The rising threat of corporate cybercrime

Understand cybercriminal motives and methods to create an effective defense

Contents

1 Introduction
2 The value of corporate cybercrime
2 The difficulty of preventing the unseen
3 The methods of corporate cybercrime
7 Protection of the endpoint
8 A new protection layer
10 Conclusion
10 For more information

Introduction
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, and they are 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 across the Internet, including a wide range of web 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 gain employee-level access to the corporate network, applications and data.

“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 had been using malware and key-loggers installed on bank employee devices to obtain employee login credentials. They used the stolen credentials to initiate fraudulent international wire transfers of USD400,000 to USD900,000. Then, in October 2012, 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, communications, financial services, defense and legal (valued at over USD500 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 GBP800 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 or solution rollout stopped or slowed by a data breach, or the credible threat of a data breach.”

Beyond the economic impact of intellectual property breaches and the loss of sensitive customer data are the legal ramifications of failing to adequately protect valuable corporate assets. Investors may 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 institute proper, best-practice protections. Highly regulated industries may 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 difficulty of preventing the unseen
Cybercriminals have been targeting financial institutions for more than 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 is often discovered quickly. 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, in fact, completely oblivious to cybercrime attacks. The vast majority of cybercrime victims discovered a compromise only because a third party notified them (94 percent of victims according to Mandiant and 92 percent according to Verizon). Once a cybercriminal gains access to a corporate network, the median time to detect the intrusion is 416 days. It is highly likely 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 10 organizations report all data breaches or losses suffered, while one in 10 organizations will only report breaches or losses that they are legally obliged to, and no more. Six in 10 organizations currently ‘pick and choose’ the breaches or losses they report, depending on how they feel about them.” And despite the 2011 US Securities and Exchange Commission (SEC) guidance for disclosing cybercrime incidents, few companies have done so. This tendency follows a recent PricewaterhouseCoopers survey of 3,877 respondents from organizations in 78 countries that found the top concern regarding cybercrime is reputational damage (indicated by 40 percent of respondents). Corporate officers are often 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 USD1 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 USD60,000 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 the *Symantec Internet Security Threat Report, Verizon Data Breach Investigations Report, McAfee Threats Report and Sophos Security Threat Report.*

### Targeting employee endpoints for cyber attack

Some enterprise attacks are opportunistic (35 percent of large organization breaches), while others are highly targeted (50 percent of large organization breaches). And various newer targeting techniques fall somewhere in the middle. Trusteer, an IBM company, has found that at any point in time, approximately one percent of all devices 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 and other social networking sites) 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 by 56 percent. The malicious emails often contain a malicious file, a link to a malicious website or both. Despite best efforts to train and warn employees, phishing attacks are very difficult to prevent.

**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 (such as scams posted on Twitter or 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. Cybercriminals 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. The number of malware-hosting websites is staggering. Sophos reports that 30,000 websites are infected every day, and 80 percent of those are legitimate, compromised sites (82 percent according to WebSense). Symantec identified 9,314 malicious websites per day in 2011, and McAfee reported finding 10,000 new malicious websites per day in June 2012. The likelihood that an end-user device will be infected when the user simply browses the web is higher than ever.

**Exploiting system vulnerabilities**

After cybercriminals convince victims to open a malicious email file attachment or visit 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. Not surprisingly, a recent survey found that 74 percent of IT and security professionals believe the security of their endpoints—their laptops and desktops—is ineffective.

**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 cataloged 6,843 vulnerabilities in web-based systems, applications and computing tools in 2011 (Symantec reported 4,989 new vulnerabilities using a different vulnerability database). Although the number of vulnerabilities was down 19 percent from 2010, the percentage of high-level severity vulnerabilities increased to 24 percent 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 percent of all disclosed vulnerabilities in the first half of 2012. The remaining vulnerabilities were about evenly split between operating systems and browsers. Note that browser and browser component vulnerabilities were 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 would otherwise 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 percent of all known vulnerabilities had publicly available exploits. Approximately 91 percent of vulnerabilities were patched the same day they were publicly disclosed. Most of the other vulnerabilities were patched within a few weeks.

But the availability of a patch does not guarantee that it is installed on the end-user 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 results in approximately 2.7 percent of Microsoft programs and 6.5 percent of third-party programs that remain unpatched at any given time. Multiplying 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 lifecycle 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 organizations falsely believe that zero-day vulnerabilities pose a limited threat because disclosed vulnerabilities are patched so quickly. However, industry research discovered that attackers often exploit vulnerabilities long before they are publicly disclosed, causing zero-day exploits to last 312 days on average. 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. In fact, a Forbes article explored the underground market for zero-day exploits that are provided exclusively for the most current version of the software, and the results are shown in the table. 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.

