

Malware *Deep Dive*



New malware needs new defenses

Copyright © 2010 InfoWorld Media Group. All rights reserved.

Sponsored by



Fighting today's malware

How bad is it? Worse than you think. Here's what the new breed of malware looks like – and what you can do to stop it.

 By Roger A. Grimes

IF MALWARE WERE BIOLOGICAL, the world would be in the grip of the worst pandemic in history. In 2009, over 25 million different unique malware programs were identified, more than all the malware programs ever created in all previous years (see the [Annual Report from Panda Labs](#)). That's a pretty incredible statistic. Malicious programs now outnumber legitimate ones by many orders of magnitude.

The world's largest cloud computing user? Not Microsoft, not Google, not Amazon. The ringleaders of the [Conficker](#) botnet, with more than 4.6 million infected computers under their control, win by a mile. Some antimalware vendors report that 48 percent of the computers they scan are infected (see the [APWG Phishing Activity Trends Report](#), p. 10) with some sort of malware. Trojan horse programs make up 66 percent of all threats (see the [Annual Report from Panda Labs](#), p. 4).

No one need wonder what malware is trying to do. It's trying to steal money, whether it's through data theft, bank transfers, stolen passwords, or swiped identities. Each day, tens of millions of dollars are stolen from innocent Internet victims. And yet many computer defenders can't tell you what the biggest threat is to their environment. If you don't know the biggest threats, how can you defend against them properly?

Today's malware differs dramatically from the threats we faced just 10 years ago, when most malicious programs were written by young men looking to earn cyber bragging rights. Most malware made the user aware of its existence through a displayed message, music (as in the Yankee Doodle Dandy virus family), or some other sort of harmless mischief. Those were the days.

THOROUGHLY MODERN MALWARE

Today's malware is written by professional criminals. In

most cases, end-users are unwittingly tricked into executing a malicious program in the form of a Trojan horse. End-users think they are installing needed software, often "recommended" by a site they trust.

In fact those sites are recommending nothing of the kind. Malware producers routinely break into legitimate Websites using found vulnerabilities and modify existing Web pages to include malicious JavaScript redirects. Or the malicious code will be hidden [inside a banner ad](#) added to the Website by legitimate ad services. Either way, when the end-user surfs to the legitimate Website, the malicious JavaScript is loaded, and it either prompts the user to install a program or redirects the unknowing user to another Website where they are told to install a program.

TROJANS LEAD THE PACK

Trojans typically camouflage themselves as downloadable antivirus scanners, "needed" patches, malformed PDF files, or add-on video codecs required to display an exciting video. Most of the fake programs have the clean look and feel of a real program. Even career antimalware defenders find it hard to tell the difference between what is real and what is fake.

Fake programs are even more successful at duping victims when they appear to come from popular, well-known Websites that an end-user has trusted and visited, without incident, for years. Or they launch from one of the popular social networks, like Facebook and Twitter, which are all the rage among the least savvy computer users. Some malware programs scan the user's computer for vulnerable software that lacks security patches, but typically, end-users cause infections themselves by installing apps they should not.

This is not to rule out the obvious impact of spam, phishing, adware, or other attack methods. It's just that computer worms, viruses, and the other methods for exploiting computers, added up all together, don't equal

the threat of the socially engineered Trojan – even though some multivector worm programs, like Conficker, have victim figures that number in the millions.

In a common scenario, the first malicious program installed is called a downloader. A downloader’s goal is to be installed on the victim’s PC and then to “phone home” to the “mothership” Web server for more instructions (see Figure 1). The downloader often

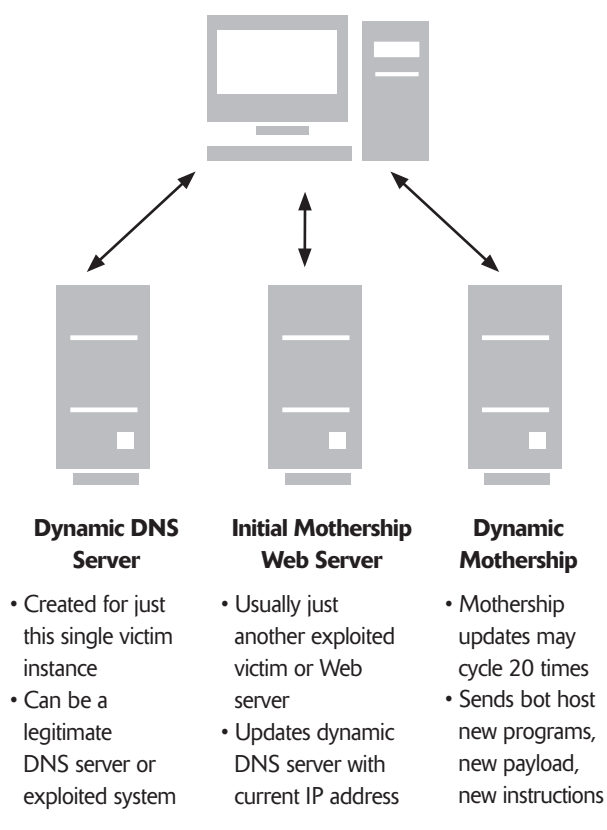
has instructions to contact a dynamic DNS server to get the mothership Web server’s current location. The Dynamic DNS server is just another Trojan-infected computer installed on an innocent user’s desktop. The DNS address record received by the downloader has an address that is good for only a short time – sometimes as little as 3 minutes. These “fast flux” techniques complicate efforts to investigate or eradicate malware.

