Trusteer

# The Rising Threat of Corporate Cybercrime

## Cybercriminal motives and methods

*new threats,* ***new thinking***

Trusteer

# Table of Contents

# The Perfect Crime

If the "perfect crime" is one that goes completely undetected, corporate cybercrime is the perfect example. Corporate entities are being breached on a daily basis, often completely unaware that their valuable corporate information assets are being stolen. Cybercriminals, operating quietly and anonymously, are rummaging through corporate accounts for confidential data, leaving without a trace, and then using or selling the information for economic gain.

This widespread, coordinated criminal effort is enabled by a plethora of vulnerabilities of the Internet, browsers, operating systems, and applications that are easily exploited by cybercrime techniques. Cybercriminals have found that compromising employee endpoints is a far simpler path into the corporate network than directly attacking networks. Unpatched "zero-day" vulnerabilities allow cybercriminals to secretly install malware on employee endpoint devices and essentially gain the same level of access to the corporate network, applications, and data that employees have.

> *There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again. Maintaining a code of silence will not serve us in the long run.*
>
> *FBI Director Robert Mueller*

## The Value of Corporate Cybercrime

Examples of corporate cyber theft abound. In September 2012, the FBI issued a warning to US banks that cybercriminals have been using malware and keyloggers installed on bank employee devices to obtain employee login credentials. They use the stolen credentials to initiate fraudulent international wire transfers of $400,000 to $900,000[1]. Just this past October, the FBI created a new squad in its Washington field office focused on intellectual property thefts to combat the increasing numbers of cybercrimes.

Government agencies have been reporting widespread state-sponsored corporate espionage aimed at a variety of industries, including high technology, pharmaceuticals, communication, financial services, defense, and legal (valued at over $500 billion by *Bloomberg News*). Compromised companies represent a veritable who's who of the high-technology world, including Google, Intel, Adobe, Pfizer, and Abbott Laboratories. Because of the anonymous nature of the crimes, it is often difficult to distinguish between state-sponsored and "private" cybercrime networks that are also actively pilfering valuable intellectual property.

Earlier in 2012, Jonathan Evans, the director-general of MI5, the United Kingdom's internal counterintelligence and security agency, revealed a "major London listed company with which we have worked" had lost revenue of "some £800 million" to a state-sponsored cyber attack. The security company McAfee found "around a quarter of organizations have had a merger and acquisition or a new product/solution rollout stopped or slowed by a data breach, or the credible threat of a data breach."[2]

Beyond the economic impact of intellectual property breaches and the loss of sensitive customer data are the legal ramifications for failing to adequately protect valuable corporate assets. Investors will increasingly seek damages from breaches that are due to a lack of adequate security measures. Given all the attention and warnings related to corporate cybercrime, corporate executives and officers may also face litigation for failing to put proper, best-practice protections in place. Highly regulated industries will also face the wrath of regulators for failing to properly assess the risks associated with cybercrime and to put the appropriate mitigating technologies in place.

> *The greatest trick the devil ever pulled was convincing the world he doesn't exist.*
>
> *Charles Baudelaire*

## The Difficulty of Preventing The Unseen

Cybercriminals have been targeting financial institutions for over a decade by compromising their customers' devices to access online banking accounts. During this time, cybercriminals have also been quietly targeting enterprise assets. When money is stolen from a customer's bank account, it will almost always be discovered. However, when cybercriminals steal intellectual property and other sensitive information from a corporation, the trail is not so obvious and the theft may never be discovered.

Most companies are completely oblivious to cybercrime attacks. The vast majority of cybercrime victims discovered a compromise only because a third party notified them (94% of victims according to Mandiant[3] and 92% according to Verizon[4]). Once a cybercriminal gains access to a corporate network, the median time to detect the intrusion is 416 days[5]. It is highly likely then that a significant number of compromises go completely undiscovered. And when compromises do occur, cybercriminals typically spend well over a year pilfering corporate information assets.

