A New Phase of TheMoon

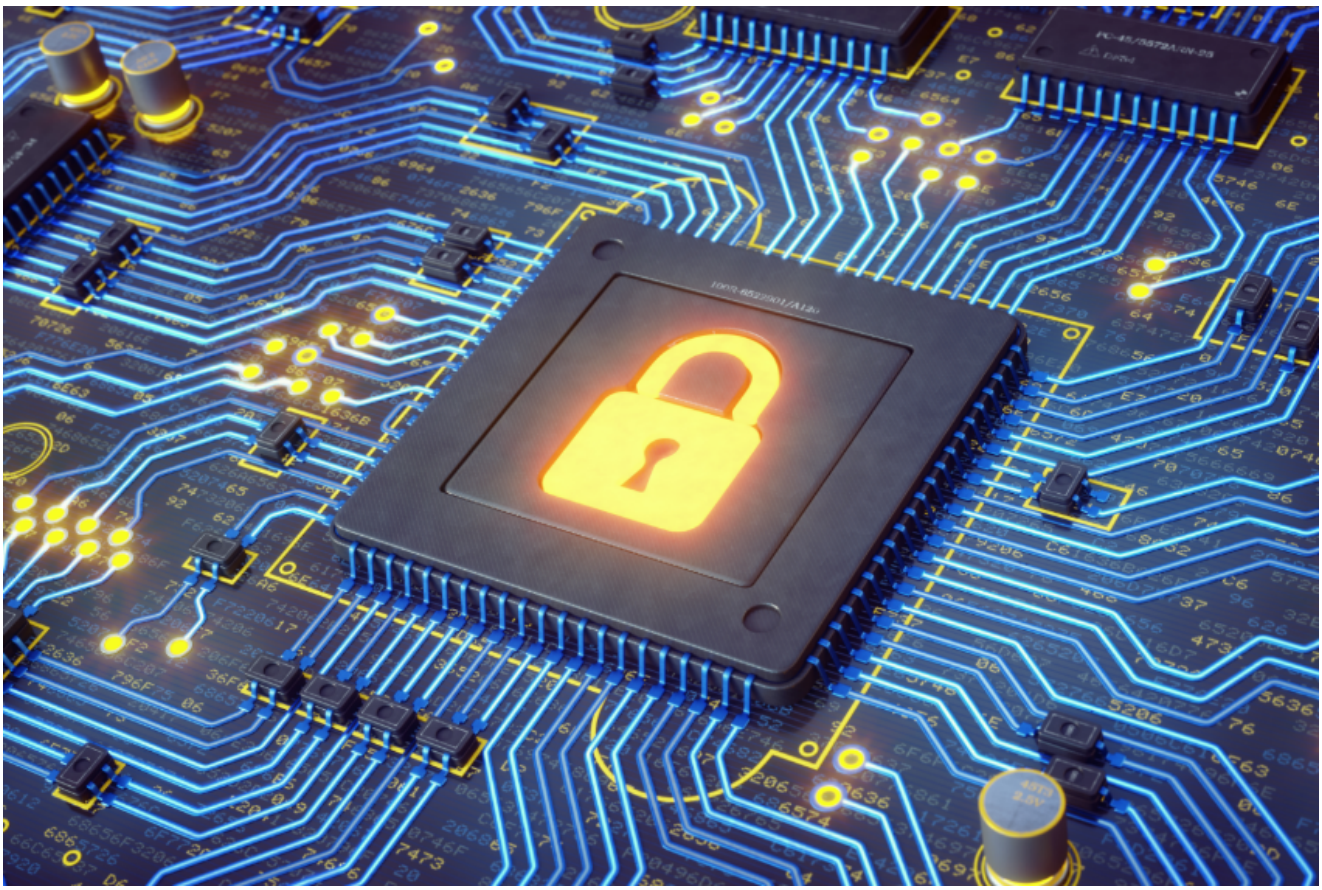
blog.lumen.com/a-new-phase-of-themoon/

Black Lotus Labs Posted On January 31, 2019

0
1.4K Views

0

Shares



Over the past year, CenturyLink Threat Research Labs has been tracking an IoT botnet called “TheMoon”. TheMoon is a modular botnet specifically targeting vulnerabilities in routers within broadband networks. Since its identification in early 2014 [1], the botnet has evolved to target a broader set of device types using commonly published exploits [2] [3]. The exploits target broadband modems or routers developed by companies such as Linksys, ASUS, MikroTik and D-Link, with the most recent exploit added in May 2018 targeting GPON

