

Heloag has rather no friends, just a master

SL securelist.com/heloag-has-rather-no-friends-just-a-master/29693/



Incidents

Incidents

03 May 2010

minute read



Authors

Expert Georg Wicherski

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: Owing 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. 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", InternetOpenUrlIA based
 - HTTP DDoS crawling links from / with User-Agent "Google page"
2. Download and execute an URL of up to 0xA4 bytes, zero-padded URL
3. Send the current computer name
4. Stop with the currently executing DDoS command
5. **Disconnect from current server and connect to new C&C server**

```

loc_4015C6:          ; jumtable 004014A1 case 4
mov     edx, connstruct_ptr ;
                    ; connect to new main c&c
                    ; copies 5*4 bytes plaintext IP + 4 bytes raw port
mov     ecx, 6
mov     esi, (offset recvbuf+1)
mov     edi, offset cc_ip
rep     movsd
mov     perform_commands, bl
mov     eax, [edx+conninfo.socket_handle]
push   eax          ; s
call   closesocket
mov     ecx, connstruct_ptr
push   ecx          ; Memory
call   free_wrapper
push   14h          ; unsigned int
call   ??2@YAPAXIQZ ; operator new(uint)
mov     esi, eax
add    esp, 8
cmp    esi, ebx
jz     short loc_401653

loc_4015C6:
mov     edi, hostshort
push   ebx          ; protocol
push   1           ; type
push   2           ; af
call   socket
push   offset cc_ip ; cp
mov     [esi+conninfo.socket_handle], eax
mov     [esi+conninfo.af_inet], 2
call   inet_addr
push   edi          ; hostshort

loc_401653:
xor     esi, esi
mov     connstruct_ptr, esi
call   restart_mainloop
mov     ecx, [ebp+var_C]
pop    edi
pop    esi
mov     large fs:0, ecx
pop    ebx

```

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 interesting 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 controlling DDoS types. Additionally, the DDoS related code makes heavy usage of C++ std::string's while the rest of the main code uses sprintf 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 sprintf 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).

- [Botnets](#)
- [DDoS-attacks](#)
- [Malware Creators](#)

Authors



Heloag has rather no friends, just a master

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm

17 Jun 2020, 1:00pm

26 Aug 2020, 2:00pm

22 Jul 2020, 2:00pm

From the same authors



Live Twitter XSS



Different x86 Bytecode Interpretations



Is there really a Storm out there?



