Microsoft Security Intelligence Report

Volume 12

July through December, 2011

DETERMINED ADVERSARIES AND TARGETED ATTACKS

www.microsoft.com/sir

Microsoft Security Intelligence Report

Authors

Dennis Batchelder
Microsoft Protection Technologies

Shah Bawany
Microsoft Windows Safety Platform

Joe Blackbird
Microsoft Malware Protection Center

Eve Blakemore
Microsoft Trustworthy Computing

Joe Faulhaber
Microsoft Malware Protection Center

Sarmad Fayyaz
Bing

David Felstead
Bing

Paul Henry
Wadeware LLC

Nitin Kumar Goel
Microsoft Security Response Center

Jeff Jones
Microsoft Trustworthy Computing

Jimmy Kuo
Microsoft Malware Protection Center

Marc Lauricella
Microsoft Trustworthy Computing

Ken Malcolmson
Microsoft Trustworthy Computing

Nam Ng
Microsoft Trustworthy Computing

Mark Oram
Microsoft Trustworthy Computing

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Dave Probert
Microsoft Security Engineering Center

Tim Rains
Microsoft Trustworthy Computing

Frank Simorjay
Microsoft Trustworthy Computing

Holly Stewart
Microsoft Malware Protection Center

Matt Thomlinson
Microsoft Trustworthy Computing

Scott Wu
Microsoft Malware Protection Center

Terry Zink
Microsoft Forefront Online Protection for Exchange

Contributors

Doug Cavit
Microsoft Trustworthy Computing

Chris Compton
Microsoft Trustworthy Computing

Mike Convertino
Microsoft Trustworthy Computing

Enrique Gonzalez
Microsoft Malware Protection Center

Heather Goudey
Microsoft Malware Protection Center

Roger Grimes
Microsoft IT Information Security and Risk Management

Satomi Hayakawa
CSS Japan Security Response Team

Jenn LeMond
Microsoft IT Information Security and Risk Management

Le Li
Microsoft Windows Safety Platform

Jenner Mandel
Microsoft Trustworthy Computing

Hideya Matsuda
CSS Japan Security Response Team

Patrick Nolan
Microsoft Malware Protection Center

Takumi Onodera
Microsoft Premier Field Engineering, Japan

Anthony Penta
Microsoft Windows Safety Platform

Kathy Phillips
Microsoft Legal and Corporate Affairs

Hilda Larina Ragragio
Microsoft Malware Protection Center

Laura A. Robinson
Microsoft IT Information Security and Risk Management

Richard Saunders
Microsoft Trustworthy Computing

Jasmine Sesso
Microsoft Malware Protection Center

Adam Shostack
Microsoft Trustworthy Computing

Maarten Van Horenbeeck
Microsoft Trustworthy Computing

Henk van Roest
CSS Security EMEA

Patrik Vicol
Microsoft Malware Protection Center

Steve Wacker
Wadeware LLC

Dan Wolff
Microsoft Malware Protection Center

Table of Contents

About this report iv
Trustworthy Computing: Security engineering at Microsoft v
Determined Adversaries and Targeted Attacks 7
Introduction 9
Determined Adversaries 11
Same old tricks, new era 12
The role of the Internet 13
Targeted Attacks 14
Challenges in defending against Targeted Attacks 19
The risk management challenge 19
Prevention 20
Detection 21
Containment 22
Recovery 22
Communication and Information Sharing 24
The Role of Governments 24
Conclusion 26

About this report

The *Microsoft® Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, and malicious and potentially unwanted software. Past reports and related resources are available for download at www.microsoft.com/sir. We hope that readers find the data, insights, and guidance provided in this report useful in helping them protect their organizations, software, and users.

Reporting period

This volume of the *Microsoft Security Intelligence Report* focuses on the third and fourth quarters of 2011, respectively, with trend data for the last several years presented on a quarterly basis. Because vulnerability disclosures can be highly inconsistent from quarter to quarter and often occur disproportionately at certain times of the year, statistics about vulnerability disclosures are presented on a half-yearly basis, as in previous volumes of the report.

Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, where *yy* indicates the calendar year and *n* indicates the half or quarter. For example, 2H11 represents the second half of 2011 (July 1 through December 31), and 4Q11 represents the fourth quarter of 2011 (October 1 through December 31). To avoid confusion, please note the reporting period or periods being referenced when considering the statistics in this report.

Conventions

This report uses the Microsoft Malware Protection Center (MMPC) naming standard for families and variants of malware and potentially unwanted software. For information about this standard, see "Microsoft Malware Protection Center Naming Standard" on the MMPC website.

