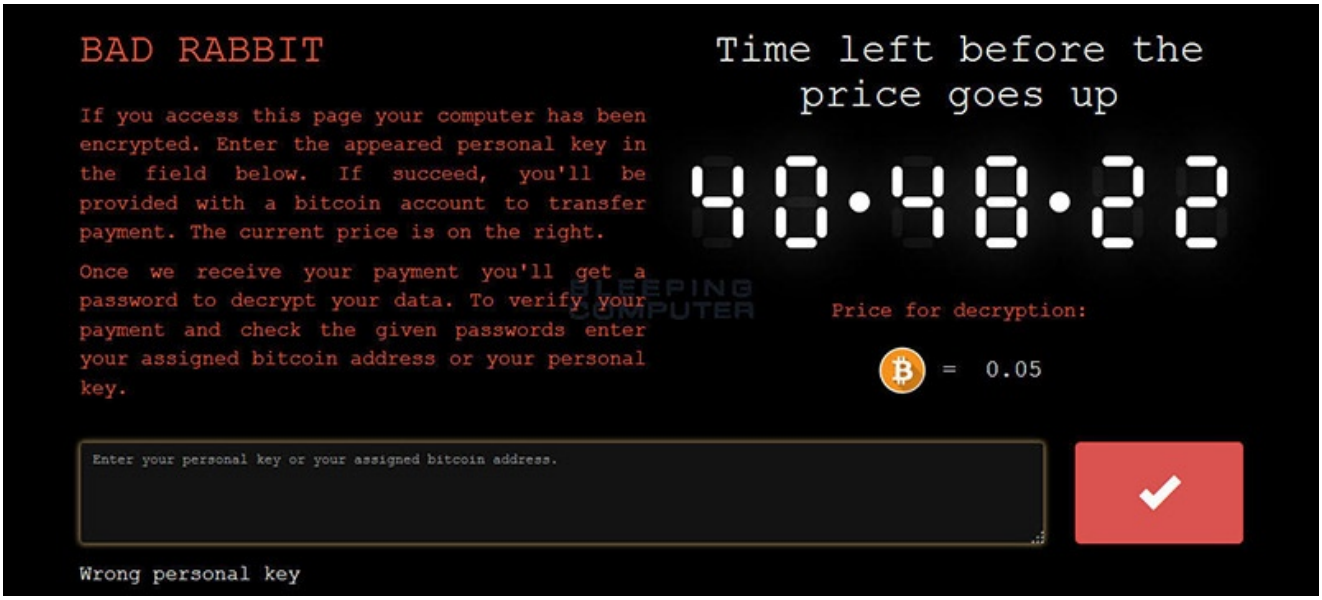
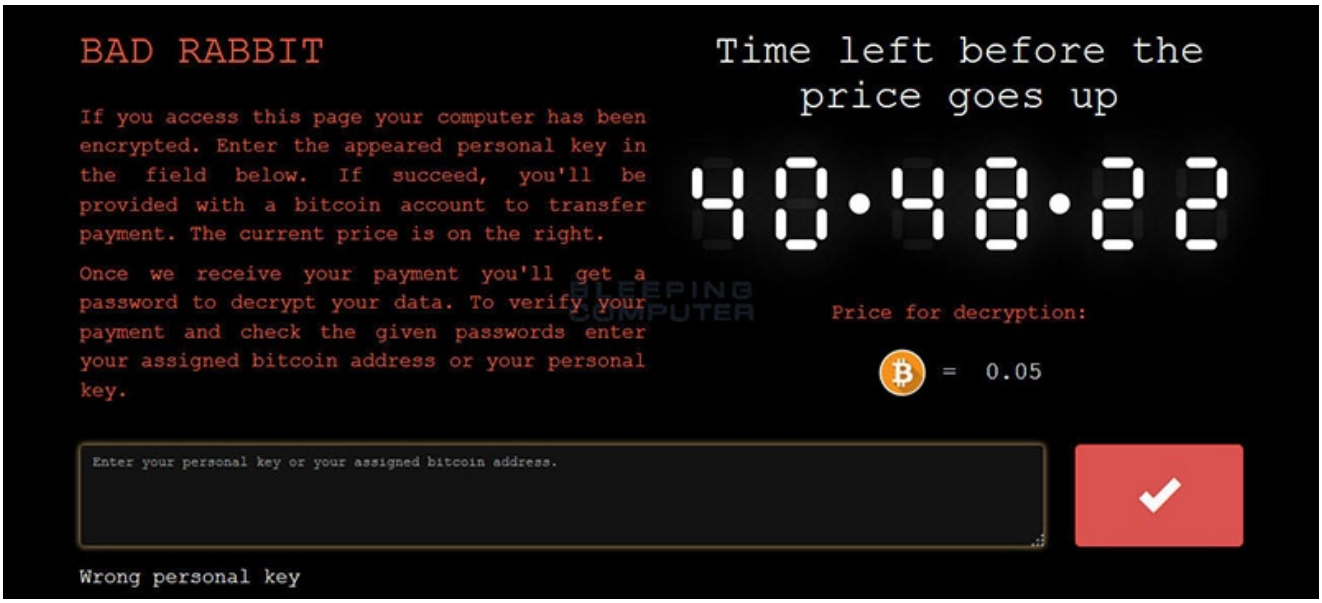
ReversingLabs' YARA rule detects BadRabbit encryption routine specifics

