

Botnet

快讯：使用21个漏洞传播的DDoS家族WSzero已经发展到第4个版本



Hui Wang, Alex.Turing

Dec 7, 2022 • 7 min read

概述

近期，我们的BotMon系统连续捕获到一个由Go编写的DDoS类型的僵尸网络家族，它用于DDoS攻击，使用了包括SSH/Telnet弱口令在内的多达22种传播方式。短时间内出现了4个不同的版本，有鉴于此，我们认为该家族未来很可能继续活跃，值得警惕。下面从传播、样本和跟踪角度分别介绍。

传播分析

除了Telnet/SSH弱口令，我们观察到wszero还使用了如下 21 个漏洞进行传播：

VULNERABILITY	AFFECTED
CVE_2014_08361	Realtek SDK
CVE_2017_17106	Zivif Webcams
CVE_2017_17215	Huawei HG532
CVE_2018_12613	phpMyAdmin 4.8.x before 4.8.2
CVE_2020_10987	Tenda AC15 AC1900
CVE_2020_25506	D-Link DNS-320 FW v2.06B01 Revision Ax
CVE_2021_35395	Realtek Jungle SDK
CVE_2021_36260	Hikvision DVR
CVE_2021_46422	Telesquare SDT CW3B1

VULNERABILITY	AFFECTED
CVE_2022_01388	F5 BIG-IP
CVE_2022_22965	Spring
CVE_2022_25075	TOTOLINK A3000RU
CVE_2022_26186	TOTOLINK N600R
CVE_2022_26210	TOTOLINK A830R
CVE_2022_30525	Zyxel Firewall
CVE_2022_34538	Digital Watchdog DW MEGApix IP cameras
CVE_2022_37061	FLIR AX8 thermal sensor cameras
DLINK	D-Link DSL-2750B
CVE-2018-10561	Dasan GPON home router
SAPIDO RB-1732 command line execution	SAPIDO RB-1732
PHP Backdoor	PHP 8.1.0 dev Backdoor

样本分析

简单来说，wszero是一个Go语言编写的DDoS类型的僵尸网络家族，它被命名为wszero的原因是它的下载链接中的文件名多为 `zero.*` 这种形式，并且最新版本C2协议基于 `websocket`，所以将其缩写为 `wszero`。基于样本的C2协议、主机行为和C2加密等方面特征，我们把已经捕获的wszero分为4个大的版本，其捕获的时间线如下：

- 2022年11月18日，首次捕获到wszero v1
- 2022年11月21日，捕获到V2样本
- 2022年11月24日，捕获到V3样本
- 2022年11月26日，捕获到V3.x样本
- 2022年11月29日，捕获到V4样本

