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

By Ignacio Sanmillan

Published: 2019-01-07 · Archived: 2026-04-05 22:43:34 UTC

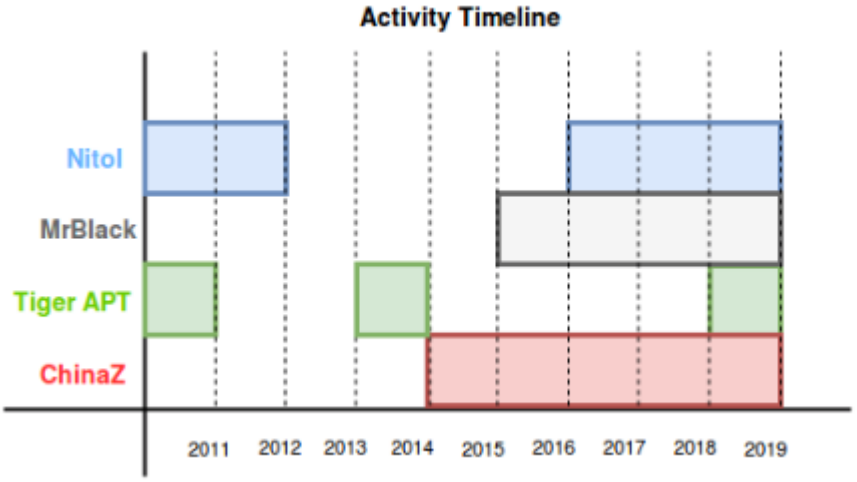
Introduction

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.



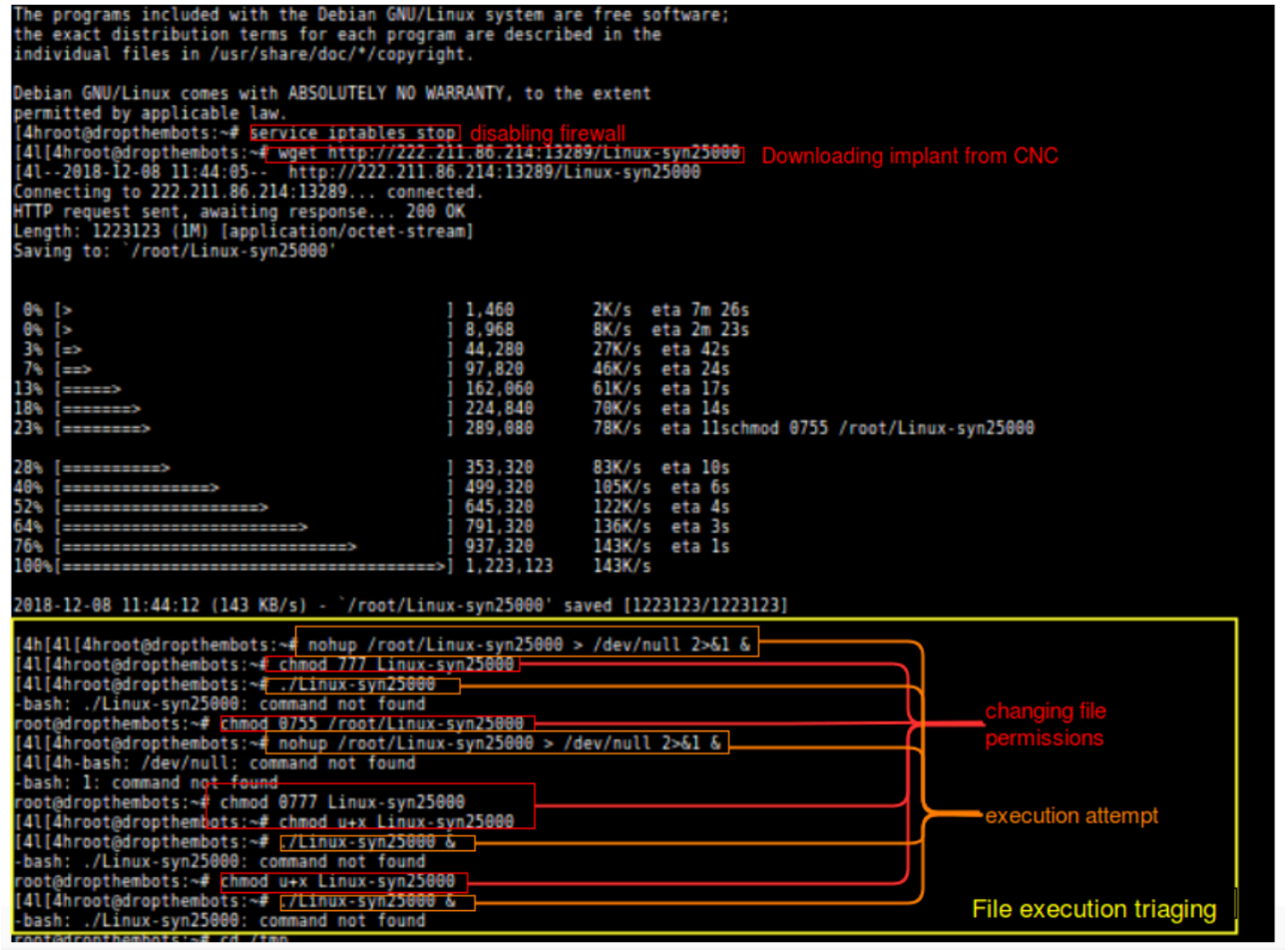
Initial ChinaZ Discovery via Honeypot Hit

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.

https://twitter.com/ulexec/status/1065743509376954368

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 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:

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:

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:

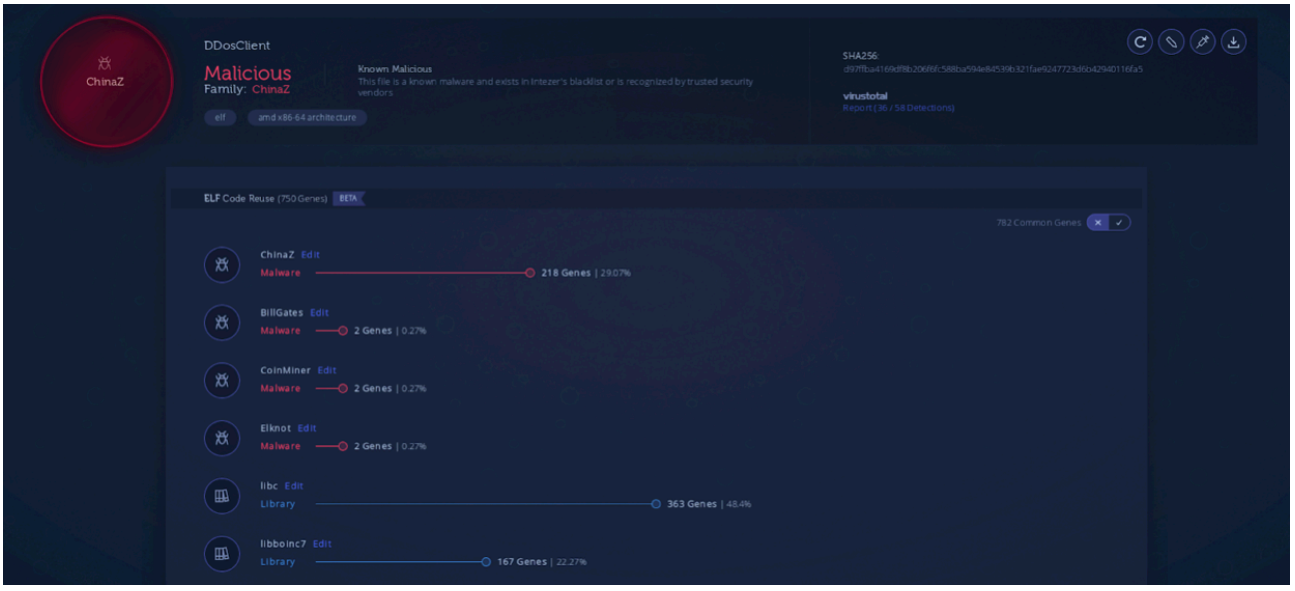
```
.text:00407C47 mov     [ebp+String], bl
.text:00407C4D rep stosd
.text:00407C4F stosw
.text:00407C51 push    354h
.text:00407C56 push    offset aWsfvsbUztqfsml          ; "Wsfvsb uztqfsml"
.text:00407C5B stosb
.text:00407C5C call    MyDecode
.text:00407C61 push    19Ah
.text:00407C66 push    offset cnc_address              ; "ak-74.top"
.text:00407C6B 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.

