

Anatomy of a Targeted Attack

Introduction: The Attack Begins

We've never met. We'll never, ever meet. But I know a few things about you. And I'm about to learn a whole lot more – more than you want me to know. And you and your company will never know anything about it.

See, I know how to get my malware onto your computer. Or onto one of your servers. Or onto a system belonging to any one of your coworkers or employees. Let's face it – you're worrying about how to do your job. You're not worrying about network security. So I've worked out a whole bunch of cool tricks to slip past your security without anyone being the wiser.

I can intercept your Web surfing and redirect you to a fake Web site that's under my control. Or I can compromise a trusted Web site¹ and get you to download malware from there. I can send you a malicious email. I can send you a JPEG image or a PDF file that's actually malware code². I can even take over one of your internal servers, and use it to distribute my malware from behind your defenses.

It's easy. In fact, a typical enterprise already has between 3% and 5% of its network assets compromised by target attack malware³. And that's with firewalls, antivirus (AV), intrusion detection/intrusion prevention systems (IDS/IPS) in place – the works.

Yes, every one of these systems is under my control – silently, untraceably, without you or your IT department being aware of it.

Motivation

Why do I do this? Simple – I'm a businessman, just like you. I'm in it to make money – lots of money. I get that money from your less-than-ethical competitors. From criminals who want credit card numbers. Sometimes, I even get it from disgruntled employees and former employees. Anyone who wants what you have is a potential customer for me.

That's why I go to such trouble to create malware that your AV and IDS/IPS can't find. See, it's not just me you're up against. It's my whole organization. We are salesmen, marketers, programmers – professionals. We pay our talent well. Some of our competitors even guarantee results.

We connect these individual compromised systems with thousands of others across the world into organized malicious networks. It's a stable platform for whatever

¹ Sophos, Inc., other references

² Damballa research

³ Damballa research, based on data generated at real-world enterprise organizations and confirmed by multiple other organizations

purpose we choose. We make money off the information we steal, and we make money renting parts of our BotArmies to other criminals. On a good day, we can create a tiny army of just a few compromises inside your enterprise, looking for a special trade secret or sales forecast. Anything specific is worth a lot of money to the right people. We know how to deliver.

Once Inside

The first thing my malware does once it's inside one of your systems is hide. That code may be tiny, but it's smart – much more independent and intelligent than viruses or worms. It disables your anti-virus technology while it leaves the user interface shell in place. That's right – your antivirus system tells you that it's working, but it's not really doing anything.

Next, my malware deletes any logs that might have recorded its download and installation. So, there's no trace of how it got onto your system. If you're running Windows Vista, it reconfigures Windows Defender, the built-in anti-malware application, so that it let's my malware operate while locking out any of my competitors. Now, I've got you and your systems all to myself.

Finally, my malware goes out to the Internet to connect with my Command-and-Control (CnC) network. The first order of business is to download new instructions for other locations and times for future communications. That way, I can move my network all across the Internet, making my BotArmy much harder to track or disrupt.

Back in the old days, BotArmy malware might try to use obscure ports to connect to a CnC. Today's malware is smarter than that. We use the same ports that you use for Web surfing, so trying to find my malware is like looking for a very small needle in a very large, always-on haystack.

My malware is only active at irregular intervals, and we know how to piggy-back on your users' legitimate activities so that we can hide better. Once again, we make it that much harder to track what we're doing. This stealth is why our malicious networks are so robust, and why it's so easy for us to download new instructions to our malware any time we want – including how or what to attack, when to be active or dormant and where and when to connect next to our CnC.

Take Action

What do I do with all this secrecy and control? Oh, I have all kinds of options.

Go Dormant

That's right – one of the best options for my BotArmies is to go dormant once they're inside your enterprise. I can hide for any pre-determined interval and you can't find me when I'm not doing anything. My malware turns your compromised systems into "sleeper cells" that can be activated when I need them, either to launch a sudden

attack or to replace other nodes that have been lost to discovery (unlikely) or attrition (systems replaced, reimaged for new users, etc.).

My ability to wake, organize and launch a targeted attack on very short notice is a great money-maker for me. I can grab the data I'm looking for and be gone again far faster than your network defenses can recognize or respond to the threat.

Seek New Victims

We've already talked about how easy it is for my malware to get on your systems. Once inside, it's even easier for me to co-opt your coworkers through altered email messages, misleading JPEGs and malicious PDF files, each of which looks like it comes from someone they trust. Basically, every email from any system I control is all the opportunity I need to compromise someone else. I've taken all that good will you've worked so hard to earn and turned it against you.

Look for Sensitive Information

My malware knows how to look for specific words, phrases, names and addresses within documents, databases or spreadsheets. That means your hard drive is mine to read, as is as any data stored across your networks or transmitted to or from your PC. I know your sales forecasts, your product formulas, credit card numbers, customer information or anything else I want to steal. I sell it to the highest bidder.