routers [4]. The danger posed by TheMoon stems from its ability to distribute malicious modules of differing functionality after initial infection. For example, CenturyLink identified a previously undocumented module that is only deployed on MIPS devices and turns the infected device in to a SOCKS proxy. We have reason to believe the botnet actor has sold this proxy botnet as a service to other malicious actors and has used it for credential brute forcing, video advertisement fraud, general traffic obfuscation and more.

TheMoon first came to our attention when several devices were discovered performing credential brute force attacks on multiple popular websites. Using the IP addresses of the infected devices, additional malicious infrastructure was uncovered by looking at the common IP addresses with which they communicated. This revealed the Command and Control (C2) operating at 91.215.158[.]118. This IP was within the network range previously reported as associated with TheMoon and was later reported as a C2 by a secondary source [4].

How TheMoon Operates

To continue expanding the botnet, the actor will scan for hosts by looking for vulnerable services running on IoT devices. Once a vulnerable service is found, a shell script is dropped using one of the many previously mentioned exploits. Most of the exploits target vulnerabilities in IoT web applications typically running on port 8080. The shell script is then executed, which downloads the initial stage payload from domstates[.]su. According to VirusTotal, domstates[.]su has been used to distribute TheMoon since July 2017 [5]. Most binaries and modules distributed by TheMoon use zlib compression to compress and obscure components within the files. In order to manage the botnet, the main binary uses three different ports for command and control communication: one for initial registration when the binary starts executing, one for command and control communication and one for downloading additional payloads to run. These ports vary between binaries and architecture types. For example, MIPS binaries use port 5784 for registration, 5184 for command and control and 4584 for downloading payloads while ARM binaries use ports 5732, 5132 and 4532, respectively. TheMoon has the ability to run any additional payload, making it particularly dangerous and allowing the botnet author to evolve its capabilities over time.

Figure 1 below represents a simplified architecture of TheMoon botnet for one of the main MIPS binaries 057d56b7de1e9460bd13c5c6eafd4559. Each binary typically has multiple hardcoded C2 IPs. In the case of 057d56b7de1e9460bd13c5c6eafd4559 these are 91.215.158[.]118, 149.202.211[.]227, 208.110.66[.]34 and 173.208.219[.]42. For simplicity, the following detail focuses on C2 91.215.158[.]118 as this is the only C2 that currently appears to be active. Analytical focus was placed on the MIPS binaries since the credential brute forcing devices were identified as MIPS-based platforms. These devices were also

observed communicating with TheMoon C2 on the MIPS C2 port 5184. By emulating the C2 protocol and monitoring the MIPS C2 port, a secondary payload was obtained called “sox” with md5 db5221aa43cb13f76333705998171f04.

