including source code for OpenCalais and salary, bonus details of hundred of thousands of executives and employees of various corporations from all around the world[198].

2.2.6 Global Cyber-espionage Campaigns

In October 2011, it was reported that 760 organizations worldwide have been under attack by a cyber-espionage campaign stealing sensitive information[199].

In January 2013, another global malware campaign, called *Red October* was exposed and is believed to have been active since May 2007[200]. The campaign exploited vulnerabilities in

[4]http://dictionary.reference.com/browse/hacktivism

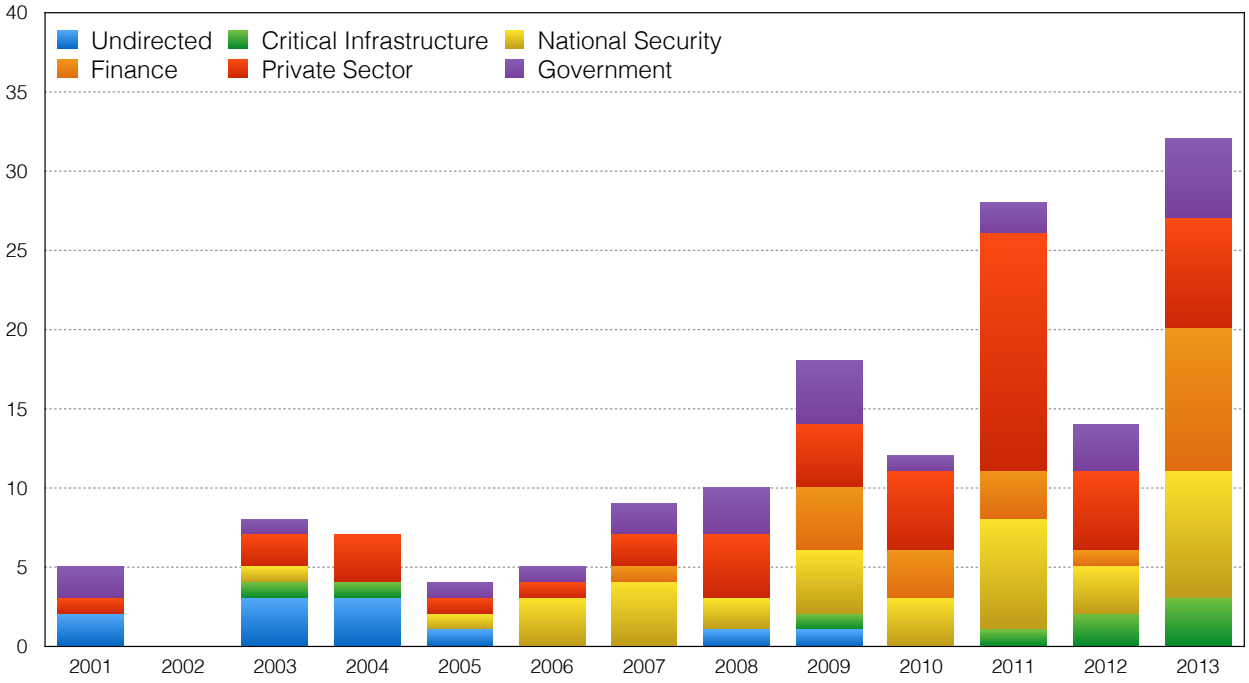

Figure 1: Sectors affected by Cyberattacks

Java, Microsoft Execl and Word softwares for stealing information from governments, embassies, research institutions, organization in trade and commerce, nuclear/energy research, oil and gas, aerospace and military sectors[201, 200].

In June 2013, cyber-espionage campaign named *NetTraveler*, allegedly by China, was discovered with victims across multiple sectors including government institutions, embassies, oil and gas industry, research institutes, military contractors and activists in 40 countries[202].

In September 2013, another cyber-espionage campaign, *Operation IceFrog*, was revealed. It had attacked military, shipbuilding, maritime operations, research companies, telecom operators, satellite operators, mass media and television organizations in South Korea and Japan. The malware exploited known vulnerabilities and hijacked sensitive documents and credentials for accessing internal networks[203].

3 Analysis of Cyberattacks

This section provides an analysis of surveyed cyberattacks from various perspectives. Figure 1 shows the numbers of attacks and their targeted sectors over the years. The increasing trend in number of cyberattacks can be attributed to adoption of computers in more and more operations and tasks across all sectors. Figure 3 sums up the motivation behind various cyberattacks. Techniques and exploits used by the attackers for cyberattacks have been summarized in Figure 2.

