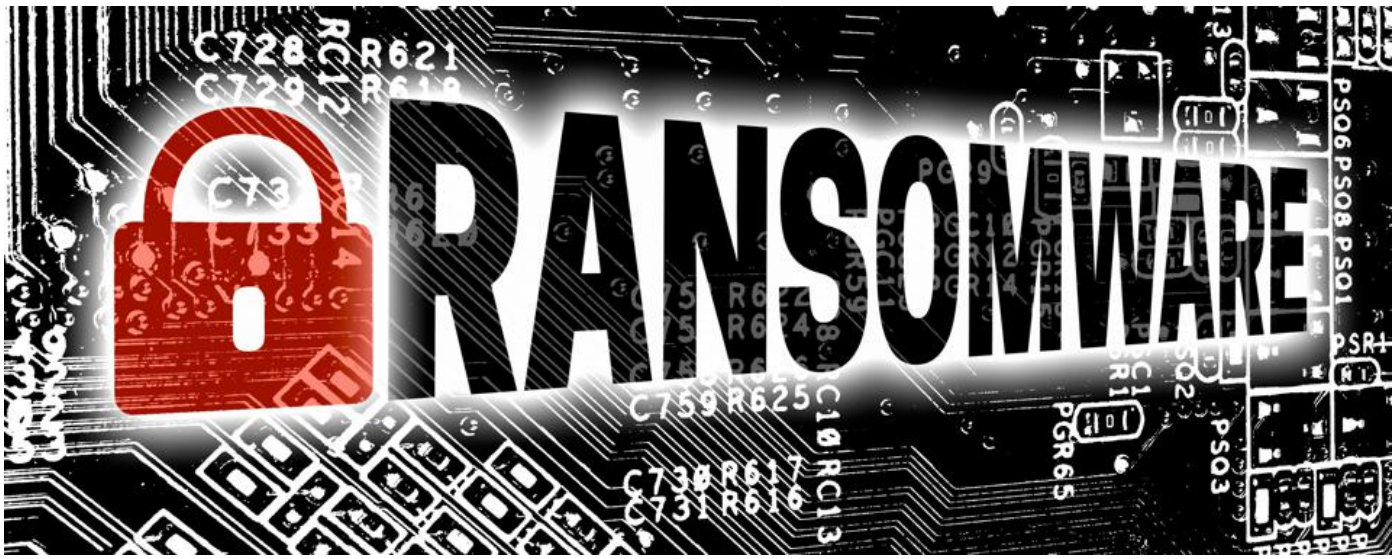
RANSOMWARE

UDURRANI



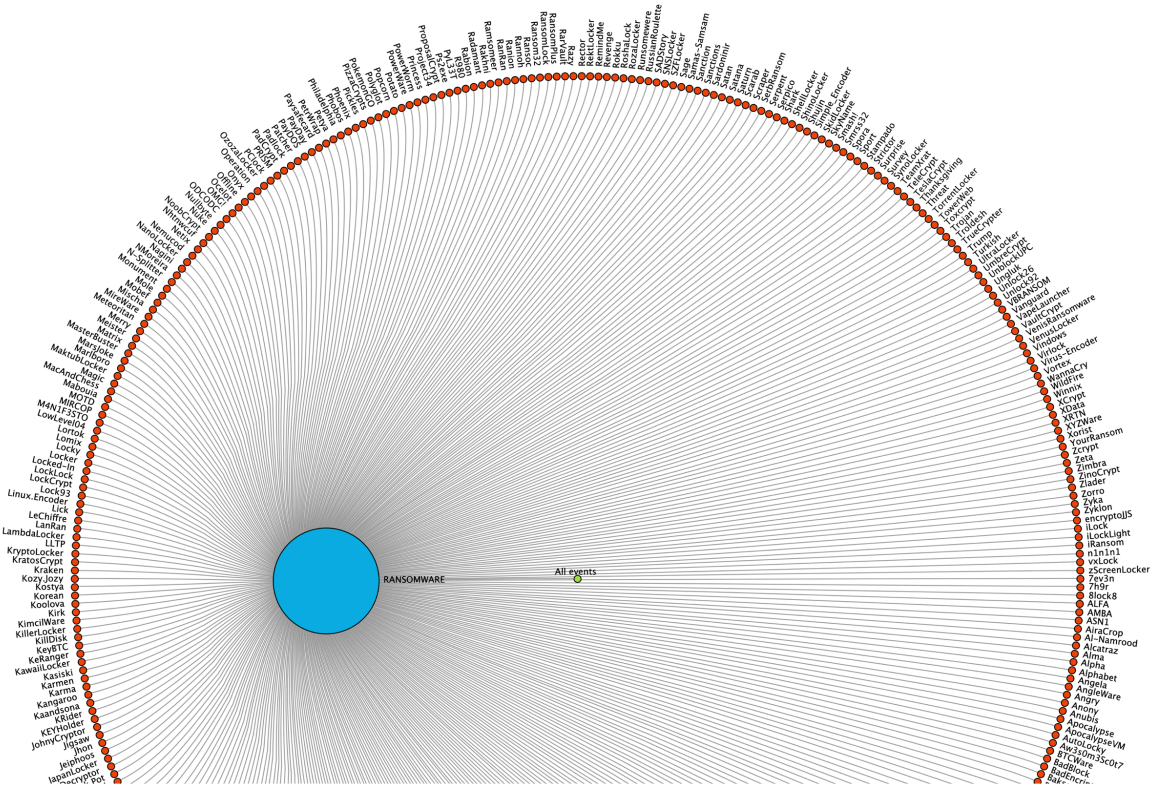
Intro

Ransomware is a piece of software that encrypts specific files on your computer. All your files are held hostage unless a ransom is paid. This ransom is normally paid in cryptocurrency. Hence the main purpose is "Extortion of money". In many ways, ransomware is like a denial of service attack, where services are denied for a victim/user e.g. access to files or file system. In the past few years, ransomware infection techniques have increased exponentially. This is because of the fact that ransomware has become a lucrative business and a success story for the bad guys:

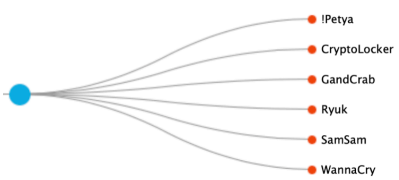
- 40 - 50 % will pay the ransom money
- High gains with low risk.

Diversity:

With the huge financial gains, the ransomware industry became really diverse. In the past few years, we have seen a range of ransomware families.

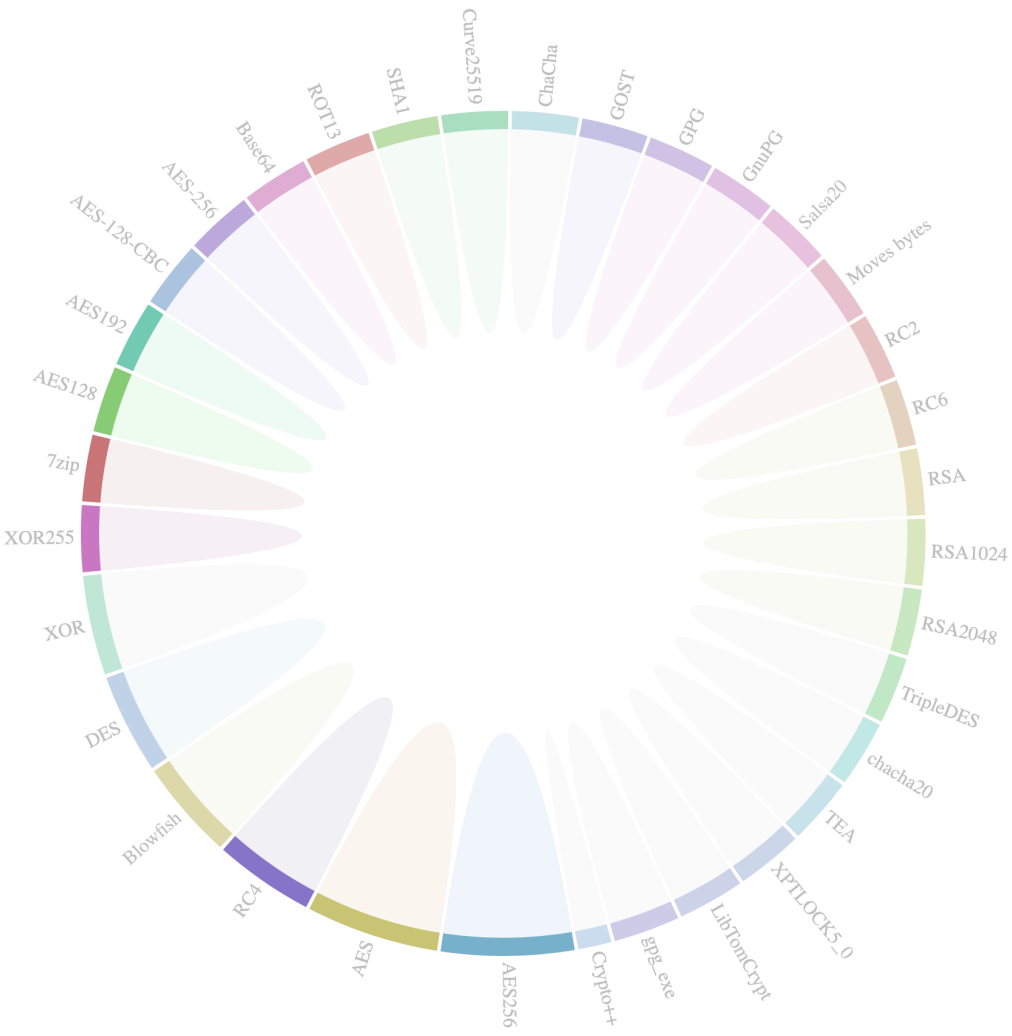


Some, more critical than others:

