



A Brief Look at the Evolution in Malware and Network Security

July 1st, 2008

The motivation behind exploits has become financial gain, and the technological challenge in these exploits has become absolute stealth.

The purpose of this paper is two-fold: first to give you a high level overview of the evolution in network security threats, and second to discuss advances in technologies that help administrators increase the security and the productivity of their network. Since both topics are vast, the first section will sample three areas: key loggers, bots/zombie distribution and social engineering. The second section will cover network productivity and security challenges.

You may already be a SonicWALL customer, but as the threat landscape evolves, so do the tools and solutions that protect against these threats. Let this paper be a call to action for you to evaluate whether your current network security solution is adequate.

A Sample of Evolution among Network Threats

The motivation behind exploits for software vulnerabilities has undergone a dramatic shift over the past five or so years. Originally, exploits were written and released as proofs-of-concept, or with the motivation of prestige and ego stroking acting as the primary drivers. These threats manifested themselves by doing something highly disruptive and visible, such as defacing Web pages, bringing down databases and corrupting user data. Organizations and individuals who became victims of these attacks suffered a nuisance at best and downtime at worst while a Web server was restored from a backup or a user's laptop was being disinfected or reimaged. However, once these maintenance tasks were completed, operations came back to normal.

With the proliferation of always-on broadband and an explosion of online services such as banking and stock trading, the motivation behind viruses and exploits started shifting more towards financial gain, manifesting itself through identity, bank and stock accounting theft. Simultaneously, an added benefit to computers being permanently online with a fast broadband connection is that besides providing potential identity theft victims, they offer a perfect distributed platform for launching DDOS attacks and for routing spam.

Key-loggers

Identity theft and its derivatives started becoming a serious concern in network security as more and more computer security illiterate people started utilizing services online that require sensitive information. The explosion of these services, such as banking, e-payment and stock trading, created a tremendous financial opportunity for exploit writers if they could only capture what the users typed when visiting these sites. Trojans were modified to now come with a payload that would detect a user visiting a site of financial interest, at which point a key logger would be started. All data captured by this key logger is then sent to the central Command and Control site (often through P2P means) where the information is sold, again, to the highest bidders.

You may wonder, **“How could someone possibly benefit from accessing my stock account, or that of my employees? Theoretically, if the hackers wire money to their own bank accounts, those transfers can be traced down to a person very reliably, thus making this**

approach to theft impractical.” While this line of reasoning is correct, there are ways around it. One of the most common techniques utilized is a simple “pump and dump” scheme involving stolen accounts.

First, a stock with a low price and a relatively low trading volume is selected, and either “call” options, or the stock shares themselves, are bought at a “regular” price. Then, using stolen trading accounts, this stock is bid up, using money in the stolen accounts, to unreasonable levels that are not supported by any fundamentals. At this point, those running this scheme sell their originally purchased shares or options and make a serious profit in their own trading account, leaving those with compromised accounts holding shares that are fraudulently and artificially inflated.

Another low hanging fruit is e-payment accounts such as PayPal. Those daring enough, or foolish enough, would transfer funds directly to their own accounts. More enterprising hackers simply bid on auctions set up by their friends or by themselves, using a compromised PayPal account to pay \$200 for a one dollar bill, or \$10 for a pencil and 200 of “shipping” charges. Going through an auction house adds a layer of plausible deniability if the perpetrators are even caught on the receiving end of the auction.

Attacks of this kind leave a long lasting trail of damage that does not end the moment that the Webserver is rebuilt or the laptop is reimaged. Identities can be stolen, credit ruined, savings destroyed – these are not ephemeral nuisances that can be resolved easily.

Distribution of Bots and Zombies

Not satisfied with taking over a stock account or clearing out a PayPal account, the writers of these Trojans pack another piece of software that acts as a remote control for the compromised machine. By controlling literally tens of thousands of machines in this manner, hackers can launch distributed attacks and send out spam, making it seem like it’s all coming from random sources and thus bypassing blacklists and IP blocks.

This is not news to anyone who has had even the slightest awareness of practical computer security in the past 8-10 years, so what makes this topic interesting today is the method through which this malicious payload gets distributed. Originally, these bots were distributed through fake shareware, attachments and pirated software. This was not much of a concern for businesses, other than malicious attachments, and besides – the solution didn’t really scale. If money was to be made from compromising as many machines as possible, a quicker and sneakier method had to be devised in order to be successful. This became possible through the realization it takes any exploit that allows remote execution on the remote machine to install a small payload on a Windows machine, and thus browser exploits became a favorite target. The costs of such malware distribution are minimal – a single server serving malicious content that often exploits IE or Flash without user intervention. This way, the distribution is fast, cheap and wide – **and all it takes is to get someone to click on a link in a spam email while running a weak browser.** Unfortunately, even fully patched systems that are running an anti-virus solution can be vulnerable to a browser or a Flash vulnerability.

Social Engineering – “Error Exists Between Keyboard and Chair”

Once money and the potential for large profit enters any sector, including exploit writing, the organizational capabilities and the skill attracted to this field grows tremendously, resulting in an increasing level of sophistication among these attacks. Some of the most sophisticated viruses today can evade the majority of desktop virus scanning techniques, and can only be discovered

when a much higher level of scrutiny is applied on the system in question. But sometimes all this effort is unnecessary when there are people willing to forget about security, especially when facing a simulated authority or an unexpected situation.

One of the most creative ways to distribute malware is through video codecs. The scheme is as follows: a “viral” video with a catchy title is sent out through email or is posted to an online forum. Having a reference to pets and kids doing something silly usually helps to entice people into opening the video. Once the video is opened, it requests a download of a codec in order to be played, which to most people is a reasonable request. However, the codec is served up from a site operated by the malware providers, who install not just the necessary codec, but also the aforementioned key loggers and bots.

UTM – A Step in the Right Direction

With the introduction of Unified Threat Management (UTM) solutions several years ago, the fight to protect networks from network borne attacks shifted focus from the desktop to the gateway. UTM appliances don't have to rely on the facilities provided by the already compromised operating system while scanning for threats, and attacks can be detected via signatures at all layers. Instead, UTM solutions accomplish this protection by scanning, at the gateway, the entire payload in each packet for known signatures and attack patterns while this data is just on its way to the target machine. A close analogy would be sounding the alarm when a burglar is just trying to enter the house, rather than when he is already inside and is loading up on valuables (and has a chance to deactivate the alarm internally). Of course, UTM appliances don't replace the value of educating end users in safe computing practices, but they reduce the chances of coming in contact with malware by orders of magnitude.

Early deployments of UTM solutions uncovered a serious road block to widespread adoption of these appliances in larger environments: lack of performance. Even though the benefits of UTM solutions became crystal clear, the performance penalty incurred by enabling all security services became crippling and many businesses opted for performance over security by disabling these services.

This limitation is currently being overcome thanks to advances in both processor technology in the form of multi-core solutions, and through advances in the scanning engines that moved away from a proxying approach and more towards a streaming-scanning approach (at least for some vendors like SonicWALL). The new multi-core products allow all traffic to be scanned on all ports, while still maintaining a more than sufficient level of performance even after the severe performance penalty incurred by this inspection.

All of this comes back to productivity – both from a personal and from a business perspective. A single prevented virus outbreak already saves unnecessary downtime and IT costs associated with the cleanup and recovery. A single instance of prevented identity theft keeps an employee's mind at peace and at work, rather than worrying about recovering his or her financial history while simultaneously remaining a productive worker. As UTM platforms grow in power, the tradeoff between security and performance disappears and gateway security becomes not a choice, but a necessity.