Symantec™
Security Response

Crisis: The Advanced Malware

Takashi Katsuki
Software Engineer

Contents

Executive summary

Until a few years ago, there were few complex malware created to run on Apple Mac computers. As Mac usage increased, malware for Macs has also increased. For example, in the last year alone we have discovered new Mac malware, including OSX.Flashback, OSX.Imuler, and OSX.Sabpab. Then, more recently, we discovered OSX.Crisis. The Crisis malware is an advanced malware that runs on both Windows and Mac computers, and has information-stealing functionality that includes stealing browser activities and contact lists, as well as the ability to record both audio and visual information from the computer's microphone and webcam respectively.

The features found in this malware suggest that it may have been designed for the purpose of either private investigation or espionage, and are much more advanced than those found in the average information stealing malware. Furthermore, the Windows version of the Crisis malware drops its modules on Windows Mobile devices and also may be the first malware that attempts to spread to virtual machines.

This paper details these advanced features of the Crisis malware as well as the commonalities and differences between the Mac and Windows versions of the malware.

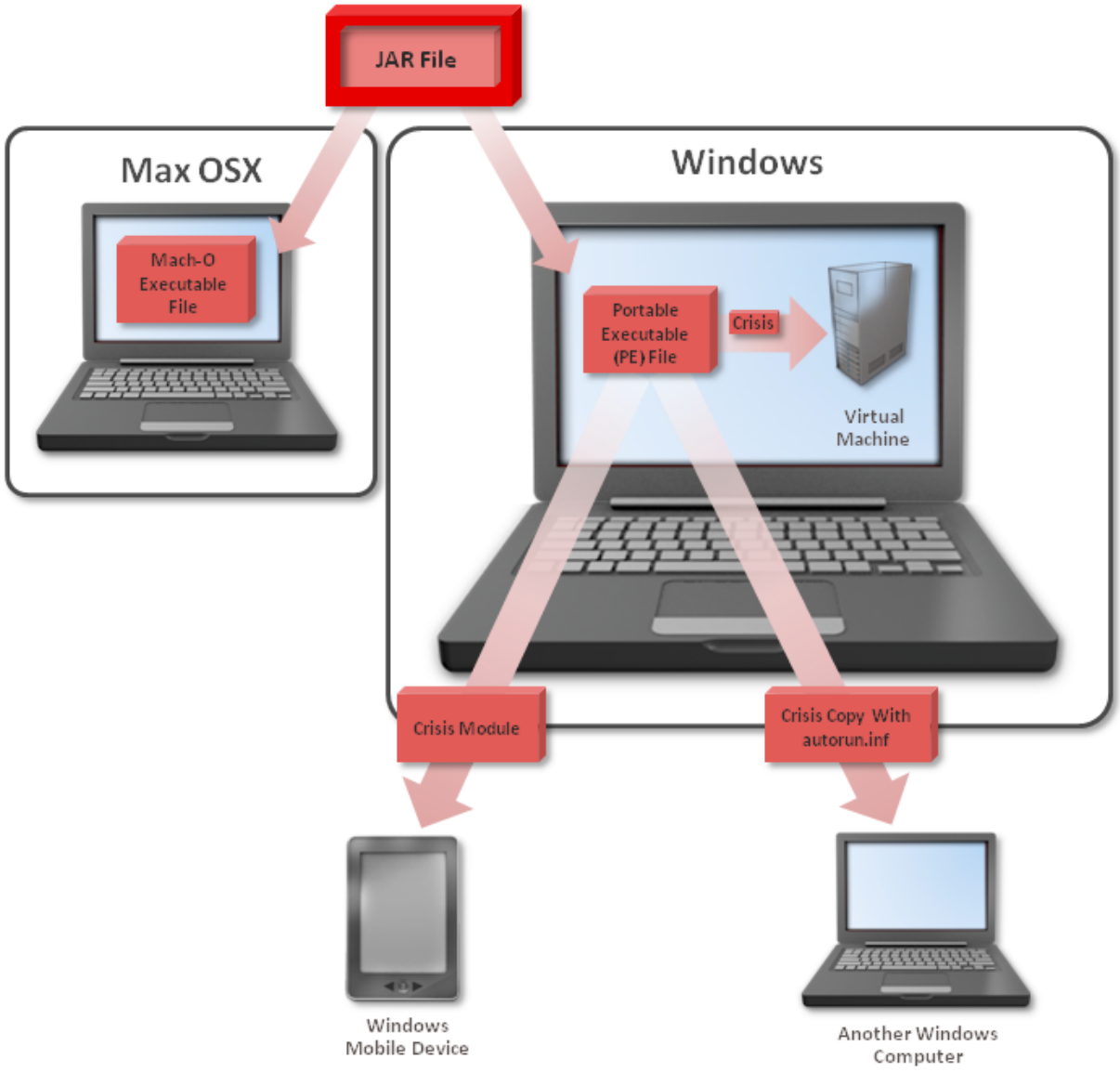
Malware structure

Java applet dropper

A Crisis infection starts from a Java applet. It checks the operating system of the compromised computer and drops an installer suitable for that computer.

Figure 1

Crisis infection technique



The malware does not exploit any vulnerabilities to drop its components but it has a digital signature to create a local file and execute it. We are not aware of the method the malware author uses to make the user load this applet, but it is possible that the author uses social engineering tricks because it does not exploit any vulnerabilities.

Generally speaking, Java applets cannot access local resources, such as the file system, without exploiting a vulnerability, but if it is signed and the user accepts it, it can gain full access to perform any action it wants.

While many threats exploit Java vulnerabilities as the first step of a drive-by-download attack, Crisis does not. It is possible that the Crisis author did not want to take the risk of the malware being detected by antivirus applications as the chances of being detected may increase if it exploits vulnerabilities.

If a malware does not use any vulnerabilities, it can be harder to compromise a computer because the malware needs to use social engineering techniques instead,the success of which is then dependent on the user.

