Floki Bot – A Zeus Wannabe with Delusions of Grandeur?

By SC Staff

Published: 2016-10-31 · Archived: 2026-04-05 21:11:31 UTC

Well, it was a nice summer and, as I waited for the magazine to finish developing the new look on our website I spent a lot of time crawling around the Dark Web looking for tidbits of interest. That's the good news. The bad news is there were more than I could consume over the entire summer. So, on the advice of one of our Lab Approved vendors I decided to take a deep dive into a bot that has been on the horizon since September - a relative newcomer. The story behind this one is, on the surface, innocuous. But, as the infomercials say, "Wait! There's more!"

Floki Bot is now well-advertised in the underground marketplaces and I pulled information from a variety of sources, not the least of which was Alphabay. This is a fairly open, but mildly vetted, pay-for-play underground marketplace where you can buy anything for bitcoins from malware to drugs to hackers for hire. The actor in this case is advertising heavily in several marketplaces including Alphabay. So it is safe to say this bug is likely to hit the streets fairly soon if it hasn't - and I suspect that it has based upon the ease with which I found my sample and other information about it - already.

This week we'll take a look at the bot, the author's claims and what the likely truth is along with how to prepare for it in case it does become active. That is one of the themes for Threat Hunter 2.0: we want to help you become proactive. I'll be looking for things that are still in their formative stages, but which have a reasonable likelihood of becoming pesky in the near future.

The second theme is that I have teamed with our Lab Approved vendors along with a few others to provide the tools I'll use in each week's analysis. At the end of each blog I'll list the tools I used that week so you can consider how they might fit in your security/threat hunting stack. Some of those tools, by the way, will be open source or free in addition to the commercial tools I'll use. When you're threat hunting everything that can help you be proactive is on the table.

There are, really, two kinds of threat hunting: pre and post event. Post event I equate to dead-box forensics. The damage has been done and now we are left with the analysis. Pre event is proactive and seeks to predict what possible threats really will become threats in the future. We will focus on pre but touch on the cleanup aspects where it makes sense. Now on to our bug....

The actor burst on the scene in underground marketplaces in September with the claim of a new bot that is built from Zeus 2.0.8.9. The bot has appeared in the wild in a limited way so we can expect that this proof of concept will blossom into a full-blown bot net when our actor gets a customer.

He claimed that the bot could not be detected by deep packet inspection. That appears to be at least partially true. We ran our sample through our Cuckoo sandbox and it failed to find any network connections. Then we detonated the bot in a sacrificial host and monitored with Wireshark. We saw some activity to several IP addresses, most of which host malware, largely Trojans of various flavors. Running our sample through VirusTotal we got hits on 26

of 56 anti-malware programs and those 26 showed everything from Zbot to various Trojans and droppers. A closer look will explain some of that.

We went back to AlphaBay and found a demo of the bot bypassing IBM's Trusteer Rapport. This yielded an IP address - 46.165.210.17 - that we started digging on that traces to a German ISP (germany.privateinternetaccess.com). Running that IP in OpenDNS Investigate did not get us much, but running it in CyMon and ThreatCrowd did. ThreatCrowd was especially interesting because it provided a web of interconnects with other IPs and domains, virtually all of which host malware. The domain in OpenDNS Investigate also was more fruitful than the IP alone.

Expanding the domain name out to the IPs and other domains that it hosts gave a bunch of malicious sites, mostly branching off of 178.162.199.99. It also gave us the MD5 for a piece of malware hosted on the IP (10375c3524c5271d487b141aa00a1a18) which turns out to be an iFrame Trojan. The Trojan shows up on the following:

- 178.162.199.99
- 68.232.35.90
- 173.194.65.95
- 149.126.72.131
- 173.194.65.120
- 108.161.188.209
- 149.126.72.124
- 85.25.149.38
- 69.55.52.73
- 108.162.197.244
- 88.212.196.75
- 74.206.167.145
- 95.211.221.247
- 95.211.221.145
- 95.101.0.88
- zxeutaa.myvnc.com
- asianalbum.com
- ads.juicyads.com
- mobile.juicyads.com
- fonts.googleapis.com
- code.jquery.com
- fonts.gstatic.com
- alientraf.com
- www.juicyads.com
- twiant.com

