malware-notes/Ransomware-Windows-Yanluowang at master · albertzsigovits/malware-notes · GitHub

github.com/albertzsigovits/malware-notes/tree/master/Ransomware-Windows-Yanluowang

albertzsigovits

albertzsigovits/**malware-notes**

Notes and IoCs of fresh malware

1 Contributor | 0 Issues | 27 Stars | 5 Forks

SHA256

```
d11793433065633b84567de403c1989640a07c9a399dd2753aaf118891ce791c
49d828087ca77abc8d3ac2e4719719ca48578b265bbb632a1a7a36560ec47f2d
```

Password for execution (--pass):

```
D86BDXL9N3H
```

RC4 decryption key (RSA public key and ransom note):

```
RSCNFZJCXGCGF8Q6TOY7IKPE9J3PO6DAPGZFKLHARGXW
```

RSA Public key: 1024-bit

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDghZ1IjKZQIMvxDBd6BtWu6ytb
VtkGOQItQivbeKA4yFnVPlpX7X/vm8CPnspbmzxEmr13DTcT6N0+Uvaz/cw6FDzA
qThpj2Xl3OKW0Ph3ACSIezg3h187ITcOiOuMu0wn3QjNamNwWhQ7Q9uLiwLk1HNb
A1LD9h4cDMfQvwq3oQIDAQAB
-----END PUBLIC KEY-----
```

Crypto APIs used:

```
CryptAcquireContextA
CryptAcquireContextW
CryptDecodeObjectEx
CryptEncrypt
CryptGenRandom
CryptImportPublicKeyInfo
CryptReleaseContext
CryptStringToBinaryA
```

Encryption details:

```
32-byte random key, via CryptGenRandom
dwProvType: PROV_RSA_FULL (0x00000001)
szContainer: Crypto++ RNG
OID: 1.2.840.113549.1.1.1
Encryption Scheme: RSAES-PKCS1-V1_5
```

Following the encryption:

```
32-byte random key via CryptGenRandom
00F15CF0  4F 46 95 F1 DC 2C CA 36 F3 C9 57 60 97 B5 6A 05  OF.ñÜ,Ê6óÉW`.µj.
00F15D00  1C 25 7D CD 7A AE 62 48 03 A1 DE 2E 7C 0C C2 2A  .%}Íz®bH.¡Þ.|.Â*

RC4 decryption of RSA public key
00F15DF0  2D 2D 2D 2D 2D 42 45 47 49 4E 20 50 55 42 4C 49  -----BEGIN PUBLI
00F15E00  43 20 4B 45 59 2D 2D 2D 2D 2D 0A 4D 49 47 66 4D  C KEY-----.MIGfM
00F15E10  41 30 47 43 53 71 47 53 49 62 33 44 51 45 42 41  A0GCSqGSIb3DQEBA
00F15E20  51 55 41 41 34 47 4E 41 44 43 42 69 51 4B 42 67  QUAA4GNADCBiQKBg
00F15E30  51 44 67 68 5A 31 49 6A 4B 5A 51 49 4D 76 78 44  QDghZ1IjKZQIMvxD
00F15E40  42 64 36 42 74 57 75 36 79 74 62 0A 56 74 6B 47  Bd6BtWu6ytb.VtkG
00F15E50  4F 51 49 74 51 69 76 62 65 4B 41 34 79 46 6E 56  OQItQivbeKA4yFnV
00F15E60  50 6C 70 58 37 58 2F 76 6D 38 43 50 6E 73 70 62  PlpX7X/vm8CPnspb
00F15E70  6D 7A 78 45 6D 72 31 33 44 54 63 54 36 4E 30 2B  mzxEmr13DTcT6N0+
00F15E80  55 76 61 7A 2F 63 77 36 46 44 7A 41 0A 71 54 68  Uvaz/cw6FDzA.qTh
00F15E90  70 6A 32 58 6C 33 4F 4B 57 30 50 68 33 41 43 53  pj2Xl3OKW0Ph3ACS
00F15EA0  49 65 7A 67 33 68 31 38 37 49 54 63 4F 69 4F 75  Iezg3h187ITcOiOu
00F15EB0  4D 75 30 77 6E 33 51 6A 4E 61 6D 4E 77 57 68 51  Mu0wn3QjNamNwWhQ
00F15EC0  37 51 39 75 4C 69 77 4C 6B 31 48 4E 62 0A 41 31  7Q9uLiwLk1HNb.A1
00F15ED0  4C 44 39 68 34 63 44 4D 66 51 76 77 71 33 6F 51  LD9h4cDMfQvwq3oQ
00F15EE0  49 44 41 51 41 42 0A 2D 2D 2D 2D 2D 45 4E 44 20  IDAQAB.-----END
00F15EF0  50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D 2D 2D     PUBLIC KEY-----