The downloader will eventually be redirected to another server (which is, of course, just another compromised host) and download a new program or receive instructions. This sequence of finding and downloading new programs and instructions can go on for dozens of cycles. Eventually, the final program and instructions will be installed on the victim’s computer, with a handful of command-and-control servers under the direction of the botnet owners.

Botnets can be used by the owners themselves to steal money, to conduct distributed denial of service (DDoS) attacks, or to break into other computers. Often the botnet owner will rent the botnet to other criminals who then use them to do their bidding.

A good example of a common bot and botnet is [Mariposa](#). At one point, it controlled more than 13 million PCs in 190-plus countries. The masterminds of Mariposa were not ultraskilled malware writing geniuses – they were three guys who bought a botnet “kit” on the Internet for \$300.

Fig. 1 Typical malware “phone home” life cycle



1. Bot program exploits victim PC and installs itself
2. It “phones home” using dynamic DNS server to find “mothership”
3. Finds mothership, downloads new code and instructions
4. Repeats 1-20 times
5. Infects new victim PCs
6. Sometimes plays role of bot host, sometimes of dynamic DNS server, sometimes mothership

DIY KITS: TOOLS OF THE TRADE

Do-it-yourself malware kits have been around for two decades, but now they are soup-to-nuts efficient. The typical kit can spit out (currently) undetectable malware to do the customized bidding of its owner.

Using these kits is as easy as clicking a few check boxes. The resulting malware will break into Websites to start infecting innocent visitors, generate enticing spam and phishing e-mails, and do everything it takes to create the botnet – including bots, dynamic DNS servers, roving mothership Web servers, and the command-and-control servers. Many of the kits are directed toward bypassing particular types of authentication and focus on particular financial institutions.

The better bot kits include a sophisticated administrative back end so that the hackers can read statistics on total infections, OS versions exploited, and tricks used. For another \$30, the kit creators will include 24/7 tech support



courtesy of Skype. These kits aren't hidden. With just a little bit of searching, you can find them on the open market, often marked as "experimental" or "test-only" products. And there are plenty of "service providers" willing to help malware hackers turn their ill-gotten gains into hard cash.

DOING BUSINESS UNDER SIEGE

Today's malware poses a huge challenge to computer security vendors. Simple encrypted malware programs have evolved into polymorphic code using millions of pseudo-random encryption keys. In turn, polymorphic code has evolved into metamorphic malware, which rearranges its own code on the fly, even recompiling the code for each new victim.

Many botnets essentially generate new-looking malware for each new victim. The spam or phishing email enticing the user contains a Web link that is unique for that one victim. The malware sent to the victim never existed before and will never exist again; each resulting malicious program is a one-off. Why send a signature to the antivirus companies if the program will never exist again? Instead, antimalware vendors do their best to detect variants as part of malware families based upon common characteristics.

Trojan malware is frequently packed (similar to file archiving using Pkzip) and written in foreign-language character sets using HTML encoding and obfuscation. The malware files are often zipped into password-protected files to bypass network scanners on the way in and use SSL/TLS tunnels over TCP port 443 on the way out to escape network inspection.

When antimalware companies proactively scan for malware on the Internet, the bad guys block their scans. They pass around an updated whitelist of IP addresses and domains known to be owned and used by the malware companies. Infected Websites may present only the malware-formed page containing the malicious JavaScript redirect once every 50 visits – or present the original, uncompromised pages when the owner or antimalware company visits. The captured malware often has anti-debugging mechanisms to frustrate antimalware vendor investigation.

TOO MUCH MALWARE TO DETECT

When tens of millions of new malware programs are created each year, antimalware vendors are going to have an

accuracy problem. Dozens of scanners are 100 percent accurate in detecting days-old malware, but that level of perfection can't be achieved with brand-new, just-created malware. Check out the [statistics at VirusTotal](#) – they show that only a very small percentage of confirmed malware programs submitted over the latest 24-hour period is detected by all antimalware engines.

