proofpoint

Defense Against the Dark Arts:
Finding and Stopping Advanced Threats

Contents

Executive Summary

Today's most-damaging targeted attacks don't occur by happenstance. They are carefully planned and executed by a new breed of professional adversaries. Their methods are stealthier and more sophisticated than anything we've seen in the prior decade. And if you don't take appropriate precautions, your organization could make headlines for all the wrong reasons.

According to Verizon's 2013 Data Breach Investigations Report , 92 percent of the 621 data breaches it investigated in 2012 were perpetrated by outsiders, and 52 percent of these breaches resulted from some form of hacking. Many of these data breaches were the result of highly sophisticated advanced threats, which according to security researcher, Mandiant, took the organizations it assisted in 2012 an average of 243 days to detect!

So why are high-profile advanced attacks so common these days? And why are some threats more difficult to detect than others?

This paper defines a new class of IT security threat collectively called advanced threats and describes exactly how they are perpetrated. It also depicts the limitations of today's typical information security approaches and describes why they often fail to detect advanced threats. But more importantly, this paper details effective strategies for finding—and ultimately stopping—advanced threats, including now infamous advanced persistent threats, or APTs.

Although motivations for launching advanced threat campaigns against commercial and government organizations vary, the tactics used are quite similar regardless of whether the attacker is a hacktivist, a state-sponsored threat actor, or a cyber criminal hacking for financial gain. Let's now explore the dark arts of advanced threats by reviewing today's advanced threat landscape and understanding how these targeted attacks are delivered.

Today's Advanced Threat Landscape

In today's threat environment, the only constant is change. In fact, everything is changing—the way our users work, the types of adversaries we face, and the techniques hackers use to infiltrate our networks and exfiltrate our data. Such threats have become more sophisticated than ever, bringing new risks and uncertainties.

The following are descriptions of advanced threats faced by virtually every enterprise and government agency the world over:

Polymorphic Threats

Polymorphic threats are designed to evade signature-based defenses—such as traditional antivirus software and intrusion prevention systems (IPSs)—by constantly changing (or 'morphing') its own code. Polymorphic threats may alter their filenames, file sizes, and encryption techniques using variable keys. Although the code within a polymorphic threat changes with each mutation, the essential function usually remains the same.

Blended Threats

A blended threat is a popular term for a multi-vector attack against a computer network. A blended threat often combines spear phishing attacks, Trojans, DoS (Denial of Service) attacks, advanced malware, and other techniques as part of a single, coordinated advanced targeted attack. Sometimes components of a blended threat are initiated as decoys to distract security analysis so they are less likely to focus on an in-progress attack.

Advanced Persistent Threats

The most widely talked about type of attack in recent years is by far the advanced persistent threat, or 'APT' for short. But it's also the most widely misunderstood. APTs are highly sophisticated, well-coordinated attacks directed at business and political targets perpetrated by highly trained and well-funded cyber attackers. These attackers employ "low and slow" hacking techniques—including the aforementioned techniques referenced in this section—to evade traditional security defenses. Many APTs incorporate advanced malware designed to exploit zero-day (not yet publicly reported) vulnerabilities in operating systems and applications.

Examples of high-profile APTs over the past five years include:

- New York Times attack (2013)
- Flame (2012)
- RSA SecurID attack (2011)
- Stuxnet (2010)
- Operation Aurora (2009)

Delivering Advanced Threats

Today's advanced threat perpetrators leverage a variety of social engineering attacks against unsuspecting employees of enterprises and government agencies. These workers might be victimized while sitting at their desks reading email or surfing the web, or perhaps even when stepping out of their cars within their employers' parking lots.

Let's explore common ways these adversaries use to deliver advanced threats.

Spear Phishing

Unlike your run-of-the-mill phishing attacks, which are sent to thousands (or even millions) of recipients at once, spear phishing emails are sent to only a handful of individuals, are extremely targeted, and are crafted with a specific target and objective in mind. Spear phishing emails are well disguised as legitimate messages sent from trusted friends, family members, and colleagues after the attacker has researched the target recipients using social media sites, such as Facebook and LinkedIn.