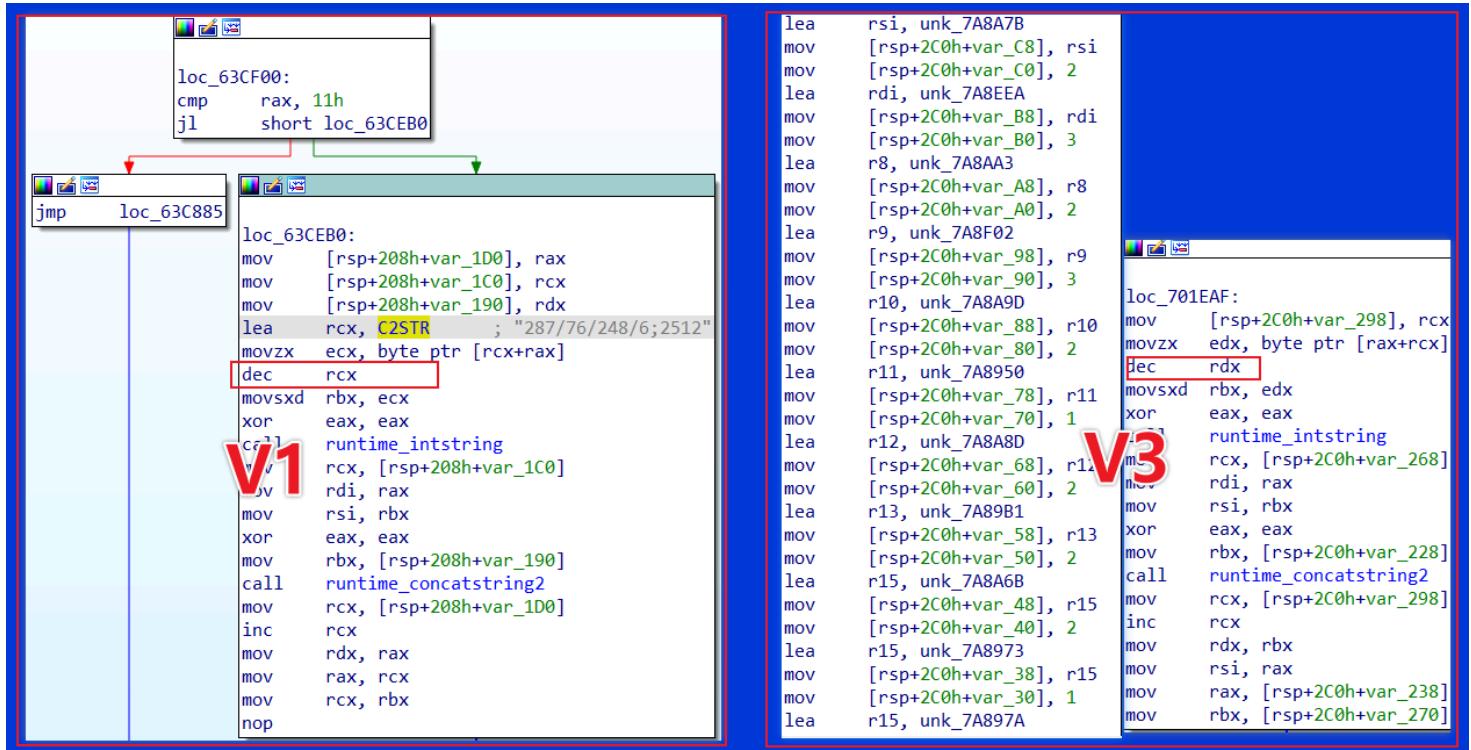
下面是这4个版本一些具体特性的对比：

VERSION	C2	DECRYPTION	EXPLOIT	TEL/SSH CRACK	PROTOCOL	PLATFORM
v1	176.65.137.5:1401	SUB1	0	No	TCP	Linux
v2	176.65.137.5:80	NO	0	No	WS	Linux
v3	zero.sudolite.ml	SUB 1	0	No	WSS	Linux
v3.x	zero.sudolite.ml	SUB1	21	YES	WSS	Linux/Winc
v4	176.65.137.5:80	SUB1	21	YES	WS	Linux/Winc

因为使用Go编写并且未作混淆，从wszero样本中能容易的恢复出函数符号和功能逻辑等，因此我们不做详细的样本分析，下面着重介绍下wszero的C2存储和通信。

C2存储和解密

V1和V3都使用了加密的方式存储C2，其中V1的C2保存在样本的rodata段中，而V3则存放在局部变量中，如下图所示。



它们的解密方法相同，都为**SUB 1**算法，即逐字节减一。上图中将V3的局部变量拼接后，再进行解密就得到了C2以及URI。

The screenshot shows a hex editor interface. On the left, under 'Recipe', there's a 'SUB' operation with a key of '1' and a 'HEX' dropdown. The 'Input' field contains the string 'xtt;00{fsp/tvepmjuf/nm0iboemf'. The 'Output' field contains the string 'wss://zero.sudolite.ml/handle'. Both the 'Input' and 'Output' fields are highlighted with a red border.