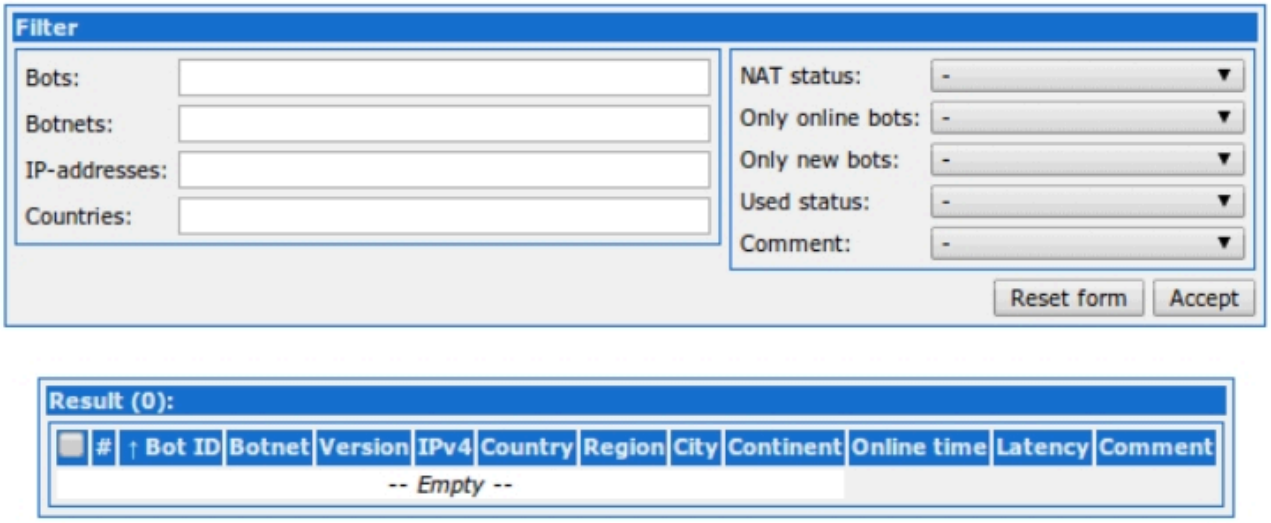
The next treasure trove came when we ran the IP through BotScout. This gave us a good amount of information in the form of registrant emails, many of which appeared to be created using DGAs. As well, many email addresses use the .xyz top level domain[1].

So, what do we know so far? First, the IP in the video may or may not be a direct C&C connection with the bot. Let us assume, for safety, that it is a command and control server. There is some evidence for this assumption at VirusTotal[2]. The site lists over 15 malicious files that communicate with this IP. If we do the same lookup on the 178.162.199.99 IP we get even more, including a hash for a piece of malware that is served by that IP. While not the same malware that we found in this IP earlier, it has a similar purpose. We also see a couple of malware hashes for files that communicate with this IP. The evidence for the IP - or, at least, the hosting company - being used as a C&C for the Trusteer test is piling up.

Will that end up being a C&C of the bot net? Probably not. The actor is selling the bot so whomever he sells it to likely will set up a botnet for it. Would I block the hosting company? Yep. And, I'd block the IPs just for safety since they are hosting domains as well.

Figure 1 shows the control panel for the C&C.

Figure 1 - Floki Bot Control Panel



What about detecting the bot at your gateway? We cannot depend upon detecting Zeus as a way to detect Floki bot. Also, I was interested to note in the demo video that the actor referred to the bot as "loki" rather than "floki". Loki bot is a password and wallet stealer. So this raises the question as to whether this is a variant of loki rather than Zeus, or if the demo used loki to try to scam buyers, or if our actor just got careless with his keyboard.

Let's dig into the floki bot's general functionality as claimed by the actor.