Trustworthy Computing: Security engineering at Microsoft

Amid the increasing complexity of today's computing threat landscape and the growing sophistication of criminal attacks, enterprise organizations and governments are more focused than ever on protecting their computing environments so that they and their constituents are safer online. With more than a billion systems using its products and services worldwide, Microsoft collaborates with partners, industry, and governments to help create a safer, more trusted Internet.

Microsoft's Trustworthy Computing organization focuses on creating and delivering secure, private, and reliable computing experiences based on sound business practices. Most of the intelligence provided in this report comes from Trustworthy Computing security centers—the Microsoft Malware Protection Center (MMPC), Microsoft Security Response Center (MSRC), and Microsoft Security Engineering Center (MSEC)—which deliver in-depth threat intelligence, threat response, and security science. Additional information comes from product groups across Microsoft and from Microsoft IT (MSIT), the group that manages global IT services for Microsoft. The report is designed to give Microsoft customers, partners, and the software industry a well-rounded understanding of the threat landscape so that they will be in a better position to protect themselves and their assets from criminal activity.

Determined Adversaries and Targeted Attacks

Introduction

Over the past two decades the internet has become fundamental to the pursuit of day-to-day commercial, personal, and governmental business. However, the ubiquitous nature of the internet as a communications platform has also increased the risk to individuals and organizations from cyberthreats. These threats include website defacement, virus and worm (or *malware*) outbreaks, and network intrusion attempts. In addition, the global presence of the internet has allowed it to be used as a significant staging ground for espionage activity directed at industrial, political, military, and civil targets.

During the past five years, one specific category of threat has become much more widely discussed. Originally referred to as *Advanced Persistent Threats (APT)* by the U.S. military — referring to alleged nation-state sponsored attempts to infiltrate military networks and exfiltrate sensitive data — the term APT is today widely used in media and IT security circles to describe any attack that seems to specifically target individual organization, or is thought to be notably technical in nature, regardless of whether the attack was actually either advanced or persistent.

In fact, this type of attack typically involves two separate components — the action(s) and the actor(s) — that may be targeted against governments, military organizations or, increasingly, commercial entities and civil society.

The *actions* are the attacks themselves, which may be IT-related or not, and are referred to as *Targeted Attacks* in this paper. These attacks are initiated and conducted by human *actors*, who are collectively referred to in this paper as *Determined Adversaries*. These definitions are important because they emphasize the point that the attacks are carried out by human actors who may use any tools or techniques necessary to achieve their goals; these attacks are not merely malicious software or exploits. Using an encompassing term such as APT can mask this reality and create the impression that all such attacks are technically sophisticated and malware-driven, making it harder to plan an effective defensive posture.

For these reasons, this paper uses Targeted Attacks and Determined Adversaries as more specific and meaningful terms to describe this category of attack.

- **Targeted Attacks**. The attackers target individuals or organizations to attack, singly or as a group, specifically because of who they are or what they represent; or to access, exfiltrate, or damage specific high-value assets that they possess. In contrast, most malware attacks are more indiscriminate with the typical goal of spreading malware widely to maximize potential profits.
- **Determined Adversaries**. The attackers are not deterred by early failures and they are likely to attack the same target repeatedly, using different techniques, until they succeed. These attackers will regroup and try again, even after their attacks are uncovered. In many cases the attacks are consciously directed by well-resourced sponsors. This provides the attackers with the resources to adapt to changing defenses or circumstances, and directly supports the persistence of attacks where necessary.

Determined Adversaries and Targeted Attacks may employ combinations of technology and tactics that enable the attacker to remain anonymous and undiscoverable, which is why these methods of attack might appeal to agencies of nation states and other entities who are involved in espionage-related activities.

Hardening the perimeters of computer networks is not a sufficient defensive strategy against these threats. Many computer security experts believe that a well-resourced and determined adversary will usually be successful in attacking systems, even if the target has invested in its defensive posture.[1]

Rather than the traditional focus on preventing compromise, an effective risk management strategy assumes that Determined Adversaries may successfully breach any outer defenses. The implementation of the risk management strategy therefore balances investment in prevention, detection, containment and recovery.[2]

Microsoft has a unique perspective on Targeted Attacks, as both a potential target of attacks and a service and solution provider to potential victims. This paper shares Microsoft's insights into the threat that Determined Adversaries and Targeted Attacks pose, identifies challenges for organizations seeking to combat this threat category and provides a context for other papers that will directly address each of those.