C2协议

Wszero的C2消息使用了一个自定义的JSON串，不同版本间有几个JSON字段的微小差别。最初版本的底层传输协议使用TCP，后续版本换成了WEBSOCKET，以及TLS保护的WEBSOCKET，下面分别介绍。

上线包格式

当C2连接建立后，C2会主动向BOT发送Banner信息提示输入用户名，BOT首先向C2发送硬编码的用户名，接着再发送JSON格式的BotInfo，形如 `{"platform": "%s", "gcc": "%s", "cpu": %d, "payload": "%s"}`，其中payload指的是分组信息。

00000000 ff fd 18	...
00000003 1b 5d 30 3b 57 65 6c 63 6f 6d 65 20 74 6f 20 42	.]0;Welc ome to B
00000013 75 6e 6e 79 4e 65 74 2c 20 4c 6f 67 69 6e 20 52	unnyNet, Login R
00000023 65 71 75 69 72 65 64 07	equired.
0000002B 55 73 65 72 6e 61 6d 65 20 c2 bb 20	Username ..
00000000 42 75 6e 6e 79 42 6f 74 37 34 38 35 32 32 32 32	BunnyBot 74852222
00000010 36 0d 0a	6..
00000013 7b 22 70 6c 61 74 66 6f 72 6d 22 3a 20 22 6c 69	{"platfo rm": "li
00000023 6e 75 78 22 2c 20 22 67 63 63 22 3a 20 22 61 6d	nux", "g cc": "am
00000033 64 36 34 22 2c 20 22 63 70 75 22 3a 20 33 32 2c	d64", "c pu": 32,
00000043 20 22 70 61 79 6c 6f 61 64 22 3a 20 22 44 69 72	"payloa d": "Dir
00000053 65 63 74 22 7d	ect"}

V1

V1版本采用了TCP，V2和V4基于WEBSOCKET，V3同样基于WEBSOCKET，但强制使用TLS对WEBSOCKET进行保护。

以V2为例，BOT和C2首先进行建立ws连接，

```
GET /handle HTTP/1.1
Host: 176.65.137.5
User-Agent: Go-http-client/1.1
Connection: Upgrade
Sec-WebSocket-Extensions: permessage-deflate; server_no_context_takeover;
client_no_context_takeover
Sec-WebSocket-Key: 3E1j7U00nfQWi4Q6mzAZqg==
Sec-WebSocket-Version: 13
Upgrade: websocket

HTTP/1.1 101
sec-websocket-extensions: permessage-deflate; client_no_context_takeover;
server_no_context_takeover
sec-websocket-accept: FjX18MpTMoj36hOAN2bj03HHzs=
upgrade: WebSocket
connection: Upgrade
date: Wed, 23 Nov 2022 01:06:49 GMT
server: hypercorn-h11
```

接着再发送BotInfo，内容格式依然为JSON串。

```
> WebSocket
> Line-based text data (1 lines)

0000  7b 22 50 6c 61 74 66 6f  72 6d 22 3a 22 6c 69 6e
0010  75 78 22 2c 22 47 43 43  22 3a 22 61 6d 64 36 34
0020  22 2c 22 43 50 55 22 3a  33 32 2c 22 50 61 79 6c
0030  6f 61 64 22 3a 22 44 69  72 65 63 74 22 7d 0a          {"Platform": "lin
                                                               ux", "GCC": "amd64",
                                                               ", "CPU": 32, "Payl
                                                               oad": "Di rect"}.
```

V2

指令

当Bot注册成功后，就开始等待并执行C2下发的指令。指令消息同样是JSON格式，有**Type**, **Data**, **Command** 3个key，其中**Type**用于指定DDoS或Command任务类别，**Data/Command**则分别用于存储DDoS选项，系统命令及参数。相关解析代码如下。

```

    lea    rax, _type_Struct_695fc0
    lea    rbx, [rsp+1F8h+var_D0]
    call   runtime_convT
    lea    rcx, _type_Struct_695fc0
    mov    qword ptr [rsp+1F8h+var_150], rcx
    mov    qword ptr [rsp+1F8h+var_150+8], rax
    mov    rbx, cs:os.Stdout
    lea    rax, go_itab_os.File_io_Writer
    mov    edi, 1
    mov    rsi, rdi
    lea    rcx, [rsp+1F8h+var_150]
    call   fmt_Fprintln