CryptStringBinaryA and LocalAlloc (30 81 9F 30)
00F182F8  30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01  0..0...*.H.÷....
00F18308  05 00 03 81 8D 00 30 81 89 02 81 81 00 E0 85 9D  ......0......à..
00F18318  48 8C A6 50 20 CB F1 0C 17 7A 06 D5 AE EB 2B 5B  H.¦P Ëñ..z.Õ®ë+[
00F18328  56 D9 06 39 02 2D 42 2B DB 78 A0 38 C8 59 D5 3E  VÙ.9.-B+Ûx 8ÈYÕ>
00F18338  5A 57 ED 7F EF 9B C0 8F 9E CA 5B 9B 3C 44 9A BD  ZWí.ï.À..Ê[.<D.½
00F18348  77 0D 37 13 E8 DD 3E 52 F6 B3 FD CC 3A 14 3C C0  w.7.èÝ>Rö³ýÌ:.<À
00F18358  A9 38 69 8F 65 E5 DC E2 96 D0 F8 77 00 24 88 7B  ©8i.eåÜâ.Ðøw.$.{
00F18368  38 37 87 5F 3B 21 37 0E 88 EB 8C BB 4C 27 DD 08  87._;!7..ë.»L'Ý.
00F18378  CD 6A 63 70 5A 14 3B 43 DB 8B 8B 02 E4 D4 73 5B  ÍjcpZ.;CÛ...äÔs[
00F18388  03 52 C3 F6 1E 1C 0C C7 D0 BF 0A B7 A1 02 03 01  .RÃö...ÇÐ¿.·¡...
00F18398  00 01                                           ..

CryptDecodeObjectEx and LocalAlloc (05 00 AD BA)
CryptImportPublicKey OID: 1.2.840.113549.1.1.1
00F19588  A0 95 F1 00 02 00 00 00 B8 95 F1 00 8C 00 00 00   .ñ.....¸.ñ.....
00F19598  C0 95 F1 00 00 00 00 00 31 2E 32 2E 38 34 30 2E  À.ñ.....1.2.840.
00F195A8  31 31 33 35 34 39 2E 31 2E 31 2E 31 00 F0 AD BA  113549.1.1.1.ð.º
00F195B8  05 00 AD BA 0D F0 AD BA 30 81 89 02 81 81 00 E0  ...º.ð.º0......à
00F195C8  85 9D 48 8C A6 50 20 CB F1 0C 17 7A 06 D5 AE EB  ..H.¦P Ëñ..z.Õ®ë
00F195D8  2B 5B 56 D9 06 39 02 2D 42 2B DB 78 A0 38 C8 59  +[VÙ.9.-B+Ûx 8ÈY
00F195E8  D5 3E 5A 57 ED 7F EF 9B C0 8F 9E CA 5B 9B 3C 44  Õ>ZWí.ï.À..Ê[.<D
00F195F8  9A BD 77 0D 37 13 E8 DD 3E 52 F6 B3 FD CC 3A 14  .½w.7.èÝ>Rö³ýÌ:.
00F19608  3C C0 A9 38 69 8F 65 E5 DC E2 96 D0 F8 77 00 24  <À©8i.eåÜâ.Ðøw.$
00F19618  88 7B 38 37 87 5F 3B 21 37 0E 88 EB 8C BB 4C 27  .{87._;!7..ë.»L'
00F19628  DD 08 CD 6A 63 70 5A 14 3B 43 DB 8B 8B 02 E4 D4  Ý.ÍjcpZ.;CÛ...äÔ
00F19638  73 5B 03 52 C3 F6 1E 1C 0C C7 D0 BF 0A B7 A1 02  s[.RÃö...ÇÐ¿.·¡.
00F19648  03 01 00 01                                       ....