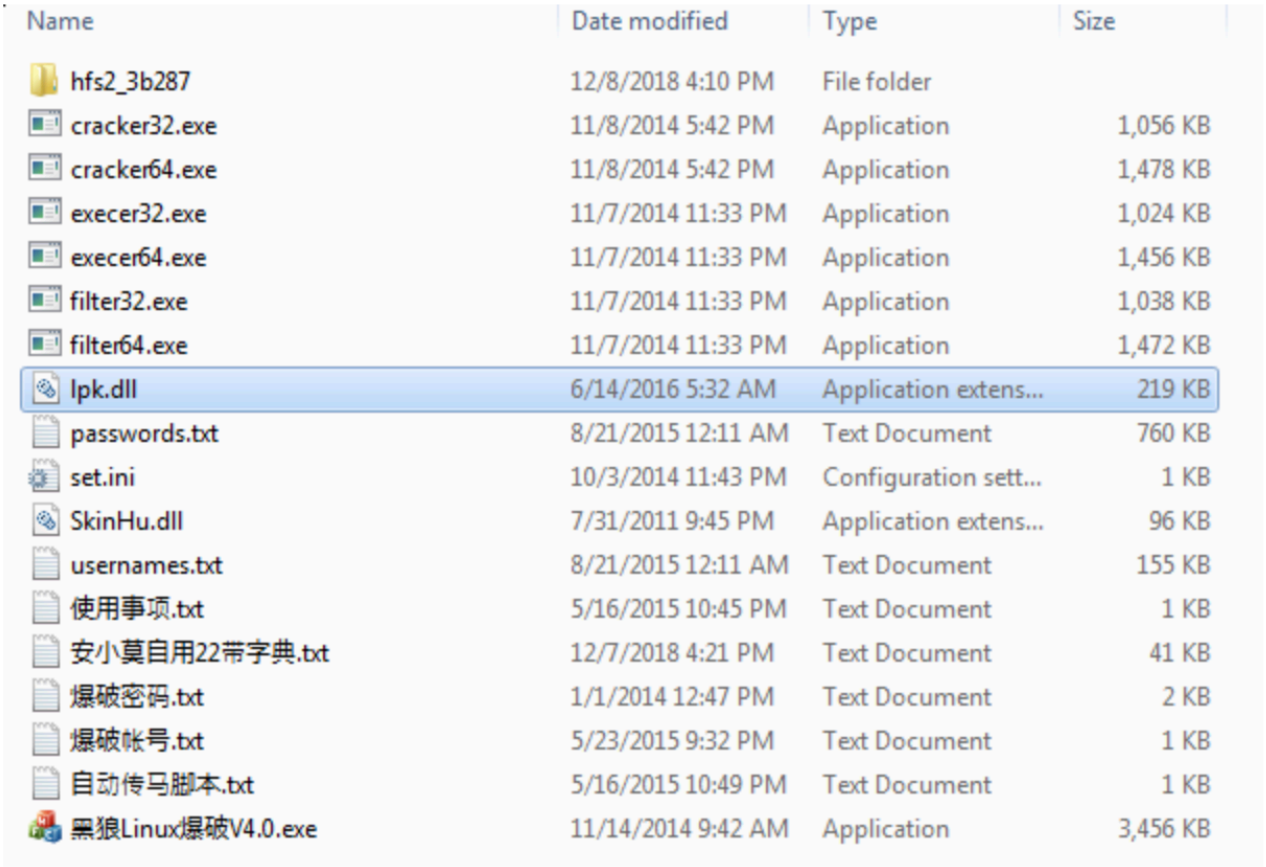
The following is a code reuse analysis of these new samples:



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

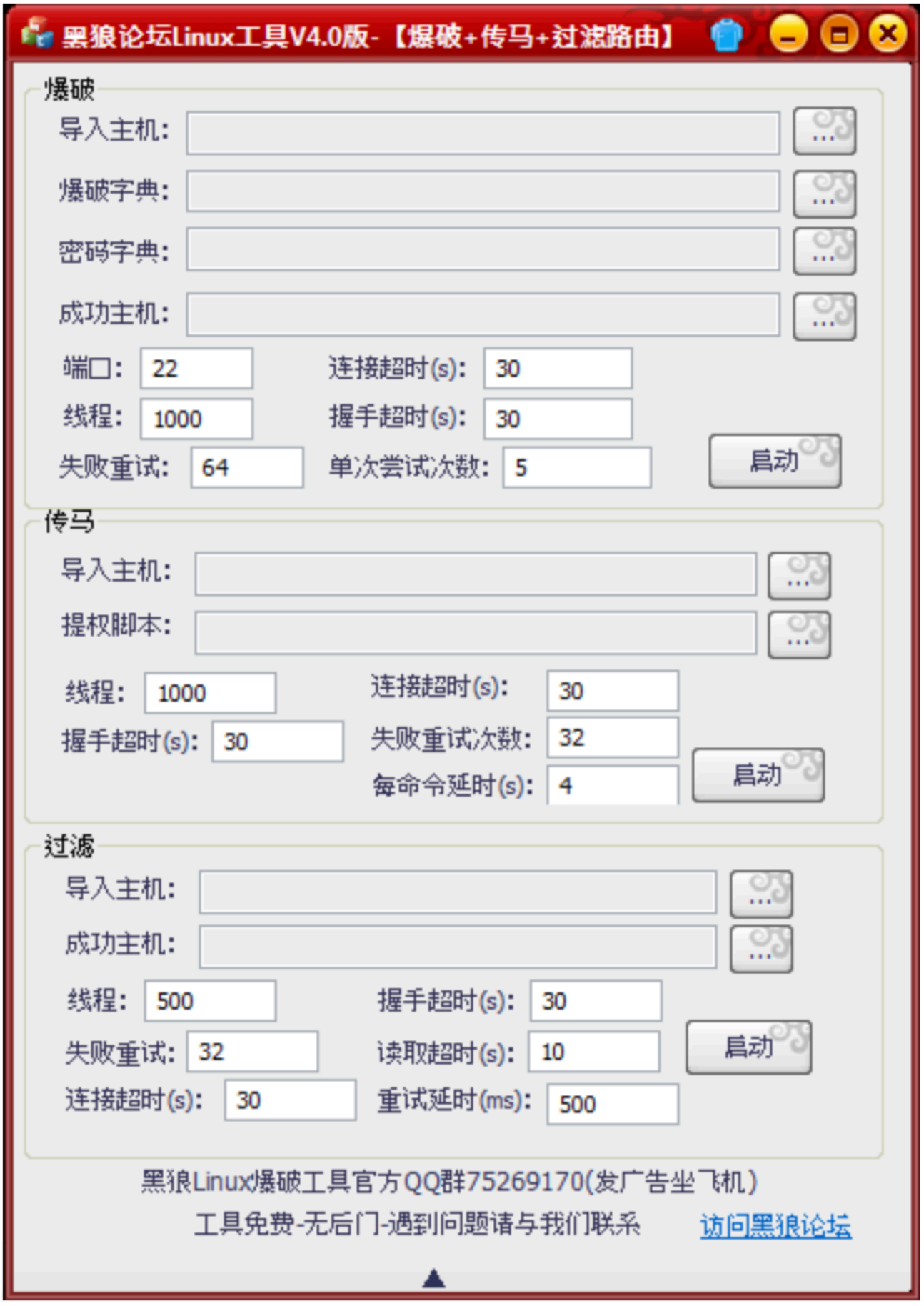
DDoSClient malware is a DDoS client known to be leveraged by ChinaZ. As an interesting fact about the progression of this threat actor group, at some point in time the source code of this client was hosted in GitHub, although DDosClient was originally code of ChinaZ. MalwareMustDie exposed this source 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:

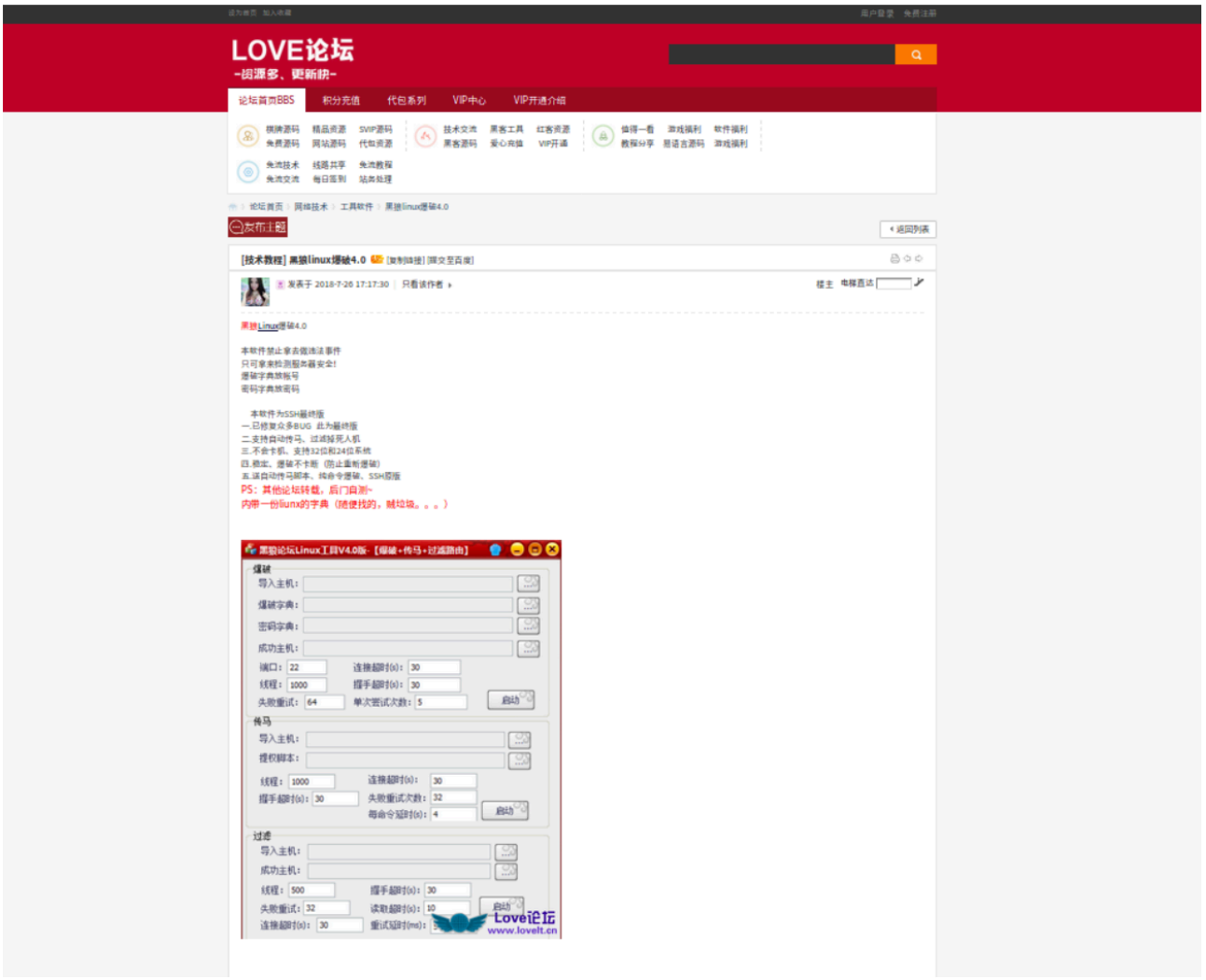


Name	Date modified	Type	Size
hfs2_3b287	12/8/2018 4:10 PM	File folder	
cracker32.exe	11/8/2014 5:42 PM	Application	1,056 KB
cracker64.exe	11/8/2014 5:42 PM	Application	1,478 KB
execer32.exe	11/7/2014 11:33 PM	Application	1,024 KB
execer64.exe	11/7/2014 11:33 PM	Application	1,456 KB
filter32.exe	11/7/2014 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

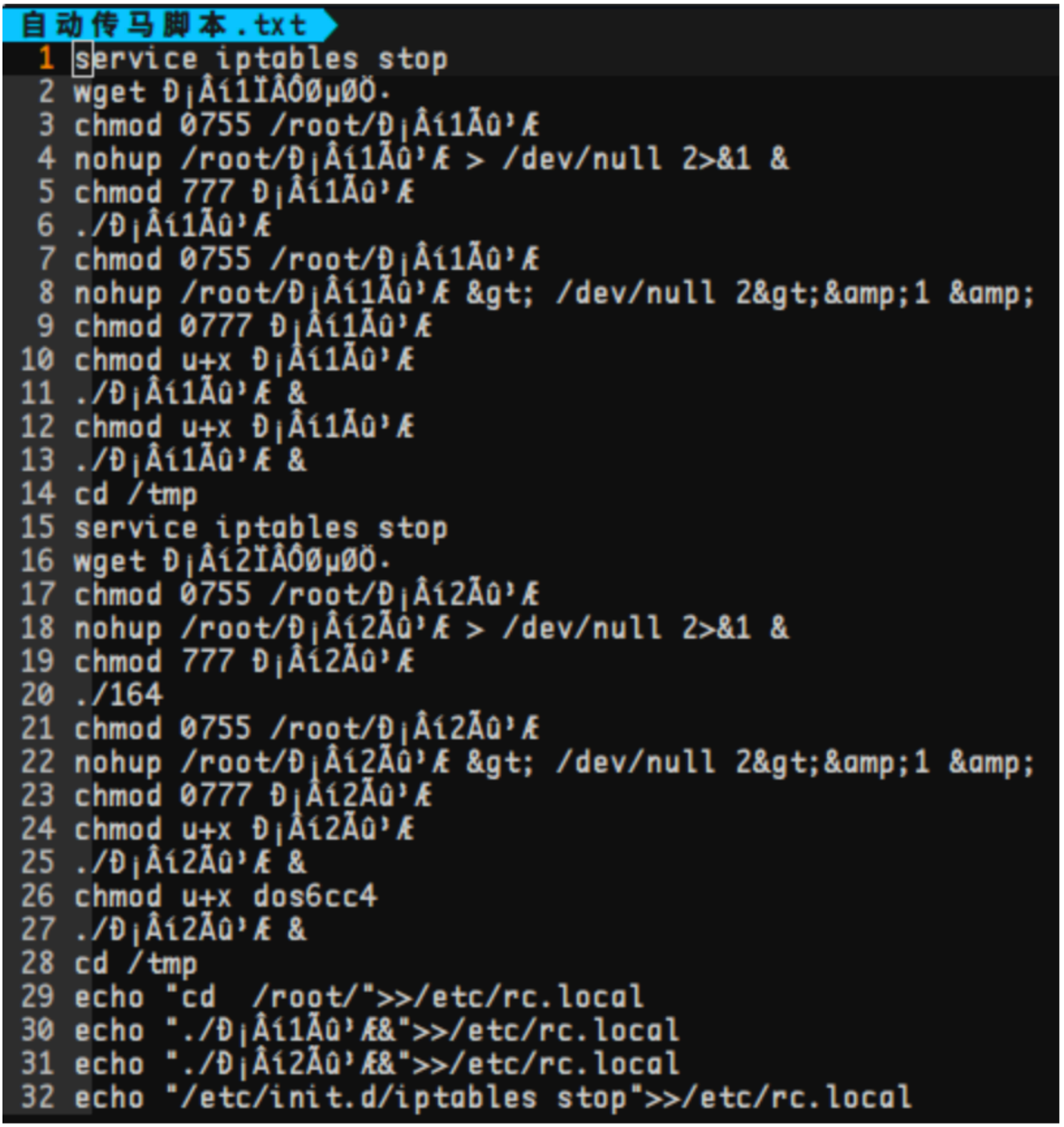
