Chapter 2
Types of Malware and Malware Distribution Strategies

Using data from the Identity Theft Supplement to the National Crime Victimization Survey [1], the US Department of Justice estimates that approximately 7% of all Americans over the age of 16 have been victims of identity theft. Over 45% of the victims of identity theft reported over 6 months of stress resulting from the incident. The situation in other developed economies is similar—according to CIFAS, the UK's Fraud Prevention Service, 108,500 people had their identity stolen in the UK in 2013 [2].

The stress placed by these statistics—both on the victims of identity theft and those who fear it—is substantial. It is not helped by reports in late 2014 of highly targeted attacks on consumers such as the *Darkhotel* "espionage campaign" reported by Kaspersky Labs [3] in which a sophisticated ring of cyber-criminals target individuals who are wealthy enough (and presumably influential enough) to stay at high-end luxury hotels. When these individuals access the hotel's Wi-Fi network, they are asked to update a piece of software which induces most such individuals to download a malicious piece of code onto their devices. Once on the unsuspecting victim's device, *Darkhotel* runs in the background, downloading, installing, and deleting at will, advanced software such as keystroke loggers, Trojans, and various malware designed for data and information theft.

Likewise, Kaspersky Labs [4] reports that a 2013–2014 joint study with Interpol found that approximately 20% of Android devices protected by Kaspersky Labs detected attacks on those devices, suggesting that perhaps 20% of all Android devices are thus targeted. This is a very steep rise on numbers reported from just 1 year earlier.

All of this makes consumers worldwide fearful of malware and its ability to derail their finances, and eventually their lives. Businesses are equally nervous about the asymmetric nature of the threat posed by malware developers and nation states. Businesses are worried both about *insider threat* (where insiders steal corporate secrets) [5] as well as commercially motivated external threats [6]. For example, the FBI issued a warning in November 2013 describing a piece of malware that over-writes hard drives, thus destroying corporate data. According to an earlier

V.S. Subrahmanian et al., *The Global Cyber-Vulnerability Report*, Terrorism, Security, and Computation, DOI 10.1007/978-3-319-25760-0_2

report by the security firm Mandiant, "APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously" [7, p. 5]. They identify APT1 as being located in the same location as the People Liberation Army's Unit 61398 in the Pudong area of Shanghai.

Governments are constantly fearful of cyber-espionage attacks by foreign states. For years, PLA's Unit 61398 was viewed in the US and EU as being the poster child for unwarranted and unethical cyber-espionage [7–9] (though this has been dialed down since allegations of widespread cyber-espionage by the US government hit the news in the summer of 2013 following the revelations of Edward Snowden). Nonetheless, the FBI recently warned [10] that an even more deadly adversary codenamed *Axiom* within the PLA has been stealing intellectual property from US companies, engaging in cyber-espionage, and in targeting Chinese dissidents. The Chinese government has steadfastly denied all such allegations. But we should note that there are allegations that the US too maintains a stock of zero-day attacks and does not disclose all vulnerabilities it has discovered in software to the software vendors involved [11].

In short, there are huge numbers of zero day attacks and advanced persistent threats being developed by a number of actors ranging from individual hackers to criminal groups to nation states. In the rest of this chapter, we provide the briefest insights into the different types of malware that are exploited by many of these entities, as well as some of the mechanisms used to distribute these attacks.

2.1 Types of Malware

We describe six type of malware: Trojans, viruses, worms, spyware, adware, and misleading software. These are the types of malware that we studied in the WINE dataset from Symantec. Of course, there are many other kinds of malware as well, and we will summarize some of these other types of malware toward the end of this section.

2.1.1 Trojans

A Trojan is a hidden threat, much like the famed Trojan horse left by Odysseus on the shores of Troy.