---

[1] Charney, Scott – Rethinking the Cyber Threat – A Framework and Path Forward
www.microsoft.com/download/en/details.aspx?id=747
[2] Charney, Scott – Trustworthy Computing Next
aka.ms/nextwp

Determined Adversaries

Since the beginning of history, there have been people willing to steal the possessions of others to satisfy a wide variety of motives. Targeted Attacks are simply the inevitable consequence of the digitization of previously physical processes and assets.

Determined Adversaries who deploy Targeted Attacks tend to be well funded and organizationally sophisticated. Examination of several Targeted Attacks shows that the attackers operate in a team model, to meet the requirements of a threat sponsor. The existence of the threat sponsor is critical in understanding the overall actions of Determined Adversaries. In the case of traditional cybercrime, such as attacks against on-line banking, a technically able attacker can be self-motivated. However, in other cases, such as espionage, the sponsor provides the motivation and resources for the attacker to determinedly collect the information that meets their specific requirements. Because new requirements will emerge, it is logical for the attackers to maintain persistent access to existing or potential future targets.

Detailed information about specific Determined Adversaries is often difficult to obtain. The institutions victimized by Targeted Attacks are often reluctant to share information because of the highly sensitive nature of the networks or assets that they protect.

Many of the early Targeted Attacks focused on military and defense networks,[3] which are typically among the more well-defended networks in the world. Consequently, attackers were forced to develop a wide range of technical and non-technical skills to conduct successful attacks.

Today, many of the actors involved in earlier attacks on military networks have started to put their skills to use by attacking commercial networks in order to meet a sponsor's economic goals. For this reason, security professionals consider Determined Adversaries to be among the more serious security threats that computer networks currently face.

[3] www.businessweek.com/magazine/content/08_16/b4080032218430.htm

Institutions such as military forces, defense contractors, and critical infrastructure providers have been popular targets for espionage since long before the internet existed, and they remain popular targets for Determined Adversaries. However, in a broad sense almost any institution that possesses information assets that an attacker might value can be a target.

Same old tricks, new era

The operational model often employed for human intelligence gathering will be familiar to readers of espionage novels. In this traditional espionage model, a sponsor organization or "pay master" working on their behalf provides a threat actor in the form of an intelligence officer, and requirements for the information they wish to be collected. The intelligence officer then develops operational intelligence to support the identification and recruitment of a vulnerable individual who is likely to have, or be in a position to facilitate, access to the required information. Since it may be dangerous for the intelligence officer to physically meet with the individual (or agent), they will employ a "dead drop". This is a physical location through which the intelligence officer can pass requirements to the agent, and through which in turn the agent will pass the collected information. Once the agent is established, they may then go on to recruit other agents.

The model employed by Determined Adversaries in conducting Targeted Attacks has striking similarities to this approach. The sponsor and the threat actor roles, albeit it with a different skill set, are a constant. However, the target is now a vulnerable computer system against which the attacker will employ operational intelligence to achieve compromise. Once the system is compromised, the attacker then employs a "dead drop" in the form of a command-and-control server through which information can be exchanged while protecting the identity of the attacker.

In the traditional espionage scenario, there is significant risk to both the sponsor and the threat actors of being identified. However, the same model implemented by Targeted Attacks is significantly more attractive as there is less risk of the actors being identified, detained and their activities made public.

The role of the Internet

Internet technologies provide a basis upon which to achieve huge efficiencies in communications, storage, data processing and business tractions. Given the ever-increasing use of the internet (2 billion users in 2011 with forecasts of another billion users coming online in the next four years),[4] it is no surprise that bad actors are using this near-ubiquitous communications medium for their own ends. With almost all individuals, governments, and organizations connected to one another through the internet, geography is increasingly irrelevant. Low risk attacks can be launched from locations around the world, perhaps originating in countries or regions that do not have regulations or laws governing cybercrime, or lack the resources to effectively enforce such laws.

One observation of this trend is the trickle-down effect on attack techniques and technology. Ten years ago, attackers had to build bespoke capabilities to conduct many forms of attack. Today there are kits available in illicit online marketplaces that let prospective attackers achieve the same results with much less effort and expertise. The same trickle-down effect can be observed in the evolution of financially motivated attacks employing techniques that originated with Targeted Attacks. For example, the operational model and techniques employed in the targeting of a company's payment system to facilitate online banking fraud can be similar to those used in espionage orientated Targeted Attacks.

Understanding this change in threat, and reflecting it in consideration of an organization's risk profile is now essential. For example, a luxury fashion manufacturer might think that a potential attacker would spend significant resources to acquire military or state secrets, but not to target the company's product designs. It is worth reiterating that this assumption no longer holds because cybercriminals are using the same attack knowledge and tools that were previously focused exclusively on espionage to support the traditional criminal activity of counterfeiting goods. However, in many cases, organizations are simply not prepared for this shift in the threat environment.

