

Targeted Attacks for Fun and Profit

An Executive Guide to a new and growing enterprise threat

At-A-Glance

- Targeted attacks are a new and rapidly growing threat that easily evades enterprise network defenses such as antivirus and intrusion prevention/intrusion detection systems.
- Targeted attacks are operated by sophisticated professional criminal organizations whose prime motivation is profit.
- Targeted attacks involve networks of compromised systems that span the Internet. As a result, it takes a multinetwork, global approach such as Damballa's to deliver the knowledge needed to identify and stop targeted attacks.

Abstract

A senior manager looks at the security dashboard and sees nothing but green lights. That's good. Everything is working as expected. The enterprise is protected.

A few floors below, IT and security staff sees the same dashboard but reach a very different conclusion. No security solution is that effective. If everything looks that good, then something has learned to slip through. The first question is what. The second is how much damage is it doing. And the third is how to stop it.

In many cases, the answer to Question One is a targeted attack. One leading analyst organization defines a targeted attack as a threat that aims, "to achieve a specific impact against specific enterprises, and are the growth area in Internet attacks."

Regarding Question Two, targeted attacks easily evade enterprise defenses such as antivirus and intrusion detection/intrusion prevention systems. So the damage can be severe, ranging from stolen user credentials to proprietary trade secrets to confidential customer and financial information.

And stopping a targeted attack, per Question Three, requires a different approach to network security, one that both fills in the gaps within existing security infrastructure plus provides additional capabilities specific to targeted attacks – without adding layers of cost or complexity. This white paper explains why these threats are so prevalent and profitable, and how Damballa's products and services deliver the protection against targeted attacks that other solutions cannot.

Introduction

You and your organization are upright and ethical. You would never rent a BotArmy or hire an online criminal organization to ferret out industrial secrets from your competitors. Nor would you use illegally obtained information to set up a new business to compete with one of your close business partners.

Nevertheless, these activities take place every day. Online criminal organizations build sophisticated networks of compromised computers that target the valuable information created and stored inside enterprise networks like yours. Then they sell this information to the highest bidder, or open up their networks on a for-hire basis to anyone who wants to use your systems to troll for specific information or to launch an Internet-driven attack.

What's different about these targeted attacks is that they are exceptionally stealthy, easily evade antivirus (AV) and intrusion detection/intrusion prevention defenses (IDS/IPS), and are motivated primarily by profit. Odds are that they are already at work inside your enterprise. As such, they represent a dangerously underreported risk for any business that conducts online operations.

The evolution of the threat

When enterprise organizations first looked to the Internet as a business conduit, there were three basic types of network security threats:

- Viruses and worms
- Hackers breaking into internal systems
- Web site defacements

Viruses and worms started out as an intellectual exercise designed to create bragging rights in the Internet underworld. At worst, they could disable systems or create a Denial of Service (DoS) attack, in which corporate resources became unavailable due to the extreme amount of host and/or network activity generated by the malware.

Similarly, the original hackers considered themselves to be vigilantes. Their goal was to expose shoddy security practices, and take advantage of organizations too clueless or careless to shut them out.

Insecure Web sites became another obvious target for individuals seeking to prove their capabilities as so-called black hats on the Internet. After all, a defaced Web site is an obvious and unambiguous victory for the attacker.

Eventually, easy-to-use malicious Web sites and software kits became available, so that anyone with a little time and minimal expertise might be able to launch a dangerously capable attack. It became as simple as point-and-click.

Antivirus and intrusion detection/intrusion prevention systems evolved to become very effective at stopping all three of these types of attack. Enterprise organizations

deployed these technologies on a widespread basis. And many businesses considered themselves safe from attack, as long as they kept these defenses up-to-date.

Of course, each of these classes of attack contained the seeds of much more dangerous threats to come, and the attackers themselves evolved. Viruses and worms have grown into more sophisticated malicious software (malware) that evades antivirus (AV) and intrusion detection/intrusion prevention systems (IDS/IPS). Linked together into networks that span corporate and national boundaries, these malware armies are the foundation of targeted attacks.

Hackers themselves realized two important points. First, it was profitable to compromise corporate resources, either by hijacking internal systems to attack still other organizations, or by stealing confidential information that could be sold on the black market. Second, one-to-one hack attacks are inefficient. It makes much more sense to generate automated, remotely controlled malware that enables a small group of individuals to operate a massive online criminal enterprise.