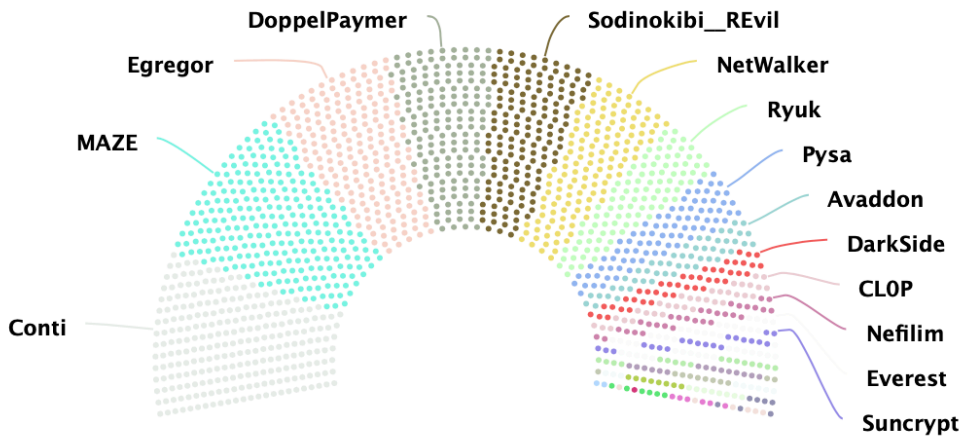


Encryption Algorithms:

Each family/variant of ransomware is using one or more types of encryption algorithms:



I compiled some ransomware stats and it's shocking that so many organizations were hit by ransomware in 2020 and 2021. Here is the list of ransomware that infected multiple organizations



The Entry Point:

Whenever I start an investigation of ransomware, I get many How's and who's. How did it happen? How did it enter the organization, Who did it? Who is the adversary? Is it state-funded? Not many care about what happened and how can we improve the current security so it won't happen again. So let's talk about how this piece of malicious software can magically get on the network:

- Asset management: Many organizations don't keep track of their internal or external assets i.e. on-prem or on the cloud.
- RDP: With no proper asset management, they don't know if any RDP is exposed or if its vulnerable?
- Phishing: Many people will open or click on anything that moves.
- Spam campaigns
- Exploit kits that can lure the users to visit specific web-sites
- Patch management: I have seen many organizations that don't take patch management seriously. If it aren't broke, don't fix it.
- VPN
- Credential theft.
- OS level vulnerabilities (LPE)

This brings us to another topic "**commoditization of malware**". With all the financial benefits the bad guys have made this process even easier. Now we have MaaS or RaaS i.e. Malware as a service or Ransomware as a service. This provides an easy entry point for ransomware. In most cases, they use a commodity trojan/backdoor as the entry point, which later downloads or drops the ransomware. Some of the famous initial payloads are Emotet and TrickBot. Here is a quick read on this topic:

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

Let's move to post exploit:

This is where the ransomware activity begins and the desktop background changes to a scary ransom note. I remember days when everything was saved on files but these days losing files on your computer is a nightmare. Let's examine this process:

- 1. Ransomware is dropped or downloaded on a computer
- 2. Ransomware creates random symmetric keys to encrypt each file
- 3. Ransomware will use another public key (asymmetric) to encrypt the key(s) used in step 2.
- 4. Ransomware will try to destroy the keys and exit. In some situations, the ransomware won't exit and continue to encrypt newly created files. Most new ransomware payloads normally exits right after encrypting files and uses a self-delete mechanism. This exit is crucial to destroy all the artifacts from the memory.
- 5. Ransomware will present the contact information i.e. how and where to pay.
- 6. Ransom is paid to get the private key i.e. to decrypt all the files.

The ransomware payload will use symmetric key encryption e.g. AES to encrypt each file. This is useful as symmetric encryption is faster and cheaper than asymmetric encryption. Finally asymmetric key encryption e.g. RSA is used to encrypt the keys. This in fact is the public key created by the threat actor/hacker. This means that the hacker creates a key pair up front, where the public key is either statically embedded in the payload or it's downloaded at run-time. If the file is encrypted via a public key, only a private key can be used for the decryption process. That is why the victim has to pay for the private key to decrypt the files.

Let's get a little more technical:

We want to see how the ransomware payload works and what activity takes place during it's execution.

Deleting the shadow copy:

Ransomware deletes the shadowCopy to make sure that deleted files can't be restored. As the name indicates the shadow copies are backups of volumes, files, folders, etc. Ransomware payload normally uses function calls like CreateProcess or ShellExecute to delete the shadowcopy. For shadow copy deletion certain vss* dll files are loaded e.g. to delete the shadow copy the following call will be used.

CreateProcess(NULL, "**vssadmin Delete Shadows /All /Quiet**", NULL, NULL, TRUE, CREATE_NO_WINDOW, NULL, NULL …);

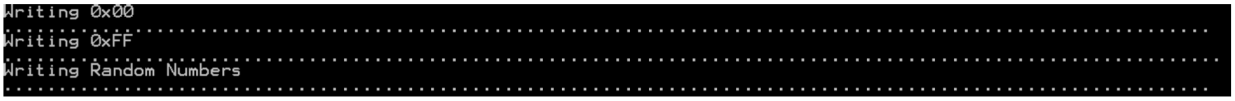
vsstrace.dll will allocate 36 bytes and followed by the deletion of shadowcopy. In some cases, the ransomware will try to trick the AV or EDR solution and run the following command. The command looks weird but it is doing the same exact thing.

C:\uud\..\Windows\px\dqf\..\..\system32\xd\vtood\..\..\wbem\isb\mv\..\..\wmic.exe

Other commands:

"C:\Windows\System32\cmd.exe" /c wbadmin DELETE SYSTEMSTATEBACKUP
"C:\Windows\System32\cmd.exe" /c wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
"C:\Windows\System32\cmd.exe" /c bcdedit.exe /set {default} recoveryenabled No
"C:\Windows\System32\cmd.exe" /c bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures

Some EDR solutions can try and retrieve the deleted files. For such scenarios, specific ransomware payload will use cypher.exe to make sure deleted files can't be recovered.



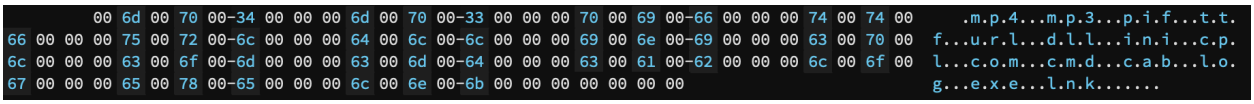
Let me explain this a bit. OS keeps track of all the files through a pointer. Think of it as a mark that tells the OS where the file begins and where it ends. What if you delete this pointer???

FileSystem will think there is no file at that location. **NOTE**: Only the pointer is removed, not the file itself. This is what the cipher.exe (Microsoft utility) is doing i.e. making sure all those pointers are overwritten.

Blacklisting/whitelisting:

Ransomware payload also looks at certain processes before they start encrypting the files. If any of the processes are running within the process stack, the payload will exit. Similarly, the payload looks for certain file extensions to encrypt and certain file extensions are ignored. The payload holds this information somewhere in the memory. The ransomware will hold the file extension info in the following fashion.

The ransomware may whitelist specific file extensions i.e. it won't encrypt the files. Some folders and locales are whitelisted/ignored as well. In the following screenshot, you can see the whitelisted extensions



Ransomware ignores some file extensions e.g. .EXE, .SYS, and .DLL or will ignore them in specific locations to make sure that ransomware activity is intact.

Terminating processes:

The ransomware payload will enumerate all the processes by using CreateToolhelp32SnapShot() and then Process32FirstW() and Process32NextW(). If it finds the processes its looking for, it will create a buffer with the appropriate taskKill command and call ShellExecute(). The buffer will have all the right values like *u" /F" *u" /IM" etc. It will just add taskkill command to the buffer and launch ShellExecute().

