BKDR_CYSXL.A

enigmasoftware.com/bkdrcysxla-removal/

Domesticus

April 23, 2012

BKDR_CYSXL.A Description

Type: Backdoors
Bkdr_Cysxl.A is a backdoor Trojan being used in a wide spread email spam campaign exploiting the excitement of the upcoming 2012 Summer Olympic Games hosted in London. Cybercriminals are not bias and will exploit any and everything they can to reap ill-gained profits. While to some people the Olympic Games are just another sports event, for many others it is a culture. Die-hard fans like to get an early jump on buying tickets, especially top category events that often sell-out.

Email scams that spoof or exploit official Olympic sites and promotions are nothing new. In fact, Internet security experts who keep watch of malware activity in the wild reported a 2012 London Olympic Game email spam surfacing as early as October, 2008.

The email spam delivering Bkdr_Cysxl.A presents as follows:

Don't be fooled by bogus websites and organisations claiming to sell tickets to the Games. Tickets will be available from this website, for the UK and EEA (European Economic Area) residents only, and official 2012 London sales channel from spring 2011. You will not be asked to make a payment or sign a contract until then.

Please read about tickets for details at the attachment in which has some bogus websites and organizations.

An official site of the London 2012 Olympic Games and Paralympic Games.

The above spam letter is sealed with a fraudulent 2012 Olympic Games logo, in which cybercriminals hopes authenticates the farce and scam to further deceive unwary PC users. Is it ironic that the first line in the bogus email letter mirrors actual verbiage posted on one of the official ticket selling sites for the 2012 London Olympic and Paralympic Games? No, it is not mere coincidence. Malware makers and cybercriminals often shape their viral warheads off of legitimate branding, even violating copyrights.

In order to execute the payload, PC users must open the infectious .DOC attachment containing 3 supposed bogus websites. If opened, however, a malicious file being detected as TROJ_ARTIEF.ZIGS exploits a RTF stack buffer overflow and unleashes or downloads Bkdr_Cysxl.A onto the infected system.

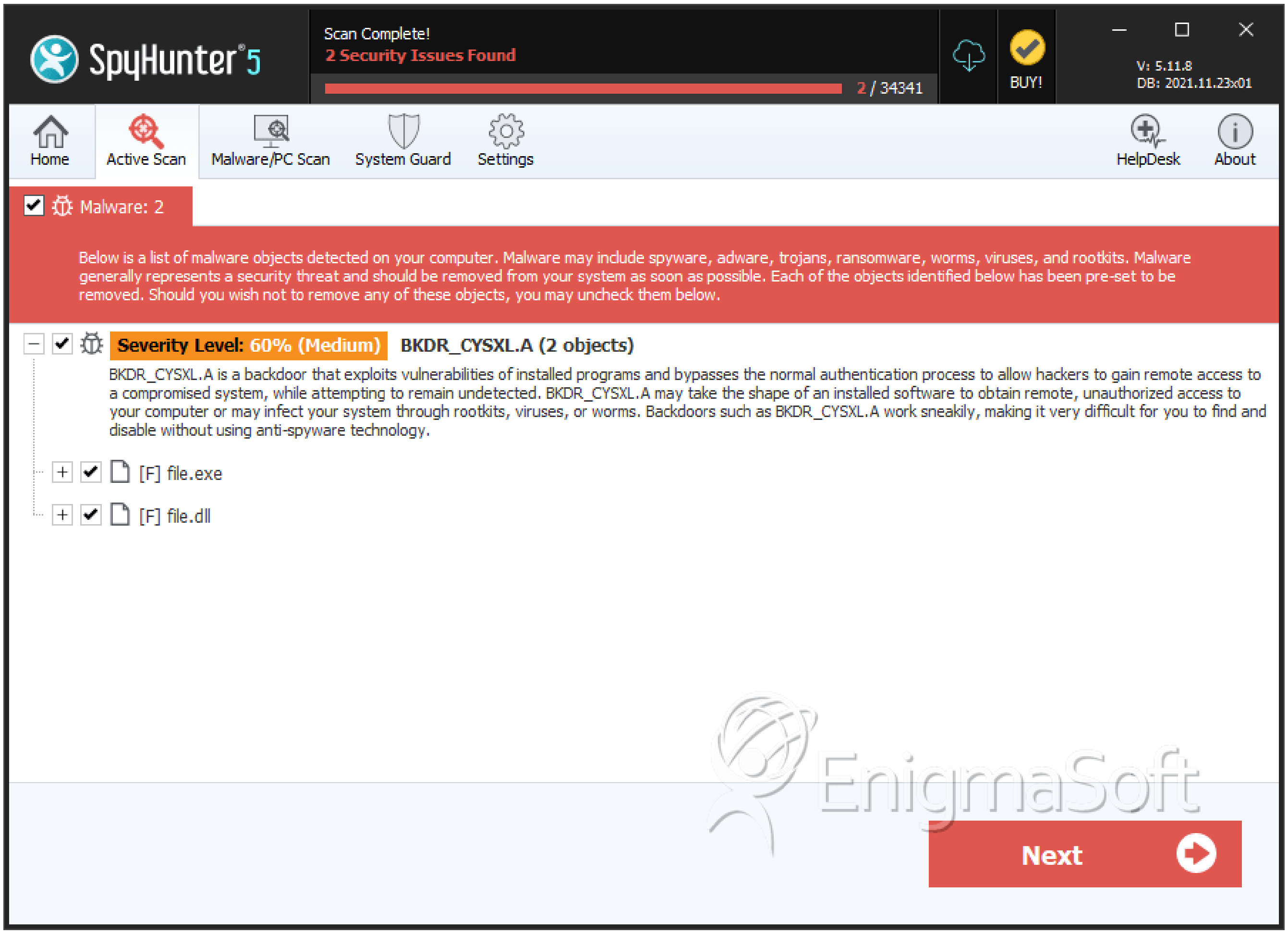
In addition to opening a backdoor for a hacker to gain access and possible administrative control, Bkdr_Cysxl.A will reconfigure the system. Files and components might be deleted to render the firewall, weaker anti-virus programs defenseless and to cripple the operating system, helping to justify the lies and behaviors of a fake online scanner or rogue security program. A port will be opened to report successful infiltration and implantation of malicious files and components, earning pay for the malware builder. Vital data will be stolen off the system and more malicious programs might be installed.

