August 21, 2012, 10:36PM

Crisis Trojan Makes Its Way onto Virtual Machines (/en_us/blogs/crisis-trojan-makes-its-way-virtual-machines-082112)

by **Anne Saita** (/author/Anne Saita)

The Windows version of the Crisis Trojan is able to sneak onto VMware implementations, making it possibly the first malware to target such virtual machines. It also has found a way to spread to Windows Mobile devices.

"Many threats will terminate themselves when they find a virtual machine monitoring application, such as VMware, to avoid being analyzed, so this may be the next leap forward for malware authors," wrote Takashi Katsuki of Symantec in a blog post (http://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines) .

Samples of Crisis, also called Morcut, were first discovered about a month ago targeting Mac machines running various versions of OS X. The Trojan spies on users by intercepting e-mail and instant messenger exchanges and eavesdropping on webcam conversations. Launching as a Java archive (JAR) file made to look like an Adobe Flash Installer, Crisis scans an infected machine and drops an OS-specific executable to open a backdoor and monitor activity.

Editor's Pick

Report: Bandwith-Burning Malware Among Biggest Consumer Threats (/en_us/blogs/report-bandwith-burning-malware-among-biggest-consumer-threats-071912)

Trojan Mimics Chrome Installer to Steal Banking Information (/en_us/blogs/trojan-mimics-chrome-installer-steal-banking-information-051612)

Travelers Cautioned When Using Hotel Internet

This week, researchers also discovered W32.Crisis was capable of infecting VMware virtual machines and Windows Mobile devices.

"The threat searches for a VMware virtual machine image on the compromised computer and, if it finds an image, it mounts the image and then copies itself onto the image by using a VMware Player tool," Katsuki said.

He cautioned that Crisis/Morcut does not exploit a vulnerability in VMware specifically; instead, it takes advantage of a characteristic of all virtualization sofware that stores as local files on a host machine. These files are then subject to manipulation, even when the virtual machine isn't running.

In addition, Katsuki said the malware can spread to Windows Mobile devices connected to compromised Windows computers through the Remote Application Programming Interface.

Connections Abroad (/en_us/blogs/travelers-cautioned-when-using-hotel-internet-connections-abroad-050812)

Threatpost Newsletter Sign-up (/en_us/node/1690)

While earlier versions of Crisis targeted activists, such as a Moroccan journalist tied to the Arab Spring, the newest discovery suggests attackers are aiming their exploits at the security-conscious who like to do sensitive transactions such as online banking or malware research using virtual machines running from a clean installation.

"What this Crisis variant does is, when it's run on a Windows system, it will mount all those virtual drive images that you created and then it will make a copy to that operating system within your operating system. It's as if they were a physical drive like a thumb drive, and the malware will copy itself to the drive. So when an infected user tries to access those images again, the malware will be spying on them without them being aware," wrote Lysa Myers Tuesday on Intego's Mac Security Blog (http://www.intego.com/mac-security-blog/new-crisis-behavior-observed-now-infecting-virtual-machines/) . The company, along with Kaspersky Labs, is credited with first discovering the Mac malware.

"In order for this to happen, you have to be running the malware (initially) outside of a virtual machine," she continued. "It's not going to escape from one virtual machine directly into other images. So this does not invalidate the usefulness of virtual machines if you're using VMWare in a security research environment. This just means that this malware can be that much harder to find and eradicate on infected machines, especially if you don't make a habit of scanning your virtual machines like you would your physical machine."

Commenting on this Article will be automatically closed on November 21, 2012.

Comments

Post new comment

Your name:

Anonymous

E-mail:

The content of this field is kept private and will not be shown publicly.

Comment: *

(#)

Path: p (javascript:;) (javasc

Save Preview