[4] www.mckinsey.com/Features/Sizing_the_internet_economy.aspx

Targeted Attacks

Although attackers have used computer networks to enable espionage for several decades, the widespread recognition of Targeted Attacks as a distinct class of security threat is a relatively recent development. Attacks of this type became publicly known in the mid-2000s following a number of security incidents that were believed to have been perpetrated by, or on behalf of, national governments or other state actors. More recently, reports of similar attacks waged by non-state actors against commercial and government targets for profit, intelligence gathering, or other reasons have increased.

Although Targeted Attacks may be perceived as an evolution of conventional malware activity to more sophisticated levels, it is more accurate to characterize them as the evolution of conventional espionage techniques to target individuals and non-state organizations to a degree not commonly seen in the past. This holds true even where the motive may be purely financial.

Targeted Attacks are technically opportunistic and technology agnostic; the attacker has the resources to use whatever techniques or technologies work. Although Targeted Attacks are sometimes characterized as highly advanced attacks that exploit previously unknown vulnerabilities in software, the reality is often more mundane.[5] Attackers often attempt to leverage the target's operational weaknesses, such as exploiting long out-of-date software, or unpatched vulnerabilities to gain access to a target. After the target is compromised, the attacker attempts to secure additional footholds within the network by compromising authentication systems, disabling audit capabilities, and even manipulating patch management/deployment servers, in an effort to become stealthier, maintain their position, and better exfiltrate data. Attackers have been observed to expand the scope of such attacks by remotely turning on webcams and telephones in conference rooms to eavesdrop on confidential communications in real time.

Although purely technical attacks are not unknown, most Targeted Attacks use an element of social engineering to gain access to information and sensitive resources

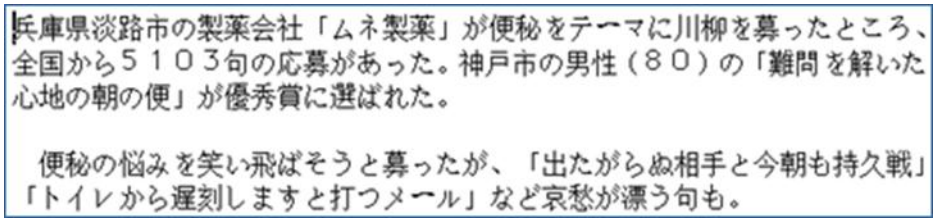
[5] www.microsoft.com/security/sir/story/default.aspx#!0day

more easily than a purely technical approach would allow. The highly targeted nature of these attacks makes it possible for a patient and thorough attacker to successfully trick even a vigilant target. Many such tactics can be considered updated versions of traditional confidence tricks in which an attacker gains the trust of the victim by appealing to basic human emotions and drives, such as curiosity, greed, compassion, and anger. Common tactics can include masquerading as a trusted party or authority figure on the telephone or in instant messenger communications in an effort to obtain the victim's network credentials, as well as customized and personalized versions of standard phishing attacks that are called *spear phishing* attacks.

In a typical spear phishing attack, the victim may receive a seemingly legitimate email that includes a malicious attachment or directs the victim to a malicious web page, in an effort to capture logon credentials or to use a browser exploit to download malware to the victim's computer. Spear phishing web pages often resemble legitimate pages on the victim's corporate intranet or externally hosted sites designed for legitimate activities, such as reviewing health insurance or employee benefit information. If the victim is accustomed to receiving internal communications about these kinds of sites, it can be difficult to distinguish between links to legitimate external sites and malicious copies.

One spear phishing technique that is often used in Targeted Attacks is the *content type attack*, in which an attacker sends an employee of the targeted organization an email message with a file attachment that contains an exploit. The attacker can individually tailor the email message to lure the recipient, making content type attacks particularly effective. Microsoft has received content type attack samples from all over the world, written in many different languages, such as the example in the following figure which announces the winner of a competition run by a pharmaceutical company.