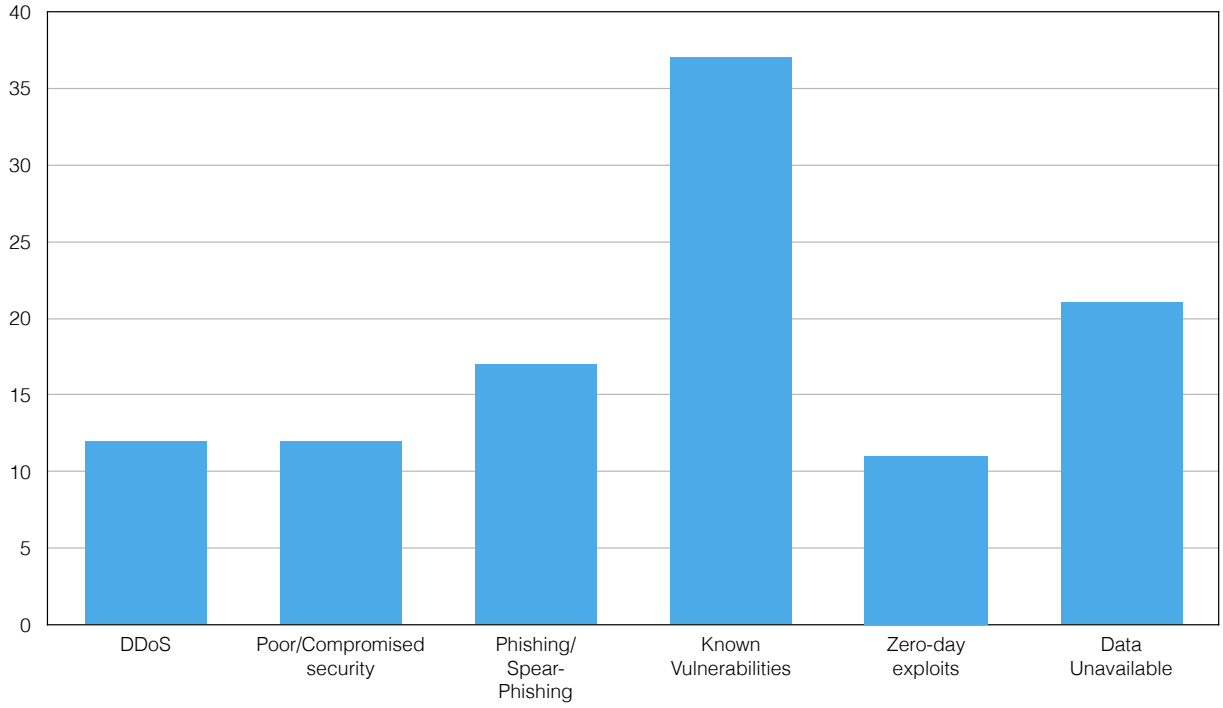

Figure 2: Exploits/Techniques employed in Cyberattacks

Undirected cyberattacks have subsided while targeted attacks have increased and diversified with respect to targeting. Cyberattacks on critical infrastructure2.2.4 and national security2.2.2 establishments have shown an increasing trend. This should be a major concern for countries who rely on computers and their interconnections for storing sensitive information and proper functioning of critical infrastructure. A continued, sophisticated cyberattack can severely cripple a nation by targeting its critical infrastructure. Private sector companies and organizations have also seen a steady rise in the number of cyberattacks. Governmental organizations as well have fallen prey to well organized and sophisticated adversaries which are going after information, both classified and unclassified, and using the stolen information in future cyberattacks. The attack strategies provide a much more vivid picture to support the argument.

Figure 2 shows that most widespread attacks like Slammer and Blaster worm[12, 14] and sophisticated global cyber-espionage campaigns mentioned in 2.2.6 and many other cyberattacks exploited already known vulnerabilities with patches already available for most of them. Next to known vulnerabilities, poor or compromised security mechanisms paved way for successful cyberattacks. For example, in the cases of Sony[132] and Target[165] breaches, poor security was responsible for the attacks. Compromised security due to attack on RSA[127] allowed attacks on Lockheed Martin and Northrop Grumman[89, 90] in 2011. Phishing/Spear-phishing was the most common mechanism used to deliver malware that exploited vulnerabilities in the system. Information stolen from non-classified sources[60, 61, 63, 75] was most likely used in the phishing attacks mentioned in 2.2.2. Distributed denial-of-service attacks remain a popular technique for disruption of services evident from attacks on Estonia[44] etc., though the damage caused by them is minimal as compared to other cyberattacks. Zero-day exploits have also surfaced in sophisticated

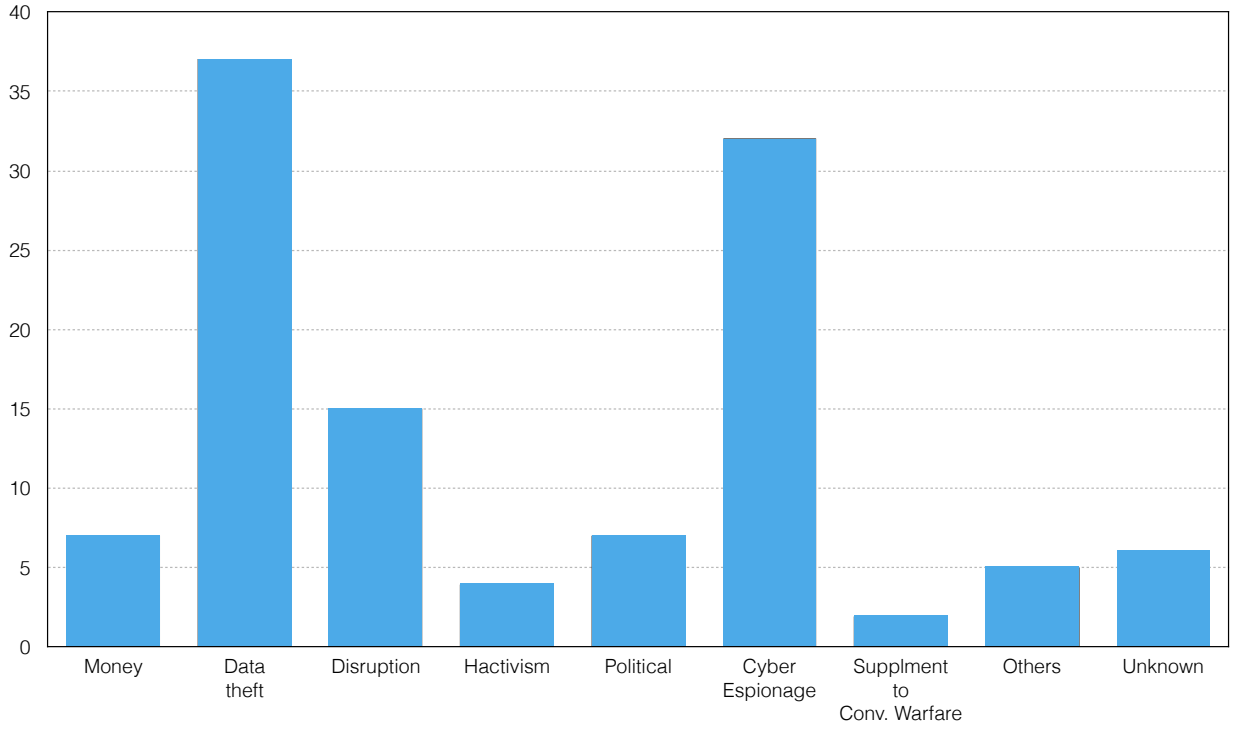

Figure 3: Motivation behind Cyberattacks

cyber attacks like Stuxnet[172]. Defending against such attacks is harder, though, measures can be taken be prevent introduction of malware in the system by limiting access and preventing common delivery mechanisms like spear-phishing. Also, exact details of many cyberattacks on companies, governments and other organizations are not disclosed publicly due to security concerns. However, sharing the details can help in developing better security mechanisms and defenses.

Understanding the motivation behind cyberattacks can shed light on the likelihood of a computer system to be targeted by a cyberattack. Data theft shows up as the biggest motivation behind cyberattacks, going after user information, credit card numbers, sensitive information like industrial secrets, corporate access credentials, banking information etc. This indicates that any computer system storing such data is a potential target and therefore, must be secured against all known vulnerabilities and exploits. After data-theft, cyber-espionage was the primary motive behind majority of cyberattacks including cyber-espionage campaigns [See 2.2.6] aimed at spying, economic-espionage, industrial-espionage etc. The persistence of these cyberattacks calls for securing all entities in the system to prevent any weak link in the security chain, which also includes the human user.