The Website [AV-Test](#) did an interesting [test in December 2009](#), in which brand-new malware programs were presented to multiple participating antimalware products. The average product was 70 to 90 percent effective. The best products detected malware 98 percent of the time and blocked it 95 percent of the time. These stats may sound good – until you realize that out of 100 users in your network, at least two of them will encounter a malware program that is not detected as malicious. Now multiply that by the size of your user base over time.

BREAKING IN THROUGH THE FRONT DOOR

In the past, most professional attackers tried to break into companies through Websites and database servers. Those assets now tend to reside on the most heavily protected computers in any environment. They are protected by firewalls and intrusion detection systems, they undergo code reviews, and they are widely audited for suspicious activity.

Today, attackers simply wait for any employee to install a Trojan horse program, and in an instant, the attacker is past all the locked doors, passwords, and firewalls. Because the attacker is now running in the security context of an authenticated and authorized user, it is doubly difficult for the computer security team to detect suspicious activities.

It gets worse. Even though cyber attackers steal tens of millions of dollars almost every day, almost none of them get caught. Certainly the biggest cyber criminals, including crimeware conglomerates such as the [Russian Business Network](#), haven't been arrested, and aren't likely to be in the near future. They often operate in countries without appropriate cyber laws, with weak enforcement, or with the tacit (sometimes paid-off) approval of the very policing agencies that are sworn to prevent them.

Rob a bank with a gun and you make off with a few thousand dollars and invite the very real risk of going to prison for a significant part of your life. Rob a million



dollars from the same bank using banking Trojans and you face almost zero chance of getting caught or prosecuted. It's easy to see why felons, including organized crime, have moved to the Internet.

THE BEST DEFENSES

With the exponential rise in malware and the self-reinforcing dynamics of criminal Internet enterprises, it may seem as if there's nothing we can do to protect ourselves. Quite the contrary: You can do a lot to minimize the risk of malware infection. The following defenses are listed in the order most likely to reduce security risks from the threat of malware.

EDUCATE END-USERS

Forewarned is forearmed. Most malware requires users to agree to download something to their computer. In an age when browsers, operating systems, and yes, antivirus programs continually prompt users to install updates, the habit of consenting to download and install code can be hard to break. Users must learn the difference between updates and other legitimate downloads and Trojans that prompt users to say Yes, not just on dicey Websites, but on trusted hangouts. Unfortunately, all it takes to infect a network is one user who didn't get the message.

APPLICATION CONTROL

Application control (also known as whitelisting) makes a lot of sense in a world where there are more malware programs than legitimate programs. Antimalware scanners are essentially blacklisting programs, telling you what you shouldn't run or download. Application control programs do the opposite: They allow administrators to define what programs should be allowed to run and block everything else. If implemented correctly, a whitelisting program can significantly minimize the security risks of malware.

Implementing application control programs takes a lot of hard work initially. Administrators must create one or more baseline images, create acceptable whitelist program lists (most application control programs help with this process), and implement whitelisting enforcement. Any good application control program requires that administrators respond aggressively to requests for new programs. Of course, most users don't want to give

up the freedom to run anything they want when they want to. And most senior managers don't want to take away that freedom.

RUN UP-TO-DATE ANTIMALWARE PROGRAMS

Antimalware defenses still have vital roles to play, from antivirus scanners to firewalls to intrusion detection systems to spam and phishing filters. Antivirus programs scan for more than viruses these days; just be sure to choose an antivirus vendor with sustained accuracy and a feature set and performance point that work for you. Antimalware programs may not be perfect, but they still give us the best chance of detecting and blocking malware that we have today.

DON'T LOG IN AS ADMIN OR ROOT BY DEFAULT

Malware writers depend on regular end-users running Internet browsers and email programs in elevated contexts. Over the past two decades, it has been common for all users to run as admin or root on their computer, a fact that hackers still love to exploit.

If you run Microsoft Windows, have at least two logon accounts, one elevated and one nonelevated. Logon as the elevated account only when needed (to install programs or make system-wide changes). If you're running Windows Vista or later, at least use User Account Control (UAC). UAC will de-elevate privileged users by default and prompt them for a password or approval acknowledgement to run in their original elevated security context. If you're running Mac OS X, Linux, Unix, or BSD, make sure you're not logged in as root for nonelevated tasks. Use Su or Sudo when you need to run in an elevated context. While running in nonelevated contexts will not prevent all malware, it does prevent most of it from working (at least until malware writers come up with new tricks).

STAY FULLY PATCHED

Make sure all programs, including the OS, all applications, and browser add-ons, are fully security patched. Running the latest versions helps, too, because they always have security features earlier versions lacked. Most people are good at keeping their operating system patched and up to date, but not as careful to keep browser add-ons patched. Again, hackers exploit this laxity, and malware watchers



see a significant increase in malformed media files containing malicious content. Go with programs that include “auto-updaters” where possible for individual users and small companies. Use enterprise patch management systems for larger enterprises. You can also find free services on the Internet that offer free patch scanning and tools to help keep any system up to date.