Figure 1: Example of a lure message in Japanese

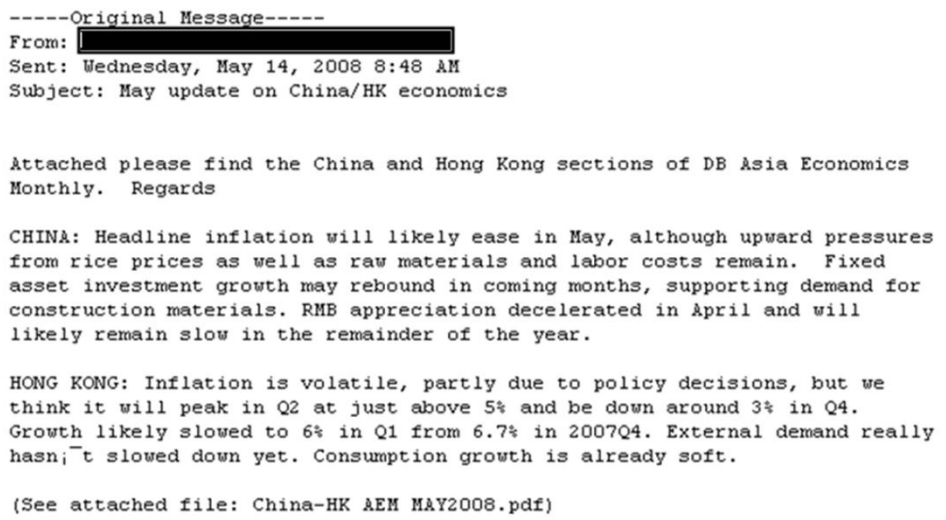

兵庫県淡路市の製薬会社「ムネ製薬」が便秘をテーマに川柳を募ったところ、全国から５１０３句の応募があった。神戸市の男性（８０）の「難問を解いた心地の朝の便」が優秀賞に選ばれた。

便秘の悩みを笑い飛ばそうと募ったが、「出たがらぬ相手と今朝も持久戦」「トイレから遅刻しますと打つメール」など哀愁が漂う句も。

The goal of the lure email message is to trick the recipient into opening the malicious file attached to the message, and attackers use a variety of psychological

tactics to accomplish this goal. Lures often masquerade as internal communications from superiors or other trusted parties, such as a trusted lawyer or business partner. A popular tactic is to represent the malicious file as containing sensitive information that the recipient might not be entitled to know, such as salary information for all of the employees in the company or department—the temptation presented by such "forbidden fruit" is often too great for recipients to resist. Another tactic is for the attacker to research the prospective recipient in advance, and then create a customized lure that appeals to the recipient's interests, as shown in the following figure.

Figure 2: An example of a lure tailored to its recipient



-----Original Message-----
From: [redacted]
Sent: Wednesday, May 14, 2008 8:48 AM
Subject: May update on China/HK economics

Attached please find the China and Hong Kong sections of DB Asia Economics Monthly. Regards

CHINA: Headline inflation will likely ease in May, although upward pressures from rice prices as well as raw materials and labor costs remain. Fixed asset investment growth may rebound in coming months, supporting demand for construction materials. RMB appreciation decelerated in April and will likely remain slow in the remainder of the year.

HONG KONG: Inflation is volatile, partly due to policy decisions, but we think it will peak in Q2 at just above 5% and be down around 3% in Q4. Growth likely slowed to 6% in Q1 from 6.7% in 2007Q4. External demand really hasn¡¯t slowed down yet. Consumption growth is already soft.

(See attached file: China-HK AEM MAY2008.pdf)

In this case, the attacker determined that the recipient was someone who worked in finance and who would be especially interested in news about financial markets in Asia. Attackers sometimes send several benign messages before any malicious ones, in an effort to build a trust relationship with the recipient.

File attachments to such messages contain malicious code that attempts to exploit a vulnerability in the application which parses the information, such as a word processor or a document reader, when the file is opened. The exploit itself is typically used to install additional malware on the computer, which performs actions such as stealing or destroying files, or connecting to other network resources. As previously stated, in most cases the malicious code attempts to

exploit a vulnerability that the software vendor has already addressed, which highlights the importance of keeping all software up to date.[6]

In early Targeted Attacks, the *payload*, or the actions conducted by the malware, was often performed by a trojan[7] that was specially crafted to search for specific files or types of files, and then upload them to servers controlled by the attacker. For example, one trojan used in a Targeted Attack was designed to search for computer-aided design (CAD) files, which often contain sensitive design diagrams. More recently, Targeted Attacks have been observed to use malware that allows the attacker to connect to the controlled computer, and then dynamically issue new commands, often using custom communications protocols designed to hide the traffic from detection by network monitoring software.[8]

A complicating factor in responding to Targeted Attacks is the difficulty in identifying that activity among the myriad of other cyberthreats that organizations may encounter on a daily basis. According to volume 12 of the *Microsoft Security Intelligence Report (SIR)*,[9] more than 700 million pieces of malware were detected on computers around the world in the second half of 2011. Identifying specific Targeted Attacks within this large threat ecosystem can be challenging for several reasons:[10]

- There are many different malicious actors.
- These actors have many different motives.
- The attacks can look similar, so the nature of the attack does not always help to identify the actor and the motive.
- The internet is a shared and integrated domain, where it is not easy to distinguish well-meaning and malicious network activity.