<table>
<thead>
<tr>
<th>Black-market value of various zero-day exploits</th>
<th>USD5,000–USD30,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader</td>
<td>USD20,000–USD50,000</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>USD30,000–USD60,000</td>
</tr>
<tr>
<td>Google Android</td>
<td>USD40,000–USD100,000</td>
</tr>
<tr>
<td>Adobe Flash or Java browser plug-ins</td>
<td>USD50,000–USD100,000</td>
</tr>
<tr>
<td>Microsoft Word</td>
<td>USD60,000–USD120,000</td>
</tr>
<tr>
<td>Microsoft Windows</td>
<td>USD60,000–USD150,000</td>
</tr>
<tr>
<td>Firefox or Safari</td>
<td>USD80,000–USD200,000</td>
</tr>
<tr>
<td>Google Chrome or Internet Explorer</td>
<td>USD100,000–USD250,000</td>
</tr>
</tbody>
</table>
The rising threat of corporate cybercrime

Typically, criminals don’t have to rely solely on developing exploits for newly discovered vulnerabilities. Because many users find it challenging to stay up to date on critical security patches, many exploits continue to be effective for months or years after a vulnerability patch has been released. For example, 39 percent of users failed to install a Microsoft Word update one year from its release, and 70 percent of users had not installed an Adobe Flash Player update within a month of its release. This lag time 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 file directly onto the endpoint. The process typically involves downloading malicious code 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 code to exploit the vulnerabilities. If it finds no vulnerabilities, the exploit kit does nothing. Malicious files are dynamically created so that they cannot be found by known techniques for signature and pattern matching used by most anti-virus 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 anti-virus 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, movies 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, as shown in the graphic. Local area network (LAN)-secured networks typically have one out of every 1,000 devices infected with advanced malware; the ratio for bring-your-own-device (BYOD) or 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.
Corporations and consumers spent over USD8 billion on anti-virus software solutions in 2012\textsuperscript{23} 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—such as malicious code, crimeware packages and malware containers—before the malware is installed on the endpoint.

**Device protection**

Device-protection applications, more commonly referred to as anti-virus solutions, 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 files under evaluation with known malware file configurations. Although device protection can be effective against known viruses, adware and general “nuisance-ware” attacks, this approach has proven to be ineffective against more advanced malware.

Today’s criminals use polymorphism to continuously alter the appearance of malware files 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 still too late.

Polymorphism is only one of several techniques that modern malware uses to avoid endpoint detection. For example, Shylock (a malware strain discovered by Trusteer in 2011) and Tilon (a malware strain discovered by Trusteer in September 2012) inject malicious code into various native Microsoft 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—that is, after all other applications are closed, including anti-virus solutions. Once these malware strains are installed, they are unlikely to be found by any anti-virus 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. Yet, advanced malware is now capable of detecting a virtual-machine environment and can 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 zero-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 anti-virus applications, files that match known malware signatures are prevented from being downloaded to an endpoint device. However, 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 by presenting itself as something different. Another evasion tactic is to have malware “sleep” for a period of time to avoid running while the system is being monitored. This helps malware avoid virtual machine detection, but it only delays the inevitable on a legitimate end-user device.

Network protection is effective 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—such as 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.

In addition to having limited threat-detection capabilities, current endpoint-detection methods are resource intensive. When files are identified as suspicious, human intervention is required 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 malware is detected, it must be fully remediated from the endpoint device. This usually requires a security specialist to 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 can be detected and what goes 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, organizations must first define the current operating environment. The following operating assumptions can help organizations build 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 being infected with advanced, dangerous and 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 endpoint 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 organizations may not be able to prevent malware from infecting the device, they can certainly determine when malware is running on the device—if they know what to look for. This means conducting real-time, persistent device monitoring to find active malware threats and prioritizing those 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. Threats that target the defined corporation assets can put the entire business at risk.

What activities might expose the presence of malware? One is identifying any tampering with the application memory, processes and application programming interfaces (APIs) that 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, malware can get control any time a page is loaded to the browser and observe and modify that page.

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 can reveal the underlying application workflow, business processes and the location of sensitive data. In short, real-time application protection catches malware in action 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—such as 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. 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 midst of a cyber war. Cybercriminals are preying on the lack of awareness in the business world 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. Organizations must root out and destroy malware the moment it “goes live” on the endpoint. 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. This is the last line of defense.

Why IBM?
IBM Security solutions are trusted by organizations worldwide for fraud prevention and identity and access management. The proven technologies enable organizations to protect their customers, employees, and business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

For more information
To learn more about Trusteer solutions for employee endpoint security, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security

About IBM Security solutions
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM® X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing


9. Trusteer was acquired by IBM in August of 2013.