Simply put, a Trojan consists of two parts—a server side that runs on an attacked host and a client piece that runs on the attacker's console. The server code (usually kept very small in size, no more than a few KBs) is dispatched to the victim via some malware distribution method. We will describe several malware distribution methods in Sect. 2.2 including phishing attacks, drive-by-downloads, and so forth. In a simple setting, the attacker sends the victim a file that contains the server code

(e.g. an image or a PDF large enough in size that the server size is miniscule when compared to the overall file size). When the user double clicks the attacked file, it launches the "server" program embedded in the infected file. The server usually runs in stealth mode and is not easily visible to the user and/or to the file manager. At this stage, the server code in the infected file can establish contact with the attacker's client code in one of many ways. One simple way is through a reverse connection in which the server code has the IP address from which the attacker wants to control the victim's computer. But much more sophisticated reverse connection methods also exist. Once launched, the server program contacts the client side code from whose console, the attacker can now take control of the victim's program. He can install new programs on to the victim's computer (e.g. keyloggers), he can read every single file on the victim's computer (e.g. credit card and banking information, personal identity information), and more. In effect, he can control the victim's computer using his keyboard from a remote location.[1]

In some cases, Trojans are very explicit and make few attempts to stay "below the radar". They take overt control of the victim's machine. The more dangerous situation, however, is when the Trojan stays below the radar and operates for extended periods of time in stealth mode with the victim unaware that his data (or his company's data) is being siphoned off by an unscrupulous attacker.

One example of a dangerous Trojan is the Zeus3 malware which was downloaded onto victims' computers through infected advertisements that may be present on various web sites. When these ads are viewed by the victim, the Trojan is downloaded onto the victim's computer. The Trojan then waited till the user visited his online bank. By observing his credentials when he logs in, it is able to siphon off a large sum of money from victims' bank accounts.

Another interesting Trojan, Obad.a infects Android devices [12, 13] by first sending potential victims an infected link (or a spam message). When the victim clicks the link, he downloads the Trojan server onto his device which immediately reaches out to his entire contact list, urging them to click on the link as well. The Trojan spreads in this way, infecting a large number of people. Unlike most Trojans, this one uses a botnet to control the spread of the Trojan.

Another Trojan, CryptoLocker, encrypts user files on a machine and demands a ransom in exchange for decrypting the file.

Most intriguing is the recent report of the *Regin* virus in a report released by Symantec [14] and Kaspersky Lab [15]. Regin is primarily used for espionage and intelligence gathering. According to Symantec [14, p. 6], 48% of infection attempts target private individuals, 28% of infection attempts target telecommunication companies, and the rest is split between the hospitality industry (hotels), airlines, energy sector, and researchers. The main affected countries are Russia, Saudi Arabia, Mexico, Ireland, Afghanistan, India, Iran, Belgium, Austria, and Pakistan—with Russia and Saudi Arabia the biggest targets. Interestingly, [15] reports that Regin also compromises GSM networks and collects data about the physical networks

[1] The ability to control an infected host from a remote machine is a featured shared by different types of malware, not just Trojans.

used by telecoms. It also collects administrative login data that allows it to manipulate the networks. According to the German newspaper *Der Spiegel* [15], Regin is a joint effort of the US National Security Agency and the UK's GCHQ.

Regin starts with a "dropper" in which the malware is dropped onto a site. Some evidence suggests that Instant Messaging services are used to inject Regin into certain hosts. From there, several complex intermediate steps (including ones involving encryption) are performed before the ultimate payload is revealed. The goal is to steal information from the compromised hosts. In order to evade detection, Regin compromises entities in a country by linking them into an intra-country peer to peer network and then using just one exit point from the country to exfiltrate the data to its creators' location. [15] shows a graphic of how India's President's office and many government institutions were linked into a P2P network with the single entry/exit point from India being a compromised node at an educational institution.

We see therefore that Trojans can vary widely in sophistication, ranging from software that is likely designed by teams of dedicated hackers working for a nation state, to individual hackers or hacker collectives taking known code and modifying it. Because this book focuses primarily on infection attempts on consumer hosts as opposed to government or business hosts, we believe that most of the Trojans described in this book are in the second category.