Attributing a Targeted Attack that has been successfully detected is central to many of these challenges. In some countries, law enforcement, the military, intelligence agencies and the private sector therefore attempt to cooperate in building a picture of the threat environment. Conclusive evidence of the "who" and "why" is often though unavailable when a system is under attack, which can

---

[6] blogs.technet.com/b/security/archive/2011/09/28/targeted-attacks-and-the-need-to-keep-document-parsers-updated.aspx
[7] www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx#t
[8] blogs.technet.com/b/security/archive/2011/09/28/targeted-attacks-and-the-need-to-keep-document-parsers-updated.aspx
[9] www.microsoft.com/sir
[10] Charney, Scott – Rethinking the Cyber Threat – A Framework and Path Forward www.microsoft.com/download/en/details.aspx?id=747

make appropriate national and organizational level responses challenging. For example, the attackers usually demonstrate operational sophistication and sometimes operate in shifts, aligning their operations to the time-zone in which the target organization or individual is located. Some attackers have even observed the same public holidays as their targets, regardless of their own physical location. Without additional information, the use of attack timing to locate the attackers can therefore have limited benefit and may even be used to mislead.

However, while attribution may never be perfect, improved categorization of specific attacks, supported by effective sharing of that information between effected parties, can help inform what an appropriate response might be. Being aware of whether the aim of a specific attack is financial crime or the theft of intellectual property, even if the actors remain unknown, will have a meaningful impact on how an organization defends itself.

Challenges in defending against Targeted Attacks

For many organizations the risks posed by the existence of Determined Adversaries presents a novel challenge. It is therefore vital for organizations to develop and implement plans that consider the possibility of Targeted Attacks. Every organization would be wise to closely evaluate their existing risk management programs, and make necessary adjustments to help reduce their overall level of vulnerability by making balanced investments in prevention, detection, containment and recovery.

The risk management challenge

Over the past 25 years, IT and information security have become more commoditized and based on a common security model, in which the focus is on infrastructure rather than asset protection. As internet technology has become cheaper and accepted as the industry standard, the emphasis has been on commercial off-the-shelf, easily deployable security mitigations to address generic threats on an enterprise wide basis. Such an approach was largely sufficient for non-military organizations 10 years ago, but during the last five years, the number of Targeted Attacks reported in industry has generally increased. And while the implementation of uniform commoditized security solutions is an important component in addressing opportunistic threats, enhanced risk management practices are more important than ever to ensure the adoption of appropriate mitigation measures to counter the more sophisticated attacks which will focus on specific assets.

However, while risk management is a well understood discipline, the most commonly taken approach has challenges when applied to addressing cyber risks, including Targeted Attacks. Since the threat environment is constantly changing, past successes in managing cyber risks are not reliable indicators of actual security and the sole basis for future planning. Additionally, many organizations have determined which risks should be managed by elevating various concerns to

senior management. Managers then considered these concerns and evaluated them relative to each other, before ultimately allocating resources appropriately across the risks. According to Aon's 2011 Global Risk Management Survey, many organizations still use this method. "Senior management's intuition and experience remains the primary method used by survey respondents to identify and assess major risks facing their organizations."[11]

This intuitive approach is bound to fail, because senior management cannot possibly understand and assess the full breadth and depth of today's cyber risks. It is also the case that, unlike many corporate risk assessments relating to security, the question of probability is a moot point. For most organizations some degree of internal compromise of computer systems is inevitable.

Considerations of the appropriate in-depth approaches to risk management are beyond the scope of this paper. It is though worth noting that regardless of the analysis and assessment models employed, addressing Targeted Attacks does specifically require that digital assets are identified, the potential business impacts of their compromise is understood and that the potential motivations and capabilities of Determined Adversaries are reflected in the deployment of countermeasures.

Prevention

Despite the high likelihood of compromise, prevention continues to be a priority in ensuring effective risk management. Commodity security solutions, such as firewalls and antimalware products, continue to offer wide ranging protection against a variety of generic threats and are essential in ensuring network hygiene.

Research has though shown that poorly configured systems—those that do not have security settings applied correctly, or those that do not have security updates applied in a timely manner—continue to be exploited in attacks. For example, volume 9 of the *Microsoft Security Intelligence Report (SIR)* contains analysis of a sample set of attacks involving exploitation of vulnerabilities in document parsing software, such as Microsoft Office. This analysis shows that—in the sample set examined—the targeted systems were compromised by exploiting software vulnerabilities after the software vendor had released a security update to address them. In some cases, the security update had been available for more than five years.