McAfee found, "Only three in ten organizations report all data breaches/losses suffered, while one in ten organizations will only report breaches/losses that they are legally obliged to, and no more. Six in ten organizations currently 'pick and choose' the breaches/losses they report, depending on how they feel about them."[6] And despite the 2011 SEC guidance for disclosing cybercrime incidents, few companies have done so.[7] This tendency follows a recent PricewaterhouseCoopers (PWC) survey of 3,877 respondents from organizations in 78 countries that found the top concern regarding cybercrime is reputational damage (indicated by 40% of respondents).[8] It is no wonder that corporate officers are hesitant to publicly disclose cybercrime incidents. Unfortunately, this lack of reporting greatly hinders general awareness of the corporate cybercrime problem. Many corporate executives are not aware of their level of exposure to cybercrime until they become victims.

> *We wouldn't share this [exploit] with Google for even $1 million. We don't want to give them any knowledge that can help them in fixing this exploit or other similar exploits. We want to keep this for our customers.*
>
> *Chaouki Bekrar, CEO Vupen Security*
>
> *(after refusing $60,000 from Google to share its Chrome web browser exploit)*

# The Methods of Corporate Cybercrime

Cybercriminals use a variety of techniques to infiltrate corporate networks. The predominant approach is to compromise an employee device, steal the employee's access credentials, and then use the employee's access privileges to identify and steal valuable information or directly initiate fraudulent financial transactions. Several security vendors issue annual and periodic reports that contain a wealth of information regarding cybercrime methods and trends, including Trusteer Blog entries, Symantec's *Internet Security Threat Report, Verizon's Data Breach Investigations Report, McAfee Threats Report, and Sophos's Security Threat Report*.

## Targeting Employee Endpoints for Cyber Attack

Some enterprise attacks are opportunistic (35% of large organization breaches[9]), while others are highly targeted (50% of large organization breaches[10]). And various newer targeting techniques fall somewhere in the middle (see the discussion on "watering hole attacks" below). In addition to new infections, Trusteer research has found that at any point in time, approximately 1% of all PCs are infected with active malware. There is no shortage of corporate targets for cybercriminals.

### Phishing

Phishing continues to be an effective method for both luring individuals to compromised websites and tricking individuals into downloading infected files. Despite ongoing admonishments regarding the dangers of clicking on unfamiliar links and opening suspicious file attachments, these methods continue to be effective. End users are not completely to blame; cybercriminals have become much better at disguising their intentions.

Cybercriminals often use highly targeted spear-phishing messages that leverage information available on the web (via Facebook, LinkedIn, Twitter, etc.) or stolen from a familiar individual to create messages that make the victim believe an email is legitimate. Between the first and second quarters of 2012, email-based attacks that successfully bypassed organizations' security defenses increased 56%.[11] The malicious emails contain a malicious file, a link to a malicious website, or both. Despite best efforts to train and warn employees, phishing attacks will continue to succeed.

### Web Threats

Web-based infections are also effective for compromising employee devices. Cybercriminals compromise legitimate websites and also construct websites specifically to host malware. Victims are lured to the malicious websites through a variety of tactics, including links embedded in phishing emails, search engine optimization poisoning, social media scams (e.g., Twitter, YouTube), fake surveys, free gift offers, and "must-see" videos.

A new technique, called a "watering hole" attack, infects victims associated with targeted companies, industries, or geographies. Criminals compromise legitimate websites that are known to cater to a particular audience. For example, employees of a defense manufacturing plant located in a small town are likely to visit the local newspaper website. Therefore, compromising the newspaper website allows the cybercriminal to indirectly find employees of the defense manufacturer. Both RSA and Symantec recently identified large-scale cybercrime campaigns that relied heavily on this technique.[12] [13]

The number of malware-hosting websites is staggering. Sophos reports that 30,000 websites are infected every day, and 80% of those are legitimate, compromised sites[14] (82% according to WebSense[15]). Symantec identified 9,314 malicious websites per day in 2011[16], and McAfee reported finding 10,000 new malicious websites per day in June 2012[17]. The likelihood that an end user's device will be infected when the end user simply browses the web is higher than ever.

