SEARCHSECURITY.COM

technical guide on

EMERGING threats

contents

TechTarget

Did you know?

79%

of Web sites with malicious code are **legitimate sites** that have been **compromised**

Think you know where the biggest threats exist on the **Web?**

Check your assumptions by reviewing our latest Threat Report. It looks back at last year and makes predictions for 2011 and it's crammed with intelligence that may surprise you.

websense®
ESSENTIAL INFORMATION PROTECTION™

Websense 2010 Threat Report
websense.com/threatreport2010

CYBERCRIME

Understanding Modern Attack and Defense Techniques

Attackers have ramped up their efforts with a dangerous cocktail of social engineering, Web-based attacks and persistence. How will your organization stay ahead?

BY LENNY ZELTSER

IT TAKES TIME and money to adjust IT security in response to evolving attack tactics. As defenders gradually update their security measures, attackers respond accordingly. Such arms-race dynamics lead to threats of increasing sophistication and efficiency. Today's cybercriminals often have a long-term interest in their targets, and often employ social engineering to get inside a protected environment. Their tactics commonly include malicious payload that attempts to compromise the victim's system and may continue spreading within the organization. They also increasingly focus on weaknesses at the application, rather than at system or network levels, to obtain data that provide the most value.

Defending IT infrastructure involves understanding attack tactics that are particularly effective today. As you assess and improve your information security program, consider the following characteristics of modern computer security threats and the recommendations for dealing with them.

HOW SOCIAL ENGINEERING BYPASSES TECHNICAL DEFENSES

Attackers increasingly employ social engineering tactics to exploit natural human predispositions with the goal of bypassing defenses. Such approaches can persuade victims into clicking on malicious links, open exploit-laden attachments and install malicious software. The psychological factors attackers incorporate into social engineering attacks include the following:

- **People pay attention to personally relevant messaging.** For instance, a variant of the Waledac worm directed its potential victims to a website that showed a news excerpt about a supposed explosion. The message was customized to include the geographic location of the visitor as the place where the supposed explosion occurred to entice the person to install a (Trojan) video player for viewing the personally relevant new

story. In another example, attackers sent targeted email messages with malicious attachments under the guise of providing an agenda for an upcoming meeting. The attacker bet on the likelihood that the recipient had a meeting coming up and would want to view the agenda.

- **People comply with social norms, looking at others for behavioral cues.** One example of this behavior is the people's tendency to click on links shared by their friends on social networking sites such as Facebook and Twitter. The Koobface worm has been highly successful at convincing people to visit malicious websites by posting its links using the victims' social networking accounts. In another example, the Nugache worm used infected systems to download its malicious components from a legitimate download-tracking site, boosting the popularity of its files to attract new victims.

Such social engineering techniques merge the line between external and internal threats because social engineering will allow external attackers to quickly gain an internal vantage point.

- **People place trust in security tools.** Much like people put trust into the individuals who look like doctors by wearing lab coats, users sometimes blindly trust the measures taken for the sake of security. Rogue antivirus tools have been highly successful at spreading by convincing victims that their computers are infected and demand immediate intervention. Attackers have also used digital certificates to sign malicious executables—as was the case with Stuxnet—with the expectation that seeing a signed file would lower the target's guard.

Such social engineering techniques merge the line between external and internal threats, because social engineering will allow external attackers to quickly gain an internal vantage point. Once inside the protected perimeter, for instance, attackers tend to pursue targets that are inaccessible from the outside. To account for this threat vector, incorporate social engineering concepts into your security awareness program to make your employees more resistant to such tactics. Assess the extent to which your employees learned key concepts, provide feedback and adjust training, if necessary.

Employ security defenses assuming that some employees will be social engineered despite the security awareness training. This involves:

- **Locking down the workstation** to minimize the damage a process running with user's privileges can cause
- **Limiting the rights employees have** to access the network and applications to match their business needs
- **Reviewing activity logs** to identify when user accounts and access is being misused.
- **Evaluating the effectiveness of your browser security software** in its ability to restrict access to dangerous content or code downloaded by the user.

TARGETING WORKSTATIONS THROUGH THE BROWSER

Attackers have been successful at penetrating enterprise defenses by taking advantage of bugs in the Web browser or in software that the Web browser can invoke. Such client-side exploits have targeted browser add-ons such as Flash and Java Runtime Environment (JRE), as well as the code that is part of the Web browser itself. They have also targeted document viewers and editors, such as Adobe Reader and Microsoft Office. The exploits might be delivered to victims via email, in the form of attachments or links, or might be presented when the victim encounters a malicious website while browsing the Web.

Although client-side exploits have been part of the threat landscape for a number of years, several factors are making workstations a more attractive target than ever before:

- Defenders seem to be getting better at locking down server infrastructure.
- The shift in corporate culture and the availability of externally hosted applications are making it more common for employees to work outside of the protected network perimeter.
- Individuals who embraced online social networking seem to have gotten more promiscuous about sharing and clicking on links.

A key characteristic of an exploit kit is the ease with which it can be used even by attackers who are not IT or security experts.

Another factor that seems to be making attacks on workstations more frequent is the increased availability and of powerful exploit kits, which automate the exploitation of client-side vulnerabilities. A key characteristic of an exploit kit is the ease with which it can be used even by attackers who are not IT or security experts. An exploit kit acts as a launching platform to deliver other payload, which may include a bot, a backdoor, spyware or another type of malware.

Attackers will continue to pursue vulnerabilities in workstations that could be exploited through victims' web browsers. Consider the following measures to improve your ability to withstand such tactics:

- **Use enterprise management system (EMS) tools**, such as Group Policy, to centrally manage Web browser settings, disabling unnecessary features, configuring proxies, turning off risky add-ons, and so on.
- **Follow the development of new browser features**, such as sandboxes incorporated into Internet Explorer and Google Chrome. Consider such evolving security capabilities when deciding which web browsers to mandate or recommend for your users.
- **Review the use of secure compilation practices**, such as ASLR and DEP, in software that might be targeted through the browser. For instance, a zero-day exploit discovered in December 2010 targeted an Internet Explorer DLL that wasn't compiled to support ASLR, allowing the attacker to compromise affected workstations. Microsoft's Process

Explorer and Enhanced Mitigation Experience Toolkit (EMET) tools can assist with this process.

- **Limit the local privileges that users have on their workstations**, making it harder for malware to reach its full potential on the host. This often involves removing administrative rights from users who don't need them, or stripping the more sensitive privileges from administrative groups. User Account Control (UAC) capabilities of Windows Vista and 7 offer similar advantages even to users logged in with local administrative rights.
- **Assess capabilities of the security tools you use to protect web browsing activities** at network and endpoint levels. Consider deploying products that have features specifically designed for identifying malicious activities in web traffic and protecting the browser.

COMPROMISING WEB APPLICATIONS

As our infrastructure security practices mature, attackers are turning their attention to Web applications. In some cases, the attackers' goal is to compromise websites so that they can be used to target client-side vulnerabilities through visitors' browsers. Attackers also commonly pursue Web applications that process or store valuable data. Such application-level attacks, which have been very successful at bypassing defenses, include the following tactics:

- **SQL injection attacks**, which bypass the application's input filters to gain unrestrained access to the underlying database
- **Business logic flaws**, which exploit the weaknesses in workflows implemented by the application, such as a way to identify all valid usernames by using the password reset page.
- **Password brute-forcing methods**, which use automated tools to guess passwords that use known dictionary words or that are otherwise predictable
- **Cross-site scripting (XSS) attacks**, which bypass the application's input or output filters to execute malicious scripts in the browser of the application's user

The list of effective application-level attack vectors is too long to be included here. For more details, take a look at the OWASP Top Ten Project. Why are so many applications vulnerable to such tactics? Partly, it's because many developers aren't trained to write attack-resistant code. Moreover, developers' incentives prioritize features and deadlines over the application's defensive posture. Yet another reason is the infrastructure focus of many security programs, which don't provide the necessary focus on application-level issues.

Here are a few suggestions for tackling the challenges of application-level threats and vulnerabilities:

- **Break down the wall between infrastructure and application security teams** in your organization, encouraging collaboration and making sure the company pays due attention to application-level security issues.
- **Understand the business purpose of the applications**, combining that knowledge

with the details regarding how sensitive data flows through the applications and the infrastructure. Use this information to prioritize your security efforts.

- **Include application components in your penetration testing projects** to mimic the likely actions of attackers seeking to bypass your defenses. Be sure to incorporate manual testing, since fully automated techniques are likely to produce numerous false positives and false negatives.
- **Include application logs as part of your log management or security information and event management (SIEM) efforts.** Incorporate security alerting and logging specs into your application development requirements to support this.
- **Incorporate application-related steps into your incident response plan.** Too often, organizations focus on only system or network-level actions when preparing to deal with security incidents.
- **Establish a practical and comprehensive Web application security program**, which should include security coding and application architecture guidelines, developer training for secure coding practices and automated ways of identifying at least some vulnerabilities during code creation, testing and deployment.

