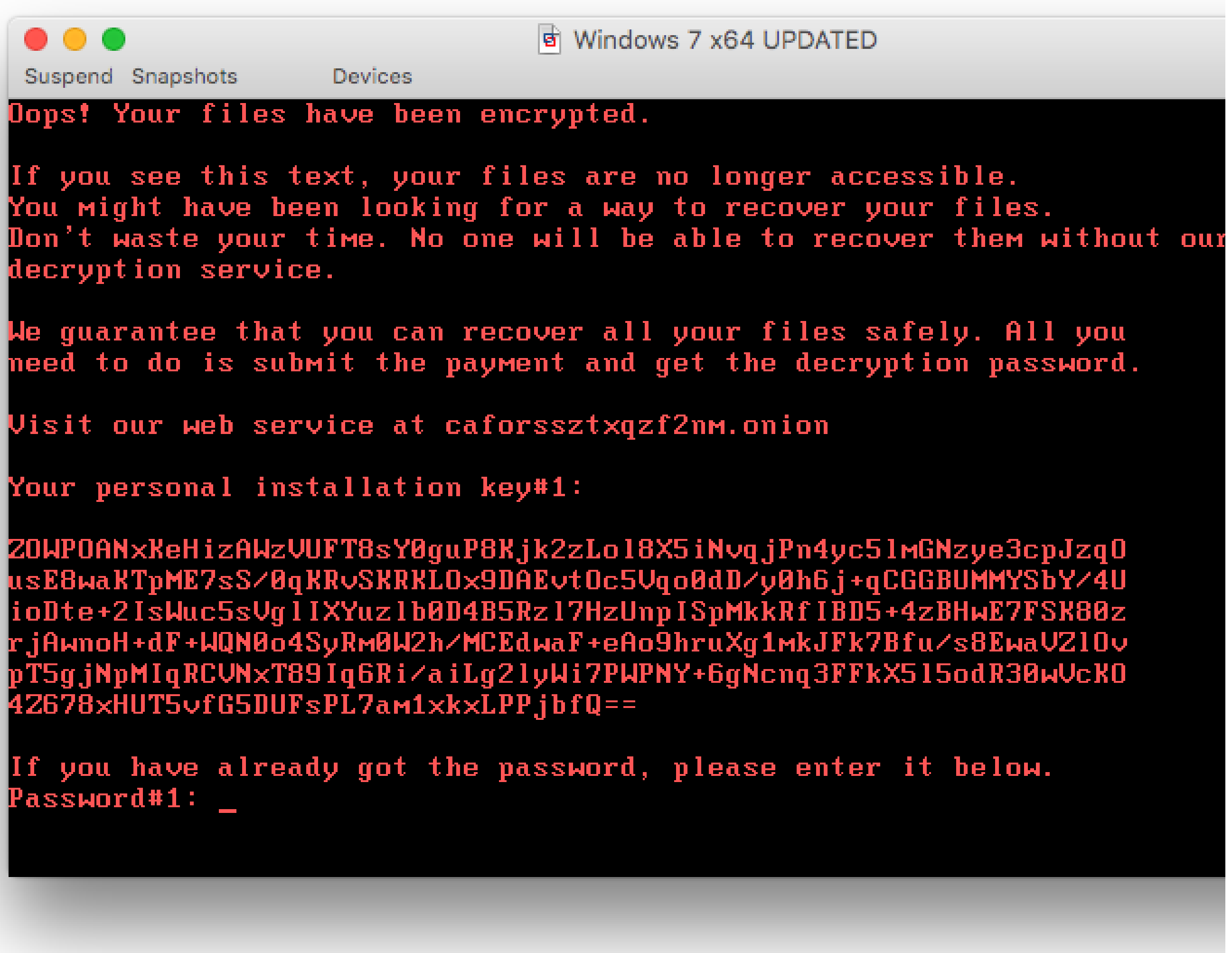
SentinelOne blog

GET A DEMO

New Bad Rabbit Ransomware Attack

October 26, 2017
by SentinelOne Labs

It's been almost exactly four months since the last Petya ransomware outbreak. On October 24th, a new variant of Petya called *Bad Rabbit* was dis
and organizations, mostly in Russia. Below is a copy of the ransom note, which is similar to Petya's ransom note:



SentinelOne customers are protected from this threat. Below is a video showing the detection:

Media error: Format(s) not supported or source(s) not found

Download File: https://www.sentinelone.com/wp-content/uploads/2017/10/BadRabbit.mp4?_=1

Operation

The malware is distributed by drive-by downloads. It's icon appears is an Adobe Flash installer.

Once it's running, it looks for and encrypts files with the following file extensions:

> .3ds .7z .accdb .ai .asm .asp .aspx .avhd .back .bak .bmp .brw .c .cab .cc .cer .cfg
> .conf .cpp .crt .cs .ctl .cxx .dbf .der .dib .disk .djvu .doc .docx .dwg .eml .fdb
> .gz .h .hdd .hpp .hxx .iso .java .jfif .jpe .jpeg .jpg .js .kdbx .key .mail .mdb
> .msg .nrg .odc .odf .odg .odi .odm .odp .ods .odt .ora .ost .ova .ovf .p12 .p7b .p7c
> .pdf .pem .pfx .php .pmf .png .ppt .pptx .ps1 .pst .pvi .py .pyc .pyw .qcow .qcow2
> .rar .rb .rtf .scm .sln .sql .tar .tib .tif .tiff .vb .vbox .vbs .vcb .vdi .vfd .vhd
> .vhdx .vmc .vmdk .vmsd .vmtm .vmx .vsdx .vsv .work .xls .xlsx .xml .xvd .zip

Additionally, Bad Rabbit tries to spread itself. It uses Mimikatz to dump credentials and uses them along with hard coded. Then it tries to spread us

- SVCCTL
- SMB2 / SMB
- NTLMSSP

The hard coded usernames are:

> Admin, Administrator, alex, asus, backup, boss, buh, ftp, ftpadmin, ftpuser, Guest,
> manager, nas, nasadmin, nasuser, netguest, operator, other user, rdp, rdpadmin,
> rdpuser, root,superuser, support, Test, User, User1, user-1, work

The hard coded passwords are:

> 111111, 123, 123321, 1234, 12345, 123456, 1234567, 12345678,123456789, 1234567890,
> 321, 55555, 777, 77777, Admin, Admin123, admin123Test123, Administrator, administrator,
> Administrator123, administrator123, adminTest, god, Guest, guest, Guest123, guest123,
> love, password, qwe, qwe123, qwe321, qwer, qwert, qwerty, qwerty123, root, secret, sex,
> test, test123, uiop, User, user, User132, user123, zxc, zxc123, zxc321,zxcv

Lateral Movement Detection

The video below shows us detecting the malware as it attempts to spread from an unprotected, infected host (right, red background) to a protectec
background).

Media error: Format(s) not supported or source(s) not found

Download File: https://www.sentinelone.com/wp-content/uploads/2017/10/BadRabbit_lateral.mp4?_=2

SentinelOne also constructs an attack storyline for the lateral movement for incident response reports and forensics:

Sample Hashes

- Primary SHA256: 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da
- Payload SHA256: 8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Weekly Recap of Cybersecurity News 10/27
- Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool
- Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results
- Threat Actor UAC-0056 Targeting Ukraine with Fake Translation Software
- From the Front Lines | Hive Ransomware Deploys Novel IPfuscation Technique To Avoid Detection
- From the Front Lines | Peering into A PYSA Ransomware Attack