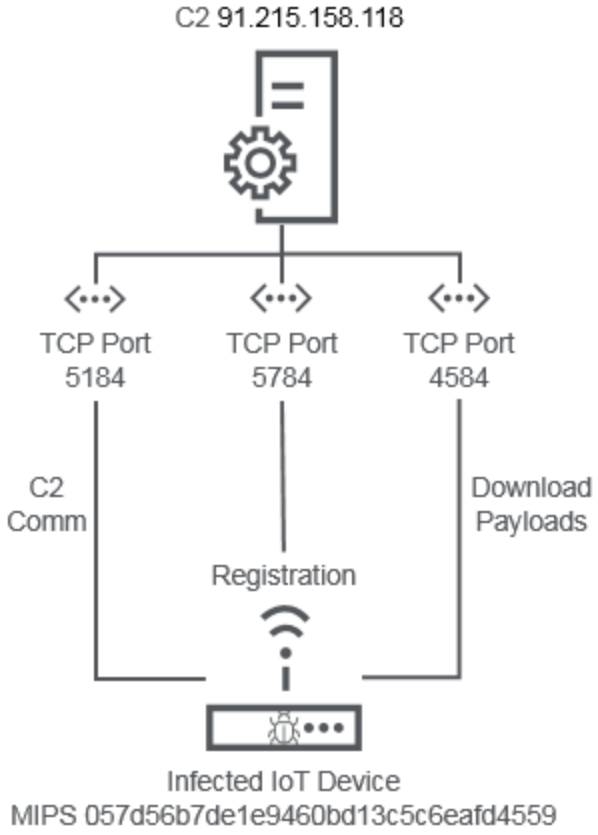


Figure 1: TheMoon Main Binary Architecture

The MIPS sox module is different than the modules currently deployed to ARM devices. Netlab 360 [3] previously documented various modules which proxy traffic based on command and control messages received by a C2. This new, previously undocumented module is slightly different: instead, it turns the infected device into a SOCKS5 proxy for others to use. Previous modules with proxy functionality only allowed the command and control server to send proxy requests; the new module allows the botnet author to sell its proxy network as a service to others. The proxy port appears to be a randomly chosen port above 10,000 and was observed changing multiple times per day. Originally this proxy port was unauthenticated, allowing anyone to route traffic through an infected device. In April 2018, the actors changed their proxies to use authentication. Figure 2 represents the architecture of this payload.

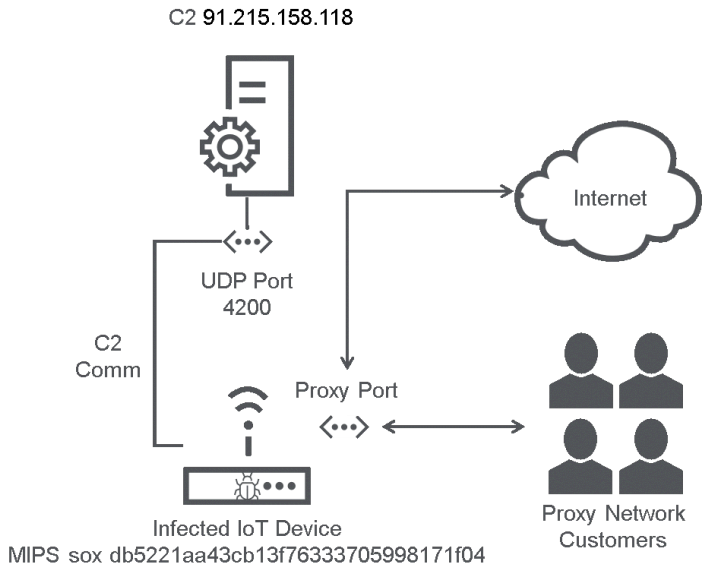


Figure 2: TheMoon MIPS Sox Binary Architecture

Since infected devices are running proxies on seemingly random high ports above 10,000, suspected proxy ports were identified by analyzing their communication patterns within this high range. Interestingly, 24 IP addresses all within the same ASN were observed communicating with infected devices in these high port ranges. We believe these IPs were managed by another actor using TheMoon proxy botnet as a service.

After further investigation of the 24 IPs, CenturyLink discovered that each IP hosted a unique service on TCP port 8002. When connecting to this port, a stream of log messages associated with a video advertisement fraud campaign was automatically received. Each server on average sent seven messages per second. Figure 3 gives an example of the logs reported by the video ad fraud servers. Within each log there is a domain and URL which is believed to represent a browsing request made to the proxy. One six-hour time period from a single server resulted in requests to 19,000 unique URLs on 2,700 unique domains. After browsing some of the URLs, it was apparent they all had embedded YouTube videos. Table 1 shows possible values of the “result” and “extendedResult” fields which appear to be related video ad impressions as indicated by the “quartile” extendedResult values.

result	extendedResult
timeout	play
noads	aderror
noads	http403
imp	firstquartile
noads	stop
noads	empty
imp	aderror
imp	complete
proxyfail	http0
noads	http404
proxyfail	vpaid
proxyfail	timeout
imp	thirdquartile
imp	stop
imp	midpoint
imp	start
imp	imp

