Cyber Espionage
The harsh reality of advanced security threats
Contents

Introduction 3
A new enemy emerges: The cyber cartel 5
The reality of cyber espionage 6
The natural evolution of cybersecurity 8
The personal cyber beacon 12
Introduction

“The new battle space is the economy. ... We spend hundreds of billions of dollars on weapons systems each year. But a relatively small amount of money focused against our financial markets through leveraged derivatives or cyber efforts can result in trillions of dollars in losses. And, the perpetrators can remain undiscovered.”

Financial Analyst Kevin D. Freeman in the Washington Times

An urban legend states that ostriches bury their heads in sand to avoid danger — the belief is that if I cannot see it, peril cannot see me. For decades, some businesses have been operating as if they were ostriches and the all-protective sand they hide in were composed of compliance requirements and safe practice regulations. In both cases, it is time to create a more appropriate and proactive security posture with business-enabling capabilities. Today, covert activities are occurring below the radar on practically every continent, attempting to embed themselves within organizations and government institutions by using stealth techniques and exploits. First-generation security practices are no longer sufficient to protect rich targets such as research and development, business strategy, intellectual property, and other business-sensitive information that, if compromised, could damage the company, its place in the industry, and its relationship with consumers or investors. Advanced Persistent Threats (APTs) are the cause and the silent perpetrator.

The automated attack

APTs are modern, automated versions of traditional espionage, which was originally more reliant on humans operating in the physical world. Operatives leverage and obfuscate cyber techniques, modeled after those in the physical world, in order to steal information and proprietary data in the cyber realm. Adversaries often use a methodical approach, similar to the one depicted in Figure 1, to research, plan, and execute their attack sequence. Unlike traditional malware, APTs are rarely

Figure 1. Cyber adversary targeting and attack
detected and do not trigger any alerts that would indicate that there is an incident occurring within the enterprise. They are challenging to detect and combat because they can covertly embed themselves into your environment and “establish a way to come back later, to steal additional data, to remain undetected by their victim.” Opportunistic in nature, they are able to act on known or unknown vulnerabilities (some of which are available for purchase). APTs search for the path of least resistance until they can get a foothold in which to insert and conceal themselves within an organization’s IT infrastructure.

Many organizations currently are not organized, equipped, staffed, or positioned to look specifically for APTs. Many organizations operate their information security practices and operations in a siloed environment, and as a result, information in separate divisions usually does not get aggregated, correlated, and analyzed. Instead, their security culture typically relies on reacting to less harmful changes in regulations, which are more visible and therefore easier to detect. In a recent study, 76% of all APTs went undetected where anti-virus software was present. Malware may not deploy until it bypasses anti-virus software. Information accrued from APTs yields insight into traditional corporate protective measures and thwarts standard commercial security, literally putting everything at risk from intellectual property to actual strategic business processes.

Skillfully planned, stealth, and sustained actions subvert the existence of communication between the victim organization and outside attackers. Various techniques abound that will mask the APTs’ actual activities. In fact, APTs rarely employ any tactics that hurt the current security infrastructure because they have an ulterior motive that benefits from hiding — that is, to set up undetected occupancy, allowing criminals a right of entry for doing surveillance, and gathering data. Injury comes later, after the information is used. Interestingly enough, cyber criminals usually gain access to the desired information via valid credentials.

Social engineering, for example, provides a low-risk environment for cyber criminals or nation-states to collect strategic information about a company, a hierarchy of employees, and organizational practices. Popular networking sites create a comfort zone for users. From posting on their own social media pages, responding to instant messages, and opening tempting e-mails, to giving access to “friends,” most people behave without a strong sense of suspicion. Instead, they operate under a false sense of security and freedom, offering criminals easy access to continuous and vast amounts of personal data and a plethora of opportunities for direct (albeit disguised) contact. A typical social-networking profile is shown in Figure 2.

