

Layer 8

How and Why Targeted Attacks Exploit Your Users

Introduction

The standard model for network management defines seven layers:

Layer 1 – A wire connects a device to the network (physical equipment enables the transmission of binary data)

Layer 2 – The light comes on next to the wire (physical addressing enables devices on a network identify themselves to each other)

Layer 3 – An IP address binds to the network interface card (logical addressing determines the path a network connection must take)

Layer 4 – TCP/IP now works (a connection is established between two or more devices using the same network protocol as the Internet)

Layer 5 – A communications flow takes place between two or more connected devices

Layer 6 – Data representation and encryption occur within a communications flow

Layer 7 – Data passes between applications running on a host and the network

Network security products and strategies apply to each of these layers, and still other protection technologies span multiple layers. However, in spite of all this innovation and expenditure, targeted attacks such as BotArmies remain a serious and growing threat across the Internet.

The reason is simple. Targeted attacks take advantage of *another* layer in the network management model, one that the standard model does not take into account – end users. It is this other layer – Layer 8 – that gives the controllers behind targeted attacks their best advantage for attacking enterprise networks.

User Behavior Affects Network Security

Everyone hates spam. But have you ever taken the time to actually look at the headers that clog your inbox? Sure, there are the classics:

- Porn
- Sexual enhancement
- Cheap software
- Fake luxury goods

And yet, buried within the usual drivel are some very interesting trends. For example, with the current economic downturn dominating the news headlines, spam promising employment opportunities or “guaranteed” moneymakers has grown dramatically in

volume. Likewise, phishing attacks that prey on fears of banks going bankrupt or confusion around financial mergers have become very popular.

It is not a coincidence. One of the biggest challenges for the organized criminal organizations behind targeted attacks such as BotArmies is figuring out how to get malicious software – malware – onto enterprise systems. End user behavior is how it happens, and it operates easily and often, in spite of the best efforts of vigilant employees and traditional network security defenses.

The common core behind these social engineering efforts is the bad guys' recognition that enthusiasm almost always trumps common sense on the Internet. Or, put another way, given a choice between security and convenience, convenience will always win. Users demand it. If IT doesn't deliver, then users will find a way to circumvent network security defenses, often with the best of intentions but potentially devastating results.

For example, targeted attack controllers actively seek to attack Web sites that feature porn, employment information, social networking, chat forums/online messaging and the like. Popular culture fan sites and sites that cater to senior citizens, teens or young adults are also popular.

People naturally trust that a Web site's operators have fully secured their online operations. But, as recent Web site compromises at BusinessWeek and Adobe Systems show¹, that trust is often a trust betrayed. Even worse, users can easily get redirected from a legitimate site to a fake Web site that looks and acts like the real one. The only tip-off is an unusual string of text in the URL address at the top of the browser – and no one really takes the time to carefully examine all of that technical gobbledy-gook.

Other attacks show increasing levels of sophistication. One recently discovered malware sample modifies a text file Windows uses for maintaining alternate names for network addresses (HOSTS). Since AV and malware removal tools look for executable code, not text files, this unauthorized modification is almost impossible to detect. If a user visits one of the addresses listed in the file (typically a bank, news site or other likely destination), the modified HOSTS file instead redirects a user to a fake Web site that then downloads a newer version of the malware – even if the malware previously has been discovered and removed from the system.

The vast majority of this malicious activity affects home users and smaller businesses. However, at any given time, 3% to 5% of enterprise systems are already compromised by targeted attack malware². In other words, your users fall prey every day to social engineering scams, and put enterprise resources at risk. These attacks are the worst of the worst. They are extremely stealthy, and all but invisible to antivirus (AV) or intrusion detection/intrusion prevention systems (IDS/IPS). Once inside your network perimeter, no confidential information or proprietary trade secret is truly safe.