Most interestingly, the contents of this compressed file appear to be a Chinese DDoS tool:


黑狼论坛Linux工具V4.0版-【爆破+传马+过滤路由】
爆破
导入主机:
爆破字典:
密码字典:
成功主机:
端口: 22
连接超时(s): 30
线程: 1000
握手超时(s): 30
失败重试: 64
单次尝试次数: 5
启动
传马
导入主机:
提权脚本:
线程: 1000
连接超时(s): 30
握手超时(s): 30
失败重试次数: 32
每命令延时(s): 4
启动
过滤
导入主机:
成功主机:
线程: 500
握手超时(s): 30
失败重试: 32
读取超时(s): 10
连接超时(s): 30
重试延时(ms): 500
启动
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:



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

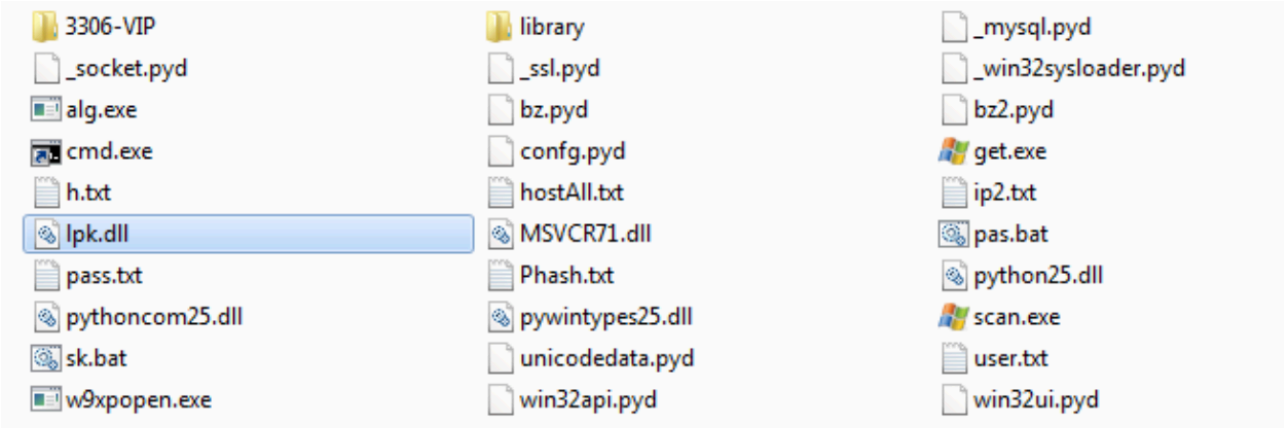
Resolve	Location	Network	ASN	First	Last	Source	Tags
58.218.66.97	CN	58.218.66.0/24	23650	2018-12-16	2018-12-16	pingly	
223.111.147.77	CN	223.108.0.0/14	56046	2018-12-16	2018-12-16	pingly	
222.211.86.214	CN	222.211.86.0/24	38283	2018-12-09	2018-12-10	pingly	
101.254.179.134	CN	101.254.176.0/22	23724	2018-09-22	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

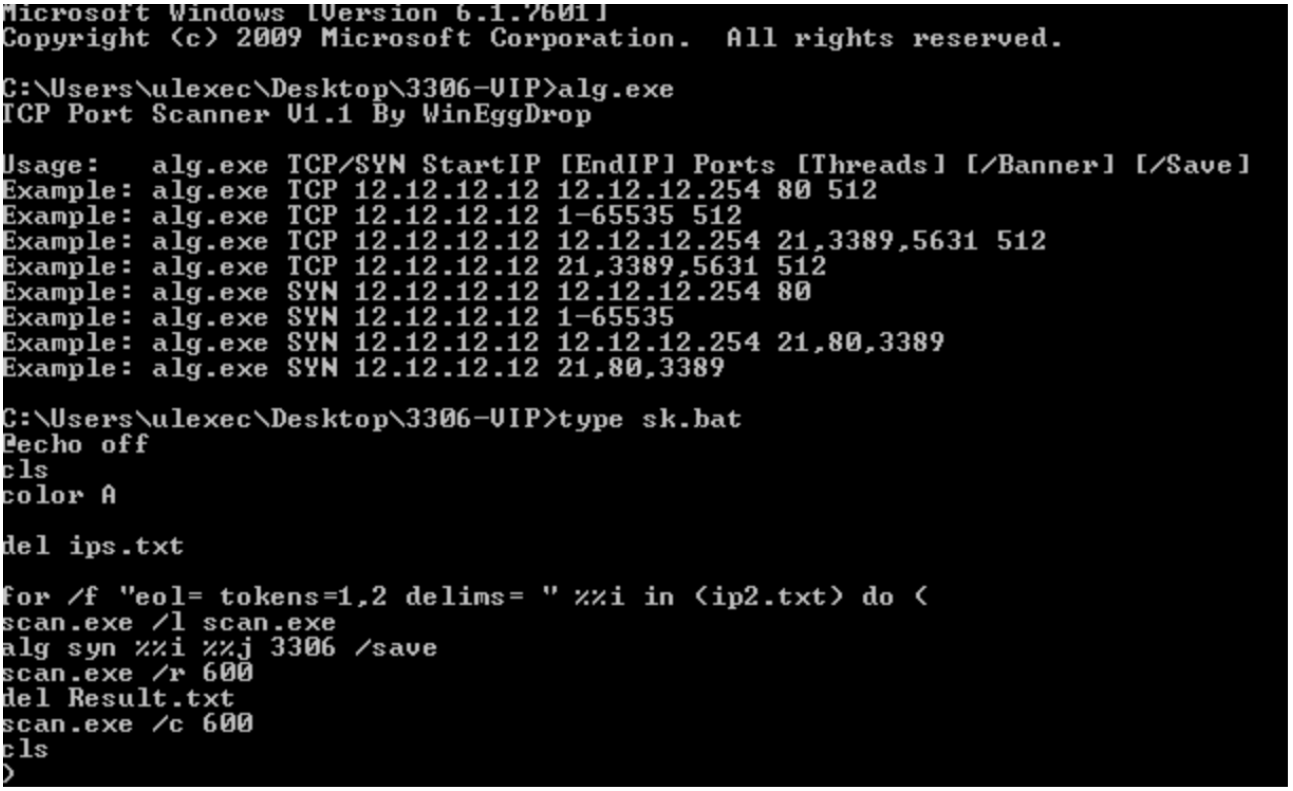