Table 1: Result Fields

```
'\x12\x00\x00\x00\x1fs:message::bee::publish new log\x00\x00&\xb8j:
    {
        "result":"noads",
        "extendedResult":"aderror",
        "vast":"1104137-MW-AOL-3.9YEP",
        "domain": "<domain visited>",
        "url": "<url visited>",
        "profile": "<base64 encoded string>",
        "ip": "<base64 encoded information about proxy used>",
        "swarm":"swarm_advert20k",
        "start":"1523556350800",
        "width":"1920",
        "height":"1080"
    }
```

Figure 3: Example Log From Video Ad Fraud Servers

```
{
     "address":"socks5://<username>:<password>@<proxy_ip>:<proxy_port>",
     "realIp":"<proxy_ip>",
     "serverIp":"<video_ad_fraud server_ip>"
}
```

Figure 4: Base64 Decoded IP Field

Of particular interest to our goal of tracking TheMoon botnet, the “ip” key has a base64 encoded string which is shown in Figure 4. This represents the proxy used for the video ad fraud request. When the actors switched to authentication on the proxy port, the username and password was added to the logs. By analyzing the large list of password and proxy

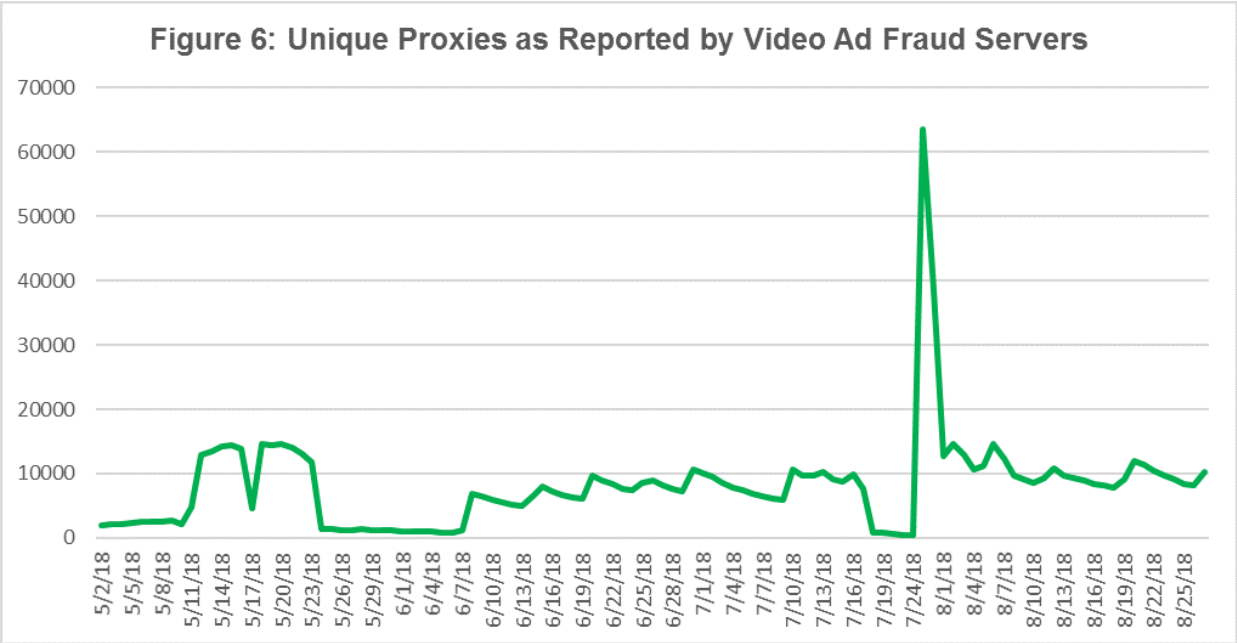
combinations, the password was determined to be a base64 encoded version of the port modified by a counter value. A Python function which generates port and password combinations is included in the appendix.