32-byte random key via CryptGenRandom gets copied to the first 32 byte (step #1)
00F19688  4F 46 95 F1 DC 2C CA 36 F3 C9 57 60 97 B5 6A 05  OF.ñÜ,Ê6óÉW`.µj.
00F19698  1C 25 7D CD 7A AE 62 48 03 A1 DE 2E 7C 0C C2 2A  .%}Íz®bH.¡Þ.|.Â*
00F196A8  0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA  .ð.º.ð.º.ð.º.ð.º
00F196B8  0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA  .ð.º.ð.º.ð.º.ð.º
00F196C8  0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA  .ð.º.ð.º.ð.º.ð.º
00F196D8  0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA  .ð.º.ð.º.ð.º.ð.º
00F196E8  0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA  .ð.º.ð.º.ð.º.ð.º
00F196F8  0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA  .ð.º.ð.º.ð.º.ð.º

CryptEncrypt and CryptBinaryToStringA (0x00F19688) (step #2)
Final session key gets appended to the end of all encrypted files
00F19688  5E C6 31 97 BE 65 F1 86 22 4F 32 0A 18 C9 2C CE  ^Æ1.¾eñ."O2..É,Î
```

```
00F19698  A3 D8 50 61 9B 1E E6 5F 9E 3E 38 87 F2 77 8D 4B  £ØPa..æ_.>8.òw.K
00F196A8  41 10 C5 FF AE B6 26 3A F8 2E 64 9B 81 39 37 43  A.Åÿ®¶&:ø.d..97C
00F196B8  83 AF 1B 6D 3E 24 31 F8 DC 74 2D AA 12 6E 98 03  .¯.m>$1øÜt-ª.n..
00F196C8  60 7B FD 3F 91 BD 1D F4 40 11 3E 65 3F 93 48 C6  `{ý?.½.ô@.>e?.HÆ
00F196D8  3C F7 49 13 35 0B 7F 14 2F 8B 21 BA 23 E0 21 D7  <÷I.5.../.!º#à!×
00F196E8  D0 18 3F CA 8E C9 2A E4 E1 4B DA BB 67 E0 50 74  Ð.?Ê.É*äáKÚ»gàPt
00F196F8  B1 47 65 2A 9C C5 9A 29 0E 4E 98 52 BD 07 DA 6F  ±Ge*.Å.).N.R½.Úo

Final session key gets converted to Base64
00F1A920  58 73 59 78 6C 37 35 6C 38 59 59 69 54 7A 49 4B  XsYxl75l8YYiTzIK
00F1A930  47 4D 6B 73 7A 71 50 59 55 47 47 62 48 75 5A 66  GMkszqPYUGGbHuZf
00F1A940  6E 6A 34 34 68 2F 4A 33 6A 55 74 42 45 4D 58 2F  nj44h/J3jUtBEMX/
00F1A950  72 72 59 6D 4F 76 67 75 5A 4A 75 42 4F 54 64 44  rrYmOvguZJuBOTdD
00F1A960  0D 0A 67 36 38 62 62 54 34 6B 4D 66 6A 63 64 43  ..g68bbT4kMfjcdC
00F1A970  32 71 45 6D 36 59 41 32 42 37 2F 54 2B 52 76 52  2qEm6YA2B7/T+RvR
00F1A980  33 30 51 42 45 2B 5A 54 2B 54 53 4D 59 38 39 30  30QBE+ZT+TSMY890
00F1A990  6B 54 4E 51 74 2F 46 43 2B 4C 49 62 6F 6A 34 43  kTNQt/FC+LIboj4C
00F1A9A0  48 58 0D 0A 30 42 67 2F 79 6F 37 4A 4B 75 54 68  HX..0Bg/yo7JKuTh
00F1A9B0  53 39 71 37 5A 2B 42 51 64 4C 46 48 5A 53 71 63  S9q7Z+BQdLFHZSqc
00F1A9C0  78 5A 6F 70 44 6B 36 59 55 72 30 48 32 6D 38 3D  xZopDk6YUr0H2m8=

