Crisis for Windows Sneaks onto Virtual Machines

1 Recommend

Aug 20, 2012 05:37 PM

Migration User

Symantec reported new malware for Mac last month that we called OSX.Crisis. Kaspersky then reported that it arrives on the compromised computer through a JAR file by using social engineering techniques.

The JAR file contains two executable files for both Mac and Windows. It checks the compromised computer's OS and drops the suitable executable file. Both these executable files open a back door on the compromised computer. However, we found two special functions in the Windows version of the threat that Symantec detects as W32.Crisis.

The threat uses three methods to spread itself: one is to copy itself and an autorun.inf file to a removable disk drive, another is to sneak onto a VMware virtual machine, and the final method is to drop modules onto a Windows Mobile device.

Figure 1. *How the threat spreads*

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.

Figure 2. *Spreads to VMware*

It does not use a vulnerability in the VMware software itself. It takes advantage of an attribute of all virtualization software: namely that the virtual machine is simply a file or series of files on the disk of the host machine. These files can usually be directly manipulated or mounted, even when the virtual machine is not running as is the case above.

This may be the first malware that attempts to spread onto a virtual machine. 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.

It also has the functionality to spread to Windows Mobile devices by dropping modules onto Windows Mobile devices connected to compromised Windows computers.

Figure 3. *Functionality to spread to Windows Mobile devices*

As it uses the Remote Application Programming Interface (RAPI), it only affects Windows Mobile devices and not Android or iPhone devices. We currently do not have copies of these modules and hence we are looking for them so we can analyze them in greater detail.

Finally, Crisis malware has functionality to spread to four different environments: Mac, Windows, virtual machines, and Windows Mobile. It is an advanced threat not only in function, but also in the way it spreads.

Symantec detects the JAR file as Trojan.Maljava, the threat for Mac as OSX.Crisis, and the threat for Windows as W32.Crisis. Users of our Norton security products are encouraged to update their virus definitions.

0 Files

0 Shares

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.