ShellExecuteW(0x0, 0x0, u"taskkill", &var_address, 0x0, 0x0);

```
CreateProcessW (
  "C:\\Windows\\System32\\taskkill.exe",
  ""C:\\Windows\\System32\\taskkill.exe" /IM zoolz.exe /F",
  NULL,
  NULL,
  FALSE,
  CREATE_DEFAULT_ERROR_MODE | CREATE_NEW_CONSOLE | CREATE_UNICODE_ENVIRONMENT | EXTENDED_STARTUPINFO_PRESENT,
  NULL,
```

This is mainly done to avoid conflict with specific processes or the software for AV vendors.

"C:\Windows\System32\taskkill.exe" /IM zoolz.exe /F	"C:\Windows\System32\taskkill.exe" /IM agntsvc.exe /F	"C:\Windows\System32\taskkill.exe" /IM dbeng50.exe /F	"C:\Windows\System32\taskkill.exe" /IM dbsnmp.exe /F
"C:\Windows\System32\taskkill.exe" /IM encsvc.exe /F	"C:\Windows\System32\taskkill.exe" /IM excel.exe /F	"C:\Windows\System32\taskkill.exe" /IM firefoxconfig.exe /	"C:\Windows\System32\taskkill.exe" /IM infopath.exe /F
"C:\Windows\System32\taskkill.exe" /IM isqlplussvc.exe /F	"C:\Windows\System32\taskkill.exe" /IM msaccess.exe /F	"C:\Windows\System32\taskkill.exe" /IM msftesql.exe /F	"C:\Windows\System32\taskkill.exe" /IM mspub.exe /F
"C:\Windows\System32\taskkill.exe" /IM mydesktopqos.exe /F	"C:\Windows\System32\taskkill.exe" /IM mydesktopservice.exe /F	"C:\Windows\System32\taskkill.exe" /IM mysqld.exe /F	"C:\Windows\System32\taskkill.exe" /IM mysqld-nt.exe /F
"C:\Windows\System32\taskkill.exe" /IM mysqld-opt.exe /F	"C:\Windows\System32\taskkill.exe" /IM ocautoupds.exe /F	"C:\Windows\System32\taskkill.exe" /IM ocomm.exe /F	"C:\Windows\System32\taskkill.exe" /IM ocssd.exe /F
"C:\Windows\System32\taskkill.exe" /IM onenote.exe /F	"C:\Windows\System32\taskkill.exe" /IM oracle.exe /F	"C:\Windows\System32\taskkill.exe" /IM outlook.exe /F	"C:\Windows\System32\taskkill.exe" /IM powerpnt.exe /F
"C:\Windows\System32\taskkill.exe" /IM sqbcoreservice.exe /F	"C:\Windows\System32\taskkill.exe" /IM sqlagent.exe /F	"C:\Windows\System32\taskkill.exe" /IM sqlbrowser.exe /F	"C:\Windows\System32\taskkill.exe" /IM sqlservr.exe /F
"C:\Windows\System32\taskkill.exe" /IM sqlwriter.exe /F	"C:\Windows\System32\taskkill.exe" /IM steam.exe /F	"C:\Windows\System32\taskkill.exe" /IM synctime.exe /F	"C:\Windows\System32\taskkill.exe" /IM tbirdconfig.exe /F
"C:\Windows\System32\taskkill.exe" /IM thebat.exe /F	"C:\Windows\System32\taskkill.exe" /IM thebat64.exe /F	"C:\Windows\System32\taskkill.exe" /IM thunderbird.exe /F	"C:\Windows\System32\taskkill.exe" /IM visio.exe /F
"C:\Windows\System32\taskkill.exe" /IM winword.exe /F	"C:\Windows\System32\taskkill.exe" /IM wordpad.exe /F	"C:\Windows\System32\taskkill.exe" /IM xfssvccon.exe /F	"C:\Windows\System32\taskkill.exe" /IM tmlisten.exe /F
"C:\Windows\System32\taskkill.exe" /IM PccNTMon.exe /F	"C:\Windows\System32\taskkill.exe" /IM CNTAoSMgr.exe /F	"C:\Windows\System32\taskkill.exe" /IM Ntrtscan.exe /F	"C:\Windows\System32\taskkill.exe" /IM mbamtray.exe /F

It can also use the windows net command to stop services.

"C:\Windows\System32\net.exe" stop "Acronis VSS Provider" /y	"C:\Windows\system32\net1 stop "Acronis VSS Provider" /y	"C:\Windows\System32\net.exe" stop "Enterprise Client Service" /y	"C:\Windows\System32\net.exe" stop "Sophos Agent" /y
"C:\Windows\System32\net.exe" stop "Sophos AutoUpdate Service" /y	"C:\Windows\system32\net1 stop "Sophos AutoUpdate Service" /y	"C:\Windows\System32\net.exe" stop "Sophos Clean Service" /y	"C:\Windows\system32\net1 stop "Sophos Clean Service" /y
"C:\Windows\System32\net.exe" stop MBAMService /y	"C:\Windows\System32\net.exe" stop McAfeeFrameworkMcAfeeFramework /y	"C:\Windows\System32\net.exe" stop MSSQL$PRACTTICEBGC /y	

File Encryption:

This is the secret to successful ransomware. Proper file encryption and path to file decryption are critical. Ransomware will begin with creating keys on the fly. Once again, the payload requires an already created public key and symmetric key(s) to encrypt each file. A separate symmetric key is used in each transaction.

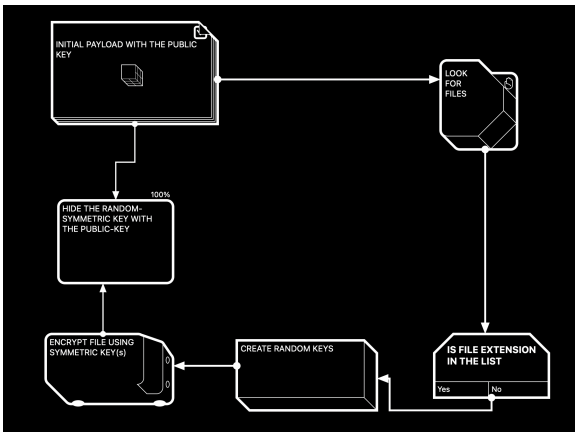
In most cases, the threat actor will create a key-pair (Asymmetric) and embed the public key in the malware. The good thing about the public key is that you don't have to secure it.

The ransomware developer has to make sure that same files are not encrypted more than once. For this reason, ransomware can add a mutex in the memory or make sure it adds a string to an encrypted file at a certain offset. In the following screenshot, the ransomware is adding a special string to identify if the file is already encrypted or not.

```
EC551559 A8D93404 A428225F CBBBEAFF 51B657DC DCFDFB78 3A40D464 8E8AD80B BCBC7543 FBB3B0D7 870E5FC2
4D64FBC2 ECD3FE8D 45E99E64 A6AC9F11 9F160FD1 31CF94AD 6DFC4439 0B7CC1F2 00F1B8F9 EF3EBFBD 4B4E4D63
09D16C5D 66D43693 F55D6CF1 7606D8D6 F9520A17 9DC9A318 ADB514E2 D00F86A4 12C63615 E1723BC3 743B5E76
7AEE3D81 9BA48506 972325D8 0510B322 A1A88775 1EEE9A70 AA56F15A 0174E145 4F283645 E88AF355 4581E79F
EF8B7653 D6C500D4 06F84[illegible]                                                    71FCFE66
823E85F2 5FABCB5A [illegible]                                                          26FFCFD2
8D325AE2 793B9350 [illegible]                                                          A214F454
29E75043 93208B2C 92203CF6 E805F109 01BE8A07 DC9BD15D 9392F861 54245A73 3B0B7401 E9E6CEE2 AAC84854
F16582DF D6735CC9 6A168471 313F7F6F A6E3C878 947A9195 9EFBADA3 526B0D45 DE7818E7 B6C13981 2A7A6058
7A39C6A9 B5DC0422 A024FD31 46234EC6 49820C65 D45893ED 8EA1011A 5F2BC3C8 2D4B1407 CB818EF0 4CAEF38D
2D8B77FA 38AF2FE3 4E257B6D C9B7C216 13D2CE03 37E93529 3CDD47D9 F2799020 BC734961 8F268BFE 6F881CDD
660EEB9D EF41CD0A 06DA5877 C3C2B7DC 97175F9D B058DA9A 8FA4D166 00000000 00000000 00020000 02000000
07030202 00000000 <-------------------- IDENTIFICATION PATTERN
```

