Malware can take ugly leap forward to virtual machines

August 23 2012, by Nancy Owano

(Phys.org) -- A piece of malware categorized as a malicious rootkit can spread via an installer disguised as an Adobe Flash Player installer and is capable of spreading to four different platform environments, including Windows, Mac OSX, VMware virtual machines, and Windows Mobile devices. The news this week is that the malware, dubbed Crisis, not only affects Macs, as originally assumed, but these other systems as well. The discovery is an example of expert security companies building on each other's efforts.

In July, security sleuths got the ball rolling in reporting that there was a Mac Trojan, dubbed Crisis, intercepting e-mails and tracking web sites. Kaspersky Lab said that it arrives on a compromised computer through a JAR file by using social engineering techniques. Symantec said it was beyond Mac and targeting Windows users. They saw executable files for more than one operating system.

For those who follow the well beaten path of tricks that malware authors use to lure victims, it all sounds too familiar. There they are again, the two words, Adobe Flash. Crisis is distributed using social engineering techniques designed to trick users into installing a Java archive file masquerading as an Adobe Flash installer. It makes itself look like the installer and proceeds to deliver a corresponding JAR file to infect the system.

But there is something not at all familiar, rather, annoyingly new. “This may be the first malware that attempts to spread onto a virtual machine," said Takashi Katsuki, a researcher with Symantec.

He thinks of it as a very unwelcome leap forward. Malware threats in the past tend to terminate themselves when they find a virtual machine monitoring application, such as VMware, to avoid being analyzed. Instead, this time, the malware authors have embraced VMware. Crisis can look for a VMware virtual machine image on the compromised computer and, finding it, the malware copies itself onto the image using the VMware Player tool.

The VMware Player tool allows multiple operating systems to run on the same computer. “VMware Player is the easiest way to run multiple operating systems at the same time on your PC,” according to the company’s site. “With its user-friendly interface, VMware Player makes it effortless for anyone to try out Windows 8 developer release, Windows 7, Chrome OS or the latest Linux releases, or create isolated

virtual machines to safely test new software and surf the Web."

According to Symantec, though, Crisis does not leverage any vulnerability in VMware's software itself but merely takes advantage of an attribute of all virtualization software, that the virtual machine is a file or files on the disk of the host machine.

The Windows version of Crisis can spread to Windows Mobile devices connected to compromised computers by installing a module on the device. Android and iOS devices are not affected.

In sum, the malware can sneak into a VMware virtual machine and drop modules onto a Windows Mobile device using Remote Application Programming Interface.

Its payback includes an ability to record Skype conversations, monitor instant messaging programs and track websites visited in Firefox or Safari.

Kaspersky Lab's assessment has been that this is no work of amateurs. Sergey Golovanov, in a July posting, found the modules were written professionally and, "from the code we can see that the cybercriminals developed this Trojan in order to sell it on hacker forums."

Similarly, Intego, an antivirus software company, pegged Crisis as "a very advanced and fully-functional threat," and noted that some of the malware's code originated with commercial spying software.

Symantec said the malware has infected less than 50 machines.

More information: www.symantec.com/connect/blogs … aks-virtual-machines