The bot works on Windows XP, Vista and Win7 with UAC as well as server 2003/2003R2 and 2008/2008R2. It runs its code on each process the user executes and requires almost no privileges so it can run in the Guest account (which should be disabled, of course). The bot runs several special processes that allow such things as bypassing firewalls and it can send the victim configuration to the server so that the server/operator can generate commands to the victim. Even though the bot communicates with http, it's communication is encrypted with a key unique to each instance of the bot. there is a Back-connect feature (apparently with some problems) that allows a connection back to the victim for such things as RDP and FTP.

HTTP injects allow modification of loaded pages on the victim and the bot can scrape the screen for useful information such as bank accounts or credentials. There are a number of blocking functions as well. The bot includes a sniffer and a keystroke monitor/grabber. It can import Windows certificates. Scripts can be run from the control panel. The bot can be removed from the victim via the control panel.

When the payload is dropped it is encrypted and stays that way until the dropper creates a process in explorer or svchost. At that point the payload is unencrypted, decompressed and injected into all running 32-bit processes. Now the final payload can be unencrypted and decompressed to execute. The bot renames itself and copies itself into a subdirectory under Application Data. In our sample it renamed to dymasa.exe. Stolen data is encrypted and stored in a different subdirectory under Application Data. An entry in the Startup folder is added for persistence.

There are a number of changes/additions to the registry as well. These modify the victim's security.

Two interesting features of the bot are its claimed high execution rate: 70% as opposed to Zeus' supposed 30%, and, its ability to read track 2 of a credit card. This gives it a future as a tool for stealing credit cards. Returning to the speculation that there may be pieces of loki code as well as Zeus, we note that some of the functionality of the loki stealer might be incorporated in the bot. A complete reversing of our sample will, perhaps, shed some light on that.

That brings us to a stopping point for this entry. We are completing the reversing of our Floki Bot sample and we'll dig into the internals next time and see if the actor's claims are accurate. For that we have partnered with one of the top malware reversing engineers in the business.... stay tuned for that one. One of the new features in Threat Hunter 2.0 is partnering with some of the best threat hunters available.

Until then, here are your new malicious sites for this week along with three new features. First, we have a pie chart that shows the top five C&C IPs that hit our honeypots as monitored by Packetsled this week. Second, another pie chart shows the top five attacking IPs as monitored on our honeypots by Packetsled. Finally, in no particular order, we have the top attack types against our honeypots as detected by our Niksun NetDetector. Watch for those indicators again as we update them later in the week.

--Dr. S

Our tools this week were:

- Niksun NetDetector
- Packetsled
- Cisco OpenDNS Investigate
- Cymon
- AlienVault OTX
- ThreatCrowd
- Intel471