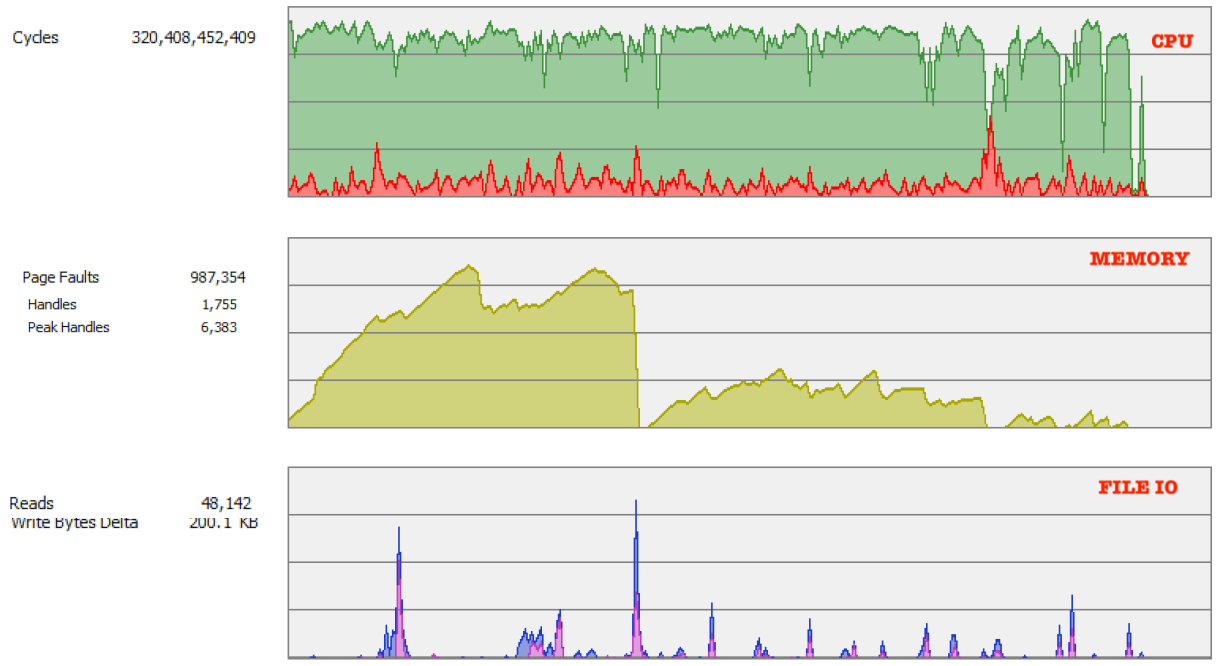

Before the file encryption begins, the ransomware needs few things:

1. Algorithms for encryption
2. Public-key
3. Random keys to encrypt files and other keys



How does file encryption work:

File encryption is very similar to any other file IO, you open a file, you modify and you close the file. This process could be handled by a single thread or multiple threads. In either case, you will notice that the payload in memory is pretty heavy and chewing up system resources.



First, the ransomware picks a path i.e. where to start the encryption process. This process involves directory enumeration. It gets info on logical drives by using GetLogicalDriveStrings(). The recursive file search is initiated by using the following functions.

FindFirstFile(LPCWSTR lpFileName, LPWIN32_FIND_DATAW lpFindFileData)

FindNextFileW@IAT)(HANDLE hFindFile, LPWIN32_FIND_DATAW lpFindFileData)

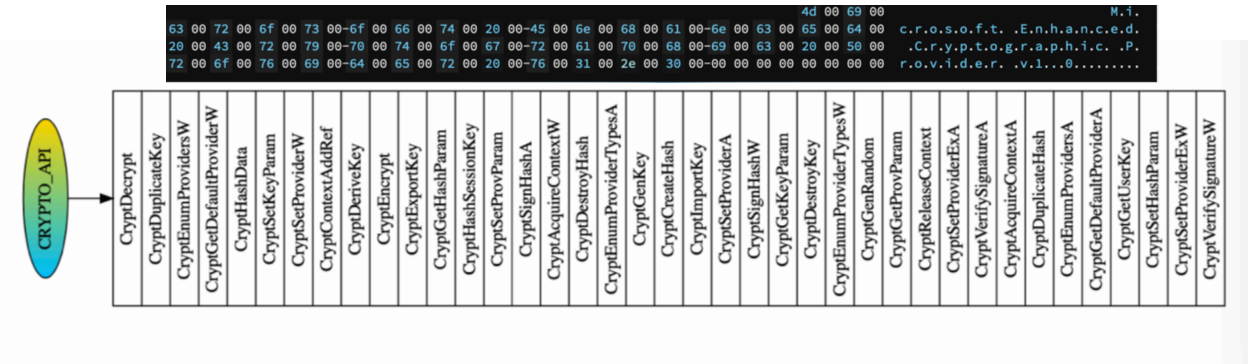
```
call    dword [imp_FindFirstFileW]
mov     ecx, dword [ebp+var_2A4]
mov     dword [ebp+var_264], eax
cmp     ecx, 0x8
```

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

Once the payload finds a file with the right extension, it will create a unique symmetric key. The process requires using multiple functions:

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

Here is the list of the API's used in cryptography.



File encryption:

File encryption is similar to file modification. The victim file is opened first in read mode. The encryption algorithm will read 'N' bytes at a time, encrypt them and write to a new file. This is done via using the following function:

NtWriteFile (0x00000150, NULL, NULL, 0x01ed0020, 0x01ed0020, **0x01ed0094**, **144**, 0x02 …)

0x01ed0094 holds the address to the actual data in the memory that needs to be written to the new file

```
0000  a3 d2 ea 12 d9 cb a7 5c 51 7e 76 5a 7a 5c 42 d3 63  .......\Q~vZz\B.c
0011  77 2d b5 ff 92 fc cc 50 c3 3f 95 d9 30 3d d7 56 ab  w-.....P.?..0=.V.
0022  fc 16 9a 5c 7f d3 41 81 75 e4 73 30 1d 68 c8 4d 12  ...\..A.u.s0.h.M.
0033  61 a7 8c 81 c5 10 cb 47 9b c8 04 df ff 63 5c 0f d9  a......G.....c\..
0044  4c b9 66 5e 7d 1a 66 4f 87 c1 dc 94 c2 1b 12 58 18  L.f^}.fO.......X.
0055  3f 85 99 1b 55 05 07 0d 7f d9 af ea d7 2f b8 cb b4  ?...U......../...
0066  4c f0 52 72 c9 b8 42 b0 4e 21 e7 81 b6 27 7e d8 61  L.Rr..B.N!...'~.a
0077  0a 5b cf f0 9e 76 c7 41 5a 73 fb 83 a6 ac 6d ff 3c  .[...v.AZs....m.<
0088  93 24 3d 76 69 b3 b4 22                           .$=vi.."
```

Data encrypted in the memory

144 = the total length of the data

Once the file is written, the file-handle is closed and this file is moved/renamed to a new name with a different file extension. This is done by basic string formatting: In the following code, the .**pysa** extension is used for renaming.

```
push dword ptr ds:[1105000]
lea eax,dword ptr ss:[ebp-1028]
push esi
push pysa.10EBCD8
push eax
call dword ptr ds:[<&wsprintfW>]
lea eax,dword ptr ss:[ebp-1028]
```

Once the file is re-named, the original file is deleted by using DeleteFile()

The encryption call used here is CryptEncrypt()

```
BOOL CryptEncrypt(
  HCRYPTKEY  hKey,
  HCRYPTHASH hHash,
  BOOL       Final,
  DWORD      dwFlags,
  BYTE       *pbData,
  DWORD      *pdwDataLen,
  DWORD      dwBufLen
);
```

Handle to AES and the CSP is done by using the following dataStructures

HCRYPTKEY
HCRYPTPROV

Lateral movement:

Not all ransomware Trojans are able to make a lateral movement. The lateral movement could be done via the commodity stage one backdoor e.g. Emotet, trickBot or the ransomware has the code path to lateral movement itself. The ransomware payload can look at the arp table and try to connect to similar ip range. If we look at the network trace, we can see the following:

An arp request is sent (Lookup)

```
+ WHO-HAS 172.16.223.1 tell 172.16.223.5

00 01 08 00 06 04 00 01 00 0c 29 9a f2 8f ac 10       | ..........).....
df 05 00 00 00 00 00 00 ac 10 df 01                | ............

+ GOT 172.16.223.1 AT HW-> fa:ff:c2:b2:4d:64
```

Once the request is successful, a SYN packet is sent to the remote ip on port 445

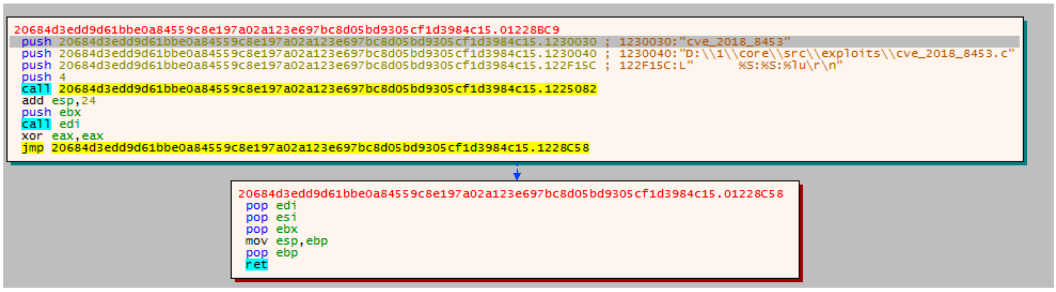
```
L3: 10.0.0.188 -> 10.0.0.10      L4: [49573:445(microsoft-ds)]     SYN
L3: 10.0.0.188 -> 10.0.0.11      L4: [49574:445(microsoft-ds)]     SYN
L3: 10.0.0.11 -> 10.0.0.188      L4: [445(microsoft-ds):49574]     ACK RST
L3: 10.0.0.10 -> 10.0.0.188      L4: [445(microsoft-ds):49573]     ACK RST

L3: 172.16.223.5 -> 172.16.223.1 L4: [49309:445(microsoft-ds)]     SYN
L3: 172.16.223.1 -> 172.16.223.5 L4: [445(microsoft-ds):49309]     ACK RST
L3: 172.16.223.5 -> 172.16.223.6 L4: [49314:445(microsoft-ds)]     SYN
L3: 172.16.223.6 -> 172.16.223.5 L4: [445(microsoft-ds):49314]     ACK RST
```