Disruption of services and networks by DDoS attacks has also motivated many cyberattacks on nation-specific targets [See. 2.2.1]. Cyberattacks on Estonia and South Korea[130] should be taken as warnings for future attacks aimed at disruption of services, as they pose threat to stability of daily activities as well as financial losses due to downtime. Hactivism can be seen as an emerging threat to computer systems, even though they have been vastly limited to DDoS attacks and defacements, the cost of attacks to the targets can be significant[204]. Criminals have also resorted to cyberattacks, stealing money being one the motives. The number of attacks directly aimed at

stealing money remains low as theft of financial information has been covered as data-theft. A rising motivation behind cyber-attacks is to supplement conventional warfare. Cyberattacks on Georgia[51] and use of cyber-offensive capability used by Israel during a military operation[49] are among the known incidents to have supplemented conventional warfare with attacks in cyber domain. With sophisticated defense technologies relying heavily on computers systems, protecting those systems against cyberattacks will be paramount in future conflicts.

4 Conclusion

Increasing trend in the number of cyberattacks will continue as more systems get connected to the Internet. Protecting these systems against cyberattacks to ensure normal operation will be the key to minimize disruptions and losses in terms of data, money and time. Majority of cyberattacks we discussed could have been prevented had the systems been kept up-to-date with latest patches. And yet, attacks exploiting known vulnerabilities are not subsiding. This shows that valuable lessons are not being learned from past experiences. Same is the story with attacks employing spear-phishing, which is known to have caused tremendous amount of damage in both classified and unclassified domain.

Attributing cyberattacks based on technical evidence is also hard due to the very basic structure of the Internet that allows redirection, proxying and spoofing of the source. Alleged sources of most of the cyberattacks described were not based on technical evidence but derived from events in non-cyber world. Therefore, a counter-offensive in response to a cyberattack may not be a feasible option at all and defending the systems in the first place becomes more important.

With increasing adoption of technology and connections of smart devices with the Internet, security of future systems must be considered as an integral part of the system design rather than it being an afterthought. Lack of security in such systems will not only worsen the known consequences but will have far more damaging effects on the society. Learning from past experiences and designing better systems in future can help in changing the trend of increasing cyberattacks.

Acknowledgment

I would like to thank Kyle Ehrlich and Valerie Palermo for reviewing this paper and giving their valuable feedback and comments.

References

[1] INSTITUTE FOR SECURITY TECHNOLOGY STUDIES. Law enforcement tools and technologies for investigating cyber attacks: Gap analysis report, 2004. 1

[2] 2013 Cost of Cyber Crime Study: United States. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf, 2013. Last Accessed November 10, 2014. 1

[3] Net Losses: Estimating the Global Cost of Cybercrime. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf, 2104. Last Accessed November 10, 2014. 1

[4] Olympic Cyber-attack Fears Keep Fans Home. http://www.bbspot.com/News/2004/08/olympic_cyber_attacks.html, 2004. Last Accessed October 15, 2014. 1

[5] Anna Kournikova virus spreading like wildfire. http://www.theregister.co.uk/2001/02/12/anna_kournikova_virus_spreading_like, 2001. Last Accessed October 23, 2014. 2

[6] "AnnaKournikova Virus"- Lessons Not Learned . http://www.theregister.co.uk/2001/02/12/anna_kournikova_virus_spreading_like, 2001. Last Accessed October 23, 2014. 2

[7] ILOVEYOU Worm. http://en.wikipedia.org/wiki/ILOVEYOU, 2000. Last Accessed October 13, 2014. 2

[8] Confession by author of Anna Kournikova virus. http://www.out-law.com/page-1387, 2001. Last Accessed October 23, 2014. 2

[9] "Code Red" worm claims 12,000 servers. http://news.cnet.com/Code-Red-worm-claims-12,000-servers/2100-1001_3-270170.html, 2001. Last Accessed October 23, 2014. 2

[10] The Spread of the Code-Red Worm (CRv2). http://www.caida.org/research/security/code-red/coderedv2_analysis.xml, 2001. Last Accessed October 23, 2014. 2

[11] The Mechanisms and Effects of the Code Red Worm. http://www.sans.org/reading-room/whitepapers/malicious/mechanisms-effects-code-red-worm-87, 2001. Last Accessed October 23, 2014. 2

[12] SQL Slammer worm wreaks havoc on Internet. http://www.zdnet.com/sql-slammer-worm-wreaks-havoc-on-internet-3002129330/, 2003. Last Accessed October 13, 2014. 2, 11

[13] Inside the Slammer Worm. http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf, 2003. Last Accessed October 13, 2014. 2

[14] Blaster worm spreading; experts warn of attack. http://www.computerworld.com/article/2571072/malware-vulnerabilities/blaster-worm-spreading--experts-warn-of-attack.html, 2003. Last Accessed October 13, 2014. 2, 11

[15] Blaster worm author gets jail time. http://www.infoworld.com/article/2643777/techology-business/blaster-worm-author-gets-jail-time.html, 2003. Last Accessed October 13, 2014. 2

[16] W32/Blaster worm. http://www.cert.org/historical/advisories/CA-2003-20.cfm, 2003. Last Accessed October 13, 2014. 2

[17] Sober email worm gives Windows users the DTs. http://www.theregister.co.uk/2003/10/28/sober_email_worm_gives_windows, 2003. Last Accessed October 13, 2014. 3

[18] E-mail worm throws up hate spam. http://news.bbc.co.uk/2/hi/technology/4552197.stm, 2003. Last Accessed October 13, 2014. 3

[19] Fake FBI virus catches net users. http://news.bbc.co.uk/2/hi/technology/4466016.stm, 2003. Last Accessed October 13, 2014. 3

[20] Security firm: MyDoom worm fastest yet. http://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed, 2004. Last Accessed October 14, 2014. 3

[21] More Doom? http://www.newsweek.com/more-doom-131157, 2004. Last Accessed October 14, 2014. 3

[22] VIRULENT MYDOOM COMPUTER VIRUS CREATED IN RUSSIA. http://www.sptimes.ru/index.php?action_id=2&story_id=12138, 2004. Last Accessed October 14, 2014. 3

[23] New Version of MyDoom Worm in Zero-Day Attack. http://www.eweek.com/c/a/Security/New-Version-of-MyDoom-Worm-in-ZeroDay-Attack, 2004. Last Accessed October 14, 2014. 3

[24] Sasser worm begins to spread. http://news.cnet.com/Sasser-worm-begins-to-spread/2100-7349_3-5203764.html, 2004. Last Accessed October 14, 2014. 3

[25] German admits creating Sasser. http://news.bbc.co.uk/2/hi/technology/4649361.stm, 2004. Last Accessed October 14, 2014. 3