· Silobreaker

· Cuckoo sandbox

Figure 2 - Top Command and Control Servers Against our Honeypots

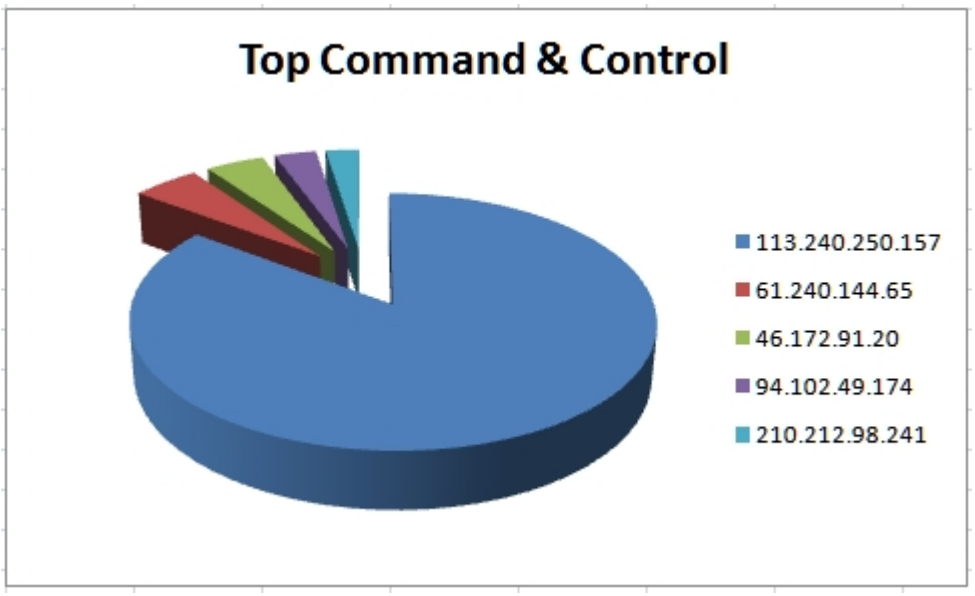


Figure 3 - Top Attacking IPs Against our Honeypots

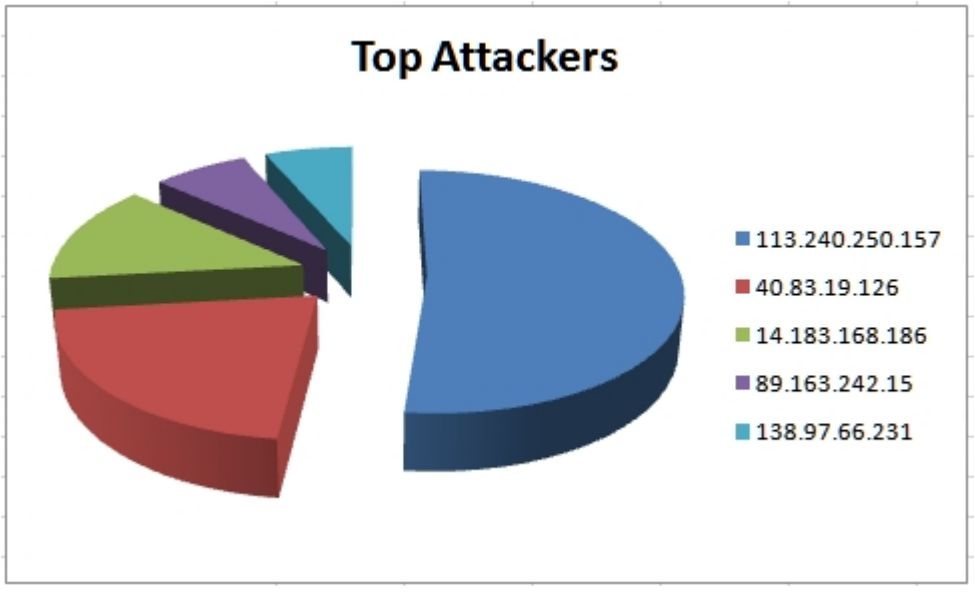


Figure 4 - Top Attack Types Against our Honeypots

```
Botnet like behavior
Non TELNET Traffic On Standard TELNET Port
Non HTTP Traffic On Standard HTTP Port
Covert HTTP
Non SSL Traffic On Standard SSL Port
```

Figure 5 - This Week's New Malicious Domains from Malware Domain List

Domain	IP	Reverse Lookup	Description
kingskillz.ru/~kingskil/Prince/Man/lucy/mine/shit.exe	85.143.215.183	62695.simplecloud.club.	Trojan.FareIt
elmissouri.fr/data.dpg	213.186.33.50	cluster017.ovh.net.	ransomware
www.family-partners.fr/data.dpg	95.142.169.132	xvm-169-132.ghst.net.	ransomware
art-archiv.ru/images/animated-number/docum-arhiv.exe	81.177.139.111	-	trojan
apexgames.org/ykxj6/par/factura.zip	166.62.112.150	ip-166-62-112-150.ip.secureserver.net.	Javascript inside zip file leads to trojan
catjogger.win/ganel/gate.php	213.145.225.170	web02.chillydomains.com.	pony loader c&c
tscl.com.bd/m/RI%20XIN%20QUOTATION%20LIST.zip	209.99.16.206	206.0/24.16.99.209.in-addr.arpa.	trojan inside zip file
ad.getfond.info	83.217.26.203	ru2.com.	PlugX C&C

---

[1] https://botscout.com/search.htm?stype=q&sterm=46.165.210.17&cc=&page=1

[2] https://www.virustotal.com/en/ip-address/46.165.210.17/information/