The Dangers of Social Networking

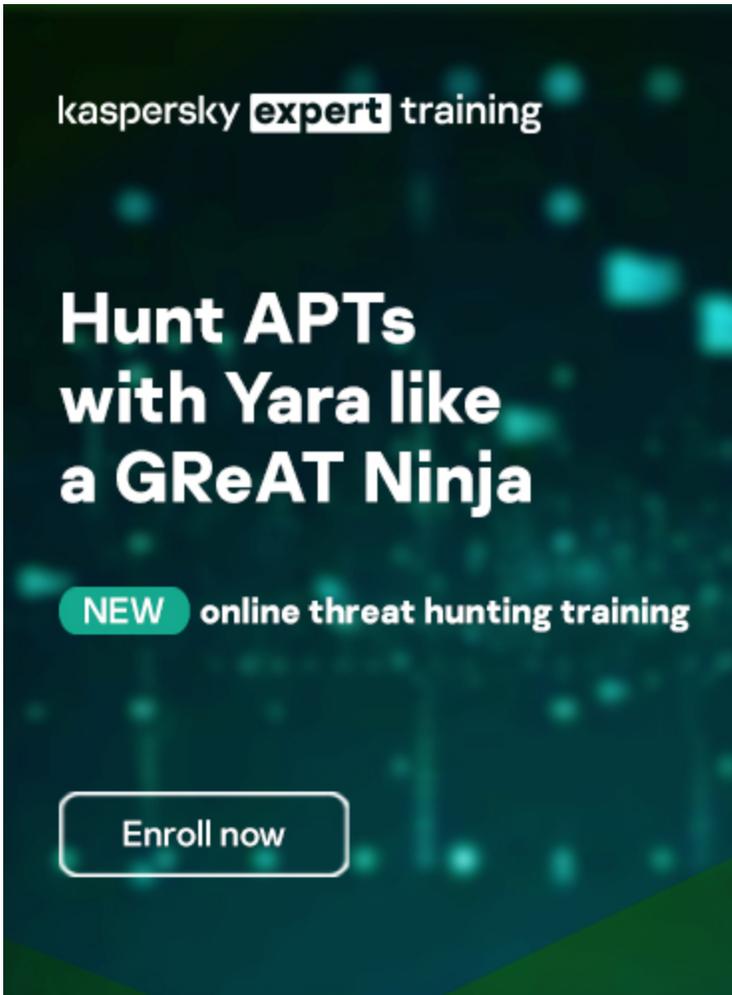


The msvidctl Internet Explorer 0day

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-



Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

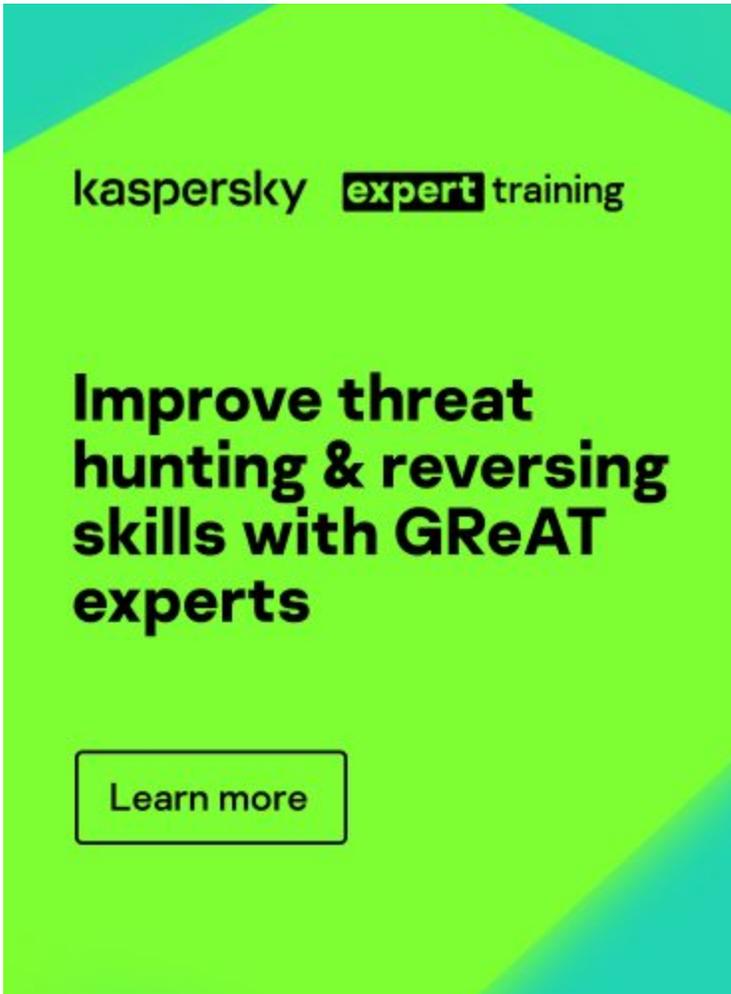
We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.

A promotional banner for Kaspersky Expert Training. The background is a vibrant green with teal triangular accents in the corners. The text is in a clean, sans-serif font. At the top left, it says 'kaspersky expert training' with 'expert' in a black box. The main headline reads 'Improve threat hunting & reversing skills with GReAT experts'. At the bottom, there is a white button with a black border that says 'Learn more'.

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-

kaspersky **expert** training

Improve threat hunting & reversing skills with GReAT experts

[Learn more](#)