```

_type_Struct_695fc0 dq 48h

```

    dq 40h
    dd 0A0A0C063h
    db 7
    db 8
    db 8
    db 19h
    dq 0
    dq offset qword_7566DE
    dd 0A65Ch
    db 0C0h
    db 41h ; A
    db 1
    db 0
    dq offset off_696020
    db 3

```

off_696020 dq offset unk_654707 ; DATA XREF

```

    dq offset _type_String_66f460 ; Type
    dq offset unk_65456F ; Data
    dq offset _type_Struct_6ac000
    dq 20h ; 0x10
    dq offset unk_65603B ; Command
    dq offset _type_String_66f460
    dq 70h ; 0x38
    db 0

```

下面是我们实际接收到的HTTP_BYPASS攻击指令，当Bot接收到这个指令后就会使用该方法对目标进行攻击。

```

{
  "data": {
    "method": "HTTP_BYPASS",
    "options": [
      {
        "key": "target",
        "value": "https://qeruya.cyoubot.cc"
      },
      {
        "key": "time",
        "value": "10"
      },
      ...
      {
        "key": "request_type",
        "value": "GET"
      }
    ]
  },
  "type": "attack"
}

```

除了HTTP_BYPASS, wszero还支持TCP/UDP/ICMP等多种协议的攻击方法，完整列表详见下图。

```
f main_AttackType_UDP_LEGIT_func1
f main_AttackType_UDP_LEGIT
f main_AttackType_UDP_LEGIT_func2
f main_AttackType_TCP_SOCKET_func1
f main_AttackType_TCP_SOCKET
f main_AttackType_TCP_SOCKET_func2
f main_AttackType_TCP_HANDSHAKE
f main_AttackType_MC_PING_func1
f main_AttackType_MC_PING
f main_AttackType_MC_PING_func2
f main_AttackType_TLS_SOCKET_func1
f main_AttackType_TLS_SOCKET_func2
f main_AttackType_TLS_SOCKET_func3
f main_AttackType_TCP_CUSTOM
f main_AttackType_UDP_RAW
f main_AttackType_ICMP_FLOOD
f main_AttackType_HTTP_RAW_func1
f main_AttackType_HTTP_RAW
f main_AttackType_HTTP_RAW_func2
f main_AttackType_HTTP_HANDLE
f main_AttackType_HTTP_BYPASS_func1
f main_AttackType_HTTP_BYPASS
f main_AttackType_HTTP_BYPASS_func2
f main_AttackType_HTTP_NULL_func1
f main_AttackType_HTTP_NULL
f main_AttackType_HTTP_NULL_func2
```

指令跟踪情况

分析出这个新家族后，我们迅速做了跟踪处理，在2022年11月23日首次接收到DDoS攻击指令，具体DDoS攻击趋势如下图所示：



能看出来其攻击指令的下发并不是很频繁，这可能跟这个家族还处于早期发展阶段有关。目前其C2仍在活跃，并且频繁下发更新指令。

结尾

今年我们已经观察到多起使用Go开发的全新botnet家族，wszero只是其中之一。其作者在10多天的时间内做了4次大的升级，说明该家族还在发展之中，未来可能会继续推出新的版本。对此我们会持续关注，有新的发现将会及时公开。

联系我们

感兴趣的读者，可以在 [twitter](#) 或者通过邮件netlab[at]360.cn联系我们。

解决方案

基于Netlab多年研究工作孵化的360全系列[DNS安全产品](#)均已支持文中远控服务器的拦截和检测，同时内置多种算法可有效发现和拦截各种未知威胁，建议企业客户接入360 DNS安全SaaS平台或部署本地360DNS安全产品，及时防范此类新型威胁，避免企业资产失陷。联系人：wangkun-bd@360.cn