## Exploiting System Vulnerabilities

After cybercriminals trick victims into opening a malicious email file attachment or visiting an infected website, the next step in the cybercrime sequence is to infect the endpoint with malware. Cybercriminals have become highly proficient at finding and exploiting system vulnerabilities in order to infect employee endpoint devices with malware while evading security controls. The average organization receives 643 web-based infections per week that succeed in bypassing its security defenses.[18] Not surprisingly, a recent survey found that 74% of IT and security professionals believe the security of their endpoints — their laptops and desktops — is ineffective.[19]

### Software Vulnerabilities

Vulnerabilities refer to software code weaknesses, due to design flaws or coding errors, that allow an attacker to compromise the underlying system. The Open Source Vulnerability Database catalogued 6,843 vulnerabilities in web-based systems, applications, and computing tools in 2011 (Symantec reported 4,989 new vulnerabilities using the DeepSight vulnerability database [20]). Although the number of vulnerabilities is down 19% from 2010, the percentage of high-level severity vulnerabilities has been on the rise, now representing 24% of all reported vulnerabilities. High-level severities are those that allow for root-level compromise of the underlying system.

Software vulnerabilities allow a cybercriminal to bypass security controls built into the operating system or provided by third-party security applications that prevent unauthorized file installation. Microsoft reported that application vulnerabilities represented just over 70% of all disclosed vulnerabilities in the first half of 2012[21]. The remaining vulnerabilities were roughly evenly split between operating systems and browsers. Note that browsers and browser component vulnerabilities are not included in the application vulnerability count.

**Exploits**

Exploits are pieces of code designed to take advantage of software vulnerabilities to deliver a payload (malware) that otherwise would be prevented by system restrictions. To combat this threat, software providers work feverishly to prevent these exploits by patching the vulnerabilities. IBM reported that in 2011, 11% of all known vulnerabilities had publicly available exploits[22]. Approximately 91% of vulnerabilities were patched the same day they were publicly disclosed[23]. The majority of the remainder were patched within a few weeks.

But availability of a patch does not guarantee that it is installed on the end user's device. End users or administrators must continually stay abreast of information on new patches across a variety of software programs used on a typical end-user device. Inconsistent patch adoption leads approximately 2.7% of Microsoft programs and 6.5% of third-party programs to remain unpatched at any given time.[24] Multiplied by millions of users, these figures reveal that a large population is regularly exposed to cybercriminal exploits.

Although the patching statistics may not seem alarming, they do not reflect the true underlying life cycle of vulnerabilities and exploits. Especially dangerous are zero-day exploits that take advantage of undisclosed vulnerabilities. Because zero-day exploits target unknown (and therefore unpatched) vulnerabilities, there is little defense against them.

Many falsely believe that zero-day vulnerabilities pose a limited threat because disclosed vulnerabilities are patched so quickly. However, recent research discovered that attackers often exploit vulnerabilities long before they are publicly disclosed, causing zero-day exploits to last 312 days on average[25]. That is, cybercriminals are able to exploit unknown system vulnerabilities to successfully infect endpoints for 10 months before any protections are put in place. This same study also revealed that immediately after vulnerabilities are disclosed publicly, cybercriminals increase the number of exploits by 2 to 100,000 times to infect as many machines as possible before the vulnerability is patched.