[26] German Teen Confirms He Created the Sasser Worm. http://www.pcworld.com/article/121709/article.html, 2004. Last Accessed October 14, 2014. 3

[27] CVE-2003-0533. http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533, 2004. Last Accessed October 14, 2014. 3

[28] Net worm using Google to spread. http://news.cnet.com/Net-worm-using-Google-to-spread/2100-7349_3-5499725.html, 2004. Last Accessed October 14, 2014. 3

[29] Anti-Santy worm spreads. http://www.zdnet.com/anti-santy-worm-spreads-3039182954/, 2004. Last Accessed October 14, 2014. 3

[30] Money motive drove virus suspects. http://news.bbc.co.uk/2/hi/technology/4205220.stm, 2005. Last Accessed October 13, 2014. 3

[31] Virus Attacks Windows Computers at Companies. http://www.nytimes.com/2005/08/17/technology/17virus.html, 2005. Last Accessed October 13, 2014. 3

[32] Zotob causes carnage in corporate networks. http://www.pcworld.idg.com.au/article/8890/zotob_causes_carnage_corporate_networks, 2005. Last Accessed October 13, 2014. 3

[33] Zotob Worm Information. http://www.cisco.com/web/about/security/intelligence/zotob-worm.html, 2005. Last Accessed October 13, 2014. 3

[34] Cybertrust Research Illustrates Worldwide Impact of Zotob Worm. http://www.prnewswire.com/news-releases/cybertrust-research-illustrates-worldwide-impact-of-zotob-worm-55580177.html, 2005. Last Accessed October 13, 2014. 3

[35] The Conficker Worm. http://www.sans.org/security-resources/malwarefaq/conficker-worm.php, 2008. Last Accessed October 17, 2014. 3

[36] The Conficker worm, three years and counting. https://nakedsecurity.sophos.com/2011/11/24/the-conficker-worm-three-years-and-counting, 2009. Last Accessed October 17, 2014. 3

[37] Conficker's estimated economic cost? $9.1 billion. http://www.zdnet.com/blog/security/confickers-estimated-economic-cost-9-1-billion/3207, 2009. Last Accessed October 17, 2014. 3

[38] AN ANALYSIS OF CONFICKER'S LOGIC AND RENDEZVOUS POINTS. http://en.ria.ru/military_news/20140819/192147952/High-Profile-Cyber-Attacks-2000-2014.html, 2009. Last Accessed October 17, 2014. 3

[39] Heartbleed. https://www.schneier.com/blog/archives/2014/04/heartbleed.html, 2104. Last Accessed November 10, 2014. 3

[40] The Heartbleed Hit List: The Passwords You Need to Change Right Now. http://mashable.com/2014/04/09/heartbleed-bug-websites-affected, 2104. Last Accessed November 10, 2014. 3

[41] Chinese and American hackers declare 'cyberwar'. http://www.theguardian.com/technology/2001/may/04/china.internationalnews, 2001. Last Accessed October 23, 2014. 3

[42] Hackers Take Down the Most Wired Country in Europe. http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all, 2007. Last Accessed October 13, 2014. 3, 4

[43] Stephen Herzog. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2):4, 2011. 4

[44] Digital Fears Emerge After Data Siege in Estonia. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0, 2007. Last Accessed October 13, 2014. 4, 11

[45] Russia accused of unleashing cyberwar to disable Estonia. http://www.theguardian.com/world/2007/may/17/topstories3.russia, 2007. Last Accessed October 12, 2014. 4

[46] Estonia has no evidence of Kremlin involvement in cyber attacks. http://en.ria.ru/world/20070906/76959190.html, 2007. Last Accessed October 12, 2014. 4

[47] Experts doubt Russian government launched DDoS attacks. http://searchsecurity.techtarget.com/news/1255548/Experts-doubt-Russian-government-launched-DDoS-attacks, 2007. Last Accessed October 12, 2014. 4

[48] Kremlin-backed group behind Estonia cyber blitz. http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz3JAjncvj4, 2009. Last Accessed October 13, 2014. 4

[49] Israel suspected of 'hacking' Syrian air defences. http://www.theregister.co.uk/2007/10/04/radar_hack_raid, 2007. Last Accessed October 18, 2014. 4, 13

[50] Israeli sky-hack switched off Syrian radars countrywide. http://www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion, 2007. Last Accessed October 18, 2014. 4

[51] Georgia: Russia 'conducting cyber war'. http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html, 2008. Last Accessed October 24, 2014. 4, 13

[52] Cyberattacks knock out Georgia's Internet presence. http://www.computerworld.com/article/2532289/cybercrime-hacking/cyberattacks-knock-out-georgia-s-internet-presence.html, 2008. Last Accessed October 24, 2014. 4

[53] Before the Gunfire, Cyberattacks. http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0, 2008. Last Accessed October 24, 2014. 4

[54] Hackers wage virtual war on Israeli sites. http://www.alarabiya.net/articles/2009/01/05/63566.html, 2009. Last Accessed October 22, 2014. 4

[55] Hamas, Hezbollah employ Russian hackers for cyber attacks on Israel. http://www.homelandsecuritynewswire.com/hamas-hezbollah-employ-russian-hackers-cyber-attacks-israel, 2009. Last Accessed October 22, 2014. 4

[56] Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea. http://www.nytimes.com/2009/07/10/technology/10cyber.html, 2009. Last Accessed October 17, 2014. 4

[57] Governments hit by cyber attack. http://news.bbc.co.uk/2/hi/technology/8139821.stm, 2009. Last Accessed October 17, 2014. 4

[58] N. Korean ministry behind July cyber attacks: spy chief. http://english.yonhapnews.co.kr/northkorea/2009/10/30/0401000000AEN20091030002200315.HTML, 2009. Last Accessed October 17, 2014. 4

[59] Cyber attackers disrupt Internet in Iran: official. http://www.reuters.com/article/2012/10/03/us-iran-cyber-idUSBRE8920MO20121003, 2012. Last Accessed October 26, 2014. 4

[60] Hackers Attack Via Chinese Web Sites. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html, 2005. Last Accessed October 18, 2014. 4, 11

[61] The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them). http://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm, 2005. Last Accessed October 18, 2014. 4, 11

[62] Hacker attacks in US linked to Chinese military: researchers. https://web.archive.org/web/20061222110758/http://www.breitbart.com/news/2005/12/12/051212224756.jwmkvntb.html, 2005. Last Accessed October 18, 2014. 4

[63] Computer Hackers Attack State Dept. http://www.nytimes.com/2006/07/12/washington/12hacker.html, 2006. Last Accessed October 18, 2014. 4, 11

[64] Response to May-July 2006 Cyber Intrusion on Department of State Computer Network. http://2001-2009.state.gov/m/ds/rls/rm/83256.htm, 2006. Last Accessed October 18, 2014. 4