¹ Sophos, Inc., other references

² Damballa research, based on data generated at real-world enterprise organizations and confirmed by multiple other organizations

Insider Attacks, As Well

Social engineering also enables sophisticated targeted attacks to originate from within the enterprise. For example, disgruntled employees or unscrupulous contractors can easily use a build-it-yourself BotArmy kit to create a surprisingly sophisticated attack network within the network perimeter. These toolkits are easy-to-use, with all of the polish of commercial software. Some even come with cash-back guarantees, should they ever be detected by AV or IDS/IPS.

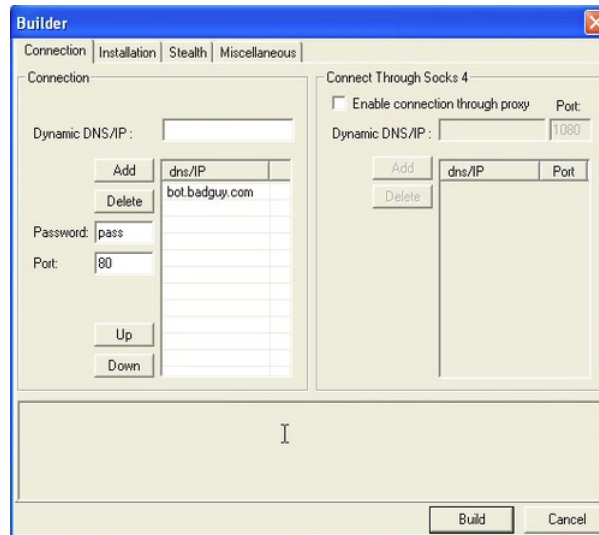
Other inside attacks can originate from partners or remote offices with less stringent security practices, or gaps in coverage that come from systems upgrades, mergers, acquisitions and the like. Given the huge numbers of local and remote users and devices that connect and disconnect from the enterprise every day, the bigger surprise is that the problem is not even larger than it already is.

Targeted attacks also appear from very unexpected sources. JPEG graphic files and Adobe Acrobat PDF documents each can be faked. The image or the file attachment looks perfectly normal. However, clicking on the image or opening the file actually triggers an executable program that downloads targeted attack malware. Malicious Web sites can contain multiple ways to compromise a computer, even by something as simple as viewing a Web page. Each of these attacks represents ongoing, increasing levels of sophistication and stealth.

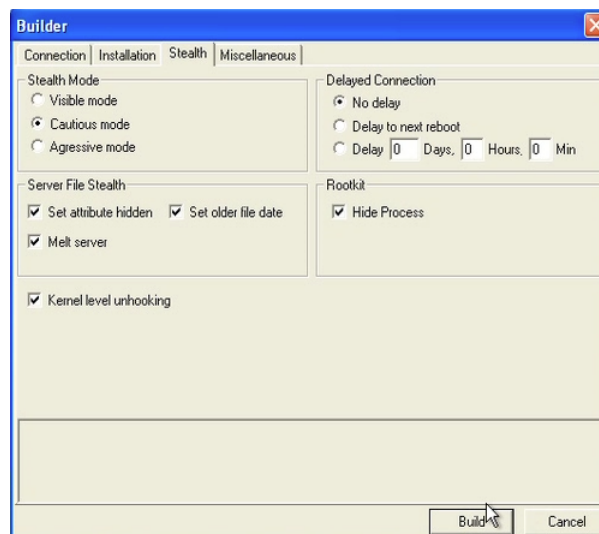
Clearly, the professional nature of targeted attack malware and the well-oiled delivery mechanisms represent a dangerous, ongoing threat to the enterprise. Odds are that the most damaging compromises will come from the best crafted, hardest to find malware. Antiphishing controls, Web access white lists and other tools can help mitigate the risk, but only to a point. Targeted attack malware will get in – the only question is how much, and at what expense to the enterprise. The steady 3% to 5% compromise rate cited above is proof of this malware's success.

Expertise Not Required

It does not take significant technical ability to launch a targeted attack. The following example is an easily available program for building the Bifrost Trojan (also called Bifrose). In effect, creating a targeted attack is a simple point-and-click operation. Leasing all or part of a BotArmy across the Internet is equally easy.