Spear phishing messages usually include a malware-infected attachment, or (more often) a link to a compromised but non-blacklisted website. If the user is tricked into opening the attachment or clicking on the link, they will effectively launch the malicious code, and typically it will execute without the user ever suspecting anything 'bad' has happened. In either case, once executed, the malware that is launched is designed to exploit system vulnerabilities and make changes that ultimately grant the attacker privileged access to the computer's resources, its credentials, and any network it may have access to.

Today, an estimated 95 percent of successful advanced threats are initiated by spear phishing campaigns. It's not surprising given insight from Verizon's 2013 Data Breach Investigations Report. According to the report, a phishing campaign that targets just three individuals at a single organization results in a better than 50 percent chance of getting at least one click. Run that same phishing campaign twice and the probability jumps up to 80 percent. Sending that same phishing email to a dozen workers virtually guarantees at least one click. One click is all it takes for a hacker to gain access to your network.

Crafting malicious URLs and email attachments referenced in spear phishing attacks is both an art and a science. The next two sections describe how they're created.

Malicious URLs. Incorporating malicious URLs into spear phishing emails is the most common way of delivering malware via a spear phishing attack. Here, the attacker constructs an email that appears to be a legitimate message from a trusted source. If the user is tricked into clicking the URL embedded in the email, the user's web browser launches and automatically initiates a connection to the malicious website.

As an example, the website shown in Figure 1 is a pixel-for-pixel replica of the actual Adobe Flash Player website. The only difference is the unusual URL displayed in the browser, which goes unnoticed by most users.

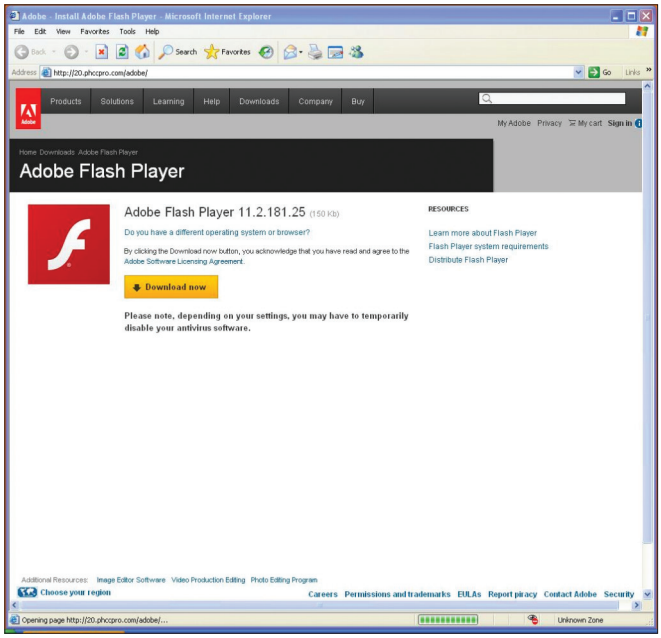

Figure 1. Fake Adobe Flash Player website.

On visiting this malicious website, a drive-by download is conducted in the background, which remains concealed from the user but completes the process of compromising the machine.

Easily licensable exploit kits are used to enable attackers to quickly create their drive-by download attacks. These kits have the necessary technology built-in to avoid detection by security solutions while offering a menu of options that the attackers can cherry-pick. The kit allows the attacker to leverage its capabilities offering various approaches to compromise a user machine using known vulnerabilities, and then infect the machine with the attacker's

code. A frequently referenced exploit kit known as Blackhole (see Figure 2) is popular among attackers. There are over 50 exploit kits today for attackers to choose from, including the Kein, Sakura, Phoenix, Nuclear, and Cool Pack exploit kits.