In the above scenario either the credentials are stolen or the remote machine is part of the Administrative group. The ransomware payload could have the set of credentials hidden/encrypted in the payload (for brute forcing). By looking at the memory dump one can find the set of credentials. Here is an example:

```
woaisha123, lzf5201314, nanzihan, a6127821, UTIBET521, caocaocaocao, asdfgh456, sc.sp851_, gengliang,
mcgradyKOBE88611, nanzhuang, bobo198768, jzw010420, xiaolan84, ypcmdbat, xiaolan520, 123456789, 12345678,
11111111, dearbook, 00000000, 123123123, 1234567890, 88888888, 111111111, 147258369, 987654321, aaaaaaaa,
1111111111, 66666666, a123456789, 11223344, 1qaz2wsx, xiazhili, 789456123, fuckfuck,
```

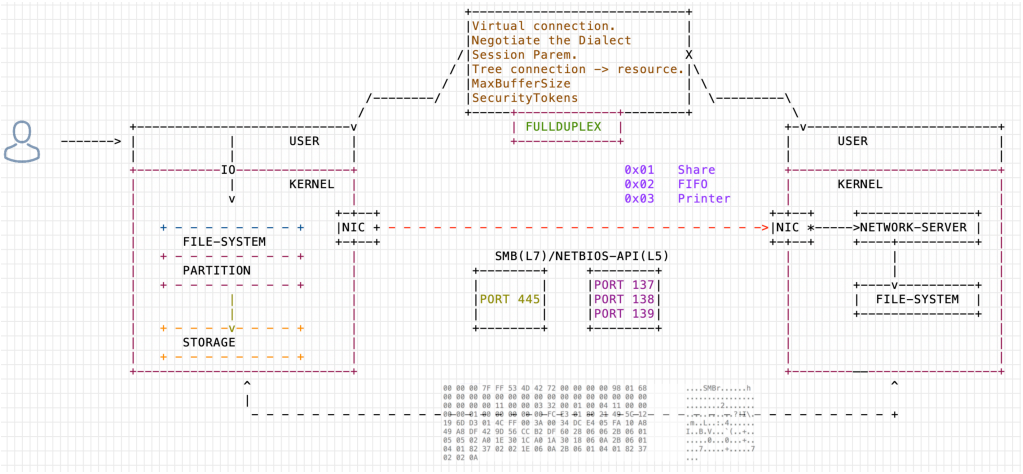
The ransomware could be equipped with some exploitation code like eternal blue or another LPE

```
0000  73 00 74 00 61 00 72 00 74 00 20 00 4c 00 50 00 45 00 20 00 28
00 63  s.t.a.r.t. .L.P.E. .(.c
0017  00 76 00 65 00 5f 00 32 00 30 00 31 00 38 00 5f 00 38 00 34 00
35 00  .v.e._.2.0.1.8._.8.4.5.
002e  33 00 29 00 0d 00 0a 00 00 00
3.).......
```



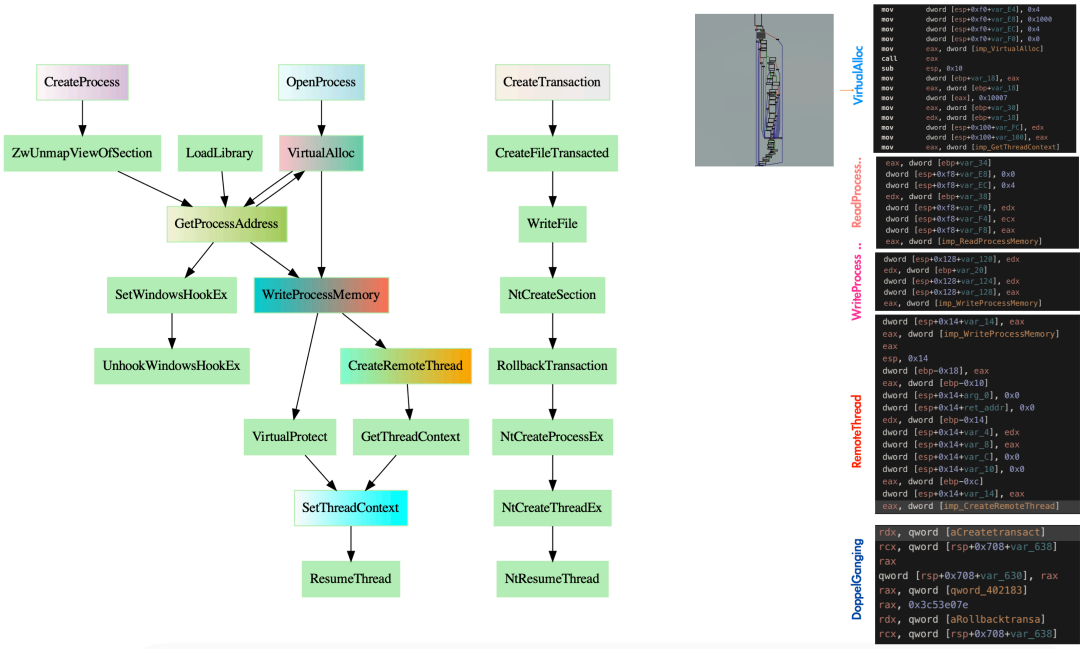
Encryption Mode:

In most cases, the encryption is local to a single machine and then the payload is moved to another workstation laterally. This situation is handled well by the AV products. If the ransomware does everything remotely i.e. encrypts remote drives without dropping any payload to the remote workstations/servers, it becomes very difficult to identify this activity. This is because of the fact that remote file IOs are handled by the kernel objects/components



Hiding behind other executables:

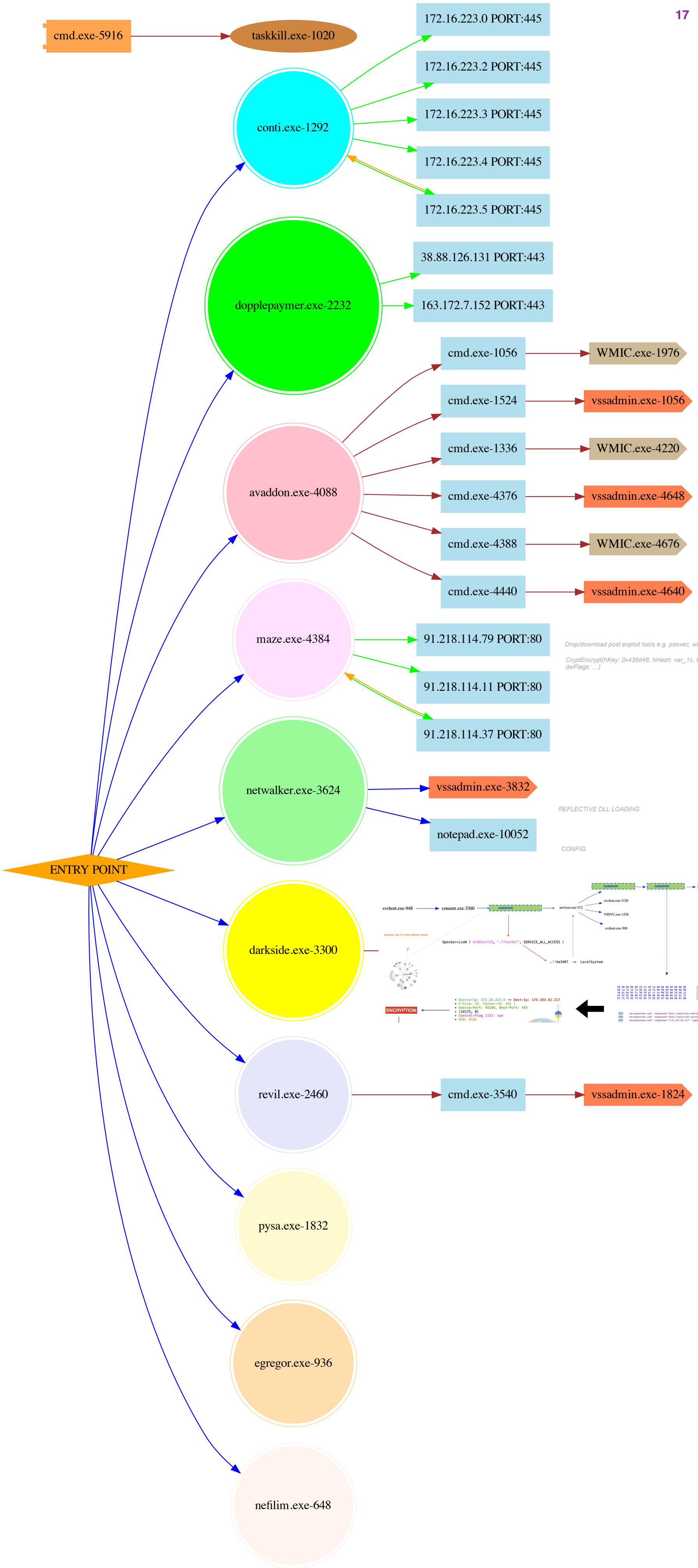
Many times ransomware will use code injection techniques to hide itself and bypass security checks. This way the ransomware can hide behind a white listed application like svchost.exe or explorer.exe. Here are some of the injection techniques used:



Conclusion:

- Manage your assets: Secure apps like RDP on-prem or on the cloud
- Take security patching seriously
- Multi-facto authentication for your critical servers
- Automation is your friend
- Invest in a good EPP/EDR solution. The endpoint is pretty critical
- Invest in a good firewall
- Make sure you gather the best intel
- Gain more visibility on your corporate network
- Test your security
- Create the best SOC by hiring the right people
- Stay away from ransomware
- CHILL!

For the research, I used multiple ransomware payloads. On the next page, you can see the detailed dynamic view of multiple ransomware payloads running together.


cmd.exe-5916
taskkill.exe-1020
172.16.223.0 PORT:445
172.16.223.2 PORT:445
conti.exe-1292
172.16.223.3 PORT:445
172.16.223.4 PORT:445
172.16.223.5 PORT:445
dopplepaymer.exe-2232
38.88.126.131 PORT:443
163.172.7.152 PORT:443
cmd.exe-1056
WMIC.exe-1976
cmd.exe-1524
vssadmin.exe-1056
cmd.exe-1336
WMIC.exe-4220
avaddon.exe-4088
cmd.exe-4376
vssadmin.exe-4648
cmd.exe-4388
WMIC.exe-4676
cmd.exe-4440
vssadmin.exe-4640
maze.exe-4384
91.218.114.79 PORT:80
Drop/download post exploit tools e.g. psexec, winrar etc
CryptEncrypt(hKey: 0x436d48, hHash: var_1c, Final: 0, dwFlags: ...)
91.218.114.11 PORT:80
91.218.114.37 PORT:80
netwalker.exe-3624
vssadmin.exe-3832
REFLECTIVE DLL LOADING
notepad.exe-10052
CONFIG
ENTRY POINT
darkside.exe-3300
svchost.exe-948
consent.exe-3360
DARKSIDE
services.exe-512
svchost.exe-3128
VSSVC.exe-1536
svchost.exe-300
MALWARE LINK TO OTHER DARKSIDE SAMPLE
OpenServiceW (0x005ef258, ".7f4a3487", SERVICE_ALL_ACCESS)
.7f4a3487 -> LocalSystem
ENCRYPTION
+ Source-Ip: 172.16.223.5 -> Dest-Ip: 176.103.62.217
+ P-Size: 52, Packet-Id: 452)
+ Source-Port: 49198, Dest-Port: 443
+ (24175, 0)
+ Control-Flag [13]: syn
+ WIN: 8192
revil.exe-2460
cmd.exe-3540
vssadmin.exe-1824
pysa.exe-1832
egregor.exe-936
nefilim.exe-648

INDICATORS

CVE-2020-0796
CVE-2019-19781
CVE-2020-0688
CVE-2019-19781
CVE-2019-11510
CVE-2018-8453
ee06c557f1acd5c4948b1df0413e49f3885f8ac96185a9d986b91a1231444541
c3c50adcc0a5cd2b39677f17fb5f2efca52cc4e47ccd2cdbbf38815d426be9e1
a9d483c0f021b72a94324562068d8164f8cce0aa8f779faea304669390775436
765327e1dc0888c69c92203d90037c5154db9787f54d3fc8f1097830be8c76ab
4ea8b8c37cfb02ccdba95fe91c12fb68a2b7174fdcbee7ddaadded8ceb0fdf97
3fd510a3b2e0b0802d57cd5b1cac1e61797d50a08b87d9b5243becd9e2f7073f
2b3518937fd231560c7dc4f5af672a033b1c810d7f2f82c8151c025ce75775bf
004a2dc3ec7b98fa7fe6ae9c23a8b051ec30bcfcd2bc387c440c07ff5180fe9a
932778732711cd18d5c4aabc507a65180bf1d4bd2b7d2d4e5506be4b8193596e
9017c070ad6ac9ac52e361286b3ff24a315f721f488b53b7aaf6ac35de477f44
6ad7b3e0873c9ff122c32006fdc3675706a03c4778287085a020d839b74cd780
3aad14d200887119f316be71d71aec11735dd3698a4fcaa50902fce71bdccb07
14e547bebaa738b8605ba4182c4379317d121e268f846c0ed3da171375e65fe4
aee131ba1bfc4b6fa1961a7336e43d667086ebd2c7ff81029e14b2bf47d9f3a7
3fc382ae51ceca3ad6ef5880cdd2d89ef508f368911d3cd41c71a54453004c55
3e5a6834cf6192a987ca9b0b4c8cb9202660e399ebe387af8c7407b12ae2da63
28f3f5a3ea270d9b896fe38b9df79a6ca430f5edab0423b3d834cf8d586f13e6
2d01c32d51e4bbb986255e402da4624a61b8ae960532fbb7bb0d3b0080cb9946
b2d79fb20a243d3f5dca96fd9e70683f7c0ba1a29668c560b83a14ce4e29d479
5fa2b9546770241da7305356d642784759828829086683762 6f621d794692c1b
2e0df09fa37eabcae645302d9865913b818ee0993199a6d904728f3093ff48c7
45.135.229.179
79.141.162.82
155.94.160.40
192.154.253.120
192.52.167.101
194.88.104.24
188.166.74.218
45.55.211.79
26c499e3f9ec79ae91fca43dd81f9d1302a913ee30474223f3f5320c10c4a4a0
633e3eaa35fa4963b68006f44b70bc29b4f0b682093468833e731df78c7c0fbc
9fbd5acd0a3ad1259ef0515e79775d5b4bcba82c9a199aad73baf84450380c3f
0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d
34dffdb04ca07b014cdaee857690f86e490050335291ccc84c94994fa91e0160

74bc2f9a81ad2cc609b7730dbabb146506f58244e5e655cbb42044913384a6ac
95ac3903127b74f8e4d73d987f5e3736f5bdd909ba756260e187b6bf53fb1a05
fa2bccdb9db2583c2f9ff6a536e824f4311c9a8a9842505a0323f027b8b51451
9958e259bad37bf1f02c9ae1a171d37abe94e50b3d846f845cb362584769f97d
362fc55f5cd3d5338827de0eafdb7eb34c26885345706852184db95ad9996a5c
2d22d812117ff4ca4d8bcbd45ec20c77f52e907bf7320d44f6a4fd6c7beb066e
d41fd38a8478bf788f5dc0acf0e070dd360ddc9bfff0804e6b5254cc0116aa81
982f8e3329ef811bde84fd0cd5009dbfda6ed5e22e10eea796ac128e787f4f50
462257012d62ead365af0198457c64cc07a0597461ce79496c0f22b91273dcde
e1e19d637e6744fedb76a9008952e01ee6dabaecbc6ad2701dfac6aab149cecf
17b89590d4a732821269f81d0e2a307554a516aac41a25386a660efc31f11579
1af8672fd4ffdf557896efd173ab031fb326846b5aa21548884506217f654a4f
1f396173c5ba8ee8504ca2bb5ff1db334d65bda15c5a767ac65b0e05da118d6b
2181579e0125e8087a3269ee8a90a973307f67eceb7122fdc7463db6bc5050b5
2b23cbb57368ec73e514473166f999c406184a786c298300cd5e5b96044b4204
337fe8b50b6db4e741246ca76f27a8dd4e505cceebf9a9577be2d03dd5c5810a
338b9b5ea11c502f5eab38c606740319ae6606e17e29106348cbddc312f0343c
4265b4461d213a6e99447fc255a5d4de9a18b92756cfb66a247472261ab01154
4c1b8b3bd83e588c701568aa9469ff3a1e9725c1b838efdf8683a1edafaefe45
5a8194f69687a52dcd478b759539eb6a2b824505f5f6659aab26ef1787d994db
67cd75a0e5e0885bb6d59b6747747473ebdef00f2870ca3eb3a4e144ae283dd9
7882c0d6116d428fcd01064021e7d71abbf386466d50fda80efe9a98186fdb48
830a8208fe916dabfc1ee63c3e889d8277fbae954a9b00d64b2c920e1d9a2536
957db5d26408685f006e113c4793b943cc5c193466cf1223416f025cc8cc308d
9a85c4fd3cbc4cd32155ce4885a057648070357eb944c9ae38678b46088b500c
b7ae354e1227e211b73cbabd1989a86da6018d6abe756c2d16506aff46b3cfa2
c40dfd58e6da0aade75d09b6a659cf165f072ba89aef2d60c10c153793535ee7
c6bbcbd392e5828b0fd1130e4c27cf352415295b0428c6b1ce6707528cfa8502
c80ded3fe04fe8fea1439d19c87d4c451683786c5bbdf9ddee4755ccde571be1
d8cb6bc96ed3c980013addb9af4f61fdfefc5e3373c36e821062c2dae565dd75
dad3431f42dd3bac7fa36ed24b40bfb6e8d7ccce71c325ee0c068e7b1a1de1ad
dcd68b47c9f98cde982318d889dbfdaadec966651f957410075bb8b413a811fa
eb3980c1bd7880ff3787efd329a368a9c3104368bd890e6e84a6612fbac38066
eccc6703bbbe261e1caf9aa3ccec69ad5c099c4af0fed4aa6da678aba17ccb16
2b23cbb57368ec73e514473166f999c406184a786c298300cd5e5b96044b4204,
7882c0d6116d428fcd01064021e7d71abbf386466d50fda80efe9a98186fdb48,
4c1b8b3bd83e588c701568aa9469ff3a1e9725c1b838efdf8683a1edafaefe45,
104.27.130.109,
104.27.131.109,
195.201.29.161,