Base64 gets added to the end of the ransom note
00F1B570  63 61 6E 67 2E 6C 65 65 6E 40 6D 61 69 6C 66 65  cang.leen@mailfe
00F1B580  6E 63 65 2E 63 6F 6D 0A 32 29 79 61 6E 2E 6C 61  nce.com.2)yan.la
00F1B590  6F 77 61 6E 67 40 6D 61 69 6C 66 65 6E 63 65 2E  owang@mailfence.
00F1B5A0  63 6F 6D 4A 58 73 59 78 6C 37 35 6C 38 59 59 69  comJXsYxl75l8YYi
00F1B5B0  54 7A 49 4B 47 4D 6B 73 7A 71 50 59 55 47 47 62  TzIKGMkszqPYUGGb
00F1B5C0  48 75 5A 66 6E 6A 34 34 68 2F 4A 33 6A 55 74 42  HuZfnj44h/J3jUtB
00F1B5D0  45 4D 58 2F 72 72 59 6D 4F 76 67 75 5A 4A 75 42  EMX/rrYmOvguZJuB
00F1B5E0  4F 54 64 44 0D 0A 67 36 38 62 62 54 34 6B 4D 66  OTdD..g68bbT4kMf
00F1B5F0  6A 63 64 43 32 71 45 6D 36 59 41 32 42 37 2F 54  jcdC2qEm6YA2B7/T
00F1B600  2B 52 76 52 33 30 51 42 45 2B 5A 54 2B 54 53 4D  +RvR30QBE+ZT+TSM
00F1B610  59 38 39 30 6B 54 4E 51 74 2F 46 43 2B 4C 49 62  Y890kTNQt/FC+LIb
00F1B620  6F 6A 34 43 48 58 0D 0A 30 42 67 2F 79 6F 37 4A  oj4CHX..0Bg/yo7J
00F1B630  4B 75 54 68 53 39 71 37 5A 2B 42 51 64 4C 46 48  KuThS9q7Z+BQdLFH
00F1B640  5A 53 71 63 78 5A 6F 70 44 6B 36 59 55 72 30 48  ZSqcxZopDk6YUr0H
00F1B650  32 6D 38 3D                                     2m8=.
```

Ransomware executable digital signature:

```
Name: AdClearance Limited
Thumbprint: 614A13CA73AE2F01D860B5F87B71CA38F5307DBD
SN: 0D 0D A8 84 0C 1A 95 9D 09 32 47 FA 33 6E 5A 2D
```

Mutex:

```
Type=Mutant
Name=\Sessions\1\BaseNamedObjects\SM0:pid:handle:WilStaging_02
```

E-mails from the ransom note:

```
cang.leen@mailfence.com
yan.laowang@mailfence.com
```

Ransomware execution arguments:

```
-h
-p
-pass
-path
--help
--pass
--path
```

Ransomware extension:

```
.yanluowang
```

Ransomware note:

```
README.txt
```

Ransomware (-h) execution helper:

```
Syntax: encrypt.exe [(-p,-path,--path)<path>]
```

Interesting commands executed:

```
cmd.exe /c powershell -command "Get-VM | Stop-VM -Force"
cmd.exe /c for /l %x in (1,1,3) do start wordpad.exe /p
```

Terminated processes via (CreateToolhelp32Snapshot):

```
veeam
sql
```

Skipped folders:

```
PROGRA~1
PROGRA~2
PROGRA~3
SYSTEM~1
Windows
WINDOWS
```

Skip-list for extensions:

```
exe
dll
conf
a
lib
bat
ps
msi
cfg
reg
sys
lnk
obj
ini
yanluowang
```

Killed processes via (ShellExecute):

```
taskkill /f /im CNTAoSMgr*
taskkill /f /im IBM*
taskkill /f /im Notifier*
taskkill /f /im Ntrtscan*
taskkill /f /im TmListen*
taskkill /f /im bes10*
taskkill /f /im black*
taskkill /f /im chrome*
taskkill /f /im copy*
taskkill /f /im ds_monitor*
taskkill /f /im dsa*
taskkill /f /im excel*
taskkill /f /im firefox*
taskkill /f /im iVPAgent*
taskkill /f /im iexplore*
taskkill /f /im mysql*
taskkill /f /im outlook*
taskkill /f /im postg*
taskkill /f /im putty*
taskkill /f /im robo*
taskkill /f /im sage*
taskkill /f /im sql
taskkill /f /im sql*
taskkill /f /im ssh*
taskkill /f /im store.exe
taskkill /f /im tasklist*
taskkill /f /im taskmgr*
taskkill /f /im vee*
taskkill /f /im veeam*
taskkill /f /im wrsa*
taskkill /f /im wrsa.exe
```

Stopped services:

