



## **Zero-day: IT's race against the clock**

By: Mari-Len De Guzman

ComputerWorld Canada (11 May 2007)

Zero-day exploits are on the rise, and the vulnerability marketplace as well as improvements in enterprise patch management are deemed contributors to this rising security risk. The SANS Institute noted a significant increase in the number of zero-day exploits last year, landing it in its Top 20 Internet Security Attack Targets for 2006.

In its latest biannual Internet Security Threat Report (ISTR), Symantec Corp. documented 12 zero-day vulnerabilities in the last six months of 2006. This is a huge jump from the previous two ISTR reporting periods, in which only one zero-day vulnerability was documented for each reporting period.

McAfee Inc. also saw an "ever-increasing number of zero-day attacks" particularly targeting Microsoft Office applications, according to the company's latest Sage report, a security journal published by McAfee's Avert Labs.

Zero-day vulnerability is a flaw in an operating system or application for which there is no known vendor fix, leaving systems wide open for an attack. Zero-day exploits are actual codes developed by hackers to take advantage of a zero-day vulnerability.

One such exploit surfaced recently as a result of a vulnerability discovered in the Windows Animated Cursor (.ANI). Exploits began surfacing on the Internet last March, prompting Microsoft to issue an out-of-cycle patch, but not before the exploits have already infected thousands of Windows systems.

Despite the high-profile status accorded to zero-day threats today, experts contend the threat has been around for several years. With attack motivations shifting from bragging rights to financial gains, however, zero-day threats have become more critical for its potential as a vehicle for data theft.

### Flaws for sale

It has become easier for attackers to get their hands on newly discovered vulnerabilities or exploits thanks to the market that's been created for buying and selling these codes, says Dean Turner, senior manager, Symantec Security Response Team in Cupertino, Calif.

Some security research companies, such as iDefense Labs and Tipping Point, have vulnerability compensation programs that offer remuneration for advanced notification of undisclosed vulnerabilities and exploit codes. The objective, the companies have claimed, is to provide protection for their customers.

Some security practitioners argue that paying for vulnerabilities creates an underground economy for vulnerability and exploit trade, where a critical flaw or exploit may end up in the hands of malicious attackers. Turner says it's already happening.

"Zero-day vulnerability could be worth a lot of money. If I am a bad guy and I have found a vulnerability in a particular piece of software, I can either go to the (legitimate) company and get \$100 to report it to them, but I know that there is an adware group in some country that's willing to pay me \$10,000; if I am a bad guy, who am I going to go with?"

One Canadian IT security executive, however, notes that while the risk does exist, compensation-based vulnerability disclosure is a good way to enhance overall security. There will always be a percentage of people who would take advantage of a flaw for malicious reasons, but the majority of security researchers and software developers want to increase the level of security, says Eugene Ng, vice-president of technical services, NCI Secured Intelligence in Mississauga, Ont.

"There's always a risk but I think it's a worthwhile approach," says Ng.

#### Patch improvements

In addition to the vulnerability market place, improvements to patch management systems lead hackers to turn to zero-day exploits, says Alexander Sotirov, chief reverse engineer, Determina Inc., provider of vulnerability protection solutions in Redwood City, Calif.

Because organizations are now better equipped to keep patches up to date, zero-day exploits give attackers a way to gain access to a network, he says.

"Zero-day vulnerabilities give attackers the advantage of time," says Sotirov, citing the .ANI exploit as an example. Sotirov discovered the .ANI flaw last year, and says he informed Microsoft as early as last December.

#### Beware of unofficial patches

Whenever a critical zero-day vulnerability is disclosed, IT security managers are on edge – fearing a security attack that can happen any moment as they anxiously await the necessary fix from the vendor.

Creating a patch for a specific vulnerability typically takes a long process of rigorous testing and quality assurance, says Alexander Sotirov, chief reverse engineer at Determina Inc. This explains why, despite having known of the .ANI flaw since December, Microsoft took months to release a patch for it, he explains.

For very critical zero-day vulnerabilities, third-party security firms would in some cases make available, free of charge, unofficial patches or workarounds as a stopgap measure to administrators and end-users, while they wait for the vendor fix.

"Third-party patches are a way to let the end-users make their own choice about what their level of risk tolerance is," says Sotirov.

One IT security analyst warns administrators should exercise extreme caution before using a third-party patch.

One downside to unofficial fixes is that the third-party developer does not have the depth of knowledge about the vulnerable code as its original producer, explains Chenxi Wang, principal analyst at Forrester Research Inc.

"You wouldn't want any run-of-the-mill car repair shop to fix your BMW; the same reason applies here," Wang says. Unofficial patches, she adds, may cause disruptions in other parts of the system or introduce other vulnerabilities.

There have been instances in the past where deploying an unofficial patch caused functionality crashes and created a whole new vulnerability, according to Dean Turner, senior manager for Symantec Security Response Team.

Deciding whether to install unofficial patches from third-party developers often boils down to determining how critical the vulnerability is and how much risk a particular organization is willing to take, Turner adds. "If you have the ability to lock down that particular platform and isolate it, it may be in your best interest to wait for the appropriate patch."

Copyright © 2007  
ITworldcanada.com