[65] State Department Computers Hacked. http://www.cbsnews.com/news/state-department-computers-hacked, 2006. Last Accessed October 18, 2014. 4

[66] Red storm rising. http://gcn.com/articles/2006/08/17/red-storm-rising.aspx, 2006. Last Accessed October 18, 2014. 5

[67] The history of cyber attacks - a timeline. http://www.nato.int/docu/Review/2013/Cyber/timeline/EN/index.htm, 2007. Last Accessed October 18, 2014. 5

[68] Chinese hacked into Pentagon. http://www.ft.com/intl/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html#axzz3JAjncvj4, 2007. Last Accessed October 18, 2014. 5

[69] Defense officials still concerned about data lost in 2007 network attack. http://www.govexec.com/defense/2008/03/defense-officials-still-concerned-about-data-lost-in-2007-network-attack/26435/, 2007. Last Accessed October 18, 2014. 5

[70] Pentagon Source Says China Hacked Defense Department Computers. http://www.foxnews.com/story/2007/09/04/pentagon-source-says-china-hacked-defense-department-computers, 2007. Last Accessed October 18, 2014. 5

[71] Hacker forces 1,500 Pentagon computers offline. http://www.nbcnews.com/id/19358920/ns/technology_and_science-security/t/hacker-forces-pentagon-computers-offline, 2007. Last Accessed October 18, 2014. 5

[72] Cyber attack on U.S. nuclear arms lab linked to China. http://www.nytimes.com/2007/12/09/world/americas/09iht-hack.1.8653712.html, 2007. Last Accessed October 18, 2014. 5

[73] Obama, McCain computers 'hacked' during election campaign. http://www.theguardian.com/global/2008/nov/07/obama-white-house-usa, 2008. Last Accessed October 24, 2014. 5

[74] Chinese hacked Obama, McCain campaigns, took internal documents, officials say. http://investigations.nbcnews.com/_news/2013/06/06/18807056-chinese-hacked-obama-mccain-campaigns-took-internal-documents-officials-say, 2008. Last Accessed October 24, 2014. 5

[75] Defending a New Domain. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, 2008. Last Accessed October 24, 2014. 5, 11

[76] Infected USB drive blamed for '08 military cyber breach. http://www.computerworld.com/article/2514879/security0/infected-usb-drive-blamed-for--08-military-cyber-breach.html, 2008. Last Accessed October 24, 2014. 5

[77] French fighter planes grounded by computer virus. http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html, 2009. Last Accessed October 17, 2014. 5

[78] MoD networks still malware-plagued after two weeks. http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong, 2009. Last Accessed October 17, 2014. 5

[79] Ghost Story. http://nnc3.com/LM10/Magazine/Archive/2010/112/026-029_pdfhack/article.html, 2009. Last Accessed October 22, 2014. 5

[80] Vast Spy System Loots Computers in 103 Countries. http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1, 2009. Last Accessed October 22, 2014. 5

[81] China‘s global cyber-espionage network GhostNet penetrates 103 countries. http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html, 2009. Last Accessed October 22, 2014. 5

[82] Computer Spies Breach Fighter-Jet Project. http://online.wsj.com/news/articles/SB124027491029837401, 2009. Last Accessed October 22, 2014. 5

[83] Chinese agents hack into India’s secret documents: Report. http://timesofindia.indiatimes.com/india/Chinese-agents-hack-into-Indias-secret-documents-Report/articleshow/5766129.cms, 2010. Last Accessed October 28, 2014. 5

[84] Cyber-spies based in China target Indian government and Dalai Lama. http://www.theguardian.com/technology/2010/apr/06/cyber-spies-china-target-india, 2010. Last Accessed October 28, 2014. 5

[85] Researchers Trace Data Theft to Intruders in China. http://www.nytimes.com/2010/04/06/science/06cyber.html?pagewanted=all, 2010. Last Accessed October 28, 2014. 5

[86] Hacker Spies Hit Security Firm RSA. http://www.wired.com/2011/03/rsa-hacked/, 2011. Last Accessed October 21, 2014. 5, 7

[87] Second Defense Contractor L-3 ‘Actively Targeted‘ With RSA SecurID Hacks. http://www.wired.com/2011/05/l-3/, 2011. Last Accessed October 21, 2014. 5

[88] Lockheed Martin hit by cyber incident, U.S. says. http://www.washingtonpost.com/national/lockheed-martin-hit-by-cyber-incident-us-says/2011/05/28/AGTkefDH_story.html, 2011. Last Accessed October 21, 2014. 5

[89] RSA confirms its tokens used in Lockheed hack. http://gcn.com/articles/2011/06/07/rsa-confirms-tokens-used-to-hack-lockheed.aspx, 2011. Last Accessed October 21, 2014. 5, 11

[90] EXCLUSIVE: Northrop Grumman May Have Been Hit by Cyberattack, Source Says. http://www.foxnews.com/tech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/, 2011. Last Accessed October 21, 2014. 5, 11

[91] 24,000 Pentagon files stolen in major cyber breach, official says. http://www.washingtonpost.com/blogs/checkpoint-washington/post/24000-pentagon-files-stolen-in-major-cyber-breach-official-says/2011/07/14/gIQAsaaVEI_blog.html, 2011. Last Accessed October 21, 2014. 5

[92] Pentagon reveals 24,000 files stolen in cyber-attack. http://www.telegraph.co.uk/technology/news/8638944/Pentagon-reveals-24000-files-stolen-in-cyber-attack.html, 2011. Last Accessed October 21, 2014. 5

[93] Report on ‘Operation Shady RAT’ identifies widespread cyber-spying. http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html, 2011. Last Accessed October 22, 2014. 5

[94] Revealed: Operation Shady RAT. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf, 2011. Last Accessed October 22, 2014. 5

[95] The Truth Behind the Shady RAT. http://www.symantec.com/connect/blogs/truth-behind-shady-rat, 2011. Last Accessed October 22, 2014. 5

[96] Chinese Military Suspected in Hacker Attacks on U.S. Satellites. http://www.businessweek.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html, 2011. Last Accessed October 22, 2014. 5

[97] Chinese Hackers Break Into WH Military Office Network in Charge of Obama's Nuclear Football. http://nation.foxnews.com/white-house/2012/10/01/chinese-hackers-break-wh-military-office-network-charge-obamas-nuclear-football, 2012. Last Accessed October 26, 2014. 6

[98] Over 10,000 email IDs hit in 'worst' cyber attack. http://archive.indianexpress.com/news/over-10000-email-ids-hit-in-worst-cyber-attack/1046874, 2012. Last Accessed October 26, 2014. 6