The value of discovering a zero-day vulnerability and developing an exploit can be lucrative for the attacker. A recent Forbes article explored the underground market for zero-day exploits that are provided exclusively for the most current version of the software (see Figure 1). Just one week after Microsoft released Windows 8, French security firm Vupen claimed to have a hack available (and for Internet Explorer 10 as well). The value of zero-day exploits is indicative of the economic gains realized from cybercrime.

| | |
|---|---|
| **ADOBE READER** | $5,000 - $30,000 |
| **MAC OSX** | $20,000 - $50,000 |
| **ANDROID** | $30,000 - $60,000 |
| **FLASH OR JAVA BROWSER PLUG_INS** | $40,000 - $100,000 |
| **MICROSOFT WORD** | $50,000 - $100,000 |
| **WINDOWS** | $60,000 - $120,000 |
| **FIREFOX OR SAFARI** | $60,000 - $150,000 |
| **CHROME OR INTERNET EXPLORER** | $80,000 - $200,000 |
| **ISO** | $100,000 - $250,000 |

**Figure 1: Black Market Value of Various Zero-Day Exploits**

*Source: Forbes, March23, 2012*

Disturbingly, criminals don't have to rely solely on developing exploits for newly discovered vulnerabilities. Because users consistently do a poor job of installing security updates that patch critical vulnerabilities, many exploits continue to be effective months or years after a vulnerability patch has been released. For example, 39% of computers failed to install a Microsoft Word update one year from its release, and 70% of computers had not installed an Adobe Flash Player update within a month of its release.[26] This lag allows cybercriminals to continue to use existing attack methods against patched vulnerabilities for months, or sometimes years.

## Infecting the Endpoint

The process for infecting an endpoint is far more complex than simply downloading a malware binary file directly onto the endpoint. The process typically involves downloading dropper binaries to modify device configuration and security settings, install some malware components, and then access up-to-date crimeware packages. The crimeware package installs and updates the main malware agent. The malware agent then locates and communicates with a command-and-control server that manages attack configurations and receives compromised information. This sophisticated approach is designed to maximize criminals' likelihood of evading security controls and installing the most potent malware.

Cybercriminals increasingly rely on exploit kits, such as Blackhole, that actively scan a user's device for a variety of vulnerabilities and then install the appropriate dropper files to exploit the vulnerabilities. If it finds no vulnerabilities, the kit does nothing. Dropper files are dynamically created so that they cannot be found by known techniques for signature and pattern matching used by most antivirus applications. And to avoid detection, communication with the command-and-control server is increasingly obfuscated, sometimes by Twitter, Voice over Internet Protocol (VoIP), or other open communication channels.

Related to zero-day exploits is zero-day malware. Zero-day exploits target unknown system vulnerabilities; zero-day malware refers to new malware strains that have not yet been identified. Zero-day malware comes in two forms: zero-day malware containers (a never-before-seen file) and zero-day malware crime logic (a never-before-seen malware attack algorithm). Signature-based antivirus applications cannot detect zero-day malware containers because they must match previously identified malware containers. It is very easy for cybercriminals to produce millions of new variants of the exact same malware container using a technique called polymorphism. Far more dangerous is zero-day malware crime logic — new, previously unseen malware algorithms that require actual design and coding by cybercrime gangs — an entirely different level of effort.

Cybercriminals also can infect user endpoints by other methods. For instance, users increasingly use unofficial software distribution websites and file-sharing sites. Criminals regularly embed malware in pirated software, movie, and music files that users are likely to access through these sites. Malware has been found preinstalled on computers sold at retail outlets as well as in media storage devices. Suffice it to say, there is no shortage of methods for infecting endpoints.

Recent Trusteer analysis of endpoint devices in large enterprises confirms the widespread presence of commercial malware (see Figure 2). Local area network (LAN) secured networks typically exhibit one out of every 1,000 devices infected with advanced malware; the ratio for bring your own device (BYOD)/ home computers stands at 1:500. However, infection ratios of several large enterprise customers have been at 1:100 on LAN secured networks. These numbers represent a critical risk level given that just one compromised device could provide devastating access to a cybercriminal.