2.1.2 Worms

A worm is a piece of malware that can independently spread through a network by exploiting vulnerabilities in existing software to compromise a system. Worms may spread through networks in a variety of ways. For instance, worms may spread through a network by using email to infect other computers, or by using other file transfer protocols to copy themselves onto other computers.

Worms may carry a payload. While some worms may do nothing other than spread from one computer to another (just using up bandwidth and slowing down a network), others may do dangerous things like delete files on a machine and encrypt files (so that the owner of the file has to pay a ransom in order to be able to decrypt his files).

[16] provides a detailed taxonomy of worms based on six factors.

- *Targeting*. This refers to the mechanism used by the worm to target potential victims. Commonly used targeting mechanisms include scanning the network for vulnerable hosts, using specified lists of targets, using a "metaserver" (which is a list of periodically updated vulnerable servers) that the worm periodically queries to find new targets, and topological worms that discover the structure of a network in order to identify new targets, and "passive" worms that lie in wait for a target.
- *Distribution Mechanisms*. Worms might spread in three ways. Self-carried worms spread independently (e.g. topological worms and worms that spread by

scanning through a network). Second-channel worms spread via an auxiliary communication channel such as remote procedure calls. Embedded worms spread by embedding themselves within a standard channel of communication.
- *Activation Mechanism.* Worms may be activated either by an explicit human action (e.g. via an infected email), an explicit human activity that is recognized by the worm, triggering it, or by a injecting themselves into part of a scheduled process on a host.

In general, topological worms and worms that spread autonomously by scanning can be incredibly fast. Notorious computer worms include:

- *Stuxnet* [17–19] is perhaps the best known example of a worm in recent years. Detected in 2013 by security vendor Kaspersky Labs [17], and reportedly launched by Israeli and US intelligence [20], Stuxnet was signed with certificates stolen from two Taiwanese software manufacturers, making it appear to be authentic and reliable. Stuxnet was targeted at Iran's Natanz nuclear enrichment facility. Though Stuxnet code infected computers in many nations, it is reported [18] that it did not adversely impact any SCADA systems other than those at Natanz. Stuxnet worked via an initial socially engineered attack in which a memory stick infected with Stuxnet was introduced. The worm spread rapidly. When infecting a host, Stuxnet first checked to see if it was a particular kind of Siemens device often used in nuclear facilities. If it was, a dropper program dropped malicious code into the main() program loop of the Siemens controller. The malicious code included several variants targeted at the specific type of controller.
- *Mydoom* [21] appears with a message in emails, prompting (mostly Windows) users to click upon an attachment, upon which their machine is infected. Different versions of Mydoom carry different payloads, one of which is the installation of a backdoor on the victim machine that allows the machine to be remotely controlled. Mydoom is believed to have used up a huge amount of Internet bandwidth when it first hit the internet in 2004.
- *Conficker* [22, 23] exploits a vulnerability in the Windows operating system to infect a host—and does this by a combination of random scans of nodes as well as neighborhood scans (i.e. scanning neighbors of infected nodes), though the latter is reported to be the dominant mode of infection [22]. Conficker was sophisticated enough to update itself dynamically and also evade signature-based anti-virus detection tools.

2.1.3 Viruses

Unlike worms, that spread independently, viruses spread by attaching themselves to another program or to files (e.g. PDF or image files). For example, a virus embedded in a PDF or JPEG file may spread when that file is opened. Some viruses also exist in the boot sector of a computer hard drive, thus executing automatically when a boot operation takes place.

Because legitimate programs and files have well known sizes, viruses that attach themselves to such "entities" may take steps to hide any increase in size. One way to hide is by copying themselves into unused space in a file or program. Another way to hide is by intercepting requests to obtain data about the program or file and returning results that appear normal and obfuscate the presence of the virus. In order to hide from "signature based" scanners used by many anti-virus companies (a signature is just a fragment of code), viruses can mutate, making their code look different. Rates of mutation vary from one virus to another.

It is unfortunate that in common parlance, the word "virus" has been collectively used to describe all kinds of malware including worms, Trojans, and viruses as described above.

2.1.4 Other Forms of Malware

Other forms of malware include "misleading software" and "spyware".

