Heloag has rather no friends, just a master

By Georg Wicherski

Published: 2010-05-03 · Archived: 2026-04-05 16:21:34 UTC

Incidents

Incidents

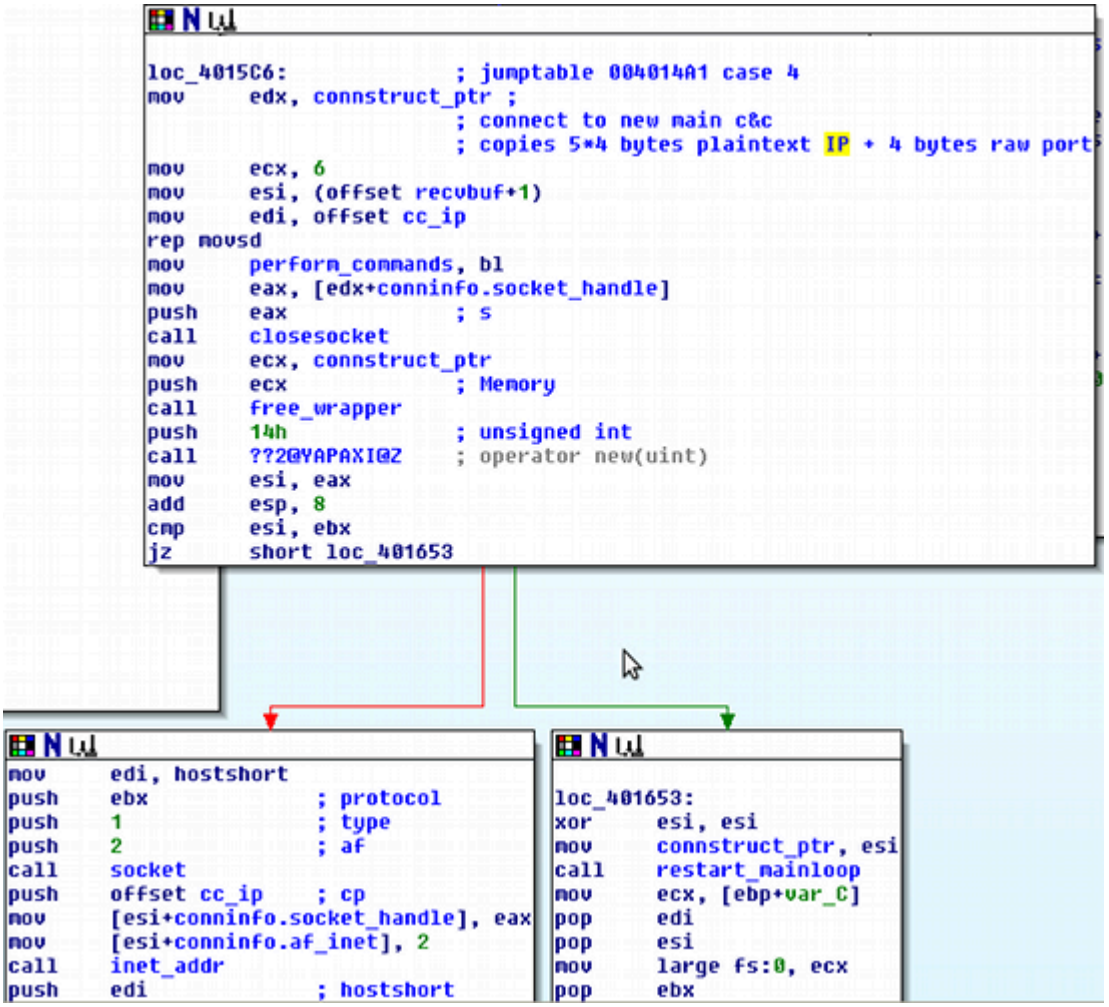
03 May 2010

1 minute read

Jose Nazario of Arbor Networks recently posted an analysis of Trojan.Heloag on their blog, mentioning that some observed behaviour might be related to Peer-to-Peer C&C functionality. However, Jose's analysis was dynamic only and thus he was not certain about this when I contacted him (also thanks to Alex Cox for sharing network traces of his honeypot). Being interested in Peer-to-Peer botnets (e.g. Stormfucker: Owning the Storm Botnet [MP4 Video]), I had to take a deeper look.

The Heloag binaries I've looked at (*6ede527bb5aa65eae8049ac955b1018d* dropped by *d9b14a7bc0334458d99e666e553f0ee0*) **did not contain any Peer-to-Peer C&C functionality**! Instead, the bot rather speaks a very simple protocol over TCP with the following command types supported (encoded as the first byte of the packet):

1. 1 DDoS another host using different techniques:
    - TCP DDoS, connect(..) based (does not send data)
    - UDP DDoS, sendto(..) based (sends some random data)
    - HTTP DDoS requesting / with User-Agent "helloAgent", InternetOpenUrlA based
    - HTTP DDoS crawling links from / with User-Agent "Google page"
2. 2 Download and execute an URL of up to 0xA4 bytes, zero-padded URL
3. 3 Send the current computer name
4. 4 Stop with the currently executing DDoS command
5. 5 **Disconnect from current server and connect to new C&C server**



Disassembly for function 4

This means that even though during dynamic analysis, multiple C&C servers were observed, it is just some kind of hand-over to another C&C server which can be used for load-balancing or renting out bots. Since there is always only one server, the bot is connected to at a time, this does not add a lot to take-down resilience (phew!).

Still, this is an intersting specimen regarding malware authorship. What strikes immediately into the eye is that while for most of the commands, there is exactly one control byte, DDoS commands are all encoded in the same byte. The additional payload of this commands then controls what DDoS is carried out to where. Instead of using one type byte like for control bytes, this code uses different boolean bytes in the payload for controling DDoS types. Additionally, the DDoS related code makes heavy usage of C++ std::string's while the rest of the main code uses wsprintf for string handling. It looks like this project was implemented by two different individuals collaborating or at least one buying some source from the other.

This malware is pretty certainly from China. First, the usage of wsprintf underlines non-western character aware path names, which you rarely see in malware with western origins. Additionally, there is one *Chinese* IP hardcoded in the binary, which cannot be attacked by DDoS, no matter what command is given to the bot (and this is checked after DNS resolution).

Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