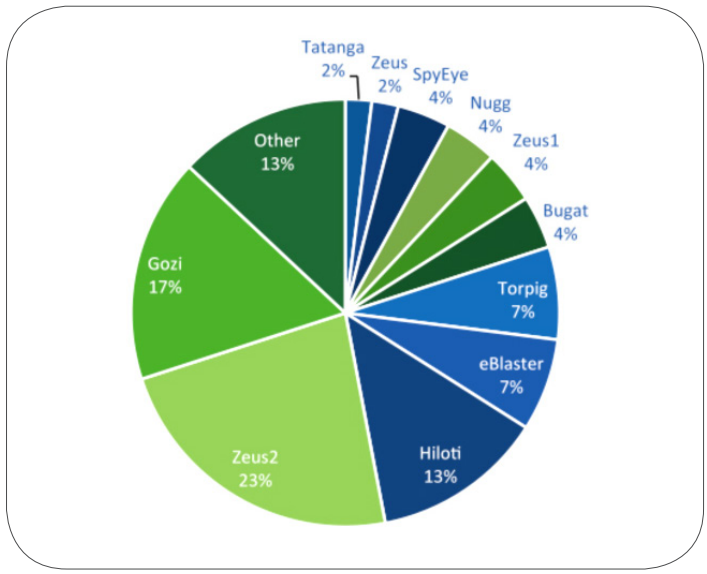


**Figure 2: A Typical Malware Family Infection Distribution on Employee Endpoints at a Large Enterprise**

*Source: Trusteer, 2012*

# Protection of the Endpoint

Corporations and consumers will have spent over $8 billion on antivirus software in 2012[27] to provide some level of endpoint protection against cybercriminal attacks. The two primary protection methods in place are broadly categorized as device protection and network protection. Both approaches primarily attempt to identify and remove malware-associated files (droppers, crimeware packages, malware containers, etc.) before the malware is installed on the endpoint.

## Device Protection

Device protection applications, more commonly referred to as antivirus or anti-X, are installed on the endpoint where they scan all (or some) installed files and evaluate new files prior to installation. Device protection approaches primarily use signature-based methods to compare all the files under evaluation with known malware file configurations. Although device protection can be effective against known virus, adware, and general "nuisance-ware" attacks, this approach has proven to be ineffective against more advanced malware.

As mentioned above, criminals use polymorphism to continuously alter the appearance of malware files specifically to evade signature-based malware detection. Cybercriminals also use stolen or forged certificates to present malicious files as legitimate applications or updates. Once the malware file is downloaded, it is too late for device protection applications to find the malware. Even if the application signature database is updated to include a malware file that was installed on the device, it is too late.

Unfortunately, polymorphism is only one of several techniques that modern malware uses to avoid endpoint detection. For example, Shylock (a malware strain discovered first by Trusteer in 2011[28]) and Tilon (a new malware strain discovered first by Trusteer in September 2012[29]) inject malicious code into various native Windows processes and then self-terminate so that no malware process can be found in memory thereafter. To survive system shutdown, the malware hooks into the Windows shutdown procedure to reinstate the files and registry keys required for reinstallation just before the system is completely shut down, after all other applications are closed (including antivirus). Once these malware strains are installed, they are unlikely to be found by any antivirus applications.

Some device protection applications are beginning to use a technique called sandboxing to execute suspect files in a virtual environment to see if the file exhibits malware-like behavior. The goal of sandboxing is to create an isolated environment on the machine where a suspicious file can be safely tested before it is allowed to execute. As to be expected, advanced malware is now capable of detecting a virtual-machine environment (as discussed in the next section) and hence take evasive measures.

Although theoretically reasonable, sandboxing is fraught with problems. Because it is a software platform, it has exploitable vulnerabilities. A recent example is the Java 0-day exploit that broke out of the JVM "sandbox" access controls. Also, a sandbox typically needs some route for users to export content out of the sandbox to the underlying device, which malware can exploit.

## Network Protection

Network protection approaches attempt to identify malicious or suspect files as they are downloaded from the Internet to the endpoint device connected to the corporate network. Like antivirus applications, files that match known malware signatures are prevented from being downloaded to an endpoint device. As discussed, criminals regularly bypass this technique using polymorphism.