All of the shown IPs in the previous screenshot denote a server that would resolve to “ak-74.top”, the CNC address seen in the first HFS server. Based on these resolutions we were able to find other panels like the following:

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:

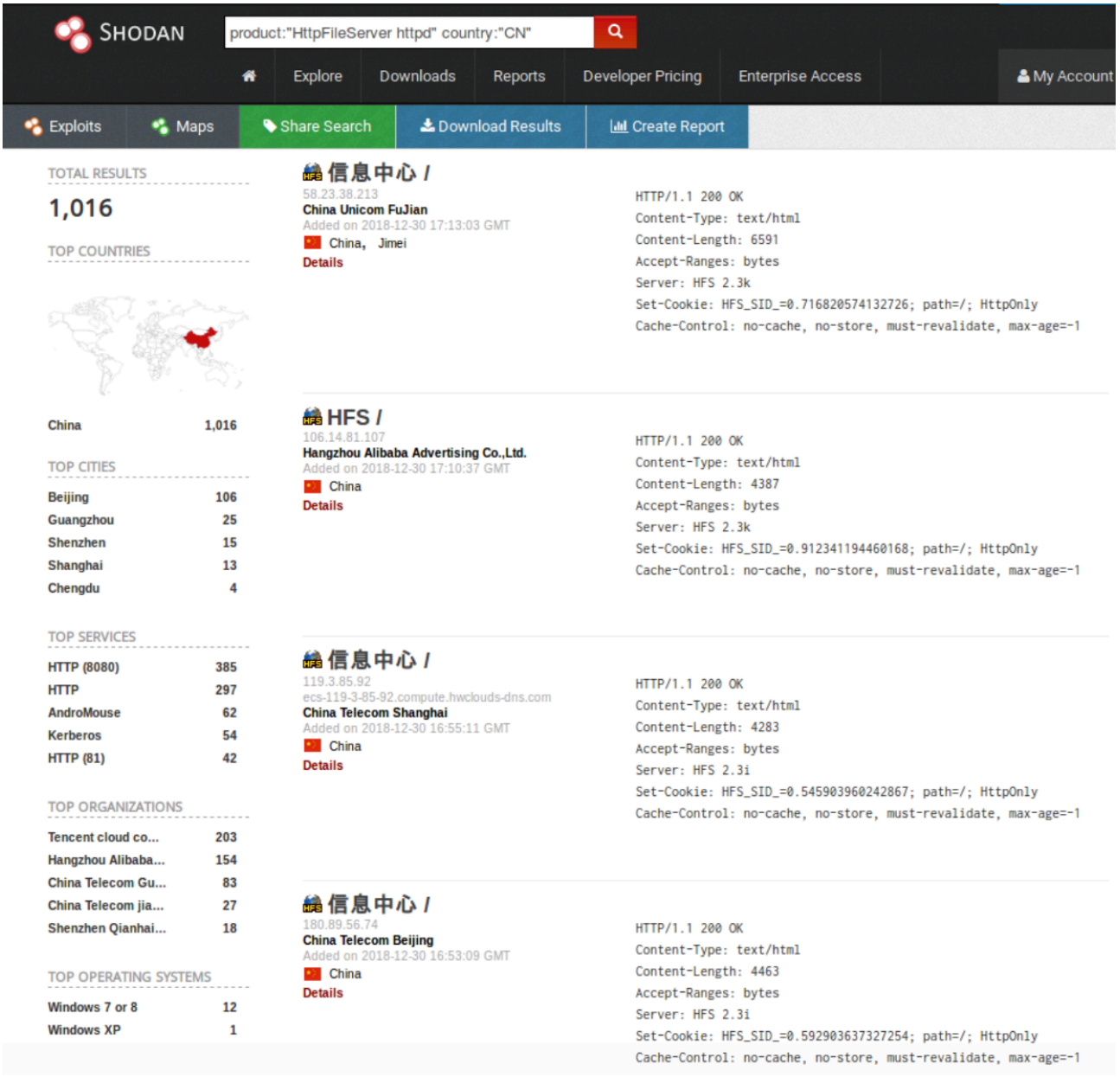


These files appear to be composing a Port Scanner tool written in python that could also be used to deploy DDoS attacks.



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.



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

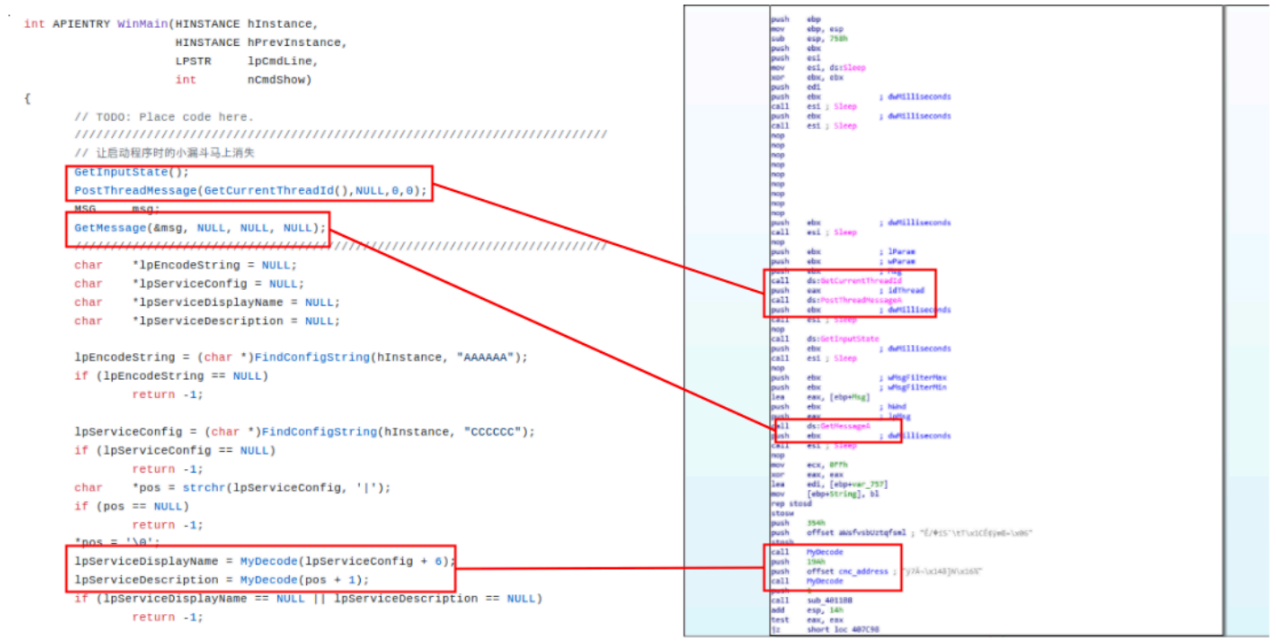
Throughout the investigation we found several interesting facts among the artifacts we collected and analyzed. The following is a brief summary of our findings:

Gh0st RAT Clients:

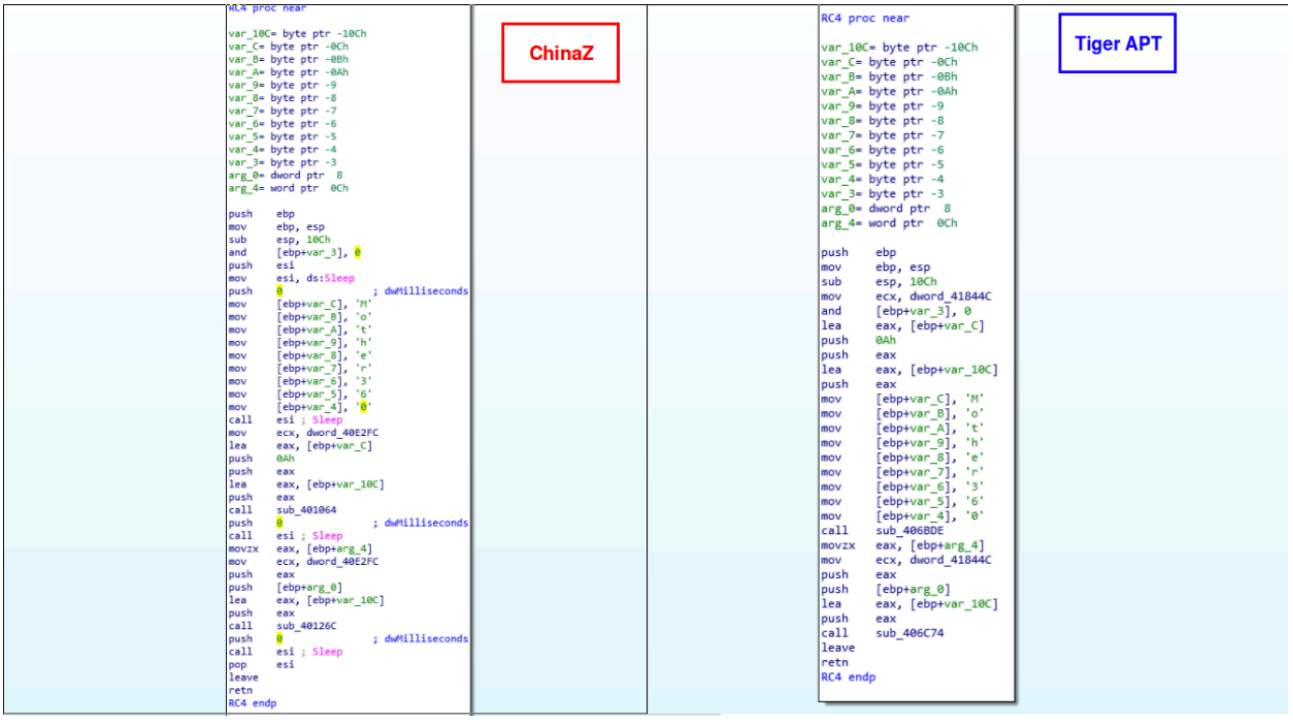
The Gh0st RAT clients we discovered among several HFS servers all appear to be modified instances of Gh0st RAT that share notable characteristics. These Gh0st RAT variants are found hosted in different HFS servers with

the names BX.exe or shadow.exe.