We use the term "misleading software" to describe software that pretends to be something legitimate, when in fact it is really a piece of malware. Examples of misleading software include fake anti-virus programs, fake media players, and fake hard disk recovery programs.

Fake anti-virus software use social engineering to make users believe their system is infected with a virus. A free Anti-Virus software is offered and shows fake infection results when it is downloaded and run. Then, the user receives an offer to upgrade the software (for a fee) to remove the supposedly existing infection. Another type of misleading software, sometimes pretends to present messages from a law enforcement agency. The user is accused of a crime and the payment of a fine is requested. Rajab et al. [24] and Stone-Gross et al. [25] provide further details on misleading software.

A related type of malware is ransomware which encrypts files on the host of a victim and demands a ransom [16]. As many users never create regular backups, a victim can only regain access to his/her files after paying the requested ransom to the attacker.

Spyware is code that enables a third party to spy on a host. Spyware has been used for a variety of purposes including identity theft and theft of personal data, spying on online activities of individuals (e.g. spouses) and watching users' online activities.

2.2 Malware Distribution

We now come to the important topic of malware distribution. Though malware distribution can occur in many different ways, we focus on four of them: drive-by-downloads, email, network intrusion, and social engineering.

2.2.1 Drive-by-Downloads

The main characteristic of drive-by attacks is that the user unknowingly downloads a malicious file while browsing the web. Some component of the web browser or one of its plug-ins (e.g. those to display PDF or Flash files), processes the malicious file. Malicious Web code (e.g. JavaScript) exploits vulnerabilities in browsers and causes a file to be downloaded and executed. Because of the availability of various injection techniques, as described below, the malicious code may be present on Web pages that are popular and otherwise benign.

Drive-by attacks require a victim to visit a website that contains attack code. Building on the injection strategies in Provos et al. [26], we can categorize injection strategies into four categories:

- They can post malicious code as a part of a submission to a user contributed website that does not carefully ensure that user inputs are malware-free.
- They can include malicious code into ads and pay unsuspecting and/or careless ad networks to deliver the ad to their client websites.
- They can provide malicious widgets like stats counter. Websites that include the widgets deliver the code to their visitors.
- Adversaries can try to get control of the web server of a benign website and add their code to it.

Though shady web sites (e.g. porn sites) seem to pose a greater risk of drive-by attacks, visiting only large and/or popular web sites does not entirely mitigate the risk of being victimized. For example, it is reported that around the turn of the year 2013–2014, visitors to Yahoo sites were served ads from Yahoo's ad network [27] that were infected with malware.

2.2.2 Email

As in the case of drive-by attacks, e-mail attacks can exploit vulnerabilities in the e-mail software or in the libraries that the e-mail software uses (e.g. to display images or to display Word or PDF files). When the email software downloads a message and displays it, a manipulated embedded media object exploits a vulnerability and causes the execution of the malicious code.

2.2.3 Network Intrusion

While drive-by attacks and email attacks require that the victim initiate communication with a remote host, network intrusion attacks are initiated by the attacker. Victim hosts run programs that process incoming data on several layers of the protocol stack. Manipulated data packages can exploit vulnerabilities and take over control of a host.

2.2.4 Social Engineering

Socially engineered attacks exploit weaknesses of humans rather than weaknesses of software. Users are manipulated into running malicious binaries.

For example, users are made to believe there is malware on their computer and offered a free Anti-Virus software (compare Sect. 2.1.4). As this malware distribution strategy does not exploit any technical vulnerability, the hurdle to overcome is that of public awareness.

A well-known example of social engineering is the Koobface attack (https://nakedsecurity.sophos.com/koobface/), which would identify the Facebook accounts accessed from the infected computers and post messages using those accounts. This leveraged the established trust between those users and their Facebook friends.

In addition to attacks that rely entirely on it, social engineering is also involved (to varying degrees) in most other distribution strategies as well. For example, malware distribution involving email may exploit vulnerabilities of software other than email software by using social engineering to make the user open an attached files. For example, an adversary may send fake invoices. When a user opens the unexpected invoice to see what it is about, malicious code gets executed.