reversinglabs.com/newsroom/news/reversinglabs-yara-rule-detects-badrabbit-encryption-routine-specifics.html



Research | October 26, 2017



The ransomware's fake FlashPlayer dropper was distributed through compromised websites via drive-by downloads.

Targets are mostly Russia based but there have also been reports of victims in Ukraine, Turkey and Germany.

Although several sources pointed to existing similarities between NotPetya and BadRabbit, besides the same compiler and similar methods being used, the source code of the two has noticable differences.

ReversingLabs' YARA rule **(download here)** detects BadRabbit encryption routine specifics.

#BadRabbit #Ransomware #DROPPER

630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da
Original name: FlashUtil.exe
File size: 431.5 KB (441899 bytes)

8911fdb8c1ac8f6098057dfbbd77fc0c5e6a55a78d4a2f9701b965230ce32cf9
Original name: FlashUtil.exe
File size: 409.6 KB (419401 bytes)

7160bd96104d2ff21d836e9585b8d869edcc0aa60ee84157b7670d9abb1cd785
Original name: FlashUtil.exe
File size: 431.5 KB (441898 bytes)

5c3dc8a0c37c55af92336fde825e8280c6fd28c3f9fe69e61facb3b1da20c0df
Original name: FlashUtil.exe
File size: 431.5 KB (441899 bytes)

#BadRabbit #unpacked

579fd8a0385482fb4c789561a30b09f25671e86422f40ef5cca2036b28f99648
C:\Windows\infpub.dat
File size: 401.1 KB (410760 bytes)

#BadRabbit #PAYLOAD

8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93
Original name: dispci.exe
File size: 139.5 KB (142848 bytes)

10e741ef66bdd9166434781d5a0ce465f50f270fdf538a351e91a5161458c888
Original name: dispci.exe
File size: 139.5 KB (142855 bytes)

#BadRabbitComponent #Diskcryptor

682adcb55fe4649f7b22505a54a9dbc454b4090fc2bb84af7db5b0908f3b7806
Original name: dcrypt.sys
C:\Windows\cscc.dat x32 diskcryptor

0b2f863f4119dc88a22cc97c0a136c88a0127cb026751303b045f7322a8972f6
Original name: dcrypt.sys
C:\Windows\cscc.dat x64 diskcryptor

#BadRabbitComponent #Mimikatz

2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035
File size: 52.4 KB (53624 bytes)
mimikatz-like x86

301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcfe347c
File size: 60.9 KB (62328 bytes)
mimikatz-like x64

#BadRabbit #debug #build

52d4747637b94db89996c9da113160eff2eee95c5528fb3abb7f85c2d7eb291c
DISCKCODER debug build
File size: 536.5 KB (549376 bytes)

ae8a2eea804cdc233a518eead2a5e050189ba183548b73b85d97d66e8dbd3fd7
DISCKCODER debug build
File size: 536.5 KB (549376 bytes)

3354967433417380fb34b1fd030f8a6aa4de4a6e2f4a69559d70be328283bc73
DISCKCODER debug build
File size: 536.5 KB (549376 bytes)

1c6fdf8b58afb6e28934acc1bc7eb50a7713dc0aff1cc58d4b0bb5a3479beca1
DISCKCODER debug build
File size: 536.5 KB (549378 bytes)

MORE BLOG ARTICLES