New Solarbot Malware Debuts, Creator Publicly Advertising

blog.malwarebytes.com/threat-analysis/2013/09/new-solarbot-malware-debuts-creator-publicly-advertising/

Joshua Cannell September 26, 2013

A new botnet known publicly as “solarbot” has been making its rounds, according to a report from ESET.

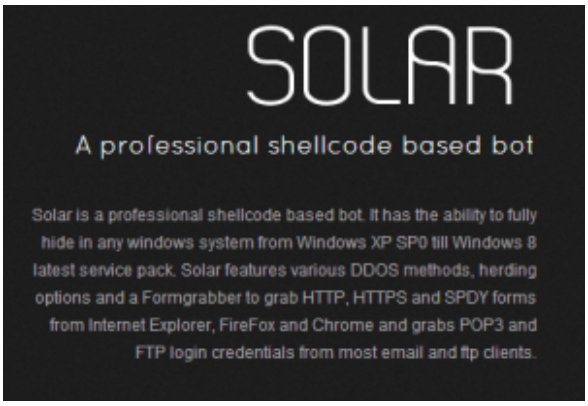


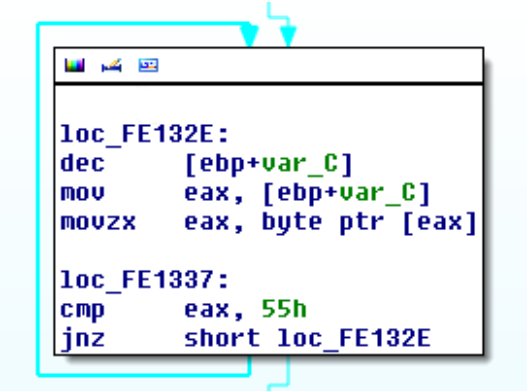
Image:ESET

In their writeup, ESET analysts explain that solarbot(which they refer to as Win32/Napolar) is capable of:

- Denial of Service (DOS) attacks
- Behave as a SOCKS proxy server
- Stealing information from web forms

Amongst the tricks employed by this bot, one in particular is self-debugging, something we mentioned here and by avast! here. The bot begins execution by unraveling code encrypted with RC4 within Thread Local Storage (TLS) callback functions. To find the starting location of the decrypted code, it searches for the PUSH EBP assembly instruction, which is 0x55.

This is a smart approach as most reverse engineers will place a software breakpoint at this location to begin executing the decrypted code. However, whenever a software breakpoint is placed, the instruction is actually replaced with an INT3 (0xCC), and therefore the malware wouldn’t continue to execute as intended. Pretty slick.



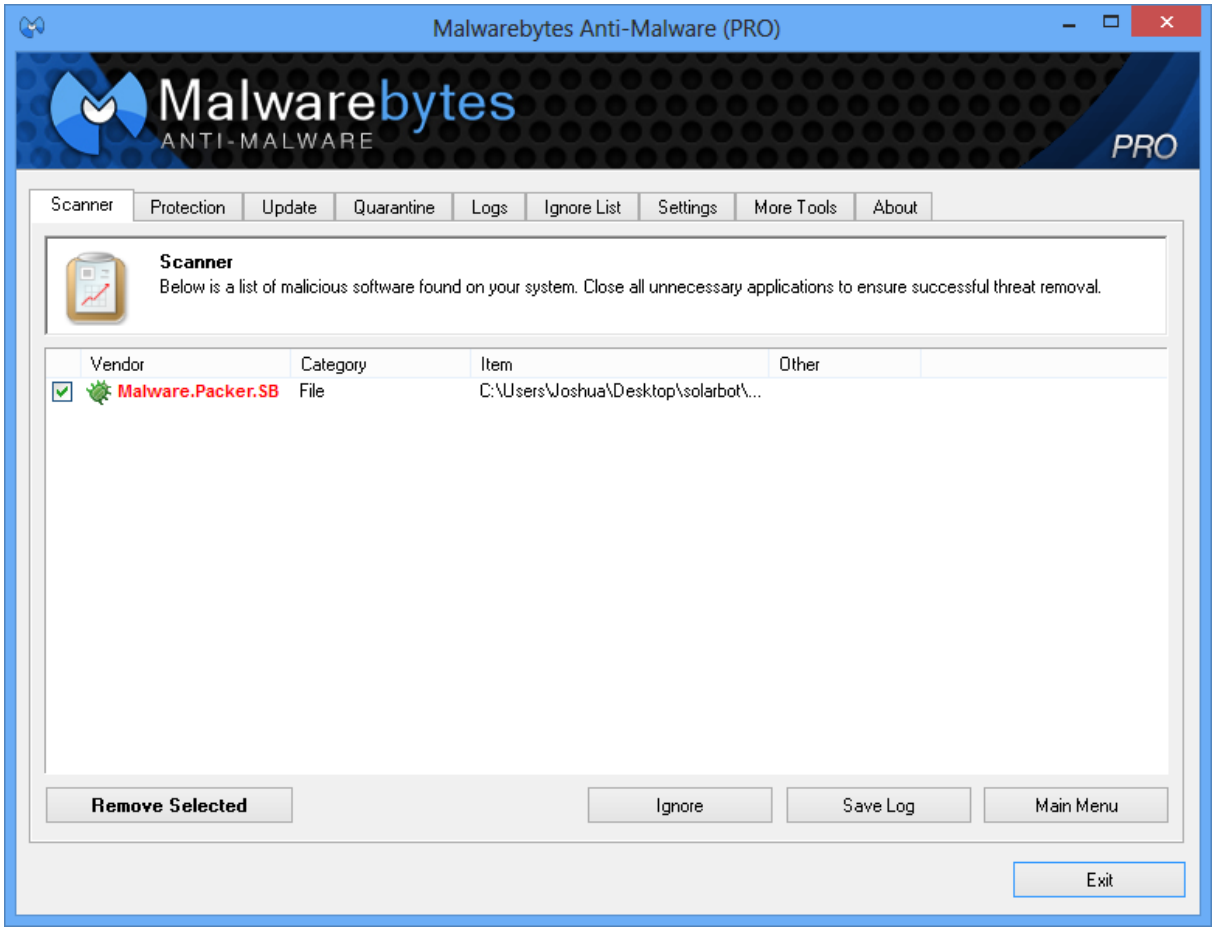
Solarbot looking for “PUSH EBP” (0x55)

It’s currently undetermined how the bot spreads, but researchers at ESET believe it’s likely spread through Facebook, based on its ability to steal login credentials.

In addition, the bot’s creator had been publicly advertising the malware on the web, before the site was taken down just recently. The bot supports multiple plugins (must be written in Delphi), and even makes some references to TOR configuration files.

TOR has seen a lot of publicity lately, after a sudden surge in traffic occured earlier this month, believed to be caused by the Mevade/SBC botnet. Perhaps we will see even more malware use TOR to route traffic to C2 servers in the coming future.

We’ll continue to keep you updated with any unique findings on the solarbot malware. As a closing note, users of Malwarebytes Anti-Malware are protected from known solarbot variants, detected as **Malware.Packer.SB**.



Joshua Cannell is a Malware Intelligence Analyst at Malwarebytes where he performs research and in-depth analysis on current malware threats. He has over 5 years of experience working with US defense intelligence agencies where he analyzed malware and developed defense strategies through reverse engineering techniques. His articles on the *Unpacked* blog feature the latest news in malware as well as full-length technical analysis. Follow him on Twitter @joshcannell