2.2.5 Downloaders

All the methods to distribute malware discussed above are initial attacks. A common way to distribute malware is to install a malware downloader using one of the initial attack methods discussed above. Once installed, a downloader downloads and installs additional malware on a previously compromised host.

A downloader system can be regarded as a special type of botnet where the downloader is a bot that specializes in retrieving and installing malware. Technical details about how downloader networks operate can be found in [28] and [29].

2.3 Business Models

In this section, we present an overview on the most common business models of the underground economy.

Making money in the underground economy is a multi-step process. The process starts with the identification of vulnerabilities of operating systems and pieces of software (Exploit-as-a-service (EAAS) [30]) and ends with a transfer of funds, e.g. through dubious payment processors for credit cards [25].

As in the case of the traditional economy, the cyber-crime economy adopted a division-of labor model where individuals or organizations specialize in one part in the value chain.

A comprehensive service in the dark economy is Pay-Per-Install (PPI) [28]. A PPI provider takes over the complex task of identifying and exploiting vulnerabilities (or buys these from other service providers) and installs downloaders on compromised hosts.

Other services include solving CAPTCHAs (Completely Automated Public Turing Test to tell Computers and Humans Apart) for a variety of purposes of dubious legality. Solving such CAPTCHAs may support posting advertisements for malicious web sites and online message boards, creating accounts at free e-mail services [31], and repacking malware to prevent signature-based identification through anti-virus software services to promote malicious websites [25].

Some money-making methods used in this underground economy are listed below.

2.3.1 Click Fraud

Cost-per-click (CPC) is a common compensation method in online advertising. The website displaying an ad gets paid not for displaying the ad, but for every click that takes a visitor to the advertiser's website. Click fraud can work in two ways. First, there are owners of websites who wants to use so called click-bots to increase the clicks on ads on their website to increase their own ad revenue. In the same vein, there are organizations who want to increase the spending of their competitors and use click-bots to click on their competitor's ads.

Another type of click fraud is fraudulent search engine optimization (blackhat SEO) [32, 33]. Search engines rank their list of result based, in part, on result entries that users clicked on in the past. Here, click fraud malware is used to fool search engines into believing a website is more popular than it actually is.

2.3.2 Keyloggers

Keyloggers collect personal information like bank account or credit card data and email credentials. This type of information is a marketable product in the underground economy [34, 35] and can be used in different types of fraud schemes or to send spam.

2.3.3 Spam

Unsolicited bulk email is the most common form of spam. But similar messages are also sent to message boards on the web, to social media (e.g. YouTube) and to social network (e.g. Facebook) sites. Spam is often used to deceive victims into buying worthless or dangerous products (e.g. counterfeit prescription drugs [36]).

However, spam is also used to distribute malware (compare Sect. 2.2) and keep the cycle of infections going. Some spam-based malware networks exfiltrate address books from compromised hosts to build email databases [37].

2.4 Cross-Country Studies

The security literature includes thorough studies analyzing malware offenders through honeypots [37], scanning network traffic [38], or by milking PPI distribution servers [28]. Studies about the victims of malware are, however, rather rare. We summarize below the cross-country results those victim-centric studies revealed.

Caballero et al. [28] infiltrated PPI networks and studied their behavior. They "milked" PPI services by using software that resembled the original downloader of a PPI service to retrieve the binaries it distributes. By accessing the PPI service with IPs from different geographical origins they were able to study the behavior of these services across different countries. They observed that while most malware was not uniformly distributed across countries, most malware families did have geographic preferences and specifically targeted either the United States or Europe. They attribute the country preferences to (1) the varying pay-per-install costs they found at dark marketplaces for such services ($100–180 for 1K US or UK host, $20–160 for 1K hosts in other European countries), and (2) the need to customize some attacks. Success in stealing credit card data or advertising and selling fake anti-virus software depends on the geography of the victims. Credit cards are not widely used in all parts of the world and payment methods need to fit local systems. Selling fake anti-virus software most likely works best when the advertising message is in the native language of the victim.