Figure 2. Social networking profile

![Social networking profile](image)

Criminal entities combine social media intelligence—harvesting techniques with spoofed e-mails (essentially a Pandora’s box) to any number of employees about a relevant topic. This process, called “spear phishing,” allows for the low-key distribution of malware once the recipient opens the e-mail. Realistically, anyone anywhere can essentially build out an entire database of actual employee profiles for those who work in the victim company. The profile can include items such as job title, cell phone, personal Web page, and social-networking memberships.
Harmful results posed by APTs can be extraordinary and rapidly increasing in scale. In fact, cyber cartels will soon surpass drug cartels in posing the largest threat to global security.\textsuperscript{8} In essence, enterprises competing in the worldwide marketplace with innovative components or solutions are in the greatest danger of experiencing impediments in conducting business, protecting intellectual property, and preventing potential future exploits by criminals who engage in gathering more intelligence, money laundering, fraud, sabotage, theft, and misdirection of communications, to name a few.

Intangible threats exist as well, including damage to the brand due to public awareness of the breach, loss of competitive edge, and loss of confidence. Continued theft of intellectual property could result in the inability for some U.S. companies to compete effectively in the global marketplace.
The reality of cyber espionage

In 2008, several well-known oil industry companies were victims of significant breaches aimed at stealing bid data. For the oil and gas industries, this information could include anything from software source code to actual valve settings. Bid data, and other like information, enables companies to remain competitive in the global marketplace. How did cyber criminals retrieve the data? They infiltrated these companies utilizing highly specialized malware and stolen e-mail passwords, messages, and the like tied to C-level executives. The path information took may have linked the crime to perpetrators in territories suspected of having potential nation-state involvement.\(^1\)

It is important to note that cybercrime can be costly, not only to the victims, but to others in the same industry, vertical industries, and even the State. In the end, whether the trophy is financial in nature or based on intellectual property, there is typically monetary loss. In 2010, a national organized crime syndicate acquired more money by performing online-banking fraud than drug cartels did selling their product.\(^1\)

However, according to the MI5, the largest threat in the APT world comes from a prominent Asian country’s government.\(^1\) It has been theorized that, as a developing power, it may be motivated to acquire intelligence for a myriad of purposes, including financial gain, competitive advancement, tactical defense, and dissident activity monitoring.\(^1\) American companies may stand in its crosshairs. A prominent Asian country’s suspected role in supporting cybercrime is hard to ignore.

U.S. companies are not alone in facing these attacks. A very well-known foreign automotive company (with ties to its home country’s government and other country’s) revealed injury from an APT that was able to leverage\(^1\) embedded insiders for assistance. In a recent legal complaint, they allege that a foreign power received intelligence from three employees — two high-level, long-term workers and one with an impressive role in developing the company’s electric car (codeveloped with an automotive company from another nation-state). The rise of new, cyber-savvy powers, like China, and the increased ease in downloading large amounts of data onto portable storage media means that the threat of corporate espionage will continue to increase.\(^1\)

**Limitless boundaries**

In cases of cyber espionage, traditional or real-world limitations, such as cost of execution and/or exposure, are irrelevant. A victim organization is unprotected because there are no international norms. Why? Essentially, no consensus exists on the issue of illegality since large numbers of countries may be actively engaged in such acts.

Cyber espionage is prevalent because it often has no or few consequences. These activities may get support from the home countries from which these criminals or crimes emanate;\(^1\) however due to the nature of the Internet, it is sometimes difficult to tell from where the true source of an attack may be coming. As depicted in Figure 3, Cyber espionage is not confined by traditional regional borders and comprises a wide array of attack techniques that can be used against target-rich organizations.
In some countries, for instance, hacker clubs watched by the government become potential recruitment candidates for the nation-state-run cyber warfare units. The remote, hidden ability to capture proprietary data increases the criminal element’s efficiency and effectiveness by reducing the time and expense of gaining the knowledge in a traditional manner.