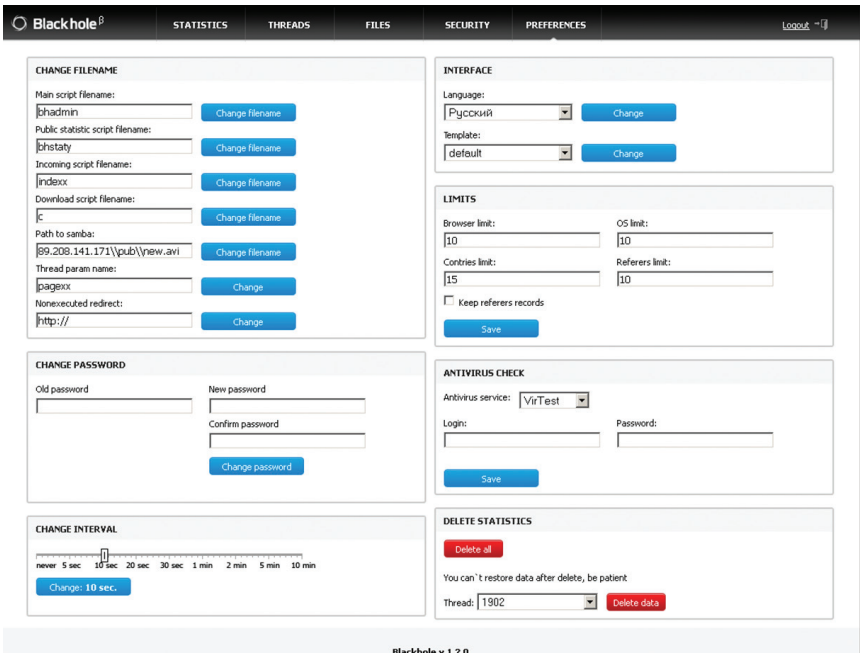

Figure 2. Blackhole exploit kit.

Malicious attachments. File attachments sent along with spear phishing emails (a.k.a., the 'bait') are usually innocuous-looking files, such as Adobe PDFs, or Microsoft Office documents with content in the email that would drive any curious user to try and open it. In many cases, the sender's information is spoofed to seem legitimate to the recipient. Most spear-phishing attachments are constructed by attackers using tools that with the simple click for a button can easily combine malware with other types of files and use crypto-functions that make detection of the malicious code difficult. The attacker's goal is to ensure that the attachment is unique, thus no signature is present on any list, at the time it passes through existing enterprise security controls. To accomplish this goal, attackers use polymorphic threats as discussed earlier in this paper. The same malware can then be used repeatedly to craft their attacks on individual organizations and users while minimizing their chance of being detected via changing specific elements of the malware.

Longline Phishing

Until recently, attackers have faced a cost/volume trade-off when it comes to manually crafting spear phishing emails. Borrowing tactics from cloud computing and database marketing, attackers are now engaging in industrial-scale phishing attacks—called 'longlining'—that leverage highly sophisticated customization and delivery techniques.

Longlining attacks owe their name to a common industrial-scale, commercial fishing technique. Longlining emails have markedly higher penetration rates than traditional phishing attacks, and they have surprisingly high recipient clickthrough rates.

Characteristics of longline phishing attacks include:

- Proportionally low volume per organization, with high volume overall
- Aggressive obfuscation and customization techniques
- Malware payloads that often leverage zero-day and other exploits that take advantage of known and unknown vulnerabilities

Longlining emails are particularly difficult to detect as so many email components are (automatically) randomly rotated, including:

- Sender IP addresses
- Spoofed sending addresses
- Email subject and body content
- Embedded URLs

The net result is that no organization targeted by longlining emails will receive more than a few email messages with the same characteristics. The "Letter.htm" attack, observed by Proofpoint took about three hours, including initial probing, and ultimately delivered more than 185,000 emails to 80 companies. No single company received more than three emails with the same variable set. In many cases, the content of each message received by a single organization was entirely unique.