Other business models do not require a country-specific approach. In order to send spam, any host connected to the internet is good—with the exception of countries that might be blacklisted or trigger spam filters.

Carlinet et al. [38] conducted a detailed study of how behaviors affect vulnerability to malware by malware. They analyzed the network traffic of several thousand ADSL-customers of the French network operator Orange to identify risky types of applications. The presence of malware was inferred by running a signature-based intrusion detection system (IDS) on the traffic data. They found that web and streaming usage is a risk factor while this is not the case for other types of applications like peer-to-peer and chat applications. This result is not surprising, given that browser-based drive-by attacks is the most popular malware distribution approach.

L'evesque et al. [39] ran a field experiment with 50 persons. They installed software on laptops to monitor web browsing behavior and malware infection and then handed them out to their subjects. Data collected over a period of 4 months indicates that higher computer literacy is positively correlated to malware infections. This is

a counterintuitive result, that we also saw in our much larger study of millions of hosts in Symantec's WINE database (see Chap. 3). L'evesque et al. [39] does not analyze how much the factors they analyze influences the infection risk.

Shin et al. analyzed the victims of botnets [40]. They collected IP addresses of hosts infected by three different botnets and analyzed the number of infected networks (/24 IP address space). The network level aggregation has been conducted to account for dynamic IP assignment. One of the analyzed botnets uses a self-propagating approach (type I) and two use a distributed malware-propagation approach (type II). Shin et al. observed that most countries have similar share of type I and type II attacks. But some countries like China have a much higher share of type I infected networks than type II infected networks. They assume network management policies could be a reason for this. The percentage of infected subnets of a country that [41] computed gives a totally different results than the percentage of infected hosts we observed (see Chap. 3). We believe their analysis suffers from the following flaws:

- Because of dynamic IP addresses, their data does not reveal how many hosts belong to a/24 subnet.
- Differences in the number of server farms or private hosts with static IP address influence the average number of hosts per subnet.
- Different ratios of desktop hosts/servers bias the results as well.

2.5 Conclusion

In short, we see that there are currently several types of malware available in the wild and are distributed to potential victims through a number of sophisticated methods. Moreover, they support business models that range from espionage and theft by nation states, to common criminals who are motivated by economic greed.

Though we have only described a few specific types of malware such as Trojans, worms, viruses, misleading applications, and ransomware to name a few, many pieces of malware can often be pieced together into complex "botnets" of malicious programs working together across networks in order to achieve their ends. Complex malware such as Stuxnet and Regin are believed to have been designed and executed by nation states.

Malware is distributed by a variety of methods ranging from spam and malicious web sites on the one hand, to infected attachments that are mailed to potential victims.

Malware supports a variety of business models. Excluding espionage and data theft at the nation state level, malware is used to promote web sites, generate spam, generate fraudulent clicks to increase revenues of web sites (or increase cost of rival web sites), and promote sales of fake products such as fake anti-virus and fake disk cleanup packages.