We can observe similarities in different functions from the open-source version hosted in GitHub. The following is a brief comparison of both files' WinMain function:

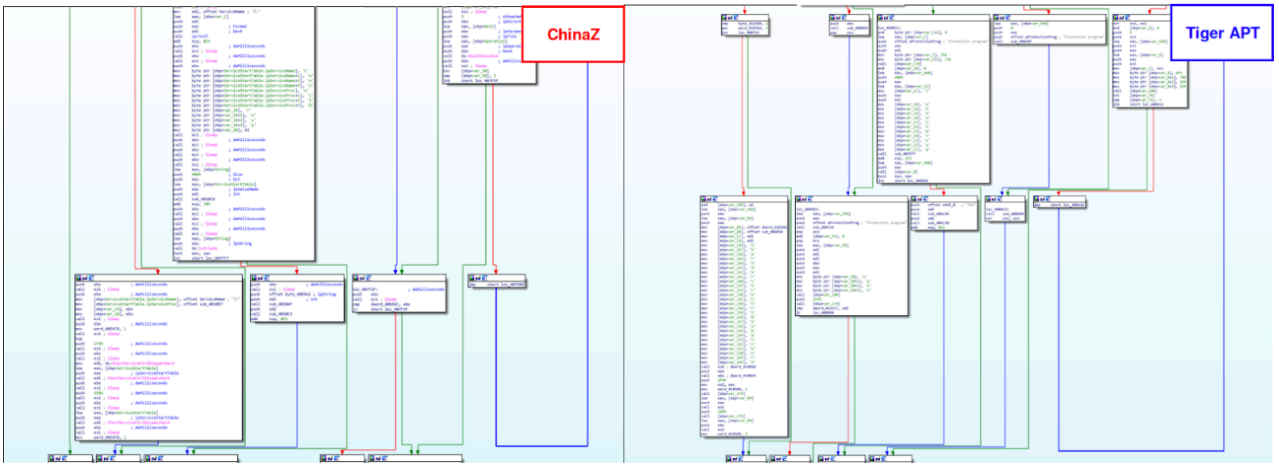


Regarding this Gh0st RAT variant, if we take a closer look we observe that it has similarities with the Gh0st RAT instance deployed on Operation PZCHAO by Iron Tiger APT, an APT group with also alleged Chinese origin. The RC4 key used to decrypt the CNC is the same as the one used in the PZCHAO campaign, "Mother360".



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:

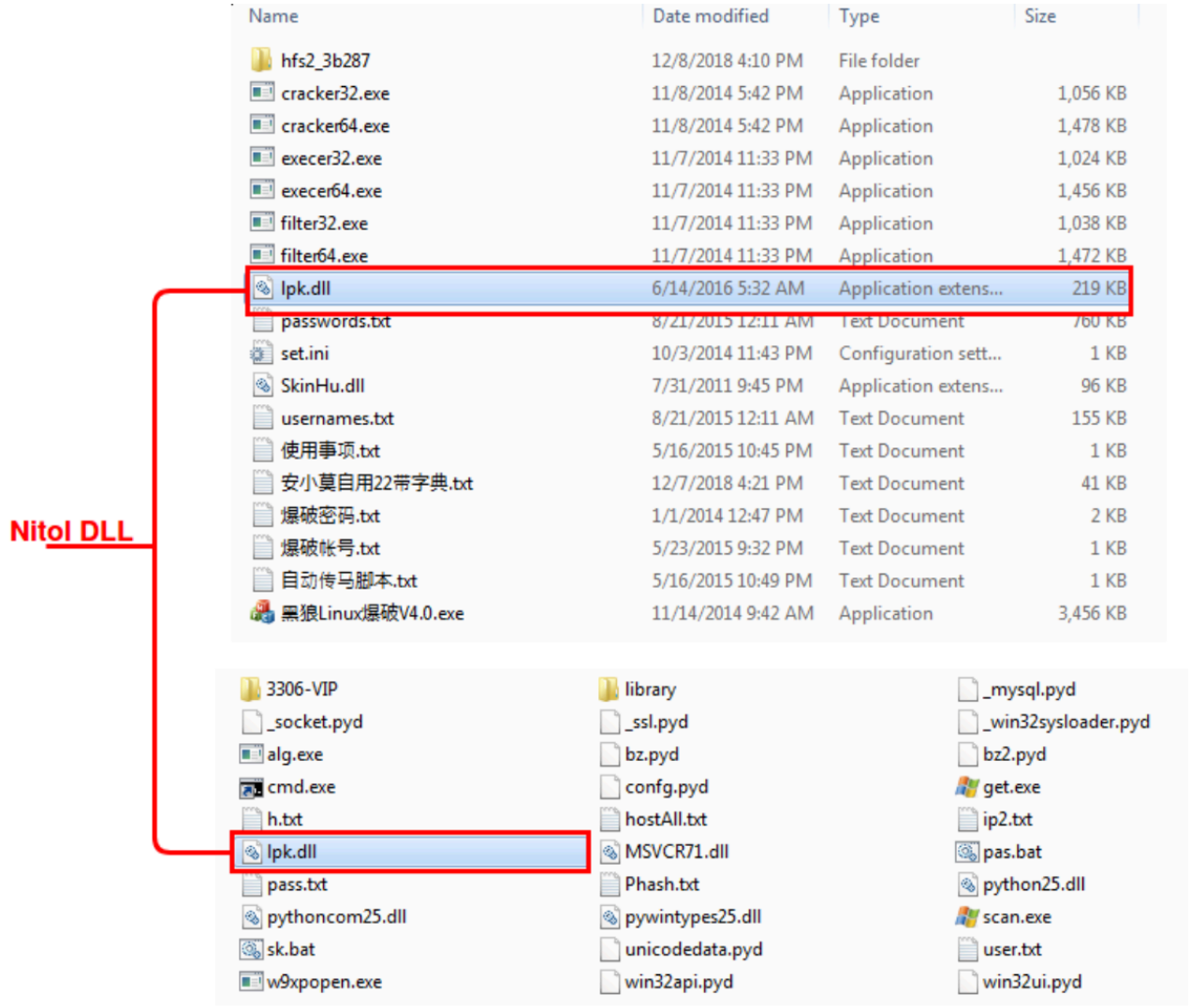


Although these two Gh0st RATs may share common code, it is important to understand how to interpret these similarities. ChinaZ has been known to employ DDoS botnets in its campaigns as previously mentioned. Usually APT groups do not rely on DDoS attacks. These similarities may not necessarily correlate 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.

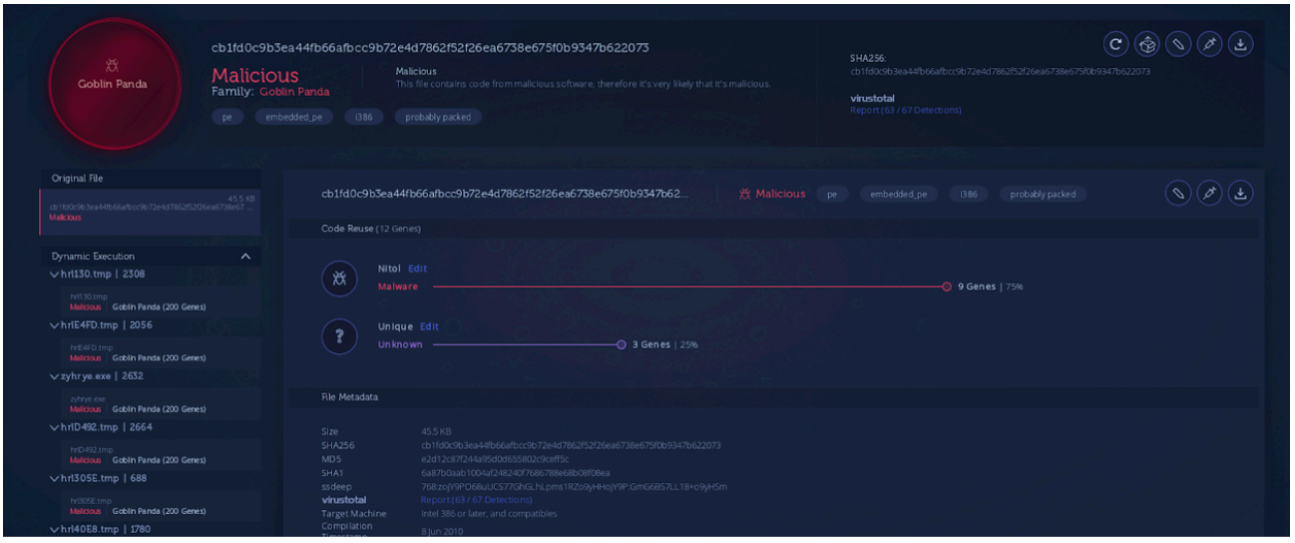
Infected Compressed Files with Nitol Artifacts:

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 Nitol, 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.



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



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.

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:

https://twitter.com/benkow_/status/961713159630393346

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.

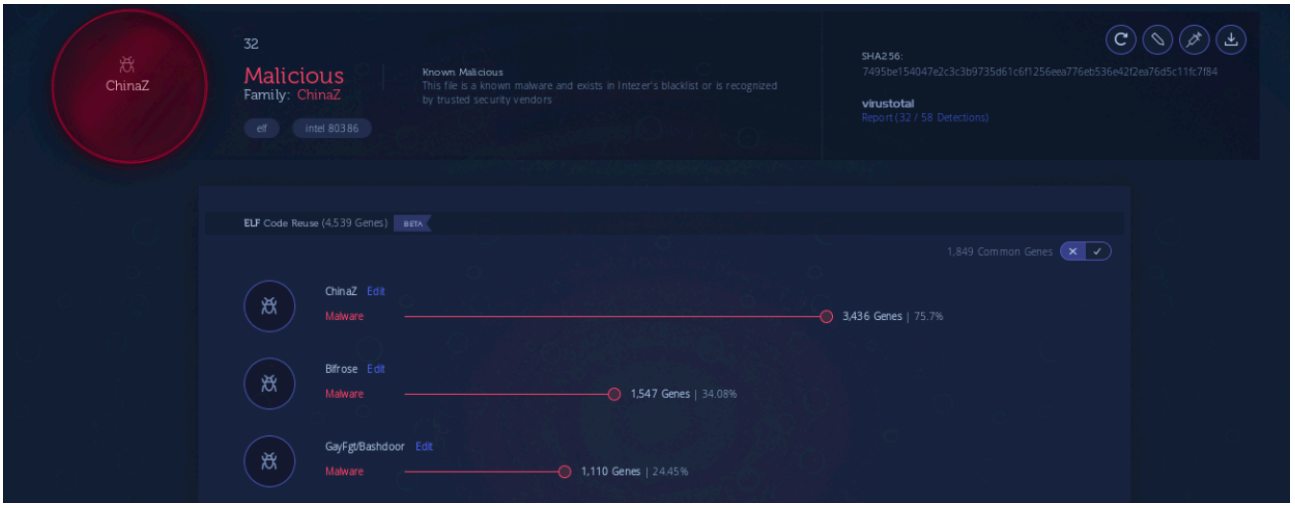
Further Connections between ChinaZ and Nitol:

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.