Figure 2

Crisis only runs on Mac and Windows

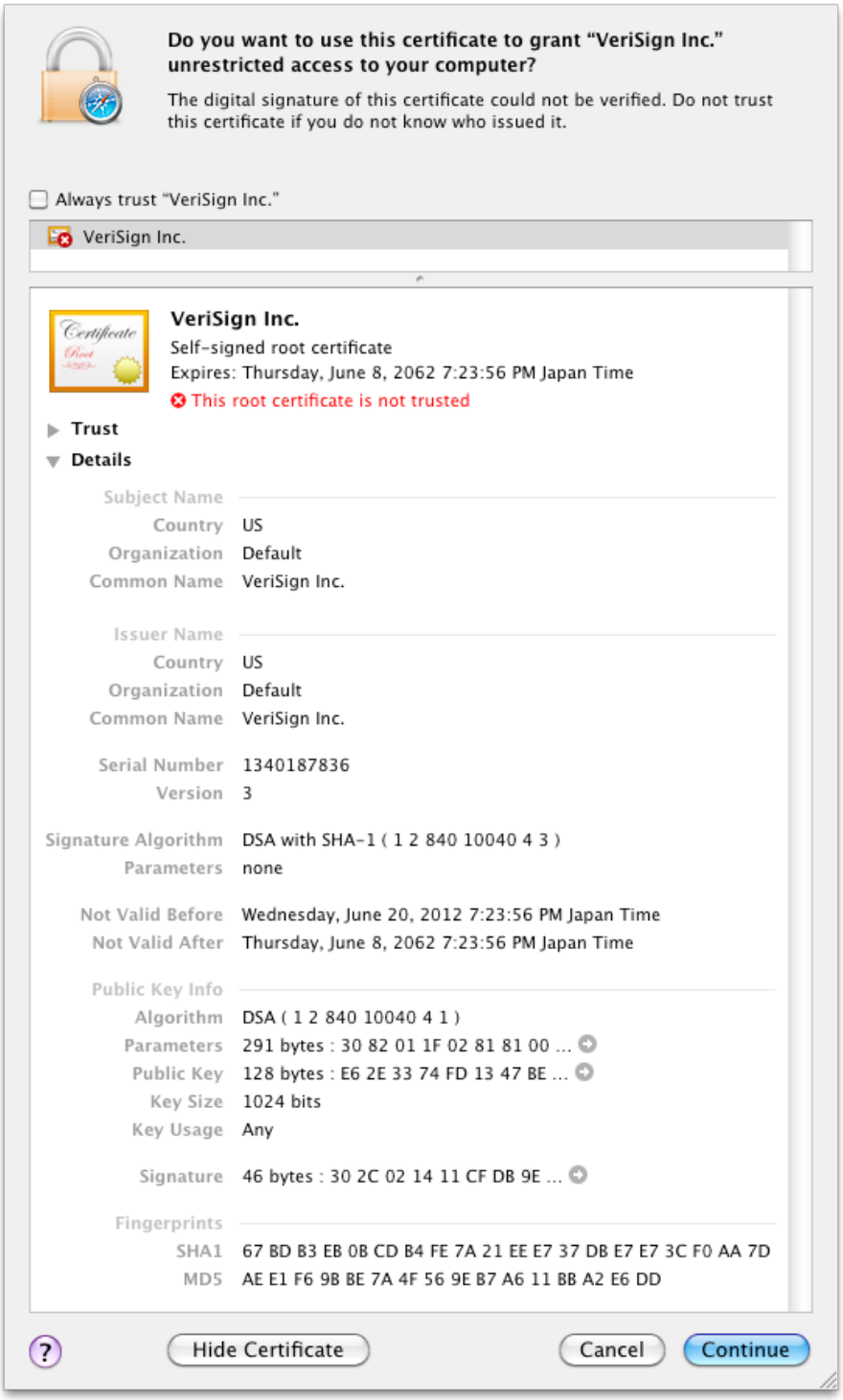
```
if (isWindows())
{
  str2 = str2 + "win";
} else if (isMac())
{
  str2 = str2 + "mac";
} else {
  System.out.println("Unknown operating system, quitting!");
  System.exit(0);
}
```

Figure 3

The message displayed when the applet runs

Figure 4

The certificate does not contain any signer details



Multi platform infection

The Java applet dropper drops only one installer for each platform in a temporary folder and the installer then drops the main components.

Binary file

Tables 1 and 2 show the file name or path of the installed binaries, the file type, and the functions for the respective operating systems.

Windows

Windows binaries are installed under the following path:
%UserProfile%\Local Settings\jlc3V7we

Table 1
Windows binaries

File name or path	File type	Function
6EaqyFfo.zIK	x86_64, executable	Driver