[99] Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage. http://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage, 2013. Last Accessed October 28, 2014. 6

[100] China's Cyberspies Outwit Model for Bond's Q. http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html, 2013. Last Accessed October 28, 2014. 6

[101] Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies. http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html, 2013. Last Accessed October 28, 2014. 6

[102] Department of Energy Hacked Again. http://blogs.wsj.com/cio/2013/08/15/department-of-energy-hacked-again, 2013. Last Accessed October 28, 2014. 6

[103] Kaspersky Lab Analyzes Active Cyber-Espionage Campaign Primarily Targeting South Korean Entities. http://www.kaspersky.com/about/news/virus/2013/kaspersky_lab_analyzes_active_cyber-espionage_campaign_primarily_targeting_south_korean_entities, 2013. Last Accessed October 28, 2014. 6

[104] Web attackers knock out Microsoft sites. http://www.zdnet.com/web-attackers-knock-out-microsoft-sites-3002083974, 2001. Last Accessed October 23, 2014. 6

[105] MyDoom-O worm attacks Google and other internet search engines, Sophos reports. http://www.sophos.com/en-us/press-office/press-releases/2004/07/va_mydoomgoogle.aspx, 2004. Last Accessed October 14, 2014. 6

[106] Report: TJX thieves exploited wireless insecurities. http://www.securityfocus.com/brief/496, 2007. Last Accessed October 12, 2014. 6

[107] Retailer TJX reports massive data breach. http://www.infoworld.com/article/2661052/security/retailer-tjx-reports-massive-data-breach.html, 2007. Last Accessed October 12, 2014. 6

[108] TJX says 45.7 million customer records were compromised. http://news.cnet.com/TJX-says-45.7-million-customer-records-were-compromised/2100-1029_3-6171671.html, 2007. Last Accessed October 12, 2014. 6

[109] TJX Hacker Gets 20 Years in Prison. http://www.wired.com/2010/03/tjx-sentencing, 2007. Last Accessed October 12, 2014. 6

[110] Estimates Put T.J. Maxx Security Fiasco At $4.5 Billion. http://www.informationweek.com/estimates-put-tj-maxx-security-fiasco-at-\protect\T1\textdollar45-billion/d/d-id/1054704?, 2007. Last Accessed October 12, 2014. 6

[111] US oil industry hit by cyberattacks: Was China involved? http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved, 2008. Last Accessed October 24, 2014. 6

[112] Hackers Targeted Oil Companies for Oil-Location Data. http://www.wired.com/2010/01/hack-for-oil, 2008. Last Accessed October 24, 2014. 6

[113] FBI probes cyber attack on Citigroup: report. http://www.reuters.com/article/2009/12/22/us-citigroup-fbi-idUSTRE5BL0I320091222, 2009. Last Accessed October 17, 2014. 6

[114] Russian hacker gang who 'stole millions from Citibank' under investigation. http://www.theguardian.com/technology/2009/dec/22/russian-hackers-citigroup-cyber-security, 2009. Last Accessed October 17, 2014. 6

[115] FBI Probes Hack at Citibank. http://online.wsj.com/articles/SB126145280820801177, 2009. Last Accessed October 17, 2014. 6

[116] Report: FBI investigating Citibank cyberattack. http://www.cnet.com/news/report-fbi-investigating-citibank-cyberattack/, 2009. Last Accessed October 17, 2014. 6

[117] A new approach to China. http://googleblog.blogspot.com/2010/01/new-approach-to-china.html, 2010. Last Accessed October 22, 2014. 7

[118] New IE hole exploited in attacks on U.S. firms. http://www.cnet.com/news/new-ie-hole-exploited-in-attacks-on-u-s-firms, 2010. Last Accessed October 22, 2014. 7

[119] Google Hackers Targeted Source Code of More Than 30 Companies. http://www.wired.com/2010/01/google-hack-attack, 2010. Last Accessed October 22, 2014. 7

[120] 'Zeus Trojan' zaps $3 million from bank accounts. http://money.cnn.com/2010/09/30/technology/cyber_crime_charges, 2010. Last Accessed October 28, 2014. 7

[121] Accounts Raided in Global Bank Hack. http://online.wsj.com/articles/SB10001424052748704483004575523811617488380, 2010. Last Accessed October 28, 2014. 7

[122] Epsilon hacking exposes customers of Best Buy, Capital One, Citi, JPMorgan Chase and others [Updated]. http://latimesblogs.latimes.com/technology/2011/04/epsilon-cutsomer-files-email-addresses-breached-including-best-buy-jpmorgan-chase-us-bank-capital-on.html, 2011. Last Accessed October 21, 2014. 7

[123] Analysis: Epsilon hacking shows new "spear-phishing" risks. http://www.reuters.com/article/2011/04/04/us-hackers-epsilon-idUSTRE7336DZ20110404, 2011. Last Accessed October 21, 2014. 7

[124] Epsilon Fell To Spear-Phishing Attack. http://www.darkreading.com/attacks-and-breaches/epsilon-fell-to-spear-phishing-attack/d/d-id/1097119?, 2011. Last Accessed October 21, 2014. 7

[125] Epsilon Data Breach to Cost Billions in Worst-Case Scenario. http://www.eweek.com/c/a/Security/Epsilon-Data-Breach-to-Cost-Billions-in-WorstCase-Scenario-459480/, 2011. Last Accessed October 21, 2014. 7

[126] RSA explains how attackers breached its systems. http://www.theregister.co.uk/2011/04/04/rsa_hack_howdunnit/, 2011. Last Accessed October 21, 2014. 7

[127] RSA Security, Inc Hacked. https://www.schneier.com/blog/archives/2011/03/rsa_security_in.html, 2011. Last Accessed October 21, 2014. 7, 11

[128] RSA SecurID Breach Cost $66 Million. http://www.darkreading.com/attacks-and-breaches/rsa-securid-breach-cost-$66-million/d/d-id/1099232?, 2011. Last Accessed October 21, 2014. 7

[129] Suspected North Korean cyber attack on a bank raises fears for S. Korea, allies. http://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html, 2011. Last Accessed October 21, 2014. 7

[130] North Korea 'behind South Korean bank cyber hack'. http://www.bbc.com/news/world-asia-pacific-13263888, 2011. Last Accessed October 21, 2014. 7, 12

[131] PlayStation Network hack: why it took Sony seven days to tell the world. http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony, 2011. Last Accessed October 21, 2014. 7

[132] How the PlayStation Network was Hacked. http://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked, 2011. Last Accessed October 21, 2014. 7, 11