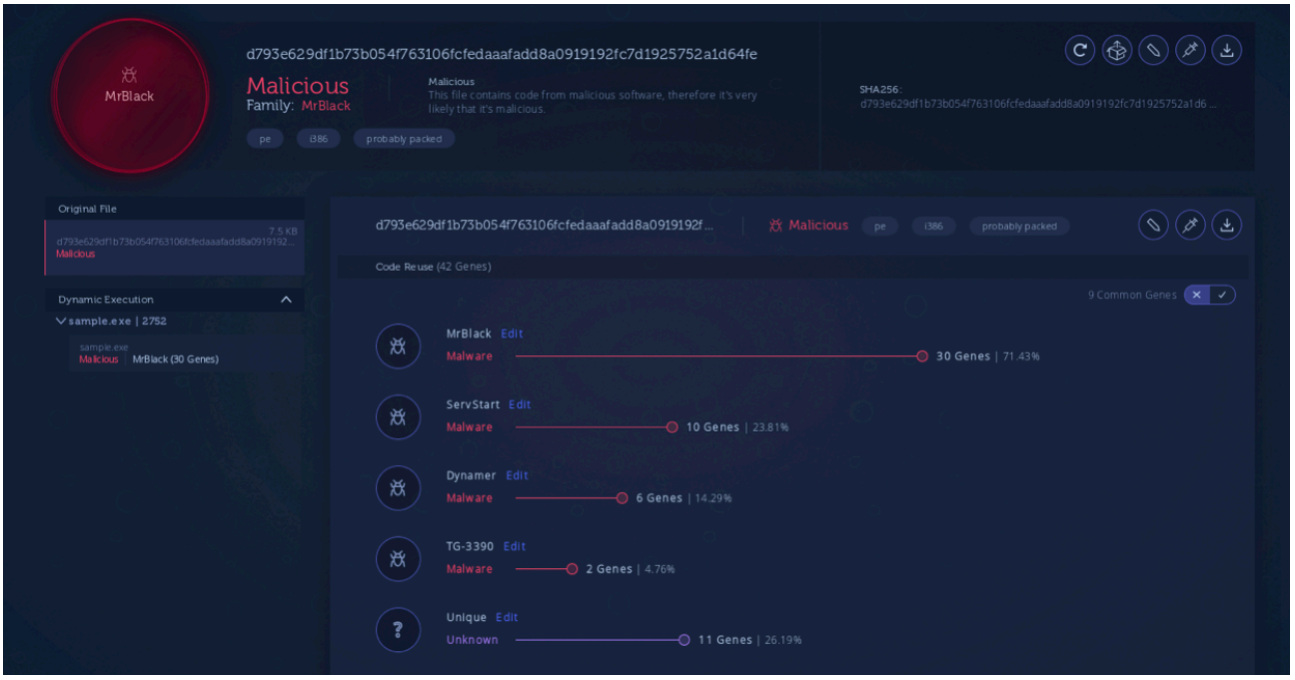
Below is a code reuse analysis of the different files found in the following HFS server:

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



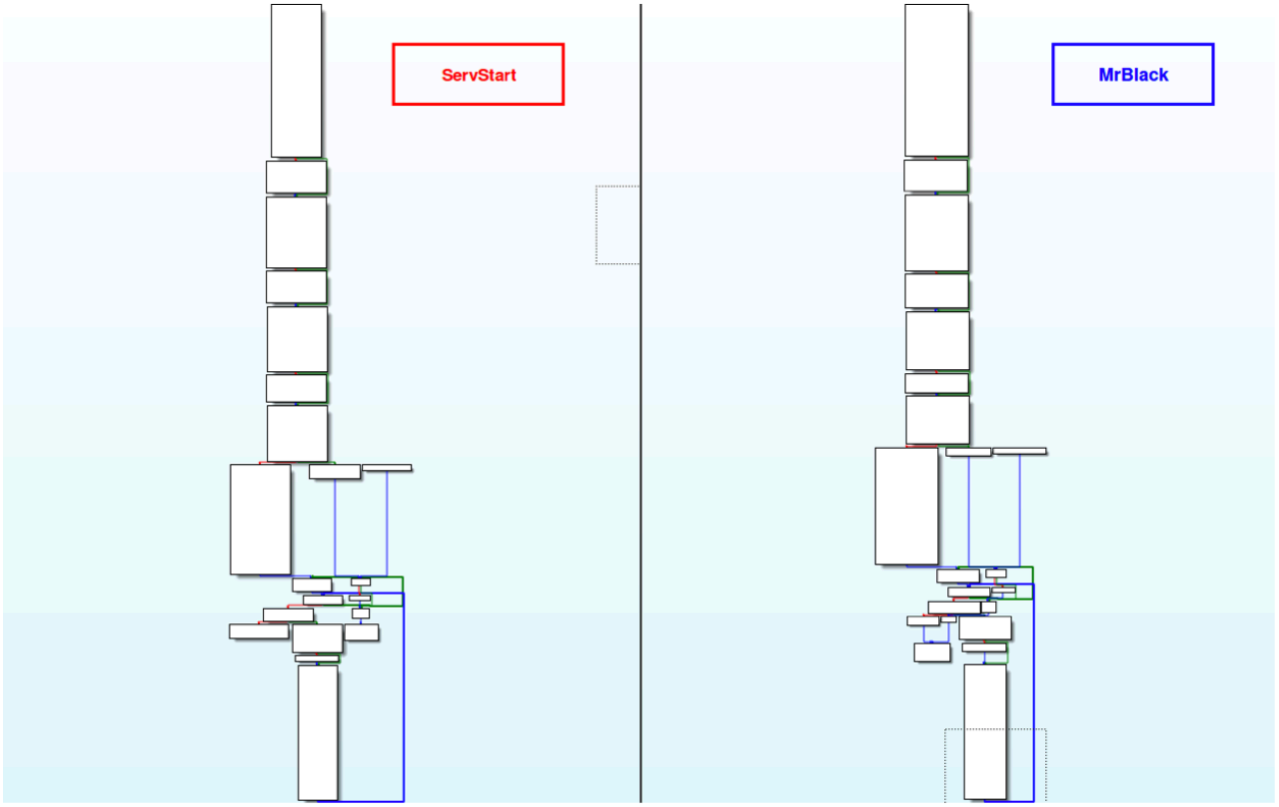
https://analyze.intezer.com/#/analyses/ab5e016c-288b-433e-aae4-a0120e55509b

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

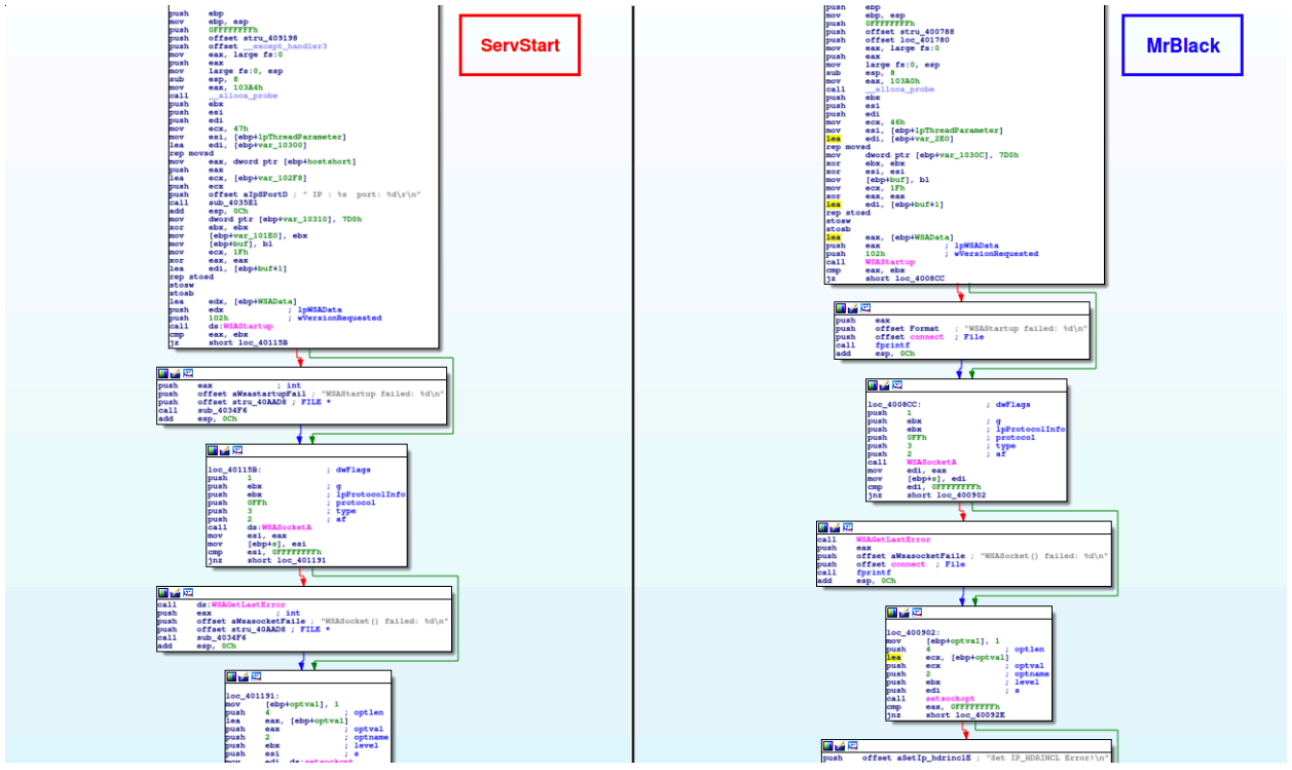


https://analyze.intezer.com/#/analyses/9ebd8c3d-2995-4bee-b5a7-6a8ae97854eb

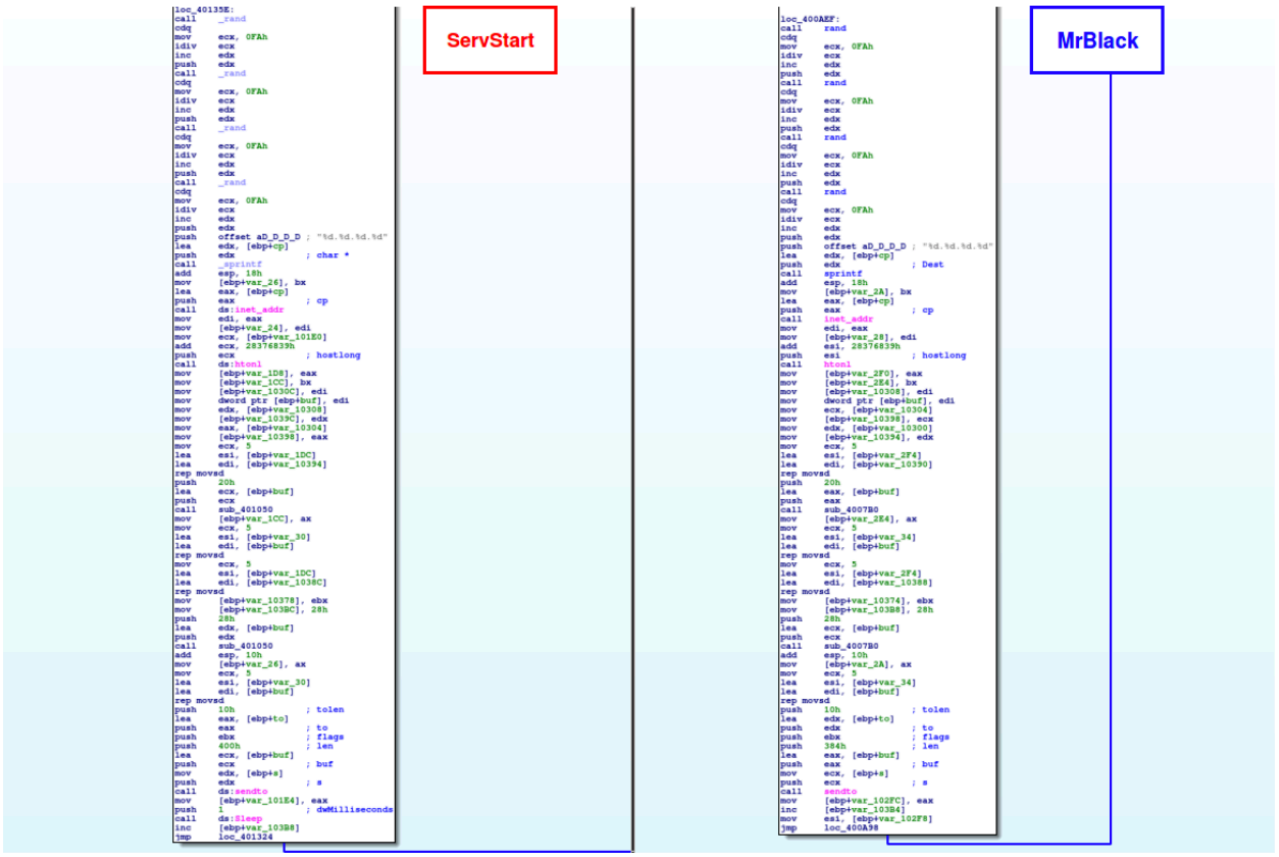
We can see that this instance of MrBlack shares 10 genes with ServStart, a trojan associated with the Nitol family. After analysis of these 10 genes we observed that this instance of MrBlack shares the exact SYN flood function as in the ServStart instance.