lZsROY7X.-MP	i386, dll	Core module
WeP1xpBU.wA-	i386, executable	Driver
hypn4cql.HSC	i386, dll	Copy of pstorec.dll
lUnsA3Ci.Bz7	i386, dll	Speex module
t2HBeaM5.OUk	x86_64, dll	64-bit process injection

Mac

Mac binaries are installed under the following path:
$HOME\Library\Preferences\jlc3V7we.app

Table 2
Mac binaries

File name or path	File type	Function
lZsROY7X.-MP	i386, executable	Core module
lUnsA3Ci.Bz7	UB(i386, x86_64), dylib	Core module
mWgpX-aI.8Vq	UB(i386, x86_64), executable	XPC module
WeP1xpBU.wA	i386, dylib	Kernel extension
6EaqyFfo.zIK	x86_64, dylib	Kernel extension
Contents/Resources/WeP1xpBU.wA-.kext/Contents/MacOS/WeP1xpBU.wA	Copy of the above file	-
Contents/Resources/6EaqyFfo.zIK.kext/Contents/MacOS/6EaqyFfo.zIK	Copy of the above file	-
$HOME/Library/ScriptingAdditions/appleHID/Contents/MacOS/lUnsA3Ci.Bz7	Copy of the above file	-

Note: UB stands for Universal Binary, which contains multiple binaries for multiple CPUs.