Water Holing

Water holing is a technique where hackers exploit vulnerabilities in popular, legitimate websites, and embed drive-by downloads using those exploited vulnerabilities. These are considered opportunistic attacks as the attackers don't 'specifically' know who will visit the website.

Water holing was first observed in the "Aurora" and "Ghostnet" attacks of 2009, but started gaining notoriety in 2012 when a local government website in Maryland and a regional bank website in Massachusetts were compromised; and again in 2013 when Facebook revealed it was attacked through a zero-day Java vulnerability when some of their developers visited a third-party website that had been compromised.

Search Engine Poisoning

Search engine poisoning attacks manipulate, or "poison", search engine query results by displaying references to malware-delivering websites amongst an array of legitimate websites. Like water holing, search engine poisoning is an opportunistic attack. Rather than infecting legitimate websites though, completely bogus websites are created, often related to and following big-breaking news stories, such as the Benghazi attack in Lybia in September 2012 and the tornado devastation in Oklahoma in May 2013.

Attackers that launch search engine poisoning websites leverage blackhat SEO (search engine optimization) kits that are readily available on the web to generate pages stuffed with keywords designed to make the website appear high up in search engine results.

Baiting

Baiting is a relatively low-tech attack that involves an attacker planting physical portable media devices—such as USB thumb drives and CD-ROMs—in parking lots, coffee shops, and restaurants in close proximity to buildings belonging to organizations that he wishes to penetrate.

The portable media device is usually labeled with an enticing title (that also references the targeted organization's name), such as "Executive Compensation" or "Company Confidential." The curious worker that picks up the media device no doubt wants to know what's on it. Unfortunately, when he plugs in the USB drive or pops the CD-ROM into his computer, the moment he accesses the content, his computer is infected with advanced malware.

Why Typical Security Approaches Fail

Despite spending billions of dollars annually on security, organizations are consistently victimized by advanced threats. That's because typical security defenses don't stand a chance at detecting them. Here's why.

Limitations of Signature-based Defenses

Signature-based defenses leverage pattern-matching technology to detect basic, known threats, such as viruses, worms, spyware, botnets, buffer overflows, phishing, and SQL injection attacks. Examples of common, everyday signature-based defenses include:

- Antivirus software (AV)
- Intrusion prevention system (IPS)
- Secure email gateway (SEG)
- Secure web gateway (SWG)
- Next-generation firewall (NGFW)

As advanced threats are highly customized, and often contain zero-day exploits that target unknown (or at least undisclosed) operating system and application vulnerabilities, these threats sail past typical signature-based defenses as if they weren't even there. Attackers continue to leverage these exploits until they can be detected by public-facing antivirus websites, such as VirusTotal—and then they simply create new variants.

Limitations of Reputation-based Defenses

Many of today's network security devices incorporate global reputation feeds—maintained by the vendor or an organization that has granted a license to the vendor—to identify host communications with known-bad external IP addresses and/or domain names. This approach is highly effective at blocking everyday phishing attacks, but it is generally ineffective at blocking spear phishing attacks perpetrated by sophisticated attackers.

As was discussed in the aforementioned "Delivering Advanced Threats" section, today's advanced adversaries frequently rotate IP addresses and domain names used in spear-phishing and longlining attacks, as well as IP addresses associated with command-and-control (CnC) servers used to remotely control compromised hosts (and botnets). These techniques are aimed squarely at remaining undetected by reputation-based security systems.

Limitations of Sandboxing

Sandboxing technology has rapidly grown in popularity in recent years as an effective method for spotting zero-day exploits and other stealthy attacks that go unchecked by typical signature-based security defenses. A sandbox is essentially a virtual machine equipped with the same operating system and (common) applications as the host targeted by malware when delivered via a URL within the email content, or an email attachment. The suspicious file is essentially "detonated" within the safety of the virtual machine in an attempt to observe malicious effects.