Finally, vulnerable Web sites are a very useful resource for spreading targeted attack malware. Unsuspecting users will implicitly trust a Web site, mainly because it is very difficult to determine it has been compromised or not. BusinessWeek's Web site, for example, recently suffered from such an attack¹. Visitors to the Web site had no reason to expect that anything was amiss. However, the Web site delivered malware along with advice for MBA students seeking employment.

Malware spread through this manner can be as simple as a malicious link on a Web page or email, or as sophisticated as an image or Adobe Acrobat PDF file that looks legitimate, but actually downloads and installs malware as soon as it is viewed. Once embedded inside a laptop, desktop or server, the malware operates without being detected by AV, IDS/IPS or any other network security defense. Added together, these combined elements provide the foundation for a successful targeted attack.

So what, exactly, is a targeted attack?

Targeted attacks require three components in order to be effective:

Malware – Malicious software code that either executes like a program or alters the configuration of its host, so that the machine is under the remote control of an unauthorized controller.

Controller – An individual or an organization that creates and controls networks of compromised computers across corporate and national boundaries, and uses these systems for illegal activities.

Command-and-Control (CnC) – a system of buffer locations spanning the Internet that are used to send instructions to compromised computers and to retrieve stolen data, as well as hide the controller's identity and location.

¹ Sophos Inc., numerous other references

According to that same analyst organization, “Targeted attacks have three major goals:

- Denial of service: disrupting business operations
- Theft of service: obtaining use of the business product or service without paying for it
- Information compromise: stealing, destroying or modifying business-critical information.”

In other words, targeted attacks represent the professionalization of criminal activity on the Internet. Rather than individuals operating with a variety of motivations, on a one-to-one basis, targeted attacks use a one-to-many model that is elusive, effective and very hard to detect.

Targeted attacks differ from the threats that AV and IDS/IPS were designed to detect.

- Malware and criminal activity is designed to be stealthy, rather than draw attention to itself
- Targeted attacks rely on the Internet itself to propagate attacks and to transport stolen information
- Malware armies operate across corporate and national boundaries, which greatly complicates investigation and prosecution of online criminal activity
- Cultural and national interests often condone malicious activity that would be considered criminal in another context

This last point is very important. A local businessman giving talented local programmers a decent paycheck in Eastern Europe may well be considered a criminal by his victims in North America. And many governments consider targeted attacks as a legitimate tool for industrial and military espionage. The Chinese government is widely believed to regard the Internet as a military tool², and Russia actively encouraged patriotic Russians to use the Internet to attack Georgian banks and governmental operations during the recent Russo-Georgian war³.

The end result is a dangerous new enemy – well-funded organizations with top-tier programming talent capable of building stable online platforms for online crime. Targeted attacks are so successful that their perpetrators operate openly in many countries. They rent out parts of their malware armies for a variety of criminal activities (spam, industrial espionage, theft of credit card numbers, etc.). They test, evolve and market their wares much like legitimate corporations. They even sell build-your-own malware kits that come with cash-back guarantees that the resulting code will evade any antivirus on the market. The reason that they can be so brazen is that they know that traditional network security infrastructure cannot keep up with them.

² NationalJournal.com, ZDNet TechNews, The Guardian, numerous other references

³ Damballa’s *The Day Before Zero* blog (<http://blog.damballa.com/?p=11>); numerous online news stories

Who is the target of a targeted attack?

Targeted attacks have multiple targets. The first is your company. Any enterprise has thousands of desktops, laptops and servers. It is all but impossible to keep every one of these devices completely patched against the latest security vulnerabilities, and all security software fully up-to-date. Indeed, security itself is often perceived to be a drain on productivity. Given a choice between ease of use and security, ease of use almost always wins.

As a result, every organization has a steady number of systems that are vulnerable to compromise. These gaps provide huge opportunities for targeted attacks to penetrate the enterprise network perimeter. More importantly, targeted attacks know how to mimic legitimate applications and otherwise disguise their activity so that detecting malicious activity is much harder than finding the proverbial needle in a haystack.

The next target is your IT infrastructure itself. Every server and Web application represents a distribution node for targeted attack malware. After all, these systems are centralized repositories and distribution points for information. Servers and Web applications also store proprietary information, such as logins and passwords, social security and tax identification numbers, credit card numbers, and much more. Any compromise that reaches even one of these key systems can deliver a tremendous amount of damage in a very short period of time.

Finally, you yourself are a prime target for a targeted attack. Any executive or senior manager carries critical, confidential information on his or her desktop and/or laptop. Everything from trade secrets to sales forecasts to your personal credit card numbers are fair game.

What do targeted attacks mean for my organization?

According to the Computer Security Institute's 13th Annual Computer Crime and Security Survey, 27% of respondents indicated that their enterprise had been hit by a targeted attack. Damballa's own data indicate that 3% to 5% of online corporate assets are already compromised by targeted attacks at any given point in time. In other words, almost every enterprise organization has been struck by a targeted attack, but less than 30% are aware of their exposure (or are willing to publicly comment on it).

Part of the reason behind this discrepancy is that targeted attacks employ as much deception and misdirection as possible. For example, some targeted attack malware disables AV, but allows a shell to operate. The defense has been neutered, but it appears to be working normally. Other tactics include masquerading as legitimate programs, using Web or email channels for communications, or encrypting traffic.

Targeted attack malware also likes to lure security infrastructure into a false sense of control. The initial set of compromised systems may do nothing more than send out spam. And security will respond by classifying the threat as much lower grade than an active attack – if it detects the spamming activity at all. Over time, this activity

becomes part of the background noise of daily online activity. Then the controller instructs some of the compromised systems to download new malware. Now, these systems are actively seeking a specific trade secret, but the network security system still sees these systems as relatively benign spam engines.

Targeted attack malware can update itself malware as often as every 30 minutes. Even the best AV vendors need at least 6-9 hours to identify a new form of malware, then test and distribute an update to their detection databases. Add in the time required to distribute those updates across an entire enterprise, and it becomes clear that enterprise networks are always open to a targeted attack, no matter how effective their current infrastructure is in stopping other types of threat.

Targeted attacks also differ in that compromised systems do not launch attacks on a regular basis. The actual malware behind the compromise can lie dormant for extended periods of time before waking up and launching malicious activity. This intermittent nature adds an additional layer of protection against detection.

In short, targeted attacks turn a compromised system into both a victim and a perpetrator. And that makes the enterprise itself both a victim and a perpetrator on a permanent ongoing basis, with all the legal and regulatory ramifications that come with an open network security exposure. Every hour of every day, some sort of online crime is being perpetrated, without anyone realizing it. Sooner or later, that exposure is going to become a very public and expensive liability.

Conclusion – How to stop targeted attacks

All targeted attacks require one element in order to link individual compromised systems into a coherent, multinetwork/multinational attack engine. They must employ some form of CnC. Without it, there is no means to tell malware what to do, when to do it and where to send anything that has been stolen.

The trick is learning to recognize targeted attack CnC communications and isolating this traffic from legitimate business operations and general Internet traffic. Other security solutions are not designed to perform this type of work. Indeed, it has taken Damballa years of research and development to create this ability and make it commercially viable.

Damballa's ability to leverage targeted attack CnC and use it against online criminals stops threats that other technologies miss and quickly restores control over compromised hosts. Whether a malware army hundreds of thousands strong or a small, tightly focused attack that operates on only a few compromised hosts, Damballa finds the hidden compromises that call out across the Internet to communicate with the criminal controllers behind a targeted attack. We use this knowledge to:

- Identify which enterprise assets have been compromised
- Understand how those compromises came about
- Measure the risks each targeted attack represents
- Recommend how best to remediate the threat

In short, Damballa provides a multi-perspective, automated approach that offers much deeper insight into targeted attacks than is possible with host- or LAN-based products, such as AV or IDS/IPS.

It is no longer enough to recognize that a threat exists, or even to identify that threat. Instead, enterprise organizations need:

- Deeper protection against targeted attacks than is possible with signature-based host, LAN or gateway security technologies
- Comprehensive, real-time visibility into targeted attack rallying activity both inside the enterprise and across the Internet, with the goal of predicting attacks before they arrive, or at least before they can damage corporate assets
- The ability to disrupt and resolve targeted attacks and the malware armies that enable them, so that remediation can take place in a planned, orderly manner

Damballa delivers this level of protection, operating as a key part of a comprehensive defense-in-depth strategy without adding unnecessary layers of complexity, headcount or expense. Our products and services deliver an exceptional stand-alone solution for combating targeted attacks. At the same time, our technology is designed specifically to integrate easily with traditional network security infrastructure so that the entire system becomes more efficient and effective.

Damballa's products and services are a proven solution for enterprise organizations seeking to combat targeted attacks used for organized, online crime. Our unique, global approach rapidly isolates the Command-and-Control (CnC) needed to launch these multi-network attacks – which means that your organization can protect itself sooner, without having to wait for antivirus or intrusion protection updates.

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.