IoC

C2

```
176.65.137.5  
zero.sudolite.ml
```

Loader IP

```
176.65.137.6  
176.65.137.5
```

Sample

```
aabca688b31eb962a7a2849c57000bea  
86827dc70c5001633b801b7b7fa8a9b9  
0642bc041c2e4a74fbf58537a2305543  
13e1966f13274c71d39e4aea7f62127e  
271aebe152b793765a75e5e89d24cdbd  
27f66ef808e5497528c653ba862822b7  
2eca5324301a55dfa5b5d2c2b67ab9d0  
342a5c7e1eb3ead0b6ddeeed4f1a811f  
3627e6848eb9f6a28c7c83b347753f26  
367b9095e93d27fc1a684a90a77e82f9  
40b3bb4e7d00377cbd9d100b39d26ac0  
45bc7cd7c7acdf679d1f3ceceb7d6602  
4a5e9ffd3ce77d5269033b8032426e45  
513a8036ca358b0acfce30903f95f12b  
52d21fbad081d699ec6e041fcdd6133c  
59d635cca6de9c417995ab5fa5501829  
5eea56fc1f7a373973dc9ff0cc8fe86f  
62c11ea75e82611b6ba7d7bf08ed009f  
62eeda48db5d0f5c6ee31112fe0c18ee  
6b6cac5bd765178545b0fa3caa0fd99b  
72ad17b874a956fdb4c969a03924aea2  
777a4bdda609735b1dd784b98fe27693  
79a7fc0ae8222f29e9c6e133f7a33b4b  
823c7b89db6a35345f205bb64769d5ef  
83d647c9749e9a5a5f9c6ae01747a713  
857dfb390d02f5ca93a37ffa2f0cbde2  
871624995190fe3310f553f0fb61b0e  
88b98664c3c901242c73e1d8f18a47eb  
8d85e3e0328cdd51c83fb68e31a28e62  
8e2efc8f7edd7dff4bad7126d30e254
```

```
8f55245e24c4e84df7e8dddd19523d93
9039df359128850de1b3ee1240b150d6
9606e8903df98f59a827be8876ace389
9d396b48773ccbc5fdb3ffc2fb7c20f6
9daae12c05a9a21c405c9319fc49c358
ae504e3f08e2fef8e95100811fe8e2be
b36b340ba9947dae7b5bab3e1330d53a
b7c841eb41d6233ff67006177a507c66
bbfefb41c71896f7433b58376218553d
bef01d6529c5250de0662547d75959b2
c5e6aae51d97acb44339ae4d5f296b4f
c8cfcc2ddb08f812f6440b8918a916c75
d418109e5d81d48da12fe271cd08c61a
da86780f3a94c1aa6ea76fdfcb5db412
de28becdc5400261a809420c5953e3
ec0d832b564606660645e15f3b28fceb
f635dfefc35ad532d2ad9a08cb4864bd
f7cde1a55211f815bc3a6aec04f731b
fcbb9872ea0fe1af63254b65c4475ee8
fe8e1f4680355b1093536165e445fa8e
```

0 Comments

 1 Login ▾



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 

Name



Share

Best Newest Oldest

Be the first to comment.

Subscribe

Privacy

Do Not Sell My Data

— 360 Netlab Blog - Network Security Research Lab at 360 —

Botnet



僵尸网络911 S5的数字遗产

Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges

警惕：魔改后的CIA攻击套件Hive进入黑灰产领域

[See all 114 posts →](#)

Botnet

警惕：魔改后的CIA攻击套件Hive进入黑灰产领域

概述 2022年10月21日，

360Netlab的蜜罐系统捕获了一个通过F5漏洞传播，VT 0检测的可疑ELF文件

ee07a74d12c0bb3594965b51
d0e45b6f, 流量监控系统提示它和IP45.9.150.144产生了SSL流量，而且双方都使用了伪造的Kaspersky证书，这引起了我们的关注。经过分析，我们确认它由CIA被泄露的Hive项目server源码改编而来。这是我...



Jan 9,

17 min



2023

read

Import 2022-11-30 11:16

P2P Botnets: Review - Status - Continuous Monitoring

Origins P2P networks are more scalable and robust than traditional C/S structures, and these advantages were recognized by the botnet authors early on and used in their botnets. In terms of time, Storm, which appeared in 2007, can be considered the progenitor of this area, when botnet threats were



Nov 3,

9 min



2022

read