Many network protection approaches identify malware by utilizing virtual machine environments to run suspicious files in an isolated environment (similar to sandboxing, but off the endpoint device). However, some malware strains can detect virtual environment execution and then evade detection. For example, malware can check for certain registry entries, process names, or mouse and video drivers (usually not present on virtual machines). Malware can then evade virtual machine detection by not running or presenting itself as something different. Another evasion tactic is simply to sleep for a period of time to avoid running while it is being monitored. Sleeping helps malware avoid virtual machine detection, but it only delays the inevitable on a legitimate end-user device.

Network protection functions only when the endpoint device is connected to the corporate network. Users often access devices used on the corporate network to connect to the Internet when they are off the corporate network (e.g., when they are at home or traveling). Devices that become infected while off the corporate network are a blind spot because network protection applications do not scan devices for malware.

### Implications of Current Endpoint Protection Methods

In addition to having suboptimal threat-detection capabilities, current endpoint detection methods are resource intensive. The above methods often identify files as suspicious, which then requires human intervention for further analysis. Depending on how the detection applications are tuned, they can generate an enormous number of false positives (files erroneously identified as being malicious). Additionally, once the above methods identify malware, the malware must be fully remediated from the endpoint device. This usually requires an additional, inconvenient step wherein a security specialist must access the endpoint device to ensure the threat is completely removed.

# A New Protection Layer

Clearly, current endpoint protection methods are falling short. As cybercriminals continue to advance their capabilities, the gap between what is and can be detected and what is completely undetected is widening. A new approach is desperately needed to fight the rising onslaught of cybercrime before corporations face irreparable damage.

## Operating Assumptions

To define the requirements for a new protection layer, we must first define the current operating environment. The following operating assumptions, even if not universally accepted, provide a conservative base for building a new protection paradigm that overcomes the weaknesses of current approaches:

- End users cannot be taught to avoid malware infections. Humans make mistakes and infection approaches are becoming increasingly stealthy.
- Software vulnerabilities will continue to emerge despite all the best software design and testing efforts. Endless software patching is the norm.
- Cybercriminals will continue to develop new methods for evading detection along the entire infection path.
- The number of endpoint malware infections will continue to increase; current endpoint protection methods simply cannot keep pace.

## A Last Line of Defense

If corporations cannot prevent endpoints from becoming infected with advanced, dangerous, evasive malware, what then? Do they throw more money and more protective solutions at the problem, hoping that more inspection will produce more detection? Or do they come to realize that they need a new approach, a new way of looking at the malware problem?

If the fundamental operating assumption is that malware will infect the end device, enterprises must find a way to detect and remove the malware before it can do harm. Malware can cause damage only when it is executing on the endpoint device. Once malware executes, it exposes itself for what it is. Although we can't fully prevent malware from infecting the device, we can certainly determine when malware is running on the device — if we know what to look for. This means conducting real-time, persistent device monitoring to find active malware threats and, importantly, specifically identifying threats that seek to compromise critical enterprise resources.

The protection must focus on defending the specific endpoint applications that provide access to sensitive corporate resources, such as application credentials or business data. Corporations can ignore other applications to reduce the noise and system resources associated with attempting to defend the entire endpoint against every possible threat. Only threats that target the defined corporation assets matter.

What activities might expose the presence of malware? One is identifying any tampering with the application memory, processes, and application program interfaces (APIs) that would provide unrestricted access to application functionality and data flowing through the application. For example, many advanced threats use browser tampering. By tampering with core browser functions (memory alteration), malware can get control any time a page is loaded to the browser and observe and modify it.

Another malware-related activity to monitor is the capturing of credentials or sensitive data through key logging, or the logging of user display activity, which could map out application workflow, business processes, and the location of sensitive data. In short, real-time application protection catches malware red-handed as it is attacking the application by any means.

Finally, this new layer should also provide remediation once suspicious activities are identified. The threat must be immediately removed or disabled not only to prevent loss but also to prevent the threat from taking evasive action (e.g., writing files and registry keys to reinstall itself after removal). This approach is far more efficient, cost effective, and user friendly than using a separate malware remediation process.