This malware generator requires only a single click to hijack the proxy settings of a victim's browser. Proxies exist almost exclusively within corporations, which may indicate the preferred target for this malware. Many corporations believe that a proxy will protect them against Internet threats. Clearly, attackers know better. One other interesting feature is that the attacker can configure this malware to communicate on any port – even ports 80 and 443, which are necessary for HTTP and HTTPS Web traffic.

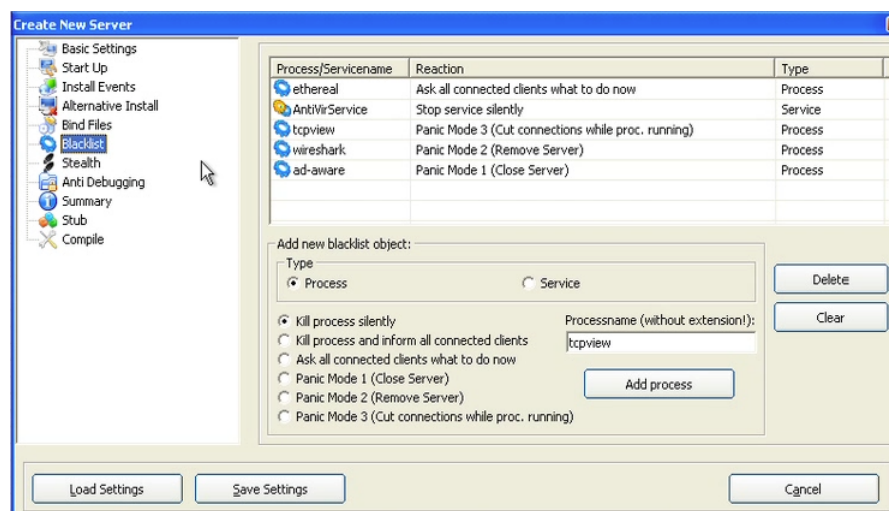


Bifrost's *Stealth Mode* settings are also interesting. The attacker can configure this bot to be completely hidden on a victim's computer – so well that AV cannot detect it. The rootkit option adds an additional level of stealth that allows the malware to operate deep within the operating system kernel. Bifrost even has the ability to unhook a Windows firewall or an AV engine, so that it appears that these defenses are active when, in fact, they are not.

The *Server File Stealth* attributes ensure that there are no visible signs of the malware either on the computer's screen or within the file system of the device. *Melt Server* deletes its own installer once executed, which removes any trace that it ever existed.

Set Older File Date makes forensic analysis more difficult since the malware acts like it installed long before it actually did.

These multiple evasion techniques mean that, once a machine is compromised, it can almost never be trusted as truly malware-free again. In fact, bot-oriented malware often requires reformatting a hard drive, or replacing the hard drive and destroying it to ensure that the malware is truly eradicated.



Finally, this screen shot illustrates Bifrost's ability to disable AV and antispysware software. *Kill Process Silently* disables the security software. It appears to run normally, but takes no useful action to stop the malware from operating.

Enterprise organization should be very concerned with how open their networks are to targeted attacks. Traditional network security defenses approach enterprise protection as a technology problem, to be applied to the different layers of the network management model. The closest they come to Layer 8 protection is when they attempt to protect users from themselves by scanning for malware or blocking suspicious behavior.

These efforts are only partially effective. A recent test of desktop security suites evaluated these product's ability to protect against 300 different types of exploits. The most effective product only stopped 64, or 21%. Other prominent products stopped as little as 2%³. Damballa's own research indicates that popular AV applications typically miss 40% of targeted attack malware, and other sources contend that over 80% of newly written malware cannot be detected by any AV product⁴.

In other words, targeted attack malware mimics legitimate applications, hides traffic by using normal Web ports (HTTP, HTTPS and email), or only surfaces for activity at infrequent, unpredictable intervals. It can disable AV tools, but leave the user interface

³ Computerworld, based on testing run by Secunia on a standardized Windows XP SP2 system intentionally missing certain patches and containing known vulnerable programs

⁴ AusCERT

running so that AV appears to be operating normally, even if it is not detecting anything. Even worse, the malware can update itself as often as every 30 minutes, which is far faster than any AV vendor can update its products, let alone enough time for an enterprise organization to deploy an update to each and every system.

