



SECURITY
dark READING
Protect The Business  Enable Access

May 26, 2011

The Top Three Malware-Based Threats To Small And Midsize Businesses

By Ericka Chickowski, Contributing Writer, [Darkreading](#)

<http://www.darkreading.com/smb-security/167901073/security/application-security/229700056/the-top-three-malware-based-threats-to-small-and-midsize-businesses.html>

SMBs wrestle to handle Zeus Attacks, website infections, and business-logic vulnerabilities

With more valuable data than consumers and far fewer security defenses than their large enterprise counterparts, small and midsize businesses have become a favorite target of malware authors around the world.

“SMBs have a hard challenge,” says Neil Daswani, CTO of Dasient, an anti-malware services vendor. “Their customers often expect the security guarantees that a large company would give them, but SMBs typically don’t have the infrastructure of their own to provide that level of security.”

Whether their computers are being controlled by botnets, their information is being stolen through a Trojan kit, their websites are infecting customers with malware, or their Web application flaws are being exploited to steal products, SMBs face malware-related attacks from all corners. Let’s look at three of the biggest threats coming from malicious code and how SMBs are dealing with them.

1. Zeus Attack Tool Kit

Preconstructed attack software, such as the dreaded Zeus toolkit, has revolutionized the cybercrime “industry,” experts say.

“Attack toolkits have lowered the bar so that anybody with even a limited amount of technical skills can get in the game -- and [these toolkits are] certainly driving the vast amount of malware that we’re seeing today,” says Kevin Haley, director of Symantec Security Technology and Response.

No kit has caused as much damage as the Zeus toolkit, says Chet Wisiniewski, senior security adviser at Sophos, who says Zeus-based attacks have been one of the biggest threats to small businesses during the past two years. That threat is only going to get

larger now that the source code to this kit was leaked, effectively turning it from a crimeware package costing \$400 to \$5000 into a freeware offering.

“In particular, small businesses are targeted specifically by this because Zeus was built to harvest banking credentials -- and what the bad guys have figured out is that small businesses are the perfect victims,” Wisniewski says. “If they go after you or me, one, we have less money, and, two, we have 30 days with our bank to reverse the fraudulent activity.”

That’s not so with SMBs, which usually have only 48 hours. “That’s a problem for small businesses because most people aren’t watching every transaction like a hawk like that,” Wisiniewski says.

Installing antivirus software is the first step to protecting an SMB from Zeus attacks, but that’s only a start, experts warn.

“Having good spam filtering not only reduces the annoyance of your mailbox filling up, but can also shrink your attack surface because if the email doesn’t show up in your mailbox, it doesn’t matter if you have a tendency to click on things you shouldn’t or not,” Haley says. Organizations should start limiting employees’ access to corporate banking account information, reducing the chance that they’ll give it away to social engineers, he advises.

Additionally, SMBs should be practicing good patching hygiene and doing a better job of inspecting the content that crosses their endpoints, experts say.

“And don’t focus only on patching the operating system and the Web browser -- look at browser plug-ins such as Java and Adobe Reader. These are the top two outdated components that are targeted by attackers,” says Michael Sutton, vice president of security research for Zscaler.

“Leverage inline solutions that can inspect content,” Sutton advises. “These solutions do not have to be expensive. Thanks to SaaS-based solutions, there are offerings available that are paid on a per-user basis and are available to all companies at an affordable price, regardless of size.”

Next: Unwitting malware distributors.

2. Serving Up Malware

As hacking-for-profit has evolved during the past few years, criminals have learned that SMBs are not only great victims of fraud -- they’re also perfect partners in crime. Not to their knowledge, of course.

“One of the things hackers want to do is have more bots in their network to use those PCs for their needs,” says David Koretz, CEO of Mykonos Software. “But it takes a long time to infect computers one by one. It’s a lot faster if you can take over someone’s website

that gets a bunch of traffic and use that as a tool to distribute malware. So a lot of e-commerce companies and small businesses are becoming malware distribution points unknowingly.”

These small business sites -- unknowingly moonlighting as malware distributors -- are usually infected through SQL injection attacks, says Wisniewski.

“[SQL injection is] a method of injecting database instructions into your website and finding a flaw that allows it to talk to your database directly -- and either extract the data that is in there or inject malicious code into the data so that if people visit your site, they get infected,” Wisniewski says. “Both of those things are typically caused by not having the software patched on the server.”

Patching is important no matter what kind of Web software or server equipment you have and no matter who’s administering it, experts say. Too often, SMBs are left vulnerable because they think someone else is taking care of their software updates.

“Make sure, if you’re not running your own server, that your ISP or whomever is scanning that server regularly looking to see if you’ve been compromised -- patching, looking for malware, and otherwise making sure you’re not hosting bad stuff,” Wisniewski recommends. “And if you run servers in-house, don’t just hire a local IT consultant one time to set it and forget it. You should have them come in once a month -- or whatever you can afford -- to make sure it is patched and up to date and is not hosting content that could harm your customers.”

Don’t let hubris get in the way of taking proper precautions when you’re working with Linux-based machines, Wisniewski warns.

“The Linux guys tend to think, ‘Ha! We’re immune!’,” he observes. “But the problem is that, since these guys aren’t running antivirus software, they don’t know they’ve got Windows viruses stored on their Web server -- and every customer visiting them is getting hosted up.”

3. Business Logic Flaws

While Web code vulnerabilities can help crooks infect an SMB site, flaws in Web applications meant for commerce can give criminals a way to steal products.

According to Koretz, such attacks happen all the time. In some cases, Mykonos has discovered flaws in the way customers’ Web applications accept orders that would allow hackers to send tens of thousands of dollars’ worth of orders without ever paying for them.

“If I were a small business, the priority I would be most concerned about is thinking about what happens when I unknowingly didn’t secure my website -- and my e-commerce site is leaking out revenue,” Koretz says. “By the time I realize it, I’m out of business.” In today’s business environment, SMBs might experience compromises before

ever realizing it because so many online retailers depend on partners to do their order fulfillment.

“Assume for a second that you’ve got an e-commerce site where you manage fulfillment -- if you see a huge order come in and you don’t validate the payment, you don’t ship it,” Koretz explains. “But all of a sudden, if you take away that variable where you’re no longer controlling the shipping, you could ship out a quarter of a million dollars before you know it.”

Such so-called business logic flaws are a difficult nut to crack because, unlike the standard Web vulnerabilities, there aren’t any automated ways to test for them. That’s why tests need to be thorough and creative, experts say. A good source to start with for advice is [The Open Web Application Security Project \(OWASP\)](#), which has written considerably about these issues during the past few years.

“Testing for business logic flaws in a multifunctional dynamic Web application requires thinking in unconventional ways,” says the OWASP testing guide. “If an application’s authentication mechanism is developed with the intention of performing steps 1,2,3 in order to authenticate, what happens if you go from step 1 straight to step 3?”

“In this simplistic example, does the application provide access by failing open, deny access, or just error out with a 500 message?” the testing guide asks. “There are many examples that can be made, but the one constant lesson is ‘think outside of conventional wisdom.’”