The Carberp Information Stealing Trojan

Carberp is the name of the latest in an increasing line-up of information stealing malware that have evolved in the last few years. As in the case of it's forerunners (Torpig/Mebroot,Clampi, ZeuS and SpyEye) the most recognised role of Carberp is to steal users e-commerce payment transaction data (e-banking, Paypal, debit/credit card etc.), although any sensitive data is at risk (personal identity or research data for example).

As mentioned in the piece on ZeuS [1]the development of which was ceased in mid 2010 and the source code was sold to the developers of the SpyEye trojan leading to elements of both malware variants in the last iteration of SpyEye. Whilst Torpig (with and without associated Mebroot MBR infection) and ZeuS (Versions 1&2) are still active the two leading info stealing trojans are SpyEye and Carberp.

The most common infection vectors are either download from web-pages containing exploit code or via email based social engineering campaigns. The trojan does not need administrator rights in order to run. Infecting Windows XP, Vista and Windows 7 hosts and will therefore run on locked down Windows Vista and Windows 7 machines as the logged on user(infection of other users or kernel components does not occur).

Infection leads to a number of files being created in the users %TEMP% directory and placement of a file (with a Win system file name) in the users start-up folder to allow activation at next start-up. This file is hidden from Windows Explorer and the command line although tools such as GMER [2] made it viewable in the past.

One other aspect which makes this malware particularly nasty is it's ability to see and control any and all online transactions in real-time recording every password, HTTP-S, EV-SSL session and user login. Harvested data is then sent to the Command & Control Server immediately, before the legitimate recipient (i.e. your bank). In addition it can inject arbitrary HTML code to change the current web page in order to steal dynamic one-time passwords from two-factor authentication tokens.

Suffice to say that Carberp is very difficult to detect an will evade most AV clients using the modular plug-in stopav.plug(written in Borland Delphi) to check and subsequently disable active AV protection. One tool which has proved effective (at least in the past) is Microsofts Sysinternals tools, process explorer (www.sysinternals.com [3]) procexp.exe. By clicking on the "explorer.exe" process, selecting "view" from the menu choose "show lower pane" any threads shown in a <non-existent process> that are shown denote infection.

Another growing trend is the use of "Mini-AV" capabilities within malware in order to rid the host of other infections. Notably those that are also engaged in information stealing (ZeuS, SpyEye etc.) The plug-in (miniav.plug) is used to clear the way for Carberp to work without competition for the stolen data. The plugin also looks debbuger values inside each sub-key of the "Image File Execution Options" registry key. This technique is used to deny the creation of

specified processes or execute the code when a specified process is run.

Carberp is more than a sophisticated info-stealing trojan. It has remote control capabilities turning the host into a zombie. Carberp communicates with a list of command and control servers which are embedded into the binary (these are encrypted with an simple xor-based algorithm) and additional servers can be added later. On contact with a C&C the host sends data (operating system, process list and it's unique identity). A configuration file is downloaded and stored in the binary using the xor-based encryption.

The infected host contacts a web page on the C&C server in a bid to receive specific commands from the server. It can update, download and run executable files, load dll and even start a remote VNC session using the plug-in vnc.plug.

Another module is the passw.plug, a grabber which is able to scan the host looking for passwords and user account credentials such Instant Messaging, password and form data saved within web browsers, e-mail account, FTP client, VNC and Cisco VPN account credentials. The data is stored within a database and uploaded to the remote C&C server.

With the rise and rise in the use of on-line transactions for banking and other e-commerce activity the development of enhanced malware such as Carberp will continue. The modular structure, the ability to run in restricted accounts, it's ability to hide from AV clients and the continued development make it very dangerous indeed.

Links
[1] http://www.ja.net/services/csirt/threats/malware/zeus/
[2] http://www.gmer.net/
[3] http://www.sysinternals.com/