State support is also a reason why attribution is so challenging and, often, even impossible. In many instances, the information gleaned from cybercrime benefits a country’s industrial development, race to market, or defense posture. Clearly, countries that have great cybercrime success would be unwilling to participate in any prosecution-based norm. Unless there is global agreement, criminal actors will simply move to where they can comfortably take root. Furthermore, when nation-states use crimeware from the APT underworld, their attacks look like every other attack, so it is nearly impossible to determine attribution. In addition, cybercrime itself may offer nation-state actors a veil under which to hide while spying.
The natural evolution of cybersecurity

Underlying organizations are usually unaware that criminals have invaded, thanks to a highly exploitable reactive defense posture. Figure 4 provides an overview of the reactive approach that many organizations are still using to address security incidents. This culture allows criminals enormous opportunities to take advantage of both known vulnerabilities and search for those that are yet unrealized. The latter constantly evolve due to human error, faulty configurations in the infrastructure, flaws in the software, and problems with applications. Advanced cyber adversaries are skilled at locating the not-yet-realized vulnerabilities; criminals are increasingly successful in thwarting technology that should protect an organization. Not surprisingly, according to an Information Week article, automated attack tool kits are responsible for at least 61% of online attacks. These kits, which are available for purchase in the cybercriminal marketplace, allow the potential for secondary attacks as well.

Compliance might not mitigate threats
It is essential to help executive management understand the breadth of what is at stake and why present-day security controls are only addressing a portion of the issue. APTs flourish because of an outdated organizational mind-set that paying the compliance minimum mitigates the potential for threats. Unfortunately, many key decision makers may view taking action as an unnecessary and cost-prohibitive effort. Ultimately, this reactionary-based approach leaves vast amounts of proprietary information easily accessed by undetected criminals — this is why businesses are strategic and/or popular targets. The key to protecting data is performing risk assessments that take into account potential negative situations that are able to occur beyond those related solely to regulatory compliance.

What about when an APT has damaged a company? "Does information about the damage become public? In many instances, there is a veil of secrecy blanketing losses experienced by companies in many industries, and often, the losses seem to be concentrated in the financial industry.

Figure 4. The old approach for information security – Reactive

<table>
<thead>
<tr>
<th>• Perimeter security focus</th>
<th>• Inward facing</th>
<th>• Organization silos</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Information silos</td>
<td>• Too many alerts</td>
<td>• Resource constrained</td>
</tr>
<tr>
<td>• Signature based controls</td>
<td>• Too much data</td>
<td>• Manual analysis</td>
</tr>
</tbody>
</table>

Security incidents are typically reported to an information security organization through a variety of different channels including other departments, external vendors, law enforcement, media outlets, and the public.

Investigations typically take a considerable amount of time and often are plagued with missing or lost information that could have assisted significantly with understanding what happened.

Quickly finding and containing compromised devices can be very challenging in large distributed network environments. This process can often involve dispatching resources on-site to locate devices of interest.

Remediation often involves having to re-image devices, which can take long period of times and also result in lost data and negative impacts to employee productivity.

Root cause analysis often involves collecting and analyzing logs from multiple internal sources. In some cases, the true root cause is not determined due to a lack of consistent logging or missing cyber intelligence.
The efficient business of APTs
Another aspect of this emerging risk deals with the efficiency of the perpetrators and their holistic approach. Attackers are operating from a business practice standpoint when designing APTs. They are actually taking time and using resources to understand the business processes used by the target entity. Unlike those for organizations, there are no standards or guiding bodies to control this criminal behavior — law enforcement is woefully behind the curve because it cannot keep up with the rapid evolution of cybercrime.

Generally, the criminal world has experienced a large shift from an individual, independent focus to a virtual, collaborative model that thrives on innovation and data sharing. Over the past 10 years, a malware ecosystem has formed that supports this cybercrime wave. An adversary has an available network of resources from which to choose, and many have specialties. Various groups include criminals from many nation-states (where this work is considered to be a badge of honor), organized crime, hackers, and others. Typically, participants are unaware of the overall mission. Rather, they focus solely on just their portion.