[11] www.aon.com/risk-services/thought-leadership/reports-pubs_2011_grms.jsp

Many organizations develop their own software applications and some of these, particularly when internet facing, can be a vector through which to compromise associated databases and other internal systems. Such organizations should therefore consider adoption and implementation of proactive mitigations, including the use of a software security assurance process, such as the Microsoft Security Development Lifecycle (SDL).[12]

It is also worth noting that the cumulative effect of effective detection, containment and recovery measures also provide a protective effect. This is because as target organizations increase their own capabilities, the likelihood of the Targeted Attack being successful is reduced. Combined with increased information sharing between organizations this can alter the risk reward equation for the attacker, who may then become more selective as to who is targeted.

Detection

Even well protected environments will be targeted by Determined Adversaries who are technology agnostic and undeterred by traditional defenses.[13] However, the deployment of intrusion detection and advanced analytics solutions that observes the real-time health of networks involves more than traditional network monitoring. In addition to security data from intrusion detection systems, organizations can also use information provided by IT assets such as routers, hosts, and proxy servers to evaluate operational and security status. The large amounts of monitoring and audit data generated by these solutions must ultimately be turned into insights that can be used to inform more effective cyber security responses. Such responses may be operational, as discussed later in this section, or they can be more strategic and involve changes in policies, controls, and oversight measures. They can also result in combinations of both, with operational incidents informing longer-term decisions.

Regardless, for this to happen, organizations must have the right data, and analyze that data in context for that data to drive action. Fusing together disparate data from a variety of organizations and systems to create a common operational picture is challenging. And building the analytic capabilities (for example, correlation) to derive valuable insights is even more difficult and is as dependent

[12] www.microsoft.com/sdl

[13] Charney, Scott – Rethinking the Cyber Threat – A Framework and Path Forward www.microsoft.com/download/en/details.aspx?id=747

upon the application of human skills as it is on technology. These skills still scarce and the recruitment of suitably skilled individuals is a significant challenge.

Containment

In many cases, the initial compromise of an environment will not immediately result in the attacker achieving their ultimate goal. Instead they will often need to reconnoiter the environment and compromise multiple additional systems. Effective operational security designs and utilization of native security features can help. For example, if the targeted organization has configured its environment with this potential threat in mind, it is possible to contain the attacker's activities and thereby buy time to detect, respond to, and mitigate the attack. In most cases, the security features required to contain attacks already exists. Existing environments, however, are often architected to mitigate opportunistic rather than Targeted Attacks. To contain an attack, consideration should therefore be given to architecting domain administration models that limit the availability of administrator credentials and applying available technologies such as IPsec based network encryption to restrict unnecessary interconnectivity on the network.

Recovery

The purpose and challenge of recovery is to mitigate the range of harmful impacts that may result from a successful compromise of critical assets.

Because of this possibility, the best approach is to be prepared with a well-conceived recovery plan, supported by suitably skilled response capability. Where many organizations fail in this regard is due to the separation of business, security, and IT operations groups—these teams must work together to ensure the highest, most effective degree of recovery capability. It is therefore advisable to maintain a "crisis committee" to set business recovery priorities and engage in desktop and other exercises to test the organization's ability to recover from different attack scenarios.

The exact capabilities required by organizations may differ, and may need to be reinforced with external expertise. In general though, the capabilities required should cover IT operations, investigations, effected business units, legal counsel and communications.

Maintaining customer confidence immediately following a breach through clear and timely messaging is also extremely important in protecting brands, as well as mitigating the direct impact on customers.

Communication and Information Sharing

The challenges to effective risk management in relation to Targeted Attacks have already been stated. The ability for risk management processes to effectively inform the operational needs for protection, detection, containment and recovery is made even more difficult if the necessary information is unavailable. Establishing sources of actionable information, whether through public sources or through specific relationships, is therefore vital.

Communicating openly about what happened to a victim organization can help other similar organizations take appropriate measures to avoid the same fate. However, it is not enough to simply share information. The key to successful information sharing is to be clear about the practical outcome. For example, an organization may share the internet address of a system that is attacking it so that other organizations can block that same address, or an organization may want to share their analysis of an event to see if other organizations have seen similar patterns of attack.

Sharing information about Targeted Attacks is very hard. This is in part because sharing information on these attacks might have consequences for an organization's brand, regulatory compliance, shareholder concern, and its bottom line. Selective sharing between private organizations is though possible, and has been demonstrated to have a high level of effectiveness and is worth the investment.