Each log also contains a base64-encoded JSON string of a device profile. Many different device types have been observed while parsing the logs. It is unclear if these requests and profiles are coming from real devices that are infected with some type of ad fraud malware or if the requests and device profiles are being generated and spoofed by the video ad fraud server itself. It may be of interest to ad fraud mitigation services that the geolocation field of the profile did not correspond with the geolocation of the proxy IP making the request.


```
{
     "type": "mobile",
     "screen": {"width": 360, "height": 640, ... },
     "window": {"innerWidth": 300, "innerHeight": 250, ... },
     "navigator": {"appVersion": "5.0 (Linux; Android 7.0; SM-J327V Build\/NRD90M)
                    AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/65.0.3325.109
                    Mobile Safari\/537.36", "platform": "Linux armv7l", ... },
     "language": "en-US",
     "languages": ["en-US", "en"],
     "hardwareConcurrency": 4,
     "maxTouchPoints": 5,
     "deviceMemory": 1,
     "onLine": true,
     "battery": {"charging": true,"chargingTime": "Infinity", ... },
     "connection": {"downlink": 1.6, "effectiveType": "4g", "rtt": 50},
     "mediaDevices": [{"deviceId": "default", "kind": "audioinput", ... }]
     "timeZone": "America\/Detroit",
     "historyLength": 28,
     "chrome": ["loadTimes", "csi"],
     "audioContext": {"baseLatency": 0.080166666666667},
     "performance": {"memory": {jsHeapSizeLimit": 364000000, ... }},
     "geo": {"latitude": <lat>, "longtitude": <long>},
     "webgl": {"7936": "WebKit", "7937": "WebKit WebGL", ... }
}
```