Load point

Crisis attempts to run if the compromised computer is restarted after the malware is installed. The following load points are used by Crisis.

Windows

It creates the following registry entry so that it runs when Windows starts: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"*J7PugHy" = "%System%\rundll32.exe, %UserProfile%\Local Settings\jlc3V7we\IZsROY7X.-MP,F1dd208"

Mac

It uses scripting additions to load itself. The Apple developer site states that, "Scripting additions provide a mechanism for delivery of additional functionality that can be used in AppleScripts. A scripting addition can provide Apple event handling and Apple event data coercion handling." Crisis automatically runs when any application is executed. This is part of the property list file for the scripting additions.

```
<key>OSAXHandlers</key>
<dict>
<key>Events</key>
<dict>
	<key>RCSeload</key>
	<dict>
		<key>Context</key>
		<string>Process</string>
		<key>Handler</key>
		<string>InjectEventHandler</string>
		<key>ThreadSafe</key>
		<false/>
	</dict>
</dict>
</dict>
```

Commonalities

This section introduces the functions that are common in both the Mac and Windows versions of the malware.

Installer obfuscation

Crisis binaries are, for all intents and purposes, neither packed nor obfuscated, although the installer executable is obfuscated. Depending on the operating system of the compromised computer, the appropriate installer is dropped and executed by the Java applet. The purpose of this installer is just to drop another file and execute it.

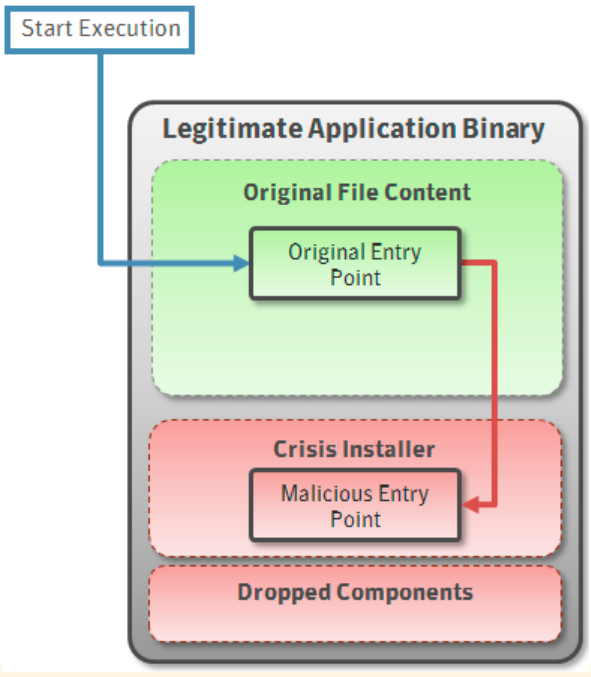
Windows

Currently there are two types of installers for Windows.

The first type is a legitimate file that has been modified. The installer code is appended to the legitimate application and the original entry point is modified in order to launch the appended code. The dropped components are appended to the bottom of the file (Figure 5).

Figure 5

Modified application binary file



One of the samples that we identified was a legitimate SSH client that had been modified to become a Crisis installer. Other samples appeared to be made by the Crisis author from scratch. These samples used a linked Lua library and were packed using UPX.

Mac

The installer for Mac is a little more complex. If you open the installer by using an analysis tool, such as IDA Pro, the code shown in Figure 6 can be seen.

The main function in the section of code in Figure 6 appears to do nothing. However, if you inspect it further, you will see the duplicated entry point (Figure 7).

The true entry point is located in a hidden section and the EIP sets this address by using an LC_UNIXTHREAD load command as usual.