Unfortunately, savvy attackers have found ways to evade rudimentary sandboxing solutions by employing various evasive techniques, including:

- Incorporating technology to detect the presence of a sandbox virtual environment (through registry key sampling and/or video and mouse driver detection), thus suppressing the payload of malware-infected files.
- Incorporating technology that hides behind subroutines governing mouse control functions, keeping malware dormant until the left mouse button is clicked.
- Incorporating technology that includes a "wait" function, keeping the malware idle until it is activated by a user's actions.

Strategies for Detecting and Stopping Advanced Threats

Now that you are aware of the limitations of today's typical security defenses, it's time to discover more effective technological approaches to finding and stopping advanced threats.

Defense-in-Depth

No matter what anyone tries to tell you, there is no silver bullet security product capable of detecting every advanced threat that your network faces. The optimal strategy for mitigating advanced threats—including detecting them when (not if) they get in—is a comprehensive, 'defense-in-depth' strategy consisting of layers of network and endpoint security defenses, each with its own role. While not every solution is recommended or feasible for every enterprise, each has a role to play and should be investigated by enterprises.

Network security defenses. Beyond the network security defenses referenced in the "Limitations of Signature-based Defenses" section—including IPS, SEG, SWG, and NGFW technologies—additional layers of network security protection are needed, such as:

- Security information and event management (SIEM)
- Data loss prevention (DLP)
- Network behavior analysis (NBA)
- Network access control (NAC)
- Privileged account monitoring (PAM)
- File integrity monitoring (FIM)
- Security configuration management (SCM)
- Vulnerability management (VM)
- Patch management (PM)
- Big Data Security Intelligence & Analytics (Big Data SIA)

Endpoint security defenses. Beyond basic antivirus, anti-spam, and anti-malware protections of today's leading endpoint security solutions, many of the aforementioned network security solutions incorporate endpoint agents to closely monitor the security and integrity of endpoint devices, including DLP, NAC, PAM, FIM, and SCM.

Incident-response capabilities. IT security professionals are no longer just measured on their ability to prevent successful attacks, but also their fortitude in identifying and containing such attacks when (not if) they occur.

Larger enterprises and government agencies assemble special teams of security analysts called CSIRTs (computer security incident response teams). CSIRT members are experts at leveraging the organization's network and endpoint security defenses to uncover answers to questions asked in accordance with any successful attack:

- How did the attack happen?
- What systems were compromised?
- What, if any, data has been exfiltrated?
- How can we be sure the attack is over?

Advanced Technology for Mitigating Advanced Threats

Although no silver bullet exists for thwarting every possible advanced threat, since over 95 percent of targeted attacks are delivered by way of socially engineered email campaigns, selecting an email security platform equipped with advanced technologies for finding and stopping advanced threats is critical.

This section explores such technologies, which all enterprises and government agencies should look for when evaluating best-of-breed email security platforms.

Anomaly detection. Today's leading email security defenses incorporate anomaly detection capabilities that continuously model 'normal' email flow (encompassing senders, receivers, message volumes, and more) to help spot 'abnormal' email anomalies. Examples of such anomalies may include:

- Email sent from a domain that the organization has never exchanged emails with before
- Email sent from an IP address that has an unknown reputation was just published less than 24 hours ago and/or is associated with a suspicious registrar
- Email has been sent five times in five minutes to individuals in the same work group
- Email contains a URL that has never been seen before

Although an email flagged by a security system equipped with an advanced anomaly detection engine could be completely innocuous, it's worth pulling aside for further review by cloud-based sandboxing and/or URL clicktime analysis.

Cloud-based sandboxing. Safely evaluating suspicious files within the confines of an isolated virtual sandbox environment has proven highly effective at detecting many advanced threats. But as mentioned in the prior "Limitations of Sandboxing" section, today's sophisticated attackers incorporate technology that evades basic sandboxing solutions. Thus, be sure to select best-of-breed sandbox solutions that are capable of overcoming these malware-inspection obstacles.