## Conclusion

Corporate endpoints are under attack. Cybercriminals have developed ingenious and effective methods for installing malware on endpoints that effectively steal all control from the end user. And nothing indicates these attacks will slow down anytime soon. Critical system vulnerabilities have been an ongoing issue with all software applications and will certainly continue. Popular defensive technologies have provided some protection against the most blatant attacks but have had little impact against more advanced threats. A new endpoint protection approach is desperately needed.

Business and technology leaders must recognize that they are in the middle of a cyber war. Cybercriminals are preying on industry's lack of awareness and are actively engaged in covert corporate espionage activities that are unlikely to be uncovered — ever. Business leaders will continue to wonder how a new entrant developed a competitive product so quickly, why another provider always seems to offer slightly better pricing, or how sensitive corporate information was leaked to the press.

The key to eliminating cybercrime is to eliminate malware. And the key to eliminating malware is to fight it head on. Corporations must root it out the moment it "goes live" on the endpoint and destroy it. Malware has evaded every other defense, but the moment it goes operational, it exposes itself. Endpoint application protection is designed to do what other approaches can't: detect live, running malware and remove it from the endpoint. It is the last line of defense.

# About Trusteer

Trusteer is the leading provider of cybercrime prevention solutions that protect organizations against financial fraud and data breaches. Hundreds of organizations and millions of end users rely on Trusteer to protect their computers and mobile devices from online threats that are invisible to legacy security solutions. Trusteer's Cybercrime Prevention Architecture combines multi-layer security software and real-time threat intelligence to defeat zero-day malware and phishing attacks, and help organizations meet regulatory compliance requirements. Leading organizations such as HSBC, Santander, The Royal Bank of Scotland, SunTrust and Fifth Third are among Trusteer's clients.

For more information visit: **www.trusteer.com**.

1 www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf, accessed September, 17, 2012

2 *Underground Economies*, McAfee, SIAC, March 2011

3 *Mandiant M-Trends*, 2012

4 *Verizon 2012 Data Breach Investigations Report*

5 *Mandiant M-Trends*, 2012

6 *Underground Economies*, McAfee, SIAC, March 2011

7 *CF Disclosure Guidance: Topic No. 2*, Division of Corporation Finance, Securities and Exchange Commission, October 13, 2011

8 *The 2011 Global Economic Crime Survey*, PWC, November 2011

9 *Verizon 2012 Data Breach Investigations Report*

10 *Verizon2012 Data Breach Investigations Report*

11 *FireEye Advanced Threat Report*, 1H 2012

12 *The VOHO Campaign: An In Depth Analysis*, RSA FirstWatch Intelligence Report, September 2012

13 *The Elderwood Project,* McDonald, O'Gorman, Symantec, September 2012

14 *Sophos Security Threat Report 2012*

15 *Websense Threat Report 2012*

16 *Symantec Internet Security Threat Report, 2011 Trends,* Volume 17

17 *McAfee Threats Report: Second Quarter 2012*

18 *FireEye Advanced Threat Report* —1H 2012

19 *2012 Bit9 Cyber Security Research Report*

20 *Symantec Internet Security Threat Report, 2011 Trends*, Volume 17

21 *Microsoft Security Intelligence Report*, Volume 13, June 2012

22 *IBM X-Force 2011 Trend and Risk Report*

23 IBM X-Force 2011 Trend and Risk Report

24 *Secunia Yearly Report 2011*

25 B*efore We Knew It, an Empirical Study of Zero-Day Attacks in the Real World*, Bilge, Dumitras, October 2012

26 *Microsoft Security Intelligence Report*, Volume 13, June 2012

27 Wired.com, *Is Antivirus Software a Waste of Money?*, March 2, 2012

28 Trusteer Blog, *Merchant of Fraud Returns — Shylock Polymorphic Financial Malware Infections on the Rise*, February 15, 2012

29 Trusteer Blog, *Tilon — Son of Silon, August 9, 2012*