[133] Sony Says PlayStation Hacker Got Personal Data. http://www.nytimes.com/2011/04/27/technology/27playstation.html, 2011. Last Accessed October 21, 2014. 7

[134] PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher. http://www.pcmag.com/article2/0,2817,2385790,00.asp, 2011. Last Accessed October 21, 2014. 7

[135] Sony Appears to Have Lost Yet Another User Database. http://www.dailytech.com/Sony+Appears+to+Have+Lost+Yet+Another+User+Database/article21697.htm, 2011. Last Accessed October 21, 2014. 7

[136] Sony BMG Greece hacked, company's security woes continue. http://www.engadget.com/2011/05/23/sony-bmg-greece-hacked-companys-security-woes-continue/, 2011. Last Accessed October 21, 2014. 7

[137] Sony Pictures hacked by Lulz Security, 1,000,000 passwords claimed stolen (update). http://www.engadget.com/2011/06/02/sony-pictures-hacked-by-lulz-security-1-000-000-passwords-claim/, 2011. Last Accessed October 21, 2014. 7

[138] Citigroup hacker attack affected more customers than first thought. http://articles.latimes.com/2011/jun/17/business/la-fi-citigroup-hacking-20110617, 2011. Last Accessed October 21, 2014. 7

[139] Citi: Millions stolen in May hack attack. http://money.cnn.com/2011/06/27/technology/citi_credit_card/, 2011. Last Accessed October 21, 2014. 7

[140] Citigroup hack exploited easy-to-detect web flaw. http://www.theregister.co.uk/2011/06/14/citigroup_website_hack_simple/, 2011. Last Accessed October 21, 2014. 7

[141] Citigroup Hackers Stole $2.7 Million. https://www.teamshatter.com/topics/database-security/citigroup-hackers-stole-2-7-million/, 2011. Last Accessed October 21, 2014. 7

[142] Citibank has lost 2.7 million USD through stolen credit card numbers. http://www.itsecurity.be/citibank-has-lost-2-7-million-usd-through-stolen-credit-card-numbers, 2011. Last Accessed October 21, 2014. 7

[143] New cyber attack targets chemical firms: Symantec. http://www.reuters.com/article/2011/10/31/us-cyberattack-chemicals-idUSTRE79U4K920111031, 2011. Last Accessed October 22, 2014. 7

[144] The Nitro Attacks Stealing Secrets from the Chemical Industry. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf, 2011. Last Accessed October 22, 2014. 7

[145] IMF cyber attack aimed to steal insider information: expert. http://www.reuters.com/article/2011/06/12/us-imf-cyberattack-idUSTRE75A20720110612, 2011. Last Accessed October 21, 2014. 7

[146] IMF cyber-attack led by hackers seeking 'privileged information'. http://www.theguardian.com/business/2011/jun/12/imf-cyber-attack-hack, 2011. Last Accessed October 21, 2014. 7

[147] Norway Cyber Attack Targets Country's Oil, Gas Systems. http://www.pcmag.com/article2/0,2817,2396611,00.asp, 2011. Last Accessed October 22, 2014. 7

[148] Zappos hacked, 24 million accounts accessed. http://money.cnn.com/2012/01/16/technology/zappos_hack, 2012. Last Accessed October 26, 2014. 7

[149] 'State-sponsored attackers' using IE zero-day to hijack GMail accounts. http://www.zdnet.com/blog/security/state-sponsored-attackers-using-ie-zero-day-to-hijack-gmail-accounts/12462, 2012. Last Accessed October 26, 2014. 7

[150] Microsoft Security Advisory 2719615. https://technet.microsoft.com/library/security/2719615, 2012. Last Accessed October 26, 2014. 7

[151] The Mirage Campaign. http://www.secureworks.com/cyber-threat-intelligence/threats/the-mirage-campaign, 2012. Last Accessed October 26, 2014. 7

[152] Facebook computers compromised by zero-day Java exploit. http://arstechnica.com/security/2013/02/facebook-computers-compromised-by-zero-day-java-exploit, 2013. Last Accessed October 28, 2014. 7

[153] Exclusive: Apple, Macs hit by hackers who targeted Facebook. http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91I10920130219, 2013. Last Accessed October 28, 2014. 7

[154] Recent Cyberattacks. http://blogs.technet.com/b/msrc/archive/2013/02/22/recent-cyberattacks.aspx, 2013. Last Accessed October 28, 2014. 7

[155] South Korea network attack 'a computer virus'. http://www.bbc.com/news/world-asia-21855051, 2013. Last Accessed October 28, 2014. 8

[156] TeamSpy – Obshie manevri. Ispolzovat' tolko s razreshenija S-a. https://www.crysys.hu/teamspy/teamspy.pdf, 2013. Last Accessed October 28, 2014. 8

[157] Cyber-attackers penetrate Reserve Bank networks. http://www.afr.com/p/national/cyber_attackers_penetrate_reserve_FEdCLOI50owRMgI0urEYnK, 2013. Last Accessed October 28, 2014. 8

[158] Japanese web portals hacked, up to 100,000 accounts comprimsed. http://www.networkworld.com/article/2165028/network-security/japanese-web-portals-hacked--up-to-100-000-accounts-comprimsed.html, 2013. Last Accessed October 28, 2014. 8

[159] Ubisoft hacked; users' e-mails and passwords exposed. http://www.cnet.com/news/ubisoft-hacked-users-e-mails-and-passwords-exposed, 2013. Last Accessed October 28, 2014. 8

[160] Ubisoft hack: users warned to change passwords. http://www.theguardian.com/technology/2013/jul/03/ubisoft-hack-users-warned, 2013. Last Accessed October 28, 2014. 8

[161] JPMorgan warns 465,000 card users on data loss after cyber attack. http://www.reuters.com/article/2013/12/05/us-jpmorgan-dataexposed-idUSBRE9B405R20131205, 2013. Last Accessed October 28, 2014. 8

[162] Over 376k credit cards compromised in LoyaltyBuild breach. http://www.net-security.org/secworld.php?id=15939, 2013. Last Accessed October 28, 2014. 8

[163] Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores. http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores, 2013. Last Accessed October 28, 2014. 8

[164] A First Look at the Target Intrusion, Malware. http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware, 2013. Last Accessed October 28, 2014. 8

[165] Target Hackers Broke in Via HVAC Company. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company, 2013. Last Accessed October 28, 2014. 8, 11

[166] Target Shares Tumble As Retailer Reveals Cost Of Data Breach. http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach, 2013. Last Accessed October 28, 2014. 8

[167] Chinese hackers spied on Europeans before G20 meeting: researcher. http://www.reuters.com/article/2013/12/10/us-china-hacking-g-idUSBRE9B817C20131210, 2013. Last Accessed October 28, 2014. 8

