RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: **SEM-M03**

RANSOMWARE AND DESTRUCTIVE ATTACKS

Raj Samani

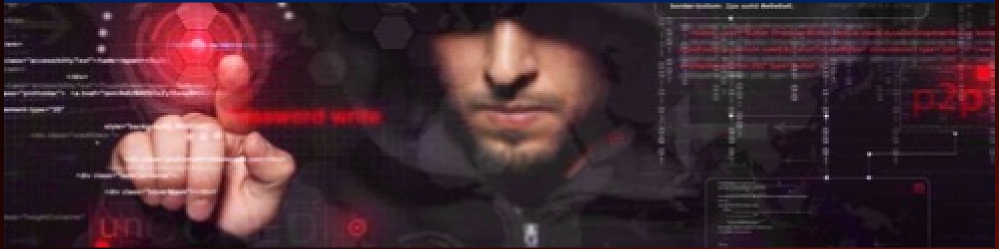
Chief Scientist & McAfee Fellow
McAfee
@Raj_Samani

Christiaan Beek

Lead Scientist & Sr. Principal Engineer
McAfee
@ChristiaanBeek

When a nation went DARK…..

Taiwan Bank Heist and the Role of Pseudo-Ransomware



Topic: ransomware partnership

good day