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

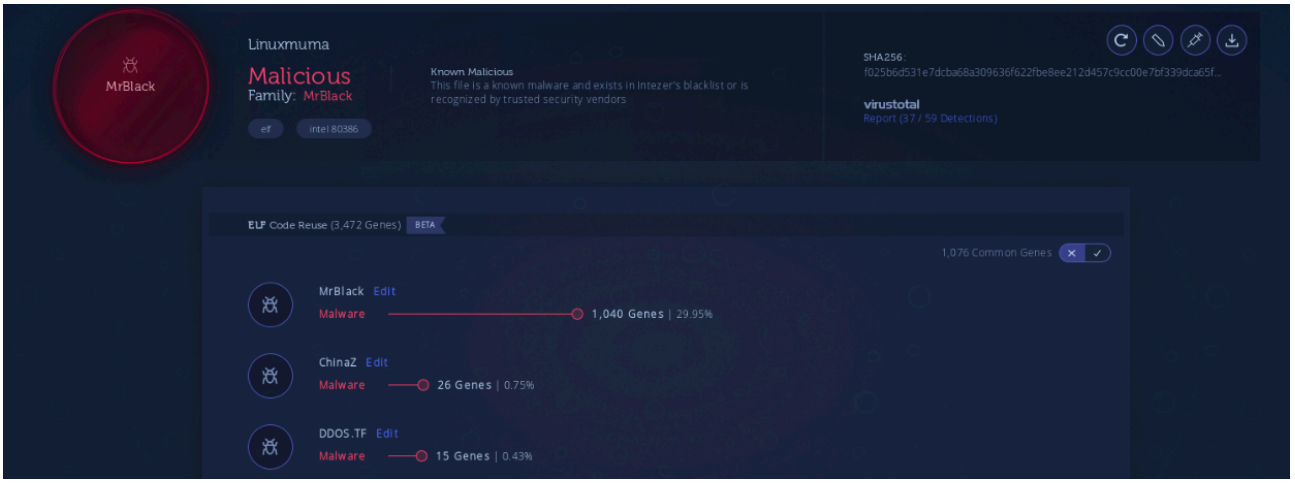


Most of the function is identical, specifically the main flood loop:



To reinforce this connection between MrBlack and ServStart, we discovered the following panel:

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:

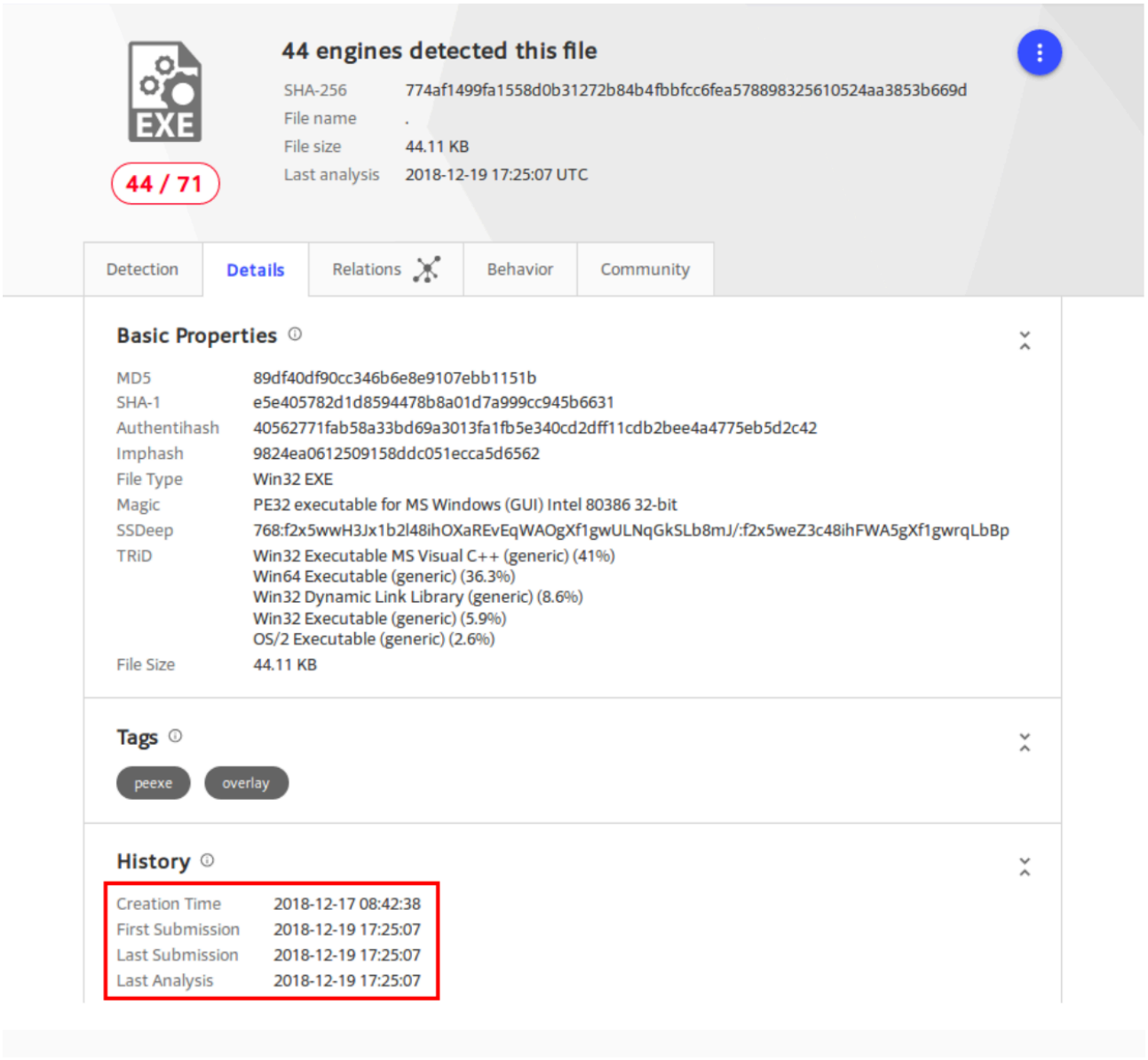


https://analyze.intezer.com/#/analyses/59ee92b0-3641-4ae0-a04e-7a4e0d21f5ce

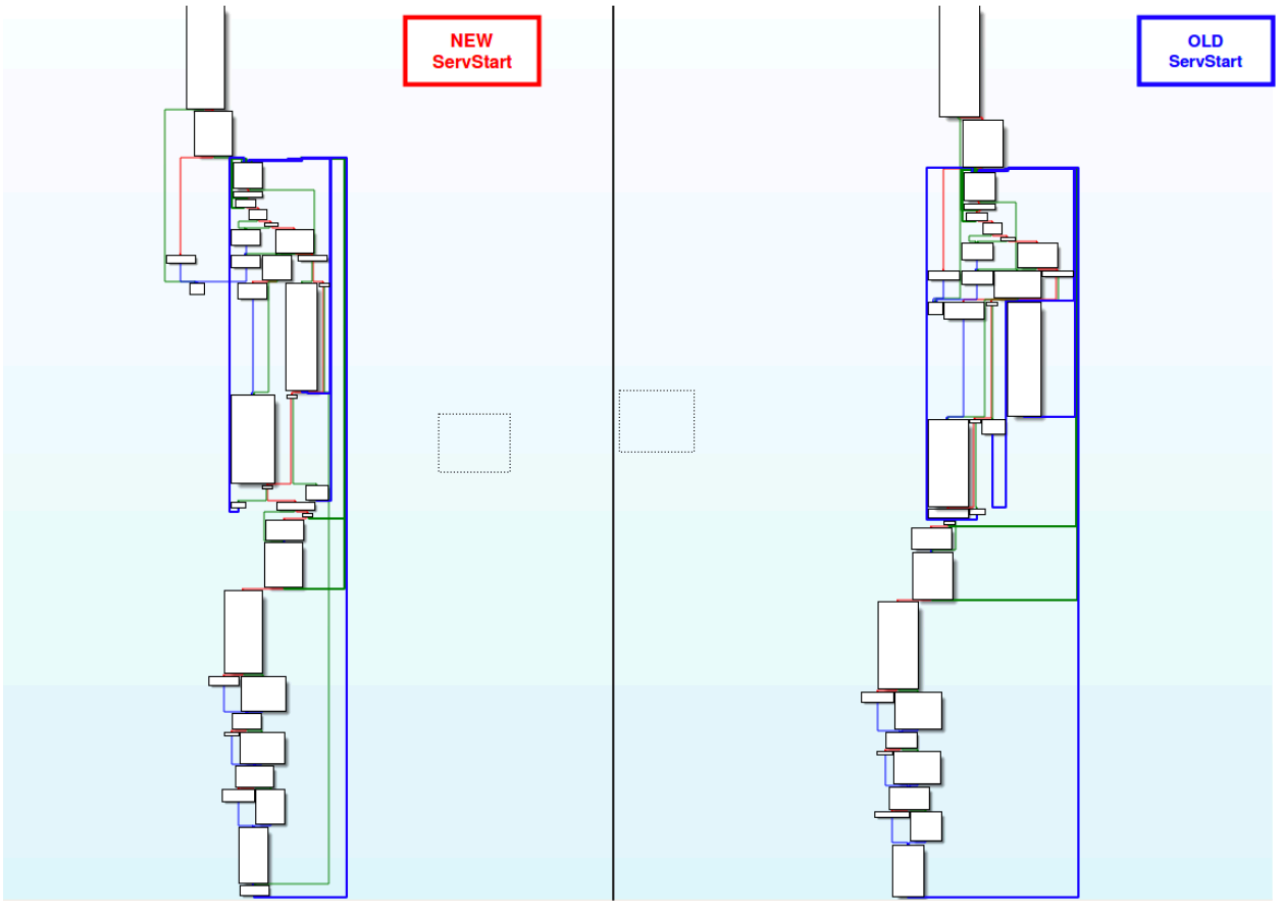
Regarding the ServStart variants, we can see that they share a substantial amount of code with respect to previous ServStart variants:

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:

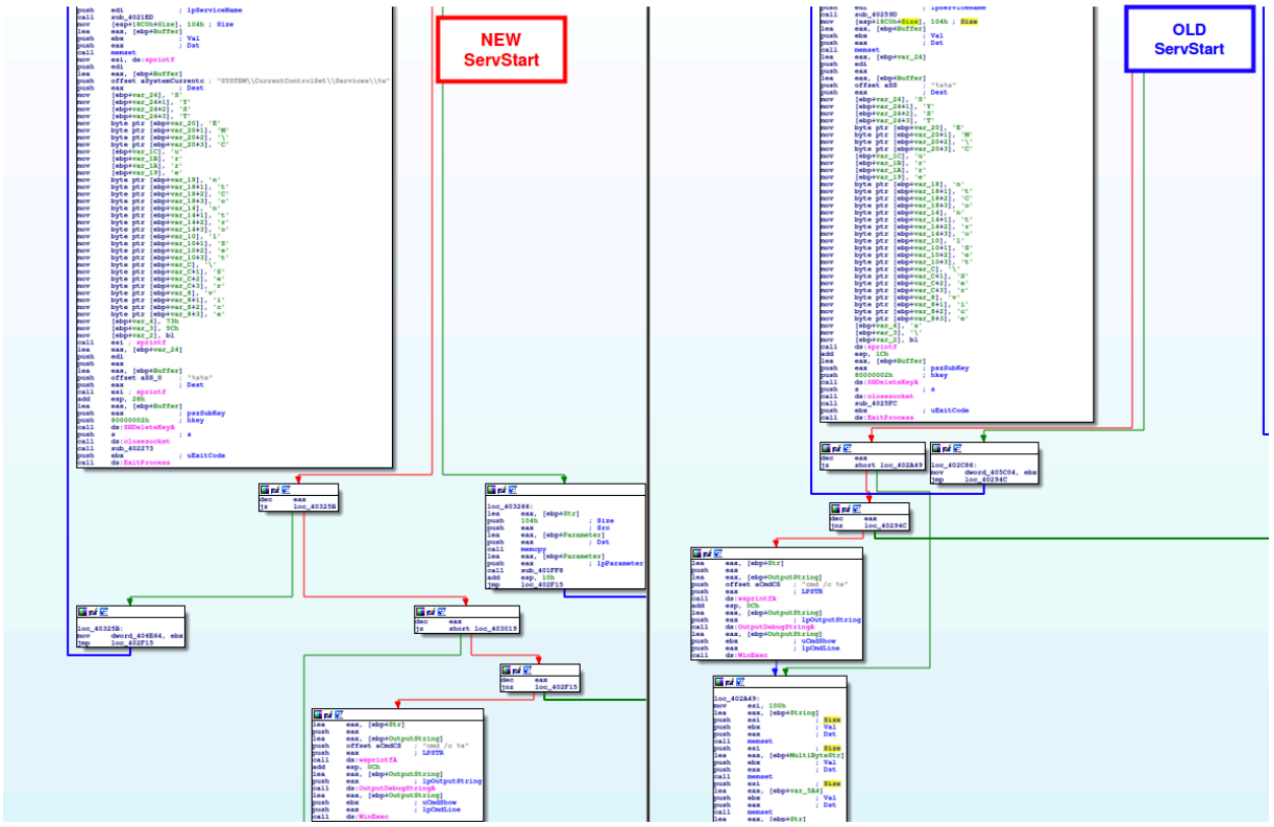


We found several nearly identical functions reused from previous variants of ServStart. The following is an example of one of these common functions.



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:

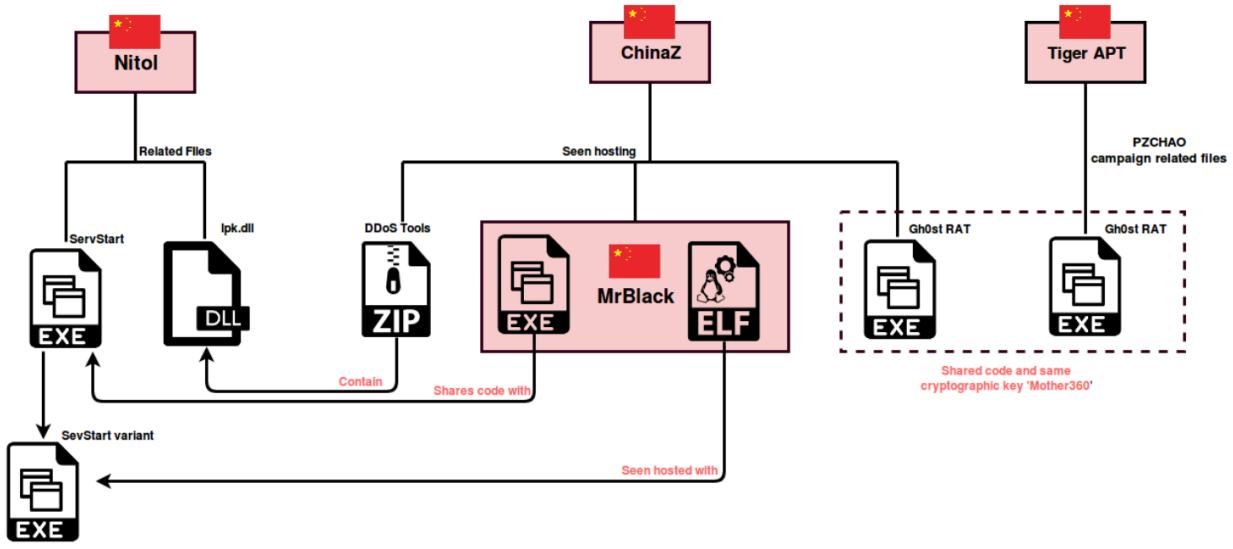
- These two groups share the same goals in their campaigns with an emphasis on the deployment of DDoS botnets.
- Both groups have alleged Chinese origins.
- A range of ChinaZ's Windows clients have been infected by old Nitol artifacts.
- These two families share relevant code with one another such as 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:

A9c54bdba780bcdc34f15b62f0ac1da8bcf4d65b4587d0d95bd2a9b5be5dfee6

908d817f81f9276f5afad1a33a7e2de7566fd5c967ad95782a4d904ca0e5efdd