Conclusion: Damballa Delivers Protection for Layer 8

Damballa recognizes that AV, IDS/IPS and other network security tools are very effective at what they were designed to do. They are a necessary part of any enterprise network security strategy. However, they are not effective against the malware that drives targeted attacks.

Damballa's approach focuses on the Command-and-Control (CnC) communications that the controllers behind a targeted attack must maintain in order to organize individual compromised systems into a coherent attack army. This element is the single component of a targeted attack that must remain constant if the controller is to build a stable platform for organized, online crime. By isolating this signal from legitimate Internet traffic, Damballa can rapidly and accurately identify compromised systems that other technologies simply cannot see.

This protection works regardless of whether the targeted attack originates inside the enterprise or enters from outside the network perimeter. It is fast and exceptionally accurate, with few if any false positives. Damballa solutions operate without impacting bandwidth or network performance, and do not introduce undue complexity or expense to network security or overall IT management.

Which brings us back to Layer 8 – your users. Most security technologies force a balance between protection and usability. For example, frequent AV scans and aggressive Web black lists/white lists can increase security to a degree, but too much security intrudes on employees' ability to perform their jobs. In addition, these steps do not provide real-time protection. Each AV scan is a snapshot, leaving its host potentially vulnerable until the next scan. Likewise, online criminals monitor black lists, and move their resources at frequent intervals. As a result, a black list degrades dramatically in value as soon as it is issued.

Firewalls and IDS/IPS can block connections, interrupt suspicious network services and drop suspect network packets, but aggressive settings will disrupt useful work. Worst of all, these measures only work for threats that these defenses can detect. They are designed for broad-based, general purpose attacks – and they do not identify or mitigate targeted attacks very well at all.

Short of disconnecting staff from the Internet, Damballa provides the only practical, cost-effective means for identifying and stopping targeted attacks. The benefits of Damballa's technology, however, go beyond its basic protection capabilities.

Damballa's appliances operate as passive taps on the network. They do not slow or interfere with normal network operations. There are no software agents to install,

maintain and manage on individual systems, or complicated multi-point deployments that must be coordinated across dozens, hundreds or thousands of computers.

When targeted attacks are detected, Damballa feeds appropriate alert information to the staff in real-time. This information contains detailed assessments of the risk presented by the compromise, which administrators can use to make a measured decision as to the best course of action. In most cases, the only impact an end user ever sees is an interrupted Web surfing session with a known malicious Web site or a legitimate session that crosses a known malicious intermediate Internet domain.

It is not possible to completely manage away the security lapses that end users inevitably create. Damballa's unique approach to targeted attacks, however, gives enterprise organizations the means to protect your end users and your networks against targeted attacks – quickly, accurately and cost-effectively. It truly is targeted protection against targeted attacks.

About Damballa, Inc.

Damballa protects businesses from targeted attacks used for organized, online crime by using the Internet cloud to identify and isolate threats that evade other technologies. Our unique, global approach monitors the Command-and-Control (CnC) needed to launch these attacks as well as compromised systems, which enables immediate identification and mitigation of malicious activity. Global 1000 corporations, large Internet service providers, OEM partners and government agencies use Damballa's signatureless solutions and industry-leading research to reinforce existing security infrastructure and stop hidden Internet attacks. The result is dramatically improved security both inside and outside the network perimeter. Damballa is privately held and headquartered in Atlanta, Georgia.

Copyright © 2008, Damballa, Inc. All rights reserved worldwide.

This page contains the most current trademarks for Damballa, Inc., which include Damballa, the Damballa logo and Harvester. The absence of a name or logo on this page does not constitute a waiver of any and all intellectual property rights that Damballa, Inc. has established in any of its products, services, names, or logos. All other marks are the property of their respective owners in their corresponding jurisdictions, and are used here in an editorial context, without intent of infringement.