104.28.23.228,
104.28.22.228,
104.18.43.85,
104.18.42.85,
173.249.46.122,
5.77.60.44,
50.63.202.77,
88.99.61.233,
93.187.234.36,
162.144.26.133,
195.210.46.47,
104.31.83.217,
104.31.82.217,
198.71.233.104,
31.47.254.18,
185.2.4.147,
http://lollachiro.com/,
http://acb-gruppe.ch/,
http://profibersan.com/,
http://datatri.be/,
http://dantreranch.com/,
http://gosouldeep.com/,
http://victorvictoria.com/,
http://belofloripa.be/,
http://rentsportsequip.com/,
http://profiz.com/,
http://jax-interim-and-projectmanagement.com/,
http://leadforensics.com/,
http://breakluckrecords.com/,
http://alwaysdc.com/,
http://sppdstats.com/,
http://thegrinningmanmusical.com/,
http://voetbalhoogeveen.nl/,
http://kellengatton.com/,
http://b3b.ch/,
http://reygroup.pt/,
http://boomerslivinglively.com/,
http://peppergreenfarmcatering.com.au/,
www.download.windowsupdate.com,
cacerts.geotrust.com,

redctei.co,
oro.ae,
lyricalduniya.com,
queertube.net,
hotjapaneselesbian.com,
omnicademy.com,
secrets-clubs.co.uk,
thepixelfairy.com,
katherinealy.com,
burg-zelem.de,
jeanmonti.com,
smarttourism.academy,
tutvracks.com,
fsbforsale.com,
avisioninthedesert.com,
legundschiess.de,
cap29010.it,
campusce.com,
bfd8d145952bca38a5d35b6cb6f7d7d296b66863e502040bf13202a7d165d568,
2aef1134cb696c922a06b71d58058d44e804391ff44cc5cd54335a1438fba58e,
575d5db61e5f1e0826feecd0950d2ba7aec2f7a3531f064f70edbc65507cc960,
d97425d15c6e374e5b79f4196507144c7cfaf71f597751c60dd55538944902e4,
093ef95531dd3e839d60d7296bf15713bf3b0b66aa3c69e2fef32036a334c1dd,
d34385f8b63ebde063cdde12a166df07d42982732a5a8381f7ef0ac17ad6b856,
c8c169ad2628ff3860c4d0bd04afeb81262051f664f9d5a334c32c78e791a7f8,
ff92178082e4a8e05cf3a798927dba0b878511812b09e1efec2598e23dd7987b,
f4f73a451c1ec493eb3b4395d06de73598fcf5b8f7d13e81418238824d90fda3,
7639a538e186a569ce499fe5da4222a735b5ee7cd611943112102c9d77424aa0,
5588332496c607b20af0b1c0e530d3713c519c47c3f9c31536ebc7da9ac342e2,
d04c7efff113ea3b882beffee52c3a3e41ce6a204440e708f4a4aebe7fa321db,
84c5a98b10bf32eca9545c6103ef7a91d2abadee956d9ebf5fc226a2731de03b,
f9be630d9b79a9b0b1d247f0a0d5f18885d586d9c91e9610881481176b8af737,
33cc60e556e7c468a45fe2d3bd1f2de8c5f42a5d686fcbaad67c83e463ff0b08,
39076ad20f1677c1d5e09b43f6a5bf412381dd1ff45f45a662b7d20cb0b1d906,
c8de17430100efffa8cf40b9a711d0765f4fd44810245f178f2a7be50a757b17,
eeeeb1d683c948d0426e253d708445817ad66460a93ef53668dd67a6f5f223d4,
a9c0755dab8270272c168507c01212b5234af0b7814b6b6ab72510e6710fa0b8,
mangimirossana.it,
sppdstats.com,
brannbornfastigheter.se,

sachainchiuk.com,
profibersan.com,
geitoniatonaggelon.gr,
hepishopping.com,
ykobbqchicken.ca,
epicjapanart.com,
condormobile.fr,
peppergreenfarmcatering.com.au,
alwaysdc.com,
leadforensics.com,
oexebusiness.com,
kristianboennelykke.dk,
futurenetworking.com,
ahgarage.com,
tages-geldvergleich.de,
palmenhaus-erfurt.de,
smartmind.net,
41a2be1ac9c6dd82251c95e06c832b4aae0a6e1c76fe3fc6227d3142754ab640,
67cd75a0e5e0885bb6d59b6747747473ebdef00f2870ca3eb3a4e144ae283dd9,
50edf5090f56c56d77d44b756ab1496d0c03a49360139861671810ac2ee617ef,
a096e7ed6b4ac331fb64a81cce1ae13e9c8c64a442b28c1556f7015f3b0ed4f4,
71cb48931890d2796611f40e1317eec6aaebd5947fe5d6ebf63b8edcbad7f11c,
1280396eb6a6f98dd92fc923c335b0cb4d5a0b6068ccf58294ea7fc77fa6892f,
4e7f5cd6ffb82ae7aba256fc09d949b724d93eabd591cc78918e488a7a2d7662,
2795841a21b15f156f30cb2196b403dcb802e6971cc28dc83b037a13d8963492,
da3cd4f45cf5816ab7de2320ad1cf822df7f02afa2b667ba829700998e514f33,
986d43dbea20c8703846ca0c8e406ce20f902d6451fe9810d6485ae61034f5d5,
128a0bfad65790d7db90f82f2ede6969e834549a48f3712130288d2cd455b2de,
249d050053a585687f5793041f2c23104162423679fe3d7a2a01c33dd6a12005,
14d09a259f72569f309fdd7bc14519753d01016706c7b9335a215b2d0b64c632,
df724c49a1401d66f690b0a940f70bd286671448a625690ccdfdc4c42b4b5b07,
0f48d0cdecc581ccc73b11ce229c21522d23996eb4f1d88c892e6a68b7a4ea19,
2ca519d47ac0ab709cabe70a89504d134475d68be47081be4ccd758d371619a4,
e8b5044a1fd6342ff6d367595a9e8cac8231c392b587d4ed94c4631d587a7feb,
e2dbd097b846feec6f4654b79ea0ac23463df4a430b750ebde3eb893d3daad36,
0e37d9d0a7441a98119eb1361a0605042c4db0e8369b54ba26e6ba08d9b62f1e,
830a8208fe916dabfc1ee63c3e889d8277fbae954a9b00d64b2c920e1d9a2536,
c678c05b05790006e56a25659eaa97520f426c6b2bbd7ccfb3ea30cc46d672f9,
eb3980c1bd7880ff3787efd329a368a9c3104368bd890e6e84a6612fbac38066,
1f396173c5ba8ee8504ca2bb5ff1db334d65bda15c5a767ac65b0e05da118d6b,