9e24ba7304ae7c4f153fa8e97d2e6779d0e4377cee270b83d20d91afef7fe6f4

Iron Tiger APT gh0st RAT:

D4262bbfe779d18b83b950bb993d3d46154bf1da5a4868ff6fa3e54c167eed71

BillGates:

92c191c41bcc701de5d633a0edb8cab6085ea13ede079651a2cc4a4ae54b29bb

6fd7aab3faabd5f071d1bc9bb039146c01acf67d941c24e99813b1375114e908

Infected ChinaZ DDoS tools with Nitol:
B883b32264bcafd0c5ede5ff7399388feb51dbdf183f7ad52024c08cd221d574

23c69edc4695f6c2184484682757f024f0e20573dba599030fde1cdaeae9915c

ChinaZ.DDoSClient:

80952e211eb98773909f0f3e7ce783ce2f410327058a4760efad2ff0dbebcb88

D97ffba4169df8b206f6fc588ba594e84539b321fae9247723d6b42940116fa5

A8d0928098cc43e7b9e8ba3b03507d342489dea832816dfc083c356b346f8a3d

7495be154047e2c3c3b9735d61c6f1256eea776eb536e42f2ea76d5c11fc7f84

Win32/MrBlack:

D793e629df1b73b054f763106fcfedaaafadd8a0919192fc7d1925752a1d64fe

Linux/MrBlack:

F025b6d531e7dcba68a309636f622fbe8ee212d457c9cc00e7bf339dca65fec2

Fb69075f4383f3537af46d2098b3bcdcb7c1bdd6896c580cd9ead6f56fb5219c

ServStart:

4f4f24f0333ed6e8883971129f216fab608b6e4d0c97c58a2b3b6a1106c77bf7

7db53e95a1339d4d023d61087907a5b07bf6720a2dd88b12882a2c5c201a92ea

7e6a2448e06a1d97ff317a5dc4ed969cef077a3568fd214cbe61854b7ff1a6d1

New ServStart:

774af1499fa1558d0b31272b84b4fbbfcc6fea578898325610524aa3853b669d

E3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

D104daec5e990de0233efdde8747a1d829c90b7b9a2169a7bcf5744fa1d95e6e

---