Figure 5. The new approach for cybersecurity — Proactive

A great example of this collaboration would be the Stuxnet worm, in which there were several different components assembled to deliver a more sophisticated and focused exploit. In this situation, there is a general belief about who the actors were who created this worm. However, it is easy to attribute APT threats to the wrong party, thus wasting valuable time and money in pursuit. This case is unique, as it represents the first one of its kind where an attacker had remote control over critical systems in a plant. Its implications are profound primarily due to its potential ability to inflict physical damage to a nation’s critical infrastructure.

Protecting assets
How do you protect your assets from this burgeoning threat? It begins with understanding the corporate ecosystem, performing a residual risk assessment, and leveraging a cyber intelligence–based methodology such as the one shown in Figure 5. It is also important to determine what information, strategic relationships, or behaviors cyber adversaries and other espionage-oriented resources would find valuable. In addition, organizations review and consider changing the way they structure their business and the way they interconnect with their environment.

A forward-looking cyber threat intelligence capability
• Conduct emerging threat research
• Establish partnerships to share intelligence
• Assign threat focus areas
• Establish live, dynamic intelligence feeds
• Implement a holistic approach to cyber threat identification
• Actively track the cyber criminal element
• Perform daily emerging threat reviews
• Maintain awareness of the changing technology and business environment
• Patch operating system, network, process, and application vulnerabilities
• Deploy and maintain signature and behavioral based controls
• Produce metrics and trending data for multiple key threat indicators
• Continuously improve automation capabilities
Ultimately, fighting APTs, or even the potential for APTs, requires continuous monitoring enriched with actionable cyber intelligence.

Until recently, most organizations have not been looking at the security space from a holistic approach. However, this threat can come from multiple vectors. The old standard point-solution mentality is no longer sufficient. Security strategies and defenses today require reviewing the entire system and all of the interdependencies.

Additionally, anti-virus software is not a complete solution to the problem. It is important to have it in place, but many companies view it as an information technology tool. Anti-virus software is ill equipped to disarm many perpetrators — protective ware deals with technology processes and not the human element behind APTs. The latter is able to adjust behavior over a length of time so that they can adapt to changes in the environment, thus controlling their illicit activity and shifting or morphing to get the desired result.28

When rethinking your approach, it is important first to understand the life cycle of an emerging threat and how the underlying workflow system should be designed and automated to help mitigate an organization’s level of risk from this threat. (Figure 6 shows the components of a type of Cyber Threat Incident Management Workflow System that could potentially be considered.) Second, organizations need to understand which devices and systems support critical business processes. When planning a proactive defense strategy, one should anticipate how or if a cyber adversary could exploit these devices and systems. A rule of thumb when protecting valuable data is that it should be required to consider and check any device that has an internal computer and is Internet Protocol (IP) enabled, such as cell phones and handheld devices. Each of these devices can potentially offer criminals multiple ways to access and exfiltrate information.29
Figure 6. Cyber threat incident management workflow

Take an inventory
Look at everything, including the pieces and components branded under trustworthy names, but that come from outside your borders, where you may not have full visibility — take a baseline of what they do and who they are reaching out to and determine whether you want these activities to take place.
The personal cyber beacon

Employees should also be included during the assessment APTs. They can be your frontline of defense or your biggest threat, sometimes without even realizing it. It begins with elaborate background checks on all potential new employees and extends to performing due diligence to make sure that those getting access deserve the right, and can handle the responsibility. However, even when you think you are covering every important hole in your security — you are compliant with all governmental regulations, have checked your supply chain for espionage-related devices, and done thorough investigations into your new employees — the enormous threat of the human element persists.

Employees today have more access than ever before to a vast amount of information and data. Copying large amounts of potentially confidential information onto small, handheld, and easily concealable storage devices is difficult to defend against. Without the appropriate protective steps and business culture to support them, almost any employee can pilfer highly sensitive pieces of information — often from the comforts of their work cubicle or home office.