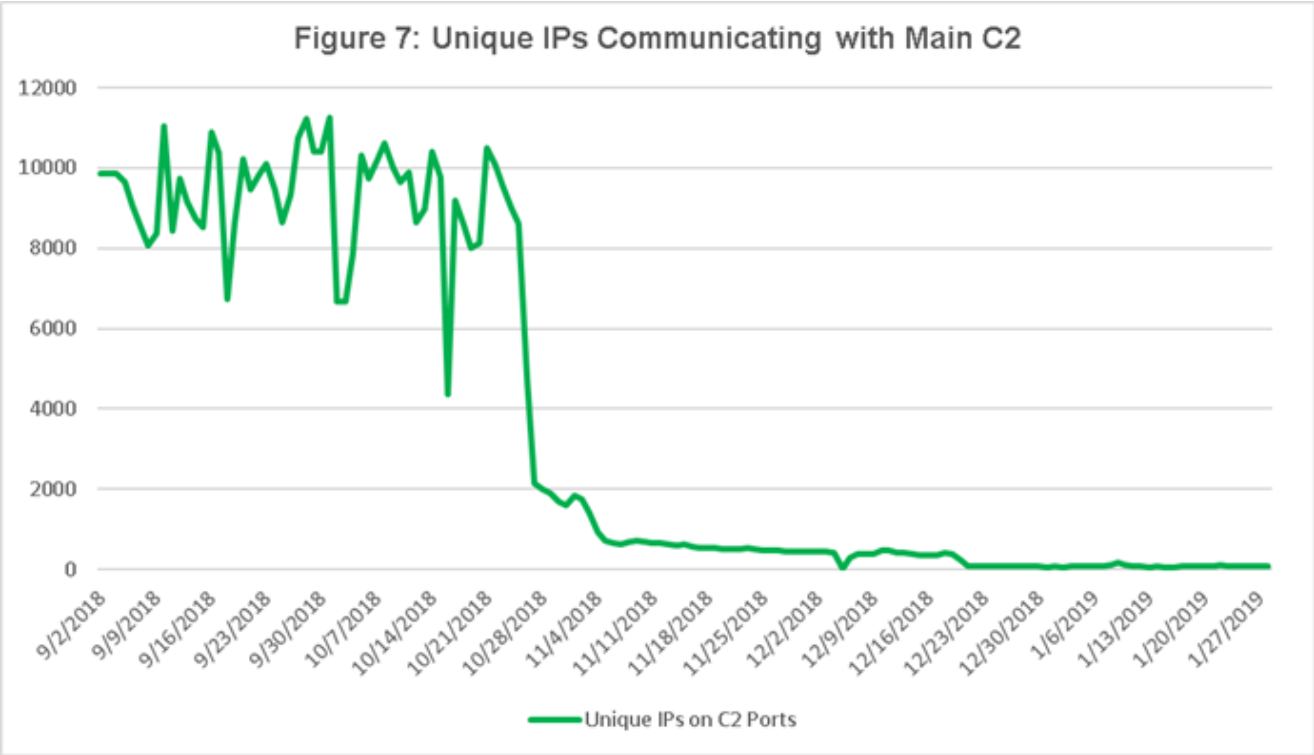

Figure 5: Base64 Decoded Profile Field

The video ad fraud servers were monitored from May to August, keeping track of the number of unique proxy IPs reported by the video ad fraud servers each day as shown in Figure 6. This gave us a high-confidence list of infected devices to act on. During several of the peaks, large sets of new device types were added to the proxy pool and were quickly reported by CenturyLink Threat Research Labs to the victims' network providers to help mitigate the threat. The video ad fraud actors unfortunately closed the port leaking the logs at the end of August, though this did not end successful tracking of the threat.



After losing visibility into the video ad fraud servers, CenturyLink continued monitoring TheMoon C2s. Figure 7 shows the unique IPs communicating with the main C2 91.215.158.118. The green line represents number of unique IPs communicating with the C2 on one of the various C2 ports. The number of unique IPs communicating with the C2 continues the trend from the previous graph in the 10,000 range. The number of IPs decreases drastically around the end of October, representing success in removing the implant from infected devices.

CenturyLink has blocked TheMoon infrastructure on our network to mitigate the risk to our customers as well as notified other network owners of potentially infected devices to help clean up and protect the internet at large. Though it appears the impact of TheMoon botnet is decreasing, the threat of IoT botnets with varying capabilities remains a powerful one. The likelihood of this actor attempting to infect new devices in the future by adding additional exploits to the existing toolkit is high. There is also a substantial market for proxy botnets targeting broadband networks to route traffic for attacks like credential brute forcing and ad fraud. The always-on nature of IoT devices and the ability to masquerade as normal home users make broadband networks prime targets for these types of attacks. It is important that IoT device manufacturers and broadband network providers limit the services open to the internet and continually provide patches to security vulnerabilities.



Appendix

TheMoon C2s (Main Binary)

91.215.158[.]118

149.202.211[.]227

208.110.66[.]34

173.208.219[.]42

TheMoon C2s (Modules)

173.208.219[.]58

185.56.30[.]189

93.191.15[.]94

149.202.211[.]227

208.110.66[.]34

173.208.219[.]42

TheMoon Hashes

057d56b7de1e9460bd13c5c6eafd4559 (.nttpd,21-mips-le-t1 MIPS)

db5221aa43cb13f76333705998171f04 (.sox module MIPS)

af30fca836142d6a0b8672f1e8f53acf (.sox module MIPS zlib decompressed)

75cc1d964ee321474c5a51e3884be524 (.nttpd,22-arm-le-t1 ARM)

20f9f7ae0c6d385b0bedcdd618c478dc (.nttpd,21-arm-le-t1-z ARM)

d0a43bbe141c3ddc9e077b5a41ba282b (.nttpd,21-arm-le-t1-z ARM zlib decompressed)

8c7e68017929afe171de59a8d2dc884c (.sox70 module ARM)

ea7f5744bdc91b1c13427f7f171338b2 (.sox70 module ARM zlib decompressed)

293b1c731def4243537d68334da3a8a0 (.sox30 module ARM)

518184d031633df1058740dd45d31668 (.sox30 module ARM zlib decompressed)

1fba1831c5590a3aaafe09b8d2281fbc (.plk module ARM)

3e6659eac8fc23d91727af7823f5b4dc (.plk module ARM zlib decompressed)

48acb7e812f22ee4f9aa49548c1a3d2c (.sox60 module ARM)