[168] Slammer worm crashed Ohio nuke plant network. http://www.securityfocus.com/news/6767, 2003. Last Accessed October 13, 2014. 8

[169] South Pole 'cyberterrorist' hack wasn't the first. http://www.theregister.co.uk/2004/08/19/south_pole_hack, 2004. Last Accessed October 15, 2014. 8

[170] FAA's Air-Traffic Networks Breached by Hackers. http://online.wsj.com/articles/SB124165272826193727, 2009. Last Accessed October 22, 2014. 8

[171] Report: US air-traffic control systems hacked. http://www.zdnet.com/news/report-us-air-traffic-control-systems-hacked/300164, 2009. Last Accessed October 22, 2014. 8

[172] Stuxnet virus targets and spread revealed. http://www.bbc.co.uk/news/technology-12465688, 2010. Last Accessed October 22, 2014. 8, 12

[173] Stuxnet attackers used 4 Windows zero-day exploits. http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347, 2010. Last Accessed October 22, 2014. 8

[174] Snowden: US and Israel did create Stuxnet attack code. http://www.theregister.co.uk/2013/07/08/snowden_us_israel_stuxnet, 2010. Last Accessed October 22, 2014. 8

[175] Obama Order Sped Up Wave of Cyberattacks Against Iran. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all, 2010. Last Accessed October 22, 2014. 8

[176] Stuxnet was work of U.S. and Israeli experts, officials say. http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html, 2010. Last Accessed October 22, 2014. 8

[177] Stuxnet Clone 'Duqu': The Hydrogen Bomb of Cyberwarfare? http://www.foxnews.com/tech/2011/10/19/stuxnet-clone-duqu-hydrogen-bomb-cyberwarfare, 2011. Last Accessed October 21, 2014. 8

[178] Duqu: A Stuxnet-like malware found in the wild. http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf, 2011. Last Accessed October 21, 2014. 8

[179] Duqu: Steal Everything. http://www.kaspersky.com/about/press/major_malware_outbreaks/duqu, 2011. Last Accessed October 21, 2014. 9

[180] Iran Admits Nuclear Sites Hit by 'Duqu' Cyberweapon. http://www.foxnews.com/tech/2011/11/14/iran-admits-nuclear-sites-hit-by-duqu-cyberweapon, 2011. Last Accessed October 21, 2014. 9

[181] HACKERS MANIPULATED RAILWAY COMPUTERS, TSA MEMO SAYS. http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498, 2012. Last Accessed October 26, 2014. 9

[182] Flame: world's most complex computer virus exposed. http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html, 2012. Last Accessed October 26, 2014. 9

[183] U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html, 2012. Last Accessed October 26, 2014. 9

[184] Discovery of new "zero-day" exploit links developers of Stuxnet, Flame. http://arstechnica.com/security/2012/06/zero-day-exploit-links-stuxnet-flame, 2012. Last Accessed October 26, 2014. 9

[185] Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers. http://www.wired.com/2012/05/flame, 2012. Last Accessed October 26, 2014. 9

[186] Hack on Saudi Aramco hit 30,000 workstations, oil firm admits. http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis, 2012. Last Accessed October 26, 2014. 9

[187] Aramco Says Cyberattack Was Aimed at Production. http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0, 2012. Last Accessed October 26, 2014. 9

[188] In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all, 2012. Last Accessed October 26, 2014. 9

[189] The Cyber-Dam Breaks. http://freebeacon.com/national-security/the-cyber-dam-breaks, 2013. Last Accessed October 28, 2014. 9

[190] Dam! Sensitive Army database of U.S. dams compromised; Chinese hackers suspected. http://www.washingtontimes.com/news/2013/may/1/sensitive-army-database-us-dams-compromised-chines/?page=all, 2013. Last Accessed October 28, 2014. 9

[191] Israel Says It Foiled Syrian Cyber Attack On Water System In Haifa. http://www.huffingtonpost.com/2013/05/25/israel-syria-cyber-attack_n_3336670.html?utm_hp_ref=technology&ir=Technology, 2013. Last Accessed October 28, 2014. 9

[192] "Operation Payback" attacks to go on until "we stop being angry". http://arstechnica.com/tech-policy/2010/09/operation-payback-attacks-continue-until-we-stop-being-angry, 2010. Last Accessed October 22, 2014. 9

[193] 'Operation Payback' Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks. http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks, 2010. Last Accessed October 22, 2014. 9

[194] Operation Payback cripples MasterCard site in revenge for WikiLeaks ban. http://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks, 2010. Last Accessed October 22, 2014. 9

[195] Anonymous Hackers Breach Booz Allen Hamilton, Dump 90,000 Military Email Addresses. http://www.forbes.com/sites/andygreenberg/2011/07/11/anonymous-hackers-breach-booz-allen-hamilton-dump-90000-military-email-addresses/, 2011. Last Accessed October 21, 2014. 9

[196] Hackers strike at a foe. http://www.economist.com/blogs/schumpeter/2011/07/security-breach-booz-allen-hamilton, 2011. Last Accessed October 21, 2014. 9

[197] Hackers steal 90,000 email addresses in cyber attack on US military contractor Booz Allen Hamilton. http://www.telegraph.co.uk/technology/news/8631458/Hackers-steal-90000-email-addresses-in-cyber-attack-on-US-military-contractor-Booz-Allen-Hamilton.html, 2011. Last Accessed October 21, 2014. 9

[198] Anonymous leaks 'Bank of America secrets' in spy revenge hack. http://www.theregister.co.uk/2013/02/27/anon_bofa_leak, 2013. Last Accessed October 28, 2014. 9

[199] Who Else Was Hit by the RSA Attackers? http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers/, 2011. Last Accessed October 22, 2014. 9

[200] The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies. https://securelist.com/blog/incidents/57647/the-red-october-campaign, 2013. Last Accessed October 26, 2014. 9, 10

[201] Surprised? Old Java exploit helped spread Red October spyware. http://www.theregister.co.uk/2013/01/16/red_october_java_connection, 2013. Last Accessed October 26, 2014. 10

[202] The NetTraveler (aka 'Travnet'). http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/07/kaspersky-the-net-traveler-part1-final.pdf, 2013. Last Accessed October 28, 2014. 10

[203] The Icefog APT: A Tale of Cloak and Three Daggers. http://securelist.com/blog/research/57331/the-icefog-apt-a-tale-of-cloak-and-three-daggers, 2013. Last Accessed October 28, 2014. 10

[204] A different motive: hacktivism by the numbers. http://www.advisenltd.com/insurance-news/2014/03/21/different-motive-hacktivism-numbers, 2014. Last Accessed November 21, 2014. 12