GCN
GOVERNMENT COMPUTER NEWS

Malware's tangled roots

08/21/06
By Patience Wait,

Identifying the source of cyber intrusions is a complicated task

The federal government's computer networks are, collectively, the single largest target in the world.

And within the government, Defense Department systems are the most aggressively pinged—the Global Information Grid, the military's primary electronic conduit for secure and unclassified network traffic, gets scanned millions of times a day.

Of even greater concern than the volume of attacks is their origin. Of the attacks not originating from the United States, the attempted intrusions come from China and other countries that are, if not exactly enemies, fierce competitors.

Webroot Software Inc. of Mountain View, Calif., issues a quarterly report on the geographic launch points of several classes of malware, such as worms, viruses, Trojan horses and key loggers, fired against systems all over the world.

The company currently does not cross-reference attacks with their targets, so there is no way to track the geographic source of attacks against DOD. But as the largest target, DOD more than likely is bearing the brunt of these international raids.

China offensive

And the source of the attacks is shifting. Historically, the largest numbers have come from within the United States. But the percentage of domestic-based attacks has been dropping, and in the first quarter of this year, China-based sites became the single largest source, continuing a trend. In the fourth quarter of 2005, China was second in volume, behind the United States; in the third quarter, China was third, behind the U.S. and the Russian Federation, according to Webroot.

"My sense is there are times that they [China] retrench, they regroup, then get ready for a new attack," said David Moll, Webroot's chief executive officer.

By contrast, attacks from the Russian Federation have been dropping—from 17.5 percent in the third quarter, to almost 4 percent in the fourth quarter, to just under 2 percent in the first quarter of this year.

Gerhard Eschelbeck, Webroot's chief technology officer, is quick to point out that tracing malware back to a server in a particular geographical location does not necessarily mean it was launched from that country, only that security measures may be lax there.

But Lt. Gen. Michael Maples, director of the Defense Intelligence Agency, said in a written statement to the Senate Armed Services Committee in February that nation-states represent the biggest threat to U.S. national security.

"The Chinese PLA [People's Liberation Army], for instance, is striving toward a[n] ... information warfare capability. Many other nations are using computer network operations for intelligence collection," he said. "Over the last few years, hackers have exploited thousands of DOD systems. Attribution has remained elusive with identities established in only a few cases."

But there are clues contained in malware that might uncover their real origins. Companies in the business of protecting IT systems have looked at thousands of unique viruses, worms, Trojan horses and key loggers, and have seen these clues.

"You can kind of tell when an engineer graduated from college or who they studied by the way they write their code," said David Minton, chief scientist at Planning Systems Inc. of Reston, Va., and chief engineer of the Worldwide Consortium for the Grid, an initiative sponsored by the Office of the Secretary of Defense. "You can tell what kinds of things they learned by how they solved their problems."

Chet Hosmer, chief executive officer and chief scientist of WetStone Technologies of Cortland, N.Y., said that nation- states are likely behind the creation of some of the most sophisticated malware, because of the resources needed to create them.

Garden-variety hackers aren't likely to have the funds or equipment to test a piece of malware across multiple operating systems and platforms.

"It is very difficult for an individual hacker to broadly experiment with a sophisticated, propagating piece of malware, because literally to do that you have to have thousands or tens of thousands of computers running in a network in order to test the weapon," he said. "So when worms or other malicious code are released that run very, very well in the Internet environment, that presumes there was a lot of testing."

He said testing malicious code by using the Internet itself would be a way around this problem, but it also would expose the hackers' methods and intent.

"One thing you're looking for is ... sophistication," Hosmer said, "what kinds of tools and technologies were used to write it, the structure and flow of the program. ... Those are

relatively easy things to define."

A second pointer to a piece of malware's origins, he said, is if it uses a component that has been found in other programs, whether it's a specific program structure, a particular attack approach, or the countermeasures built into the malware to evade detection.

A January 2005 unclassified U.S. government report obtained by GCN addressed the growth of a market for software "wrappers" in China—software to provide a shell around malicious code such as a Trojan horse to help disguise it and enable better penetration into systems.

"Most of the wrapper programs available on Chinese-language Web sites are Chinese versions of wrapper programs that are widely available elsewhere," the report concluded, but this "does not necessarily indicate an overall lack of sophistication on the part of Chinese hackers. There is a trend of the increasing use of wrappers in hacking or at least interest among hacker communities. One information security expert noted that there is discussion on [Internet relay chat] channels of how to use wrappers to evade antivirus software and other products."

Some particularly advanced malware will self-destruct if trapped on a virtual machine, such as a so-called honey pot or honey net. Or the malware may try to destroy the virtual machine itself.

"It has a sense of where it is. It includes software basically designed to evaluate the environment. If the environment appears to be a trap, it will take different actions than if it feels it's running in an unprotected host. That's a pretty significant step forward in the development of malware," Hosmer said.

The goal of self-destruction seems apparent—to avoid digital analysis. Crashing a machine could accomplish that, too, and has the added benefit that "if you crash it, systems administrators and operators may just think they had a system crash, rebuild the network and never know what caused it," Hosmer added.

"They also put mechanisms in place to prevent reverse engineering," Eschelbeck said. "It's a pretty scary environment."