USE SECURE DEFAULTS

All operating system and application software should have safe and secure defaults. Nearly every vendor’s product is under attack these days, so most vendors ship their products with a reasonable level of security. In many hacking cases, the malware programs were successful only because users accidentally (or intentionally) lowered the security of their program without realizing the consequences.

When in doubt, contact the vendor for security advice. Several organizations, such as [NIST.gov](#) and [The Center for Internet Security](#), offer excellent security guides for dozens of operating systems and devices.

USE MALWARE-AWARE SEARCH ENGINES

Use search engines that contain antimalware abilities (such as Google, Yahoo, and Bing). Malicious hackers expend a great deal of effort to “poison” search engine results, often by planting malicious Websites with a high number of popular keyword searches; they may even attempt to advertise on the search engine’s Website to snag unsuspecting customers. Today’s best search engines contain malware detection routines that have a decent (although not perfect) chance of detecting Web pages with malicious content. When the search engine detects a potentially malicious page, it will warn the user or block the link in the reported search results.

USE BROWSERS WITH ANTIMALWARE CHECKERS

Most of today’s popular browsers include antimalware checking routines. In most cases, the vendor has an active program that blacklists reported and confirmed malicious sites. When a user visits a new Website, the browser contacts the vendor’s antimalware link database to see if the intended Website is confirmed as hosting malware. The check normally lengthens browsing to a new Website by 0.5 to 2 seconds. Some people find this additional wait unacceptable and others hardly notice it.

If the site is confirmed to contain malware, the user is warned and the link blocked (at least initially). Like the malware detection capabilities of search engines, the antimalware detection functionality in browsers is not extremely accurate. Nonetheless, using a browser with antimalware detection capabilities is yet another defense that can be deployed for no additional cost.

LOOK FOR UNUSUAL NETWORK TRAFFIC PATTERNS

IT administrators should be on the lookout for unusual traffic patterns. Attackers on a network are almost certainly going to try to pull down large amounts of valuable data. Large, unexpected transfers, workstation-to-workstation traffic, or unexpected server-to-server communications should always be investigated.

TURN ON AND MONITOR YOUR LOGS

A top tool for detecting malicious activities is the humble log file. Most admins don’t turn them on, and those who do frequently don’t monitor them. Those who turn on logging typically do so only on their servers, even though most malicious break-ins occur on user workstations. [Verizon’s Data Breach Investigations Report](#), which is quickly becoming one of the most respected sources on computer crime statistics, said it best in its 2008 edition:

Evidence of events leading up to 82 percent of data breaches was available to the organization prior to actual compromise. Regardless of the particular type of event monitoring in use, the result was the same: information regarding the attack was neither noticed nor acted upon.

Every company should enable an enterprise-wide log management plan. See InfoWorld’s [Log Analysis Deep Dive Report](#) for more details.

PHISH YOUR OWN USERS

Since end-users are the weakest link on any network, here’s one quick way to deliver a lot of education value: Create a phishing campaign outside your company and phish your own users. The phishing email should be realistic enough to fool some users, but not perfect enough that all users are fooled. You want to find out which of your users would fall for least creative stuff, and when



they do fall (that is, respond to the phish), you can single them out for additional education. Some companies may even want to simulate sophisticated targeted spear phishing attacks against senior management (with the appropriate approvals, of course). The idea is become innovative with your end-user education and get employees thinking about what they should and shouldn't do.

USE HONEYPOTS

Honeypots give you a realistic view of what's going on in the wild. All you need to do is take a computer you're getting ready to throw away and place it in a strategic spot in the environment that might invite hackers. The honeypot's only job is to report any attempted logons. A honeypot, by definition, is a fake computer asset. Nobody should be trying to logon to it, and if they do, you want to capture the originating IP address and investigate. Honeypots make excellent, cheap, low-noise, early-warning systems.

ROOT CAUSE ANALYSIS

If you find an exploited computer, it will ultimately have to be reformatted and completely rebuilt. In today's sophisticated malware world, you can't be sure what the remote attacker has done to the compromised computer. But before you clean the machine, do a quick analysis and see if you can find out how the attacker initially compromised it. Once you've learned how it happened, you can examine your current policies and procedures to see if adjustments (or end-user education) can be made to minimize future risk.

Today's malware is no longer fun and games. It's a set of tools created by criminals out to steal your money or your company's money. Educate your end users about today's most common threats and invest in technologies that provide appropriate defense and analysis. If you don't, you're putting your data and quite possibly your job at risk. 