Also, when facing the choice between appliance-based, on-premises sandboxing offerings and cloud-based sandboxing solutions, aim for the cloud. Although an appliance-based sandbox platform may incorporate sophisticated malware-inspection technology, these boxes typically can't keep up with the demands of large enterprises, resulting in large quantities of uninspected content. Furthermore, it's entirely cost-prohibitive to purchase dozens of sandbox appliances to support such large organizations. Thus, cost-effective and scalable cloud-based sandboxing solutions that can rapidly expand (and contract) with the needs of the business are preferred.

URL click-time analysis. A major challenge in defending against spear phishing emails is differentiating between malicious and benign URLs. This is especially challenging when users are working at home or on the road, away from the employer's network security defenses. As most spear phishing emails associated with advanced targeted attacks incorporate URLs rather than attachments, this is particularly a concern to today's enterprises.

To overcome this challenge, consider URL click-time analysis that prevents users from reaching a URL until a cloud-based sandboxing environment has safely verified it. If the organization's entire email security platform is delivered via a cloud-based SaaS (software-as-a-service) infrastructure, then this advanced malware protection capability is delivered to all of the organization's users, whether in the office or around the world.

Attachment analysis. While the usage of embedded URLs and file attachments to deliver targeted threats varies in waves, better email security platforms also provide the ability to sandbox email attachments before delivery. Similar to sandboxing embedded URLs, analyzing file attachments for embedded threats can help enterprises combat these threats while gaining insight into them as well. Since an attachment's behavior cannot be changed once sent, unlike URL destinations where changes can be made dynamically on the destination website, the goal of the security solution is to assume the attachment is a zero-day and make a call of whether the attachment is good or bad, before it reaches the user. In order to effectively scale with attachment volume and manage attachments of all types and sizes, it requires elastic computation along with security controls to manage costs and risks.

Employee Training to Thwart Social Engineering

If network and endpoint security solutions are an organization's first line of defense against advanced threats, an organization's employees are collectively its last line of defense. Through proper training and training reinforcement, an organization's workforce can drastically reduce the likelihood of becoming victimized by a targeted threat.

Role-based security training. Every single employee—from mailroom clerks all the way up to the CEO—must be adequately trained on how to identify socially engineered email attacks. Telltale signs of spear phishing and longlining emails include:

- Emails with unfamiliar sender email addresses linked to individuals you know
- Emails with no subject line or very generic subject lines like "Check this out!"
- Emails from educated colleagues with poor spelling and grammar
- Emails with unusual requests that seem out of the ordinary

These are just a few of the signs of spear phishing and longlining emails potentially linked to advanced threats. By adapting training based on each user's role in the organization, instructors can better provide real-world examples of what to look for. After all, a spear phishing or longlining email that targets someone in accounting is likely to be vastly different than someone targeted in product development.

Security training reinforcement. Ongoing employee security training is essential. Annual coffee-and-donut training sessions simply won't cut it. Consider raising awareness of socially engineered email attacks through third-party spear phishing simulators. These solutions enable IT security to construct benign and internal spear phishing attacks in an effort to identify security knowledge gaps.

Phishing simulator vendor studies indicate up to an 80 percent decrease in successful spear phishing attacks as a result of ongoing security training.

Conclusion

There's no doubt that the bad guys have the upper hand when it comes to perpetrating advanced threats. Hopefully you've gained new insight into the "black arts" of leveraging socially engineered email campaigns to initiate targeted attacks against businesses and government agencies. You should also have a deeper understanding as to why traditional security defenses don't stand a chance at detecting today's insidious advanced threats.

By taking the time to evaluate best-of-breed email security providers (one excellent resource is Gartner's Magic Quadrant for Secure Email Gateways) and knowing which capabilities are most relevant for mitigating advanced threats, you will be doing your part to keep your organization safe from harm and out of the headlines.

To learn more about protecting your organization from targeted attacks please visit: www.proofpoint.com/tap

proofpoint™

Proofpoint, Inc.
892 Ross Drive, Sunnyvale, CA 94089
Tel: +1 408 517 4710
www.proofpoint.com