

## MALWARE ANALYSIS 3

### CHIM CHYMINE: A LUCKY SWEEP?

David Harley  
ESET

The class of malware that exploits Autorun/Autoplay as an infection vector has been an irritating fact of life for a good while. The malware known as Win32/Stuxnet could be (and indeed has been [1]) described as a worm of a different colour. It can propagate making use of a zero-day vulnerability [2] listed by CVE as CVE-2010-2568 [3]. In a nutshell – or rather the *Windows Shell* – *Windows* can be tricked into executing malicious code presented in a specially crafted shortcut (.LNK) file, linking in turn to a malicious DLL, allowing compromise of a system even where Autoplay is disabled. (It should not be forgotten that USB devices aren't the only potential entry point: network and webDAV shares are also an issue.)

#### MISSING LINKS

There's already plenty of detailed information available on both the vulnerability and the very interesting Win32/Stuxnet family, so I won't go much beyond the minimum background in this article. However, apart from generating detection for Stuxnet, *ESET* also started to detect its approach heuristically, as LNK/Autostart.A, and subsequently as LNK/Exploit.CVE-2010-2568. It was, after all, reasonable to suppose that as the proof-of-concept code gained currency, other malware families would adopt the same trick. Sure enough, our telemetry systems soon picked up some interesting vibes.

#### THE OTHER VB

As early as 20 July, our lab was seeing several Autorun worms written in Visual Basic and experimenting with LNK files. However, by 23 July things were getting really interesting. We had identified a new family exploiting the still unpatched vulnerability in order to spread by code execution through malicious LNK files. This was promptly christened Win32/TrojanDownloader.Chymine.A. At the present time, this threat is used to download and install a keystroke logger which we detect as the Win32/Spy.Agent.NSO trojan.

#### CHINA CHYMINE IN

The server used to deliver the components used in this attack is presently located in the US, hosted by the 'Managed Solutions group'. According to RWHOIS data from the hosting organization, the server IP address was

assigned to a customer in China on 22 July. The DLL downloaded from here contains a number of strings in Chinese, translated here courtesy of *Google Translate*:

Comment: 'Fire Personal Firewall, building a fun-filled safe network for you'  
File description: Fair Personal Firewall, for you to create a safety net is full of fun.  
Company name: Fair Safety Laboratory  
Product name: Fair Personal Firewall

At the time of writing, neither Chymine.A nor any of the related files seem to be generating any malicious LNK files themselves. To date, we've only found LNKs exploiting the latest vulnerability and pointing to the downloader, suggesting to us that since Chymine.A doesn't spread by itself, there must be something (or someone) else 'helping' it along [4].

#### THIS WILL (AUTO)RUN AND RUN

Even while the lab team was in the process of sharing information about this new threat with other researchers, they observed a known threat which had been refurbished to include the CVE-2010-2568 exploit as a new propagation vector. Win32/Autorun.VB.RP looks very much like an updated version of the malware written in Visual Basic and described on 21 July by Adrian de Beaupre [5]. This class of threat hides folders in the root directory of any drive to which it has Write access, creates LNKs with the same name as the hidden folders, and drops autorun.inf, EXE and SRC files. It differs from the ISC description, however, in that it *does* actually produce new LNK files exploiting the CVE-2010-2568 vulnerability to facilitate its own spreading; it doesn't simply rely on Autorun or wait for the victim to click on a malicious but uncrafted LNK. It now seems to download and install additional components on infected machines. The LNKs making use of the CVE-2010-2568 exploit use the following naming convention: z<two letters>.lnk (for example 'zTa.lnk').

There's not much doubt about which of the present crop of malware based on the original LNK vulnerability is the most novel and interesting. Win32/Stuxnet has two major points of interest.

- One, of course, is the targeting of *Siemens* control software on SCADA sites, injecting modules SystemRoot\inf\oem7A.PNF and SystemRoot\inf\oem7A.PNF into the address spaces of CCprojectMgr.exe and S7tftopx.exe processes using the mrxcls.sys driver, and reading configuration information from the registry key 'HKLM\System\CurrentControlSet\Services\MRxCLS. (This may

account for some of the interesting distribution patterns that have been noted by some sources [1, 6].)

- The second point of interest is Stuxnet's use of legitimate digital certificates to sign its device driver. These were stolen from *Realtek* and *JMicron Technology Corp* [7] and were subsequently revoked by *VeriSign* in order to prevent further misuse [8, 9, 10].

## THE EARLY BIRD LAYS THE WORM?

However, the newer malware we're seeing is far less sophisticated than Stuxnet, and suggests bottom feeders seizing on vulnerabilities flagged by others, and hijacking exploitative techniques developed by the early birds. This is interesting in its own way (not least for the speed with which it has appeared). We expect to see plenty more worm cast [11] on the beach before (and after) *Microsoft's* update [12] appears on the horizon.

This article synthesizes the research and thoughts of many people, not only within *ESET* but in the anti-malware community at large, and too many to mention individually. However, particular thanks are due to Richard Baranyi, Peter Košinár, Juraj Malcho, Pierre-Marc Bureau and Aleksandr Matrosov for sharing their research data and insights.

## REFERENCES

- [1] <http://blog.eset.com/2010/07/17/windows-shellshocked-or-why-win32stuxnet-sux>.
- [2] <http://www.microsoft.com/technet/security/advisory/2286198.mspx>.
- [3] <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568>.
- [4] <http://blog.eset.com/2010/07/22/new-malicious-links-here-we-go>.
- [5] <http://isc.sans.edu/diary.html?storyid=9229>.
- [6] <http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx>.
- [7] <http://blog.eset.com/2010/07/19/win32stuxnet-signed-binaries>.
- [8] [https://blogs.verisign.com/ssl-blog/2010/07/code\\_signing\\_certificates\\_used.php](https://blogs.verisign.com/ssl-blog/2010/07/code_signing_certificates_used.php).
- [9] <http://blog.eset.com/2010/07/22/why-steal-digital-certificates>.
- [10] Goretzky, A. <http://blog.eset.com/2010/07/22/a-few-facts-about-win32stuxnet-cve-2010-2568>.
- [11] [http://en.wikipedia.org/wiki/Worm\\_cast](http://en.wikipedia.org/wiki/Worm_cast).
- [12] <http://www.microsoft.com/technet/security/advisory/2286198.mspx>.