When greyhats turn to blackhats

Business

Throughout December, Websense Security Labs(TM) reported a number of cases where browser and Operating System vulnerabilities were being used to install Potentially Unwanted Software onto end-users machines without user-intervention. In several cases, dozens of pieces of code were installed, and often report false information in order to entice the end-user to clean their machine from spyware. We are now seeing some of those same entities using their exploit code to install more reprehensible crimeware, such as key loggers and phishing traffic redirectors. This code is designed to steal information in addition to the installation of potentially unwanted software. Users are typically infected through an IFRAME, loaded silently from a compromised website or an advertisement network pop-up.

The exploit code loaded through these IFRAME tags attempts to use several dozen vulnerabilities, including the two recent zero-day vulnerabilities: MS05-054 and MS06-001. Users who are patched against these vulnerabilities are displayed an ActiveX prompt to install the exploit code. The IFRAME SRC loads a URL similar to these: NOTE: The URLs have been removed. http:// too1barXXX. biz/dl/fillmemadv470. htm http:// too1barXXX.

biz/dl/sploitadv470. anr http:// too1barXXX. biz/dl/xpladv470. wmfThese exploits function as downloaders, and performing HTTP GET requests to other websites to install their payload. Initially, the primary goal of these downloaders was to install unwanted software, such as counterfeit anti-spyware removal tools, toolbars, adware and other potentially unwanted software.

Recently, we have seen the downloaded files performing additional functions, including: Banking keyloggers Trojan horses with root-kit functionality Traffic redirectors that direct you to fraudulent Paypal websites Trojan horse backdoors Internet Explorer process injectionKey capturing exampleThe keylogger is usually retrieved from a URL such as: http:// too1barXXX. biz/progs/kl. txtkl. txt is a not a text file; it is a Windows binary Trojan horse that is packed with NSPack. file output: file kl.

txtkl. txt: MS-DOS executable (EXE), OS/2 or MS WindowsThe dropper includes a number of files. The dropped keylogger files are typically named ibmXXX. exe and ibmXXX. dll.

This keylogger monitors for every POST request made by the client computer (such as a logon to a banking website) and sends the captured information to a URL running a script named ‘ x25. php’. This program also injects itself into the Explorer process and silently redirects attempts to login to specific financial sites. Screen shot 1: Password captured –> Content of HTTP POST stolenThe malicious code also has additional functionality. If you visit one of a set of predefined websites and attempt to log in, you are redirected to a fraudulent site, which asks for additional credential information.

In Screenshot 2, we connected to paypal. com. After entering any user name and password, we were redirected to a fraudulent page and personal information was requested. The toolbar still shows the original site, however the site that is hosting this code is on another server not owned by Paypal. Screen shot 2: Paypal example –> IE Process injection traffic redirectionFor additional details and information on how to detect and prevent this type of attack: http://www. websensesecuritylabs. com/alerts/alert. php? AlertID=

395