Figure 6

Mac installer code snippet

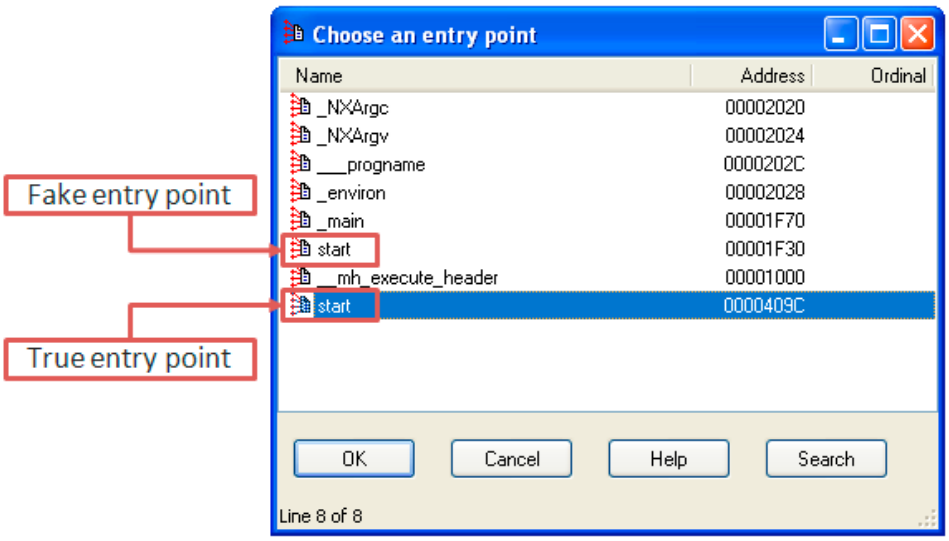
```
                public _main
_main           proc near               ; CODE XREF: start+30↑p

var_8           = dword ptr -8
var_4           = dword ptr -4

                push    ebp
                mov     ebp, esp
                sub     esp, 8
                mov     [ebp+var_8], 0
                mov     eax, [ebp+var_8]
                mov     [ebp+var_4], eax
                mov     eax, [ebp+var_4]
                add     esp, 8
                pop     ebp
                retn
_main           endp
```

```
Load command 11
        cmd LC_UNIXTHREAD
    cmdsize 80
     flavor i386_THREAD_STATE
      count i386_THREAD_STATE_COUNT
    eax 0x00000000 ebx    0x00000000 ecx 0x00000000 edx 0x00000000
    edi 0x00000000 esi    0x00000000 ebp 0x00000000 esp 0x00000000
    ss  0x00000000 eflags 0x00000000 eip 0x0000409c cs  0x00000000
    ds  0x00000000 es     0x00000000 fs  0x00000000 gs  0x00000000
```

All important code is contained within the hidden section, so the Crisis author can easily create new binaries or choose another legitimate application to convert into a new Crisis installer. Effectively, this means that any executable file can be changed into a Crisis installer.

Figure 7

Duplicated entry point



Information stealing

Information stealing is the primary goal of the Crisis malware. It can gather information and data generated by many applications or activities performed on the computer. The collected information is then sent to the remote attacker. Figure 8 illustrates the myriad of functions that are monitored by Crisis.

Figure 8

Monitored functions

Table 3

Details of functions monitored by Crisis

Function	Details
File system	Upload/download files from/onto the compromised computer.
Creating process	Creates a new process and gets the result.
Recording	Audio and video recording using the microphone and the webcam.
Key logging	Records all key strokes that are typed by the user.
Clipboard	Data held in the clipboard.
Screen shot	Takes screen shots.
Wi-Fi	Gets Wi-Fi information, such as SSID and RSSI. This function is called “position” in the Windows version of Crisis, which could be used to determine the location of the compromised computer.
Address book	Steals contact lists.
Browser	Steals Web browser activities.
Instant messenger	Steals instant messenger activities.

All of the functions in Table 3 are common malware activities, which we encounter every day. However, this is the first time that we have seen all of them at once for both the Windows and Mac operating system platforms. Of course, the targeted applications are different between Windows and Mac, as can be seen in Table 4.

Table 4
Targeted applications for each platform

	Windows	Mac
Browser	Internet Explorer Mozilla Firefox Google Chrome Opera	Safari Mozilla Firefox
Contact list	Windows Live Mail Windows Mail Microsoft Outlook Mozilla Thunderbird	Address Book
Instant messenger	Google Talk Skype Yahoo Messenger Trillian	Adium Microsoft Messenger Skype

Table 4 shows that the Crisis malware has been developed with a bias for the Windows operating system rather than Mac due to the much longer list of applications supported in the Windows version. Furthermore, the Windows version of the Crisis malware contains functionality to steal account and password details related to the applications listed, but the Mac version does not have this functionality.

In fact, data relating to almost all activities performed on the compromised computer can be stolen by Crisis, making this an extremely comprehensive malware.

Command-and-Control (C&C) server

All of the Crisis samples that we have analyzed connect to C&C servers located in England using static IP addresses. Both the Crisis for Windows and Mac connect to the same server and the configuration file from the server for both is a JSON file encrypted with AES128.

Interestingly the C&C server is hosted by a well known virtual private server (VPS) service in England. The VPS service is mainly used for Linux virtual machines but the URL used by the Crisis malware contains a file that has an .asp extension. Generally speaking, the .asp file extension is used for a Windows application Web service.

Features unique to the Windows version

This section describes the functionalities that are only contained within the Windows version of the Crisis malware. Unlike the Mac version, the Windows version contains some advanced functionality.

Social

A function with the name social is used to steal information from the following social-networking services:

- Facebook
- Twitter

As well as stealing posts from the above sites, it also steals the friends and followers lists. The social function is also used to steal emails from the Gmail Web mail service.

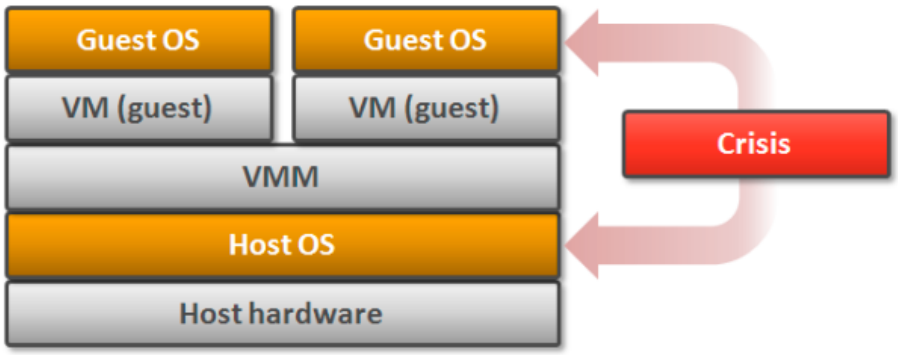
Virtual machine infection

Virtual machines are useful for many different purposes, including development and analysis of software. A virtual machine mainly consists of a host, a virtual machine monitor (VMM), software, and a guest. The VMM allows a user to execute multiple guest computers on the host operating system. Generally speaking, users can install any operating system that can be supported by the VMM. On the host operating system, the virtual machine image contains files including settings files and disk images. The Windows version of the Crisis malware targets this feature.

The Windows version of the Crisis malware has functionality to spread onto a virtual machine. Presently, the malware is designed in such a way that it is limited to certain VMware products, but the methodology that is used could be extended to cater for many VMM products.

Figure 9

VM infection method



The threat performs the following series of steps when infecting a VMware virtual machine:

1. Opens the VMware preference file. The VMware preference file can be found at the following location: %UserProfile%\Application Data\VMware\preferences.ini

```
.encoding = "windows-1252"
pref.eula.count = "1"
pref.eula0.product = "VMware Player"
pref.eula0.build = "812388"
vmWizard.guestKey = "windows7-64"
vmWizard.physicalBackend = "D:"
pref.mruVM0.filename = "C:\Users\%USERNAME%\Documents\Virtual Machines\VictimGuest
VictimGuest.vmx"
pref.mruVM0.displayName = "VictimGuest"
pref.mruVM0.index = "0"
```

The above example has a virtual machine named VictimGuest.

2. Parses the preference file to find the path of a .vmx file. The .vmx file is a settings file for a virtual machine image, which is contained within the preference file.

3. Parses the .vmx file to find the path of a .vmdk file. The .vmx file contains a .vmdk file path, which is the virtual machine disk image file.

```
scsi0.pciSlotNumber = "160"
scsi0.present = "TRUE"
scsi0.sasWWID = "50 05 05 68 67 f6 eb 00"
scsi0.virtualDev = "lsisas1068"
scsi0:0.fileName = "VictimGuest.vmdk"
scsi0:0.present = "TRUE"
scsi0:0.redo = ""
serial0.fileType = "thinprint"
serial0.present = "TRUE"
```

The above example is the parts of the .vmx file that contains the .vmdk file name.

4. Opens two registry entries to find the path for the vixDiskMountServer.exe file, which are as follows:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\vmplayer.exe\"@" = "C:\\ Program Files (x86)\\VMware\\VMware Player\\vmplayer.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\vmplayer.exe\"Path" = "C:\\Program Files (x86)\\VMware\\VMware Player\\"

The above path is just an example. It can be changed when the virtual machine is installed.

5. Mounts the .vmdk file as the Z drive. The vixDiskMountServer.exe file is a tool that is installed with a VMware program. It can be used to mount the .vmdk image. The Crisis malware searches for a device that has a name containing "vstor2-", and sets it to the Z drive.

6. Copies its installer to the startup folder on the Z drive. The malware copies its installer to the following startup folders on the Z drive:

- Z:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\mWgpX-al.exe
- Z:\Documents and Settings\All Users\Start Menu\Programs\Startup\mWgpX-al.exe

The first is for Windows Vista and Windows 7, and the second is for Windows XP. However, when attempting to copy the installer onto Windows XP, the process fails. Therefore, the virtual machine infection process as currently implemented can only succeed when the guest operating system is Windows Vista or Windows 7. This is possibly a bug in the code, but we cannot say with any certainty that it is indeed a bug.

In the past, whenever a malware detected that it was being executed in a virtual environment, the malware would cease operating, thereby attempting to thwart analysis of the threat. Crisis does not work like that, it is the first out-of-the-box malware that actively attempts to spread onto a virtual machine rather than stopping its execution. It is the nature of the malware field that once a novel concept is implemented, other malware authors soon adapt the technique for their own malicious code. This means that it is likely that we will encounter more malware employing the technique of spreading to virtual machines in the future.

Initially, virtual machines were produced for limited purposes, such as a professional tool for development, analysis, and large servers. Nowadays, virtual machines are far more prevalent as they provide compatibility features between operating systems, such as Windows XP Mode in Windows 7. We also use many Web services that are running on VPS services. Virtual machine usage has increased to the point where they can be found in many situations and the Crisis malware demonstrates a new attack vector targeting them. Fortunately the Crisis malware does not exploit any vulnerbilities in VMware software and it also cannot infect all virtual machines at this time—indeed it only infects VMware Workstation and not VMware ESX—but we should prepare for the next generation of Crisis malware.

In this paper, we have discussed the process of host-to-guest virtual machine infections. One further possibility to consider is guest-to-host virtual machine infections. The host-to-guest infection scenario depends on the privilege to access the VM disk image directly. However, if guest-to-host infection becomes a reality, it is most likely due to a vulnerability in the VMM, although, as stated previously in this paper, Crisis does not exploit any vulnerabilities in VMware software at this point in time. A guest-to-host infection would imply that software is able to break out of the virtual machine sandbox. Currently this latter technique is not possible, but if indeed became possible, these two cross-infection techniques could bring about a nightmare scenario where guest-to-guest infections could take place. This would turn the supposed safety of virtual machine isolation on its head.

The author

Finally, it is worth considering whether the author of the Crisis malware program was responsible for releasing the threat into the wild. Some security product vendors and researchers believe that a group in Italy constructed the Crisis malware as a product to sell to law enforcement agencies. In fact, several of the functions of the Crisis malware, such as recording sounds and stealing address book information, are suitable for private investigations or espionage. The brochure on the group's website and the functionality of the Crisis malware are indeed quite similar. However, this does not necessarily prove who was responsible for creating Crisis.

Generally speaking, tracing the source of a malicious program is difficult because the authors often go to great lengths to prevent their identity from being discovered. However, the section of data seen in Figure 10, taken from an analysis of a Crisis installer, appears to contain the name of the author.

Figure 10

User name present in code

```
.rdata:004421EB                 db  8Ch ; î
.rdata:004421EC                 db    2
.rdata:004421ED                 db    0
.rdata:004421EE                 db    0
.rdata:004421EF                 db    0
.rdata:004421F0 S_projectPath   db 'C:\Users\[redacted]\documents\visual studio 2010\Projects\Win3'
.rdata:004421F0                 db '2Test\Release\Win32Test.pdb',0
.rdata:0044224D                 db    0
.rdata:0044224E                 db    0
.rdata:0044224F                 db    0
```

The data contains a path to a project file and the path includes a user name. By searching for this name on the Internet, we discovered that the user is a member of the group in Italy. Consequently, there is a possibility that the said group counts the creator of the Crisis program as one of its members. Despite discovering these links, we still do not have the true identity of the person behind this scheme. As described in the Installer obfuscation section, the Crisis installer can be any legitimate software that has been modified so this may not be the same software.

Conclusion

It is certainly feasible that the Crisis malware was originally developed for law enforcement purposes in order to perform private investigations or espionage activities as the functionality contained within the code is highly advanced and appropriate for such a purpose. Notably, it provides multi-platform infection capability for the Microsoft Windows and Apple Mac operating systems as well as the ability to propagate through a virtual machine environment. We know that it can drop modules onto the Windows Mobile platform, but unfortunately we do not have the dropped modules available for analysis and therefore we have not witnessed its functionality on mobile devices.

The Crisis malware program could be the first malware capable of spreading itself onto a virtual machine. The usage of VM technology is increasing every day and so the features found in Crisis have significant ramifications for the wider security industry. However, it is worth noting that the propagation functionality as well as certain information-stealing functionality in Crisis is created only for the Windows platform. Furthermore, even the functions common to both the Windows and Mac versions have better implementation on the Windows platform.

We can never tell what the future may hold, but one thing that we can be certain of is that the Crisis malware will continue to advance and grow. In our research into Crisis, we have seen older samples of the malware that did not have virtual machine propagation techniques or the presence of the social function. By observing variants and the timeline of creation, we can surmise that there is continued investment and development of the Crisis malware. The demand for private IT investigations and espionage will never disappear and, so long as there is customer demand, it is likely that we will see new functionality emerging in this area in the near future.

Resources

W32.Crisis
http://www.symantec.com/security_response/writeup.jsp?docid=2012-081606-2200-99

OSX.Crisis
http://www.symantec.com/security_response/writeup.jsp?docid=2012-072605-1811-99

Scripting additions for Mac OS X
http://developer.apple.com/library/mac/#technotes/tn1164/

New malware for Mac: Backdoor.OSX.Morcut
http://www.securelist.com/en/blog/719/New_malware_for_Mac_Backdoor_OSX_Morcut

Symantec
Security Response

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Mountain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

About the author

Takashi Katsuki is a software engineer specializing in analysis of malicious code, in particular malware for mobile devices and Macs. Recently, he is focusing on finding advanced technologies related to malware and malware analysis.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com