While cyber adversaries also share this advantage, their view of an organization and its Internet-powered ecosystem is often broader than that of an internal employee. The cyber adversaries also typically have access to more external points of attack and targets. The diagram in Figure 7 illustrates some of the common locations and techniques that can be used by an attacker to target an organization’s cyber assets.

In the automotive company example mentioned earlier, the manufacturer fired three employees in question and placed them under investigation for possible criminal activity. Two of the three were senior level executives with lengthy careers with the company. Seen as being “… loyal company men and unlikely corporate traitors,” it was largely unforeseeable that these two would leak secret competitive information in exchange for bribe money.30

For positions of greater privilege, a more frequent and higher level of scrutiny and checks are necessary. Chief executive officers and board members are becoming bigger targets because of the ease in which criminals can access their information. In the earlier-referenced example

Figure 7. APT attack and target options

<table>
<thead>
<tr>
<th>Co-location facility</th>
<th>Corporate location</th>
<th>Social network</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

APT Approach
1 Remote control malware
2 Weak encryption-copier desk
3 Spearphish-social engineering
4 Weak wireless encryption - credentials
5 SQL injection or zero day vulnerability
6 Stolen admin credentials
about the several companies in the oil industry, the C-level employees were chiefly targeted by the e-mail-delivered APT — all it took was for one slightly distracted executive to open an e-mail and click on an innocuous-looking link. Before an e-mail warning could be sent, the worm had taken control. How does this happen so seamlessly? Figure 8 provides a sample of information about a Privileged Employee that can be available to a cyber adversary.

The same goes for your vendor supplier chain, including law firms, privileged suppliers, banks, and others you have long-standing relationships with and would not necessarily be concerned about. One of the best examples comes from various security incidents in 2010 and 2011. Essentially, any outside source that you trust and exchange information with can present an opportunity for an attacker, through various social media exploitation techniques, to monitor the exchange of information and use it to exploit your company.

A call to action – the journey from reactive to preemptive
The cyber threat continues to evolve and disguise itself with ingenious techniques to circumvent most traditional information security programs. Nations around the world continue to advertise and develop cyber warfare capabilities. These programs will teach and enable thousands of future cyber operatives with unique skills focused on traversing traditional security controls. Consequently, individuals and organizations with APT-like capabilities may likely increase. To mitigate the risks of these advancing threats effectively, organizations should evolve their current capabilities to include proactive, continuous monitoring while enhancing existing security practices to leverage cyber intelligence.

Effective security programs can no longer suggest that a successful day is a quiet day because APTs are currently going undetected. The future risk-intelligent organization will measure success by demonstrating capabilities that mitigate risk to an acceptable level while being able to leverage cyber intelligence.

“... We are in an era like the 1950s where technological innovation is transforming the tools of coercion and war. ... We tend not to see this, and look at information warfare, financial warfare, precision strike, [weapons of mass destruction], etc. as separate silos. It’s their parallel co-evolution that leads to interesting options, like counter-elite targeting. And no one is really looking at this in an overall ‘systems’ way. Diplomacy is way behind here.”

Yale University Professor, Paul Bracken
Endnotes


3 Ibid.


9 Ibid.

10 Industrial espionage: Data Out of the Door (2011) Fltimes.com (http://www.ft.com/cms/s/0/9a06c82c0-2e44-11e0-8733-00144feabdc0.html#axzz1DHoLlb4).


13 Ibid.

14 Ibid.


This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this document.
Contacts

Rhoda Woo
National Managing Principal
Security & Privacy
Deloitte & Touche LLP
+1 212 436 3388
rwoo@deloitte.com

Rich Baich
Principal
Cyber Threat & Vulnerability Management
Deloitte & Touche LLP
+1 704 887 1563
jbaich@deloitte.com

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by
guarantee, and its network of member firms, each of which is a legally separate and independent entity.
Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche
Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of
the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients
under the rules and regulations of public accounting.

Copyright © 2011 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited