Evolution of Blended Threats

By Jim Murphy

INTRODUCTION

Computer crime is rapidly evolving in two major ways: first, groups of seasoned profit-seeking professionals are replacing younger notoriety-seeking hackers as the primary perpetrators of computer crime; second, these groups of computer criminals, which often sell their services to the highest bidder, are increasingly relying on blended threats to accomplish their illicit work.

Blended threats combine elements of worms, viruses, trojans (collectively known as malware), spam and even social engineering into a variety of more dangerous, malicious forms. They propagate via both wired and wireless networks, spreading through e-mail, web pages, P2P and instant messaging. Successful blended attacks often exploit vulnerabilities found in systems and networks, and can mutate rapidly to avoid detection.

In corporate environments, blended threats result in productivity loss, higher bandwidth utilization, and costly cleanup. Companies also face legal liability if inappropriate or illegal content is accessed or stored by employees. Successful blended attacks often enable criminals to steal or corrupt valuable data and engage in extortion, potentially damaging a company's brand and credibility, and making regulatory compliance (e.g., with the Sarbanes-Oxley act or HIPAA) difficult, if not impossible.

These risks are not theoretical, and blended threats are costing businesses millions of dollars. In a recent high profile example in Israel, a custom-crafted blended attack allowed competitors to obtain a large amount of company sensitive data[1]. In another case investigated by the FBI, computer criminals hired by a competitor effectively halted the operations of a company for two weeks with a severe denial of service attack from a large network of compromised computers (bot net), causing over $1 million in damages[2].

Protecting against blended threats requires a comprehensive approach, which must include user education, securing all possible local and wide are network entry and exit points, and developing strong partnerships with vendors and law enforcement. A necessary component of the defense is dynamically updated content filtering implemented both on the network and the PC. Without a unified threat-management solution, it is certain that a company will be a target of a successful blended attack.

NATURE OF THE THREAT

At first glance, blended threats appear similar to the slew of malicious software that has plagued users worldwide for decades. Firewalls, proxies, spam filters and anti-virus software are widely deployed in an effort to deal with these problems, and this often lulls IT managers into a false sense of security. In reality, when deployed in an uncoordinated manner, these tools fail to protect against blended attacks, such as malware that arrives over instant messaging or a browser exploit, proceeds to spread to other computers by taking advantage of unpatched security vulnerabilities, and forces compromised computers to join bot nets to participate in coordinated attacks on other networks.

Blended threats are extremely dangerous precisely because they employ constantly varying combinations of methods—attack vectors—to spread and do their damage. The sheer number of potential variations is staggering; and with "zero-day" vulnerabilities frequently included in blended attacks the same day they are discovered, no single-point solution can secure the enterprise. However, by understanding the ways that criminal groups make money with blended attacks, IT managers can gain a more complete understanding of their company's risks and vulnerabilities and deploy integrated defenses which make their company a less attractive and more resilient target.

KNOW THINE ENEMY

Blended threats provide criminal organizations income from three sources:

- Personal information/identity theft
- Advertising
- Extortion, corporate espionage, and other scams

Phishing is a classic example of a blended attack, and it allows criminals to make money from all three sources. Criminals set up websites

that appear like those of legitimate organizations, and send out millions of e-mails urging people to update their personal information. These counterfeit e-mails are convincing enough that almost 20% of their recipients visit the rogue websites, and 5% actually divulge personal information[3].

Criminals can easily turn personal information into cash, most often by making fraudulent financial transactions at the victim's expense, or by selling it to advertisers, spammers, and even other criminals. This information can also provide data for the social engineering component for other blended attacks.

In addition to collecting personal information, some of the phishing websites exploit browser vulnerabilities to silently install software on the victim's computer, including spyware that hijacks the user's home page, or replaces legitimate ads in web-pages with their own, allowing criminals to make money from advertising. A "marketing" firm recently offered to pay a little over 6 cents for each system compromised to display its advertising; it was able to quickly recruit over 200,000 machines into its network[4].

Other malicious software allows criminals to steal sensitive data and capture keystrokes, or even take full control of the victim's computer. These systems often become part of a bot net that allows criminals to profit by sending millions of spam e-mails, mounting DDoS attacks, or distributing pornography and pirated software. Furthermore, if the compromised computer is on a corporate network, it can be easily used as a launch pad for further attacks on sensitive internal systems, even those not connected to the internet. Without active content filtering, most proxies and firewalls are powerless to stop this, since this illicit activity is masqueraded as normal outgoing web traffic.

The widespread presence of malware on powerful computers with broadband internet connections is allowing criminal organizations to routinely threaten thousands of corporations with distributed denial of service attacks[5]. Companies who do not comply with extortion demands see their systems crippled for days with massive amounts of traffic from the bot nets. Criminals can also place illicit materials (like child pornography or pirated software) on compromised corporate systems, and threaten to notify law enforcement authorities about it unless they are paid off. Finally, criminals are blackmailing companies into paying to keep sensitive data from going to a competitor or the highest bidder on the black market.

EVOLVING THREATS

One of the major characteristics of blended threats is the tremendous speed with which they are evolving. Pharming is one example of a recent improvement on the phishing scam. Criminal groups are now modifying DNS entries for popular domain names (like amazon.com or ebay.com), forwarding unsuspecting uses to rouge websites where they collect personal information or credit card numbers. This is accomplished by either modifying an individual computer's DNS settings with malware, or with DNS cache poisoning, which can have a devastating effect on a large group of unsuspecting users.

Another troubling development is the emergence of custom blended threats, as seen in the highly publicized industrial espionage case in Israel, and the attacks experienced by the UK's National Infrastructure Security Co-ordination Centre[6]. Unlike earlier threats that attempted to maximize the number of attack vectors and targets, the new blended threats are custom tailored to exploit specific vulnerabilities of a particular company or individual. These threats rely heavily on social engineering to increase their effectiveness. Given the increasing success of blended attacks, there is a wealth of information available for crafting new threats with a personal touch.

Custom threats generate very little suspicious activity and are not widely distributed, making them exceedingly difficult to identify. However, since these attacks are means for criminals to make a profit, by becoming a less attractive and more resilient target it is possible to reduce the risk of these and any new blended threats. This can only be accomplished with a layered defense.

REDUCING THE RISKS: A LAYERED DEFENSE

Armed with an understanding of the money-making methods of criminal groups that use blended threats, IT managers can identify their company's vulnerabilities, and build comprehensive layered defenses, which must contain the following five components:

1. **Acceptable use policies, and effective user education programs**

   Since many of the most successful blended threats have a social engineering component, it is imperative to continually educate users about risks of using the internet and wireless devices, as well as ways that users can protect corporate assets. In addition, acceptable use policies must detail the types of activities that are appropriate or not allowed in a particular corporate setting, as well as penalties for violating such policies. Furthermore, to properly enforce corporate policies, it is necessary to implement monitoring and compliance tools.

2. **Secured all entry and exit points, and desktops**

   Blended threats are rapidly spreading using arbitrary combinations of networks, protocols, and media: the web, e-mail, instant messaging, peer-to-peer, removable media (CDs, flash cards), and mobile devices[7] (cell-phones, PDAs, bluetooth and wi-fi devices). These are also the routes by which personal or corporate data can be stolen. Therefore, IT managers must implement effective defenses at all of the potential entry and exit points, at network and application levels, as well as on the desktop. Since the majority of recent threats have "backdoor" mechanisms[8], which typically only make outbound connections, networks must be secured in all directions (not just inbound), both at the perimeter as well as the LAN level. Monitoring LAN traffic and disabling or throttling nodes that exhibit suspicious activity is effective in stopping the spread such threats within a corporate network.

3. **Deep content filtering to guard against known, unknown, and custom threats**

   Blended threats are effective because they masquerade as harmless content, implementing content-aware filtering technology is an essential ingredient in reducing the risk of successful blended attacks. With content filtering, enterprises can significantly reduce the spam onslaught, restrict access to inappropriate websites, as well as protect against malware threats. Content filtering must be implemented in both in- and outbound directions, as well as on the desktop. Because malicious content is constantly evolving, IT managers must ensure that the content-filtering solution contains signature-based filters that can be updated in real time to guard against known threats. In addition, heuristic and artificial intelligence tools must

be leveraged to protect the enterprise from yet unknown, zero-day threats. Since no two organizations are alike, an effective content filtering solution must also allow administrators to easily add custom company-specific content filtering rules (for instance, filtering out any outbound e-mail containing proprietary information).

4. **Partnerships with vendors**

   Most companies are running a diverse collection of systems supplied by many vendors. To ensure that systems are implemented in optimally secure ways, and that security-related patches are applied to systems in a timely manner, it is important to establish close working relationships with software and hardware vendors. In addition, companies must work closely with their content filtering solution provider, to ensure frequent (or real-time) updates to the definition database.

5. **Relationship with law enforcement**

   In an event of a security incident, companies are likely to be dealing with organized criminals; therefore, a close relationship with local and federal law enforcement established *before* any such event occurs can be invaluable.

The need for multiple layers of content filtering is being driven by the increasing number and sophistication of threats that are capable of infecting corporate networks in a variety of ways. These threats, often referred to as blended threats, attack corporate networks through multiple vectors, including e-mail, web traffic, instant messaging, and peer-to-peer (P2P) networks. This blending of threats drives the need for integration between the protection layers to close security loopholes and deliver deployment and IT efficiencies. The harm potential and sophistication of attacks will continue to escalate. These threats have caused the effectiveness of e-mail and the Internet to suffer and thus have driven content filtering solutions to become a vital component of an enterprise security strategy. Virus infection is still the number one concern regarding corporate security, but other factors such as policy enforcement, spam, spyware, legal liability, and regulatory compliance are increasingly driving the need to manage e-mail, instant messaging, desktop applications, and web traffic for confidential data, inappropriate content, intellectual property, and unsolicited e-mail.

NaSPA member Jim Murphy works for SurfControl.

[1] Keizer. Gregg. Latest Online Menace: Custom Worms Built For Industrial Espionage. 2005. http://informationweek.com/story/showArticle.jhtml?articleID=163702855
[2] Federal Bureau of Investigations. FBI Fugitive—Saad Echouafni. 2004. http://www.fbi.gov/mostwant/fugitive/jan2005/janechouafni.htm
[3] Anti-Phishing Working Group. http://anti-phishing.org/
[4] Keizer. Gregg. From Russia With Malware. 2005. http://www.informationweek.com/showArticle.jhtml?articleID=163701736
[5] Ilett, Dan. Expert: Online extortion growing more common. 2004. http://news.com.com/Expert%3A+Online+extortion+growing+more+common/2100-7349_3-5403162.html
[6] National Infrastructure Security Co-ordination Centre. Targeted Trojan Email Attacks. 2005. http://www.niscc.gov.uk/niscc/docs/ttea.pdf
[7] Ostergaard, Bernt; Zetie, Carl. Mobile Devices Under Attack. 2004. http://www.forrester.com/Research/Document/0,7211,35188,00.html
[8] Top Internet threats: worms, spyware. http://economictimes.indiatimes.com/articleshow/msid-978691,curpg-1.cms