The Role of Governments

Besides the protection of their own systems, an important role for governments is to create environments in which their constituents (organizations and individuals) can most effectively protect themselves from Targeted Attacks. The following efforts by governments can help constituents protect themselves:

- Clearly communicate the realities of the threat environment to citizens, companies and investors so that organizations are more comfortable reporting the key aspects of breaches. This reporting can encourage learning from previous incidents and bolster specific defenses to protect key assets in the future.
- Making an organization aware that there is reason to believe they may be the target of a Determined Adversary is a critical first step in protecting their critical assets. Governments may have sources of attribution and expertise in threat assessment that provide valuable insights into the intents, motivations and capabilities of Determined Adversaries. This information, which is distinct from the technical data associated with a specific attack, should be communicated to those organizations considered to be at threat to inform their risk management decisions.
- Create a climate that encourages the exchange of technical data (at the unclassified level as much as possible) between public and private organizations to enable meaningful outcomes, with rules and mechanisms that permit both sides to protect sensitive data. This approach represents a shift from past practices that viewed information sharing as an objective itself, as opposed to a tool. It must be a two-way sharing process, in which targeted organizations share details of attacks that take place against them with governments, and governments share intelligence about the current threat environment and potential future threats. To be an effective tool against Targeted Attacks, analysis of security logs, alerts, and other intelligence information needs to take place in near-real time, which will require the establishment of solid public/private partnerships.[14]
- Some governments believe that their national security is dependent on economic security. They may therefore sponsor, or tacitly condone through inaction, the use of Targeted Attacks for stealing intellectual property to support indigenous industries. This approach is ultimately nearsighted because it inhibits the development of indigenous innovation. Governments therefore have a responsibility to address their philosophical differences and use the tools at their disposal, such as diplomacy and national policy, to establish appropriate international norms of behavior.[15]

---

[14] Written Testimony of Scott Charney Before the Senate Committee on Homeland Security and Governmental Affairs, February 2012 www.hsgac.senate.gov/download/?id=63aa804a-eb21-45fc-8cb1-014439327fdd
[15] Charney, Scott – Rethinking the Cyber Threat – A Framework and Path Forward www.microsoft.com/download/en/details.aspx?&id=747

Conclusion

Targeted Attacks carried out by Determined Adversaries are not a new phenomenon; political, military, and even commercial espionage has existed in some form for hundreds of years. Over the past three decades, the global connectivity of the internet, together with the lack of traceability and the ability to remain anonymous online, has opened up new attack vectors.

Successfully combatting such threats requires coordinated action between the public and private sectors, and an increased focus on risk management and incident response in regard to Targeted Attacks. The following summarizes these calls to action:

- **Establish a culture that promotes information exchange**. Fast, comprehensive information sharing is vital to help address the threat of Targeted Attacks. Such information sharing requires establishing a climate in which victims are sufficiently confident to share details of the attacks against them, and to enable governments to share details of the evolving threat ecosystem from their perspectives. Governments should work toward the creation and harmonization of global laws that protect cyberspace, and enable information sharing (including technical information about the Targeted Attacks and threat assessments about the Determined Adversaries) across international boundaries. How individual countries do this domestically might differ, but the desired outcome is a shared objective.
- Make risk management a key strategy for organizations, businesses, and governments seeking to prevent, detect, contain and respond to the threat of Targeted Attacks. A key element of risk management strategies must be the assumption that the organization either will be - or already has been - compromised. Another key is to create action plans that thoroughly analyze what the bad actors will do if they compromise an organization's high value assets. The goal is effective risk management; risk elimination is not possible.
- **Make creation and active operation of an analytical security enterprise a priority.** Even well protected environments will be targeted by determined adversaries, who are technology agnostic and persistent. The deployment of

intrusion detection and advanced analytics solutions that observe the real-time health and security condition of networks involves more than traditional network monitoring. In addition to security data from intrusion detection systems, organizations can also use information provided by IT assets such as routers, hosts, and proxy servers to evaluate operational and security status. The large amounts of monitoring and audit data generated by these solutions must ultimately be turned into insights that can be used to inform more effective cyber security responses.

- **Make establishing a solid incident management and response function a vital activity**, at an organizational level and at an international level. Organizations should ensure that they have the capability to react appropriately to an attack when detected, contain the attacker, and then recover from the attack. Response plans should include robust communications plans (internal and external) to help ensure that speculation and assumption do not cause additional damage. Internationally, adequate response capability and capacity needs to be built in to countries around the world. Organizations and governments should establish points of contact that are available 24 hours a day, 7 days a week to help facilitate the response process. It would be prudent for these points of contact to be established before an attack takes place.

Microsoft

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security