ATTACKERS WITH LONG-TERM INTERESTS

While a fair number of intrusions can still be classified as quick hit-and-run incidents many attackers have demonstrated the desire and ability to invest into long-term campaigns for achieving financial and, in some cases, political objectives. Such focused activities are typically comprised of a series of events that are spread over a period of months and even years. Recently, attacks with long-term interests took on the forms:

- **Attackers deploy malware that acts as a crimeware platform** diverse activities, including data exfiltration, distributed denial-of-service (DDoS) attacks and spam campaigns. For instance, the Conficker worm spread quickly without a "business" purpose that was initially observable; the for malware was later used for various money-making schemes.
- **Attackers research the people and technologies that comprise targeted organizations.** This helps ensure the success of the initial compromise and follow-up actions. Client-side attacks might be directed at specific individuals to target the software installed on their workstations in the context that wouldn't arouse suspicions. Another illustration of the preparation exhibited by attackers was evident in the Stuxnet incident.
- **Attackers adjust tactics in response to defenders actions.** For instance, the group behind the Koobface worm modified the manner in which its malware uses social networks to adjust for those sites' security improvements. Similar characteristics were exhibited by attackers in identified advanced persistent threat (APT) incidents.
- **Attackers maintain persistent presence in the compromised environment.** As a result, even if the organization discovers some of the compromised systems, the attacker is able to continue operating within the organization's infrastructure. These characteristics have been described in the context of APT scenarios.

Consider the following recommendations to prepare for dealing with incidents that might be attributed to attackers with long-term incidents:

- **Change the perspective of your security efforts from attempting to *prevent* breaches**—which unrealistic in the face of most targeted attacks—to *resisting* intrusions. The change involves accepting that a compromise will occur and considering how you will detect and respond to it.
- **Understand where your valuable data is located** and adjust your defensive spending accordingly, making it more expensive for attackers to achieve their likely objectives.
- **Identify the individuals who are most likely to be targeted**, perhaps because they are in the public eye or because they have access to valuable data. Provide them with additional security training and security mechanisms to better resists attacks directed at them.
- **Educate employees about risks of data leaked inadvertently on public forums**, such as social networks and blogs. Explain how attackers who profile activities over time can gather meaning and actionable intelligence from the bits of data that might be innocuous by themselves.

Modern computer attacks understand the weaknesses inherent in their targets' defensive capabilities sometimes better than the targeted organizations themselves. Intruders often incorporate elements of social engineering to persuade victims to take actions desired by the attackers, such as clicking on links, spreading URLs or supplying logon credentials. Attackers frequently target client-side vulnerabilities, recognizing that enterprises have a hard time keeping workstations up to date on security patches.

Modern computer attacks understand the weaknesses inherent in their targets' defensive capabilities sometimes better than the targeted organizations themselves.

Cybercriminals also target vulnerabilities in web applications to obtain access to valuable data and to gain a platform for attacking web-site visitors. Many attackers are part of well-organized profit-motivated groups, who are willing to invest time and money towards achieving their objectives. As the result, organizations need to be prepared to handle attack campaigns that might span months and years. Resisting the attack tactics discussed above involves understanding the threats, so you can build and adjust your defenses accordingly.

Lenny Zeltser leads the security consulting team at Savvis and teaches classes on combating and analyzing malware at SANS Institute. He regularly discusses information security topics on his blog and on Twitter.

TECHTARGET SECURITY MEDIA GROUP

TechTarget
Where Serious Technology Buyers Decide

"Technical Guide on Emerging Threats" is published by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

Did you know?

22.4%

of searches for trending news (buzz words) lead to **malware**

Think you know where the biggest threats exist on the **Web?**

Check your assumptions by reviewing our latest Threat Report. It looks back at last year and makes predictions for 2011 and it's crammed with intelligence that may surprise you.

websense®
ESSENTIAL INFORMATION PROTECTION™

Websense 2010 Threat Report
websense.com/threatreport2010

websense®
ESSENTIAL INFORMATION PROTECTION™

- **Websense Advanced Classification Engine video**
- **2010 Threat Report and next 12 months**

About Websense:
Websense is the global leader in integrated Web, data and email security. Websense software and hosted security solutions protect more than 42 million employees worldwide, and help more than 50,000 organizations say Yes to Web 2.0.