32e0d4bc465091839ddaeae823a11576 (.sox60 module ARM zlib decompressed)

Malware Distribution

domstates[.]su

149.202.211[.]227

217.182.218[.]156

217.182.220[.]22

217.182.113[.]179

Video Ad Fraud Servers

144.76.238[.]238

144.76.80[.]195

144.76.83[.]42

148.251.235[.]107

148.251.2[.]71

148.251.3[.]78

148.251.43[.]229

148.251.68[.]8

176.9.111[.]117

176.9.114[.]109

176.9.140[.]177

176.9.53[.]91

176.9.54[.]201

176.9.72[.]105

176.9.77[.]180

176.9.82[.]94

188.40.59[.]124

5.9.16[.]115

5.9.21[.]169

5.9.36[.]48

78.46.21[.]241

88.198.51[.]80

95.216.12[.]113

95.216.12[.]99

Password Generation Algorithm

```
import csv

import base64

def generate_passwords():

# generate a map of ports to passwords
```

```
ports_passwds = {}

# initial counter value

counter = 0xc8dcc4c0c8d

for port in range(10000,65001):

seed = hex(counter)[2:]

if len(seed) % 2 == 1:

seed = ‘0’ + seed

passwd = base64.b64encode(seed.decode(‘hex’))

ports_passwds[port] = passwd

# update counter based on the port

# convert to hex string

port_hex_str = hex(port)

# if the port ends in ‘9fff’ increment counter by (0x27c9c9ca)*2^14

if port_hex_str[-4:] == ‘9fff’:

counter += (0x27c9c9ca)*(2**14)

# if the port ends in ‘fff’ increment counter by (0xc9c9ca)*2^14

elif port_hex_str[-3:] == ‘fff’:

counter += (0xc9c9ca)*(2**14)

# if the port ends in ‘9ff’ increment counter by (0x27c9ca)*2^14

elif port_hex_str[-3:] == ‘9ff’:

counter += (0x27c9ca)*(2**14)

# if the port ends in ‘ff’ increment counter by (0xc9ca)*2^14

elif port_hex_str[-2:] == ‘ff’:

counter += (0xc9ca)*(2**14)

# if the port ends in ‘9f’ increment counter by (0x27ca)*2^14
```

```
elif port_hex_str[-2:] == '9f':

counter += (0x27ca)*(2**14)

# if the port ends in '9' increment counter by (0x28)*2^14

elif port_hex_str[-1:] == '9':

counter += (0x28)*(2**14)

# if the port ends in 'f' increment counter by (0xca)*2^14

elif port_hex_str[-1:] == 'f':

counter += (0xca)*(2**14)

# otherwise increment counter by 2^14

else:

counter += 2**14

# copy the highest 14 bits of the counter to the lowest 14 bits

first_3chars = hex(counter >> 32)[-4:]

if first_3chars[0] == 'x':

first_3chars = first_3chars[1:]

counter = ((counter >> 12) << 12) | int(first_3chars,16)

return ports_passwds
```

References

1 J. B. Ullrich, "SANS Internet Storm Center," February 2014. [Online]. Available: https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Captured/17630.

2 Fortinet, "TheMoon – A P2P Botnet Targeting Home Routers," October 2016. [Online]. Available: https://www.fortinet.com/blog/threat-research/themoon-a-p2p-botnet-targeting-home-routers.html.

3 N. 360, "TheMoon Botnet a Review and New Features," January 2018. [Online]. Available: https://blog.netlab.360.com/themoon-botnet-a-review-and-new-features/.

4 N. 360, “GPON Exploit in the Wild – TheMoon Botnet Join in with a 0day,” May 2018. [Online]. Available: https://blog.netlab.360.com/gpon-exploit-in-the-wild-iv-themoon-botnet-join-in-with-a-0day/.

5 VirusTotal. [Online]. Available: https://www.virustotal.com/#/domain/domstates.su.

CybersecurityLumen

Author

Black Lotus Labs

The mission of Black Lotus Labs is to leverage our network visibility to help protect customers and keep the internet clean.

Services not available everywhere. ©2022 Lumen Technologies. All Rights Reserved.