```
net stop IISADMIN
net stop MSExchangeADTopology
net stop MSExchangeFBA
net stop MSExchangeIS
net stop MSExchangeSA
net stop MSSQL$ISARS
net stop MSSQL$MSFW
net stop MSSQLServerADHelper100
net stop QBCFMonitorService
net stop QBPOSDBServiceV12
net stop QBVSS
net stop QuickBooksDB1
net stop QuickBooksDB10
net stop QuickBooksDB11
net stop QuickBooksDB12
net stop QuickBooksDB13
net stop QuickBooksDB14
net stop QuickBooksDB15
net stop QuickBooksDB16
net stop QuickBooksDB17
net stop QuickBooksDB18
net stop QuickBooksDB19
net stop QuickBooksDB2
net stop QuickBooksDB20
net stop QuickBooksDB21
net stop QuickBooksDB22
net stop QuickBooksDB23
net stop QuickBooksDB24
net stop QuickBooksDB25
net stop QuickBooksDB3
net stop QuickBooksDB4
net stop QuickBooksDB5
net stop QuickBooksDB6
net stop QuickBooksDB7
net stop QuickBooksDB8
net stop QuickBooksDB9
net stop ReportServer$ISARS
net stop SPAdminV4
net stop SPSearch4
net stop SPTimerV4
net stop SPTraceV4
net stop SPUserCodeV4
net stop SPWriterV4
net stop SQLAgent$ISARS
net stop SQLAgent$MSFW
net stop SQLBrowser
net stop SQLWriter
net stop ShadowProtectSvc
net stop WinDefend
net stop "IBM Domino Diagnostics (CProgramFilesIBMDomino)"
net stop "IBM Domino Server (CProgramFilesIBMDominodata)"
net stop "Simply Accounting Database Connection Manager"
net stop firebirdguardiandefaultinstance
net stop ibmiasrw
net stop mr2kserv
```

Ransom note:

```
    Hi, since you are reading this it means you have been hacked.
    In addition to encrypting all your systems, deleting backups, we also downloaded 2 terabytes of
confidential information.
    Here's what you shouldn't do:
    1) Contact the police, fbi or other authorities before the end of our deal
    2) Contact the recovery company so that they would conduct dialogues with us. (This can slow down
the recovery, and generally put our communication to naught)
    3) Do not try to decrypt the files yourself, as well as do not change the file extension yourself
!!! This can lead to the impossibility of their decryption.
    4) Keep us for fools)
    We will also stop any communication with you, and continue DDoS, calls to employees and business
partners.
    In a few weeks, we will simply repeat our attack and delete all your data from your networks,
WHICH WILL LEAD TO THEIR UNAVAILABILITY!
    Here's what you should do right after reading it:
    1) If you are an ordinary employee, send our message to the CEO of the company, as well as to the
IT department
    2) If you are a CEO, or a specialist in the IT department, or another person who has weight in the
company, you should contact us within 24 hours by email.
    We are ready to confirm all our intentions regarding DDOS, calls, and deletion of the date at your
first request.
    As a guarantee that we can decrypt the files, we suggest that you send several files for free
decryption.
    Mails to contact us:
    1)cang.leen@mailfence.com
    2)yan.laowang@mailfence.comJ0mAm8SN6C0BPAImmRDBChtERC7nTlQ49bsh2xDb4IrtDvr17bCwy+GSiq+IFUT4H
    irx+WpNuWBzpS2CUO6pR+FkYoaltOtN+fMpogxD3jzCC29ksq2BfcXqLSIr/zJuz
    HJ3saoWSBxf0XTA5SMU1xJ0d/Nx/wu2t7Vb4sethsj4=
```

The J right after the email address is hardcoded, and not part of the base64 encoded key.

`2)yan.laowang@mailfence.comJ0mAm8SN6C0BPAImmRDBChtERC7nTlQ49bsh2xDb4IrtDvr17bCwy+GSiq+IFUT4H`