References

1. Harrell E, Langton L (2014) Victims of Identity Theft 2012, US Bureau of Justice Statistics, http://www.bjs.gov/content/pub/pdf/vit12.pdf, retrieved Dec 3 2014
2. CIFAS (2014) Is Identity Fraud Serious, https://www.cifas.org.uk/is_identity_fraud_serious, retrieved Dec 3 2014
3. Kaspersky Labs Virus News (2013) Kaspersky Lab sheds light on "Darkhotels", where business executives fall prey to an elite spying crew, Nov 14 2013, http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-sheds-light-on-Darkhotels-where-business-executives-fall-prey-to-an-elite-spying-crew, retrieved Dec 3 2014
4. Kaspersky Labs (2014) Kaspersky Lab & INTERPOL Report: Every Fifth Android User Faces Cyber-Attacks, Oct 6 2014, http://www.kaspersky.com/about/news/virus/2014/Every-Fifth-Android-User-Faces-Cyber-Attacks, retrieved Dec 3 2014
5. Azaria A, Richardson A, Kraus S, Subrahmanian VS (2014) Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data, accepted for publication in IEEE Transactions on Computational Social Systems, vol 1(2) pp 135-155
6. Halleck T (2014) FBI Says Cyber Attacks On US Businesses Have Followed Sony Hack, International Business Times, Dec 1 2014, http://www.ibtimes.com/fbi-says-cyber-attacks-us--businesses-have-followed-sony-hack-1731670, retrieved Dec 3 2014
7. Mandiant Corporation (2013) APT1Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, retrieved Dec 3 2014
8. Brenner J (2011) America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. Penguin
9. Clarke RA, Knake RK (2011) Cyber war. HarperCollins
10. Nakashima E. (2014) Researchers identify sophisticated Chinese cyberespionage group, Oct 28 2014, http://www.washingtonpost.com/world/national-security/researchers-identify-sophisticated-chinese-cyberespionage-group/2014/10/27/de30bc9a-5e00-11e4-8b9e-2ccdac31a031_story.html, retrieved Dec 3 2014
11. Zetter K (2014) U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies, Nov 17 2014, Wired, http://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/, retrieved Dec 3 2014
12. Kaspersky Labs (2013) First ever case of mobile Trojan spreading via 'alien' botnets, Sep 5 2013, http://www.kaspersky.com/about/news/virus/2013/first_ever_case_of_mobile_Trojan_spreading_via_alien_botnets, retrieved Dec 3 2014
13. Unuchek R (2013) The Most Sophisticated Android Trojan, June 6 2013, http://securelist.com/blog/research/35929/the-most-sophisticated-android-trojan/, Retrieved Dec 03 2013
14. Symantec (2014) Regin: Top-tier espionage tool enables stealthy surveillance, Nov 24, 2014 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf, retrieved Dec 3 2014
15. Kaspersky Lab (2014) Regin: a malicious platform capable of spying on GSM networks, Nov 24 2014, http://www.kaspersky.com/about/news/virus/2014/Regin-a-malicious-platform-capable-of-spying-on-GSM-networks, retrieved Dec 03 2014
16. Weaver N, Paxson V, Staniford S, Cunningham R (2003) A taxonomy of computer worms. In: Proceedings of the 2003 ACM Workshop on Rapid Malcode, WORM'03, pp 11–18, NY, USA
17. Kushner D (2013) The real story of Stuxnet. IEEE Spectrum, 50(3), 48–53
18. Langner R (2011) "Stuxnet: Dissecting a cyberwarfare weapon." IEEE Security & Privacy, vol. 9(3)49–51
19. Matrosov A, Rodionov E, Harley D, Malcho J (2010) Stuxnet under the microscope. ESET LLC report
20. Nakashima E, Warrick J (2012) Stuxnet was work of US and Israeli Experts, Officials Say, June 12 2012, Washington Post http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html, Retrieved Dec 16 2014