Hopefully you did not fall for the scam and deleted the spam letter altogether as opposed to opening the malicious document. If you or someone using your PC have fallen victim, you should clean your computer by using a trusted anti-malware program to scan and eradicate all found malware, even ones hidden in the root of your PC. Before buying tickets online, make sure the website or ticket promoter is legitimate and you are not just handing your financial data over to a hacker.

Technical Information

Screenshots & Other Imagery

SpyHunter Detects & Remove BKDR_CYSXL.A



Scan Complete!
2 Security Issues Found
2 / 34341

Below is a list of malware objects detected on your computer. Malware may include spyware, adware, trojans, ransomware, worms, viruses, and rootkits. Malware generally represents a security threat and should be removed from your system as soon as possible. Each of the objects identified below has been pre-set to be removed. Should you wish not to remove any of these objects, you may uncheck them below.

☑ Severity Level: 60% (Medium) BKDR_CYSXL.A (2 objects)

BKDR_CYSXL.A is a backdoor that exploits vulnerabilities of installed programs and bypasses the normal authentication process to allow hackers to gain remote access to a compromised system, while attempting to remain undetected. BKDR_CYSXL.A may take the shape of an installed software to obtain remote, unauthorized access to your computer or may infect your system through rootkits, viruses, or worms. Backdoors such as BKDR_CYSXL.A work sneakily, making it very difficult for you to find and disable without using anti-spyware technology.

☑ [F] file.exe

☑ [F] file.dll

File System Details

#	File Name	MD5	Detection Count
1	%System Root%\Document and Settings\All users\realupdate.exe		N/A
Name: %System Root%\Document and Settings\All users\realupdate.exe Type: Executable File Group: Malware file			
2	%System%\cydll.dll		N/A
Name: %System%\cydll.dll Type: Dynamic link library Group: Malware file			
3	file.exe	14b6fcdff12b707bf660d552b2e24731	0

Name: file.exe MD5: 14b6fcdff12b707bf660d552b2e24731 Size: 73.48 KB (73483 bytes) Detection Count: 0 Type: Executable File Group: Malware file Last Updated: May 4, 2012			
4	file.dll	c10ae223f80a4aab03da384e4c89a39d	0
Name: file.dll MD5: c10ae223f80a4aab03da384e4c89a39d Size: 54.27 KB (54272 bytes) Detection Count: 0 Type: Dynamic link library Group: Malware file Last Updated: May 4, 2012			

Registry Details

BKDR_CYSXL.A creates the following registry entry or registry entries:
Registry key
HKEY_CLASSES_ROOT\Sxl
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CyService\parametersServiceDll = "%System%\cydll.dll"

Site Disclaimer

Enigmasoftware.com is not associated, affiliated, sponsored or owned by the malware creators or distributors mentioned on this article. This article should NOT be mistaken or confused in being associated in any way with the promotion or endorsement of malware. Our intent is to provide information that will educate computer users on how to detect, and ultimately remove, malware from their computer with the help of SpyHunter and/or manual removal instructions provided on this article.

This article is provided "as is" and to be used for educational information purposes only. By following any instructions on this article, you agree to be bound by the disclaimer. We make no guarantees that this article will help you completely remove the malware threats on your computer. Spyware changes regularly; therefore, it is difficult to fully clean an infected machine through manual means.