4d7bb7fc137d4e4db98835612daa8e4f36b365dad71bd5c763521d7e8a29915a,
4a52c33f67a1a47c9ffcc4dc6866bb3b887ba1817bad7bc2569c4038711d29cf,
d08339d4d2adb359db839026d0c81b2f5f097c624948b3ec9c2fc109d7357d84,
78fa32f179224c46ae81252c841e75ee4e80b57e6b026d0a05bb07d34ec37bbf,
dc788044ba918463ddea34c1128c9f4da56e0778e582ae9abdeb15fdbcc57e80,
961d562404b3c13ce130c0afa3c0d6cc612a4b4b95dab93049eb9cb8f5ca397f,
292a1fa19c845a2639eb4b62401d17950c99fb31d7916f83a8ab24c974489e4f,
1ea24f7e6413db35506b5ed391fdc269ad0647480eef3eb67aac375d54dc98d9,
92a642dd3311e442d3e9fb63f8718f31fe0ebcba8d8bc7e3b3d2bf3989c3e0f4,
b0e7f00b3b5e63313f2259844529b75edad537a9347ae0af291f3b236bc5f7f5,
db583e09ea90ded0a3c534b0c71000fd2db204ddb6ade2431faa6c2e5adc4343,
3ff14b291c37f0de3b94f6bdbf8723359e8f8f3bb6c1e893090734c7c7bd65b4,
d35ffa505a949df39eed305125c2fc99453e6392535661890aa61ceec4b77f8d,
0c7a12550ea78fd2aebeb7190f72e281700bdcb3d6dca4063e98d00899848d6b,
a73e511cbbd2593ad470771c50da9c3e7bcfa603133e5eabba13c19c3bfae32f
b345697c16f84d3775924dc17847fa3ff61579ee793a95248e9c4964da586dd1
6568e9ac34905c32255bab713c259d76fab2c162be84d913ab0076a05e2605c3
2b3518937fd231560c7dc4f5af672a033b1c810d7f2f82c8151c025ce75775bf
ab4eae618bb05b4fb4a8d3790a0d18a3e1566ab477519991cb161398803a8847
47cb648d5981581d314c94169cfefdf30a50654f4dbadac93581be0f4947d1c3
5c9b7224ffd2029b6ce7b82ea40d63b9d4e4f502169bc91de88b4ea577f52353
499e43933c5ee3bb730417e07d74c93a5f7d7dee05db31714e09dffeb7e3c285
391cfcd153881743556f76de7bbca5b19857f8b69a6f6f6dfde6fd9b06c17f5e
b345697c16f84d3775924dc17847fa3ff61579ee793a95248e9c4964da586dd1,
00d8fb80cd93aa1888c4b90bc27a65dc3f1cff5117f21dd767bf476da52fea01,
015502f17517fb0cef3af046340ddcd041fcd528baf0b9ac55b152ebed9e39b4,
019051d51461466c1a37dd02eb0d29a6c820e7b731d3c826c4fa3c52689d32c1,
0221c2a2618a9906e177bffe63cfdc13a32d02ebc8acdbfcfccf87e03d4d4c65,
02309bd91ae9dc6147cfa72f2011e0ed6527537b630ef97bb10bdfe94007c171,
0246a194f61b755983051cdc3dd9808f667b54b66a3ee236337b5521fefc1a59,
0336a5983abf7a2e3c1b0ea07f6d596679fe8226e30245280ade8ea53121c9fc,
04d43cf229e423c2b4cde19d3aac7bb268eb9feab678ab419fb52027ab90df7a,
04dae7d57d5f690b0042e0ab08a782e398f9334c7392d576cf2bb654fd4144dd,
051f2c56edd4ec03ce64316c550a86cb34f0fe2130e47f9bff7fb899f156266b,
05305e34aca88e76f72a8cd0b2e1963e7b7daf06a8f5fc554c2faf0c4484d3c7,
05f134aaf869e283bbdf67230f0c1e5da817273f37ec9449bc4b525325e1b98f,
05f90ce980d39eca47563e00c9dc9458e523da67a91199c1fb98a36bed471fae,
067ef24acb6b7d8c27ce5a013e90a7331d153e4f8d214d9ba673957d2fc052a1,
076e2c382a9dfa2dee839339312a69e525dcc58e228c171f0e844161342ae900,
07b2353e2cd42e598bd4a480d943aad474d6e1258960aa53d2ed8f3b7d390ec5,

07ba98269bdd55ef948e208b66eda81ce027ca58d04142b353815eef7b30b925,
08ff2984c867c09ab95bcb66b505e1616433c6a0e8fbe31682cf5dd21df3fdab,
09c6073f38bef8428b22e6b1aa74ca2af27c8f7d34a96953d3abe633ebc656a3,
09c9aa4da92870138e92db506bcc4186fd994dd971bb3035be5a0169235b5bab,
16bcd895f6cd67726410b022b9bef7a0b9e8af44d53a00116c00131368c0ab9f,
4596465f1dff27b089a6a6bff93c5ae8050dbb580e4c0735e08db330ed51b557,
20ea5a9b5b2e47aa191132ac12c1d6dea6b58d7a0467ea53d48e96f8a79c6acd,
91.218.114.4,
91.218.114.11,
91.218.114.25,
91.218.114.26,
91.218.114.32,
91.218.114.37,
91.218.114.38,
91.218.114.77,
91.218.114.79,
91.218.114.31,
http://91.218.114.26/ticket/messages/vekuww.html?n=0em7ol87sw&rpn=c58,
http://91.218.114.32/forum/nwgvtr.phtml?kyf=t8m&tbkh=jhrv52b022,
http://91.218.114.4/checkout/hlvwrihei.cgi?ps=ea8,
http://91.218.114.26/news/webaccess/hdfcdkml.cgi,
http://91.218.114.79/wire/lfoap.asp,
http://91.218.114.77/messages/cpikwt.aspx?ay=6n6u&tqdw=5y,
http://91.218.114.77/pfxwwrk.aspx?kuq=e2h2a53d3,
http://91.218.114.26/check/ptdecuo.action?pwv=qvwvca34bs&le=mr07n,
http://91.218.114.11/private/kwljx.php?fa=02&l=36&kup=onoyv016,
http://91.218.114.25/nh.html?kgya=hc,
http://91.218.114.11/logout/post/ubpsfh.html,
http://91.218.114.11/tracker/edit/bdsdj.jsp?ctw=751hh1&hqtd=2u3kifpl,
http://91.218.114.11/jjuwxfqe.aspx?en=jy7fom0e8&qph=hb6fwf,
http://91.218.114.26/view/register/ggygpn.shtml?mlde=v,
http://91.218.114.4/private/dxkeoqt.phtml?il=7q66hpcohs&jjo=35&nau=i661oe7i0,
http://91.218.114.25/login/create/ogwfrfe.shtml?
koy=65xtsokpp&lhc=l&r=22wqgu&ptgh=673,
http://91.218.114.37/account/view/spq.phtml?iyy=dnd8556&qb=2&yal=7rw2&rp=4i,
http://91.218.114.77/check/archive/kpujot.cgi,
http://91.218.114.38/forum/check/lggvvy.html?
r=4e306&dhm=8nxn3h2&qm=o4d2m&exif=p17hgc77v,
http://91.218.114.79/payout/r.do,
3011e087f2e7407555cadd19a4db0c14ffbe8cfe4cf2bd6ba64c94698dd9b3c3,

d863468bed27a833e7e9d66d555498679f637a229df5d02c9703081983c3f91a,
b2f91df67493e4bfacbf5845631d959712caabdfde564f465985251d55f34285,
e5a57d3df3424a52f047dfbed0b2ad02c3357bc0d0d872ba0e25d8247cbfa1a7,
b70bfcf533490432d88ea2e4f9f6d810e965c5ee9e01fb667f7cbe411fe72fc3,
ad3d774e45a9c622bba037916cfcf8185916644756442faa48f2d8e41f776058,
404c8586e7a2ebc84e8969689e8b0e1396015b5e77dc8abcc9b8653da2609c17,
39a4ea1db84babf84a3bd8cd11af01ee99cf928f8da1ebfc2d8deef742b226da,
87610305dc5200032b0bfac43ef6b092235db98c9bb471e57768a451455dac66
ee06c557f1acd5c4948b1df0413e49f3885f8ac96185a9d986b91a1231444541,
127c311d8cb03d3ef0efbbc1913a3bc0c2427ade061426f0e5834f12a2913627,
9ccdb10c6c764c19983f3db7d2dcad86f782db4576f8dc077c76921245849e63,
a9d483c0f021b72a94324562068d8164f8cce0aa8f779faea304669390775436,
932778732711cd18d5c4aabc507a65180bf1d4bd2b7d2d4e5506be4b8193596e,
6ad7b3e0873c9ff122c32006fdc3675706a03c4778287085a020d839b74cd780,
3aad14d200887119f316be71d71aec11735dd3698a4fcaa50902fce71bdccb07,
3e5a6834cf6192a987ca9b0b4c8cb9202660e399ebe387af8c7407b12ae2da63,
388997c723728bcb1a0d2338d00754311162000a1bf14b571e18980f835f7bc5,
f3f4d4e4c6704788bc8954ca6f6ddc61b006aba89d5d384794f19424a3d24132
7d41a6fc868682443ae2b5e72f31559b35c4d97549380ac2bd6ada5c2df8ae4b,
bdf49064daca3b95cadc95acabfb35435e07ff9c9d1434873789bd1f12f43d2c,
979fd34db2781977237a8f32fd3bde840ecd29c62ffd5a2a440eb9b59b3ea611,
9baeb75c1ef2eef4d182b80ef83028d23b6dd124c13e5015a0aea8f207911b68,
14da004cc96b910fb75abb86df09e318d92f4fb8dda39c8bd6a8e0601b6605d8
hxxp://217.8.117.63/jpr.exe
hxxp://217.8.117.63/sava.exe