21. Sung AH, Xu J, Chavez P, Mukkamala S (2004) Static analyzer of vicious executables (save). In: IEEE Computer Security Applications Conference, Dec 2004. 20th Annual, pp 326–334
22. Shin S, Gu S, Gu G (2010) Conficker and beyond: a large-scale empirical study. In: ACM Proceedings of the 26th Annual Computer Security Applications Conference, pp 151–160
23. Porras P (2009) Inside risks reflections on Conficker. In: Communications of the ACM, 52(10)23–24
24. Abu Rajab M, Ballard L, Mavrommatis P, Provos N, Zhao X (2010) The nocebo effect on the web: An analysis of fake anti-virus distribution. In: Proceedings of the 3rd USENIX Conference on Large-scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More, LEET'10, Berkeley, CA, USA, USENIX Assoc
25. Stone-Gross B, Abman R, Kemmerer RA, Kruegel C, Steigerwald DG, Vigna G. The underground economy of fake antivirus software. In: Schneier B (ed) Economics of Information Security and Privacy III, Springer, New York, pp 55–79
26. Provos N, McNamee D, Mavrommatis P, Wang K, Modadugu N (2007) The ghost in the browser: Analysis of web-based malware. In: Proceedings of the 1stWorkshop on Hot Topics in Understanding Botnets (HotBots)
27. Fox IT (2014) http://blog.fox-it.com/2014/01/03/malicious-advertisements-served-via-yahoo/.
28. Caballero J, Grier C, Kreibich C, Paxson V (2011) Measuring pay-per-install: The commoditization of malware distribution. In: Proceedings of the 20th USENIX Security Symposium, San Francisco, CA, USA
29. Rossow C, Dietrich C, Bos H (2013) Large-scale analysis of malware downloaders. In Flegel U, Markatos E, Robertson W (eds) Detection of Intrusions and Malware, and Vulnerability Assessment, vol 7591 of Lecture Notes in Computer Science. Springer, Berlin Heidelberg, pp 42–61
30. Grier C, Ballard L, Caballero J, Chachra N, Dietrich CJ, Levchenko K, Mavrommatis P, McCoy D, Nappa A, Pitsillidis A, Provos N, MZ Rafique, Abu Rajab M, Rossow C, Thomas K, Paxson V, Savage S, Voelker GM (2012) Manufacturing compromise: The emergence of exploit-as-a-service. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS '12, pp 821–832, New York, NY, USA
31. Namestnikov Y (2009) The economics of botnets. Technical report, Kaspersky Labs, https://www.securelist.com/en/downloads/pdf/ynam_botnets_0907_en.pdf
32. John JP, Yu F, Xie Y, Krishnamurthy A, Abadi M (2011) deseo: Combating search-result poisoning. In: Proceedings of the 20th USENIX Conference on Security, SEC'11, pp 20–20, Berkeley, CA, USA, USENIX Assoc
33. Lu L, Perdisci R, Lee W (2011) Surf: Detecting and measuring search poisoning. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS'11, pp 467–476, New York, NY, USA
34. Franklin J, Paxson V, Perrig A, Savage S (2007) An inquiry into the nature and causes of the wealth of internet miscreants. In: Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS '07, pp 375–388
35. Holz T, Engelberth M, Freiling F (2009) Learning more about the underground economy: A case-study of keyloggers and dropzones. In: Backes M and Ning P (eds) Computer Security—ESORICS 2009, vol 5789 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, pp 1–18
36. McCoy D, Pitsillidis A, Jordan G, Weaver N, Kreibich C, Krebs B, Voelker GM, Savage S, Levchenko K (2012) Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs. In: Proceedings of the 21st USENIX Conference on Security Symposium, Security'12, pp 1–1, Berkeley, CA, USA, USENIX Assoc
37. Polychronakis M, Mavrommatis P, Provos N (2008) Ghost turns zombie: Exploring the life cycle of web-based malware. In: Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, LEET'08, pp 11:1–11:8, Berkeley, CA, USA, USENIX Assoc
38. Carlinet L, Me L, Debar H, Gourhant Y (2008) Analysis of computer infection risk factors based on customer network usage. In: Emerging Security Information, Systems and Technologies, SECURWARE Aug 2008. Second International Conference, pp 317–325

39. Lalonde L'evesque F, Nsiempba J, Fernandez JM, Chiasson S, Somayaji A (2013) A clinical study of risk factors related to malware infections. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13, pp 97–108, New York, NY, USA
40. Shin S, Lin R, Gu G (2011) Cross-analysis of botnet victims: New insights and implications. In: Sommer R, Balzarotti D, Maier G (eds) Recent Advances in Intrusion Detection, vol 6961 of Lecture Notes in Computer Science, Springer, Berlin Heidelberg, pp 242–261.
41. Huang DY, Dharmdasani H, Meiklejohn S, Dave V, Grier C, McCoy D, Savage S, Snoeren AC, Weaver N, Levchenko K (2014) Botcoin: Monetizing stolen cycles. In: Proceedings of the 2014 Network and Distributed System Security Symposium, San Diego, CA, USA