I can also monitor your movements. That means every keystroke on the PC, every password – everything I need to penetrate secure and confidential systems all across your enterprise. That includes accounting, sales and marketing servers, manufacturing control systems. Anything. All I need is for you to do what you normally do, every day. I really appreciate your assistance.

Keep It Small

Sometimes, less is more. I can tell my malware NOT to propagate, to minimize its activity and only look for a very narrow piece of targeted information. It's industrial espionage at its online best, and my organization is very good at it. There's no activity except when searching for the target. Once it's found, I shut everything down until it's time to send my treasure back across the Internet. Even then, I can break down the stolen information into smaller parts and send it back a little bit at a time, at irregular intervals. Good luck tracking it down.

Transmit Stolen Data

Sometimes, all I need my malware to do is to receive something I've stolen from someone else, and forward it along to another intermediate drop-site that serves as a buffer between me and anyone who might discover my activities. The same information goes out through dozens, hundreds, even thousands of separate channels. More than a few of them find their way back to me. I can even compare what comes back from different paths across the Internet to make sure I'm not being

monitored along the way. It's like an electronic version of money laundering, except that your data is my currency.

Take Someone Offline

Say you don't like your competition. Or you're a government who wants to make things difficult for another country⁴. How about taking them offline? My BotArmies can do it for you. I can use your systems to launch a Denial of Service attack against your enemies. Or, maybe your enemies want to take *you* down. The systems I've already compromised in your network can do that, any time I want them to.

I'm Not a Crook – I'm a Professional

Viruses and worms, hacker attacks – stuff like that is for amateurs. It's noisy and inefficient. Even worse, it only lets me do one type of malicious activity at a time. My targeted attack malware can perform any of the options I told you about. Or anything else I decide I want it to do.

In fact, I can update the code that drives my targeted attack BotArmies as often as every 30 minutes. There's no way AV or IDS/IPS can adapt to a target that moves so fast. I also monitor the black lists that security vendors use to guess at where my CnC is located. If I see any of my nodes there, I simply move on to other compromised transfer points. Rather, my BotArmy does it for me. It's all automated.

Think of my malware, BotArmies and targeted attacks as the natural evolution of organized, Internet crime. In fact, what I do is as far removed from viruses and hacking as your PC is from an old cash register. Think about what I offer my customers:

- Stealth and discretion
- Flexibility
- Stable, adaptive networks
- Sophisticated technology
- Proven results

My success lets me operate openly in many countries. After all, if you and your company are stupid enough to fall for these attacks, then you deserve what we're about to do to you.

Conclusion: Don't Talk to Damballa

My business has hit the sweet spot. Targeted attacks are a great growth area for Internet crime, and among the most difficult to stop. There's only one technology out there that worries me. Damballa.

Damballa is different from the AV and IDS/IPS companies. See, viruses and worms don't change that often. And they behave in distinctive ways, which makes what they

⁴ USA Today, others

do easy to track. That's why AV companies can identify them. Hackers aren't much smarter. They need to be online and connected in order to do their work. It's just one person against the network, and there are only so many ways to get in. That's how IDS/IPS works.

My malware changes all the time. It wakes up and sleeps unpredictably. It connects to different places across the Internet all the time. There's no way that AV and IDS/IPS can stop me – and they don't.

But let's face it – there's one thing I can't change, and that's the need to coordinate the systems that I secretly control into a BotArmy. The only way to do that is with my CnC networks. Without them, these compromised systems are basically isolated and harmless. It's my only real weakness.

Damballa has figured out how to identify my CnC signals and separate them from the noise of all the other traffic across the Internet. It's a fundamentally different way to protect an enterprise, and it works against my targeted attacks.

Damballa knows how to watch what I'm doing in real-time, without having to identify the malware I'm using or even when my malware's behavior looks like normal network activity. It's almost impossible for me to tell when Damballa is protecting a network, and their products are very accurate. I've heard their false positive rate is as low as 1/10 of 1 percent. That's impressive.

Their stuff is so good that they can catch even my small BotArmies. Their information is so detailed that it lets my victims quickly identify the presence and severity of any threat I throw at them – and then take whatever action they need to take to protect themselves against me.

I hate to admit it, but it's awfully effective. Damballa's customers don't have to run blanket quarantines on suspicious systems, or drop packets and block services to potentially compromised servers. They can take measured, targeted responses to my targeted attacks, and cut me off from what I need to do my job.

They call it targeted protection against targeted attacks. I call it trouble. It works, and there's nothing I can do about it. Except find another victim who's old-fashioned enough to think that he can outwit me with AV and IDS/IPS systems, or who's naïve enough to think I'm not a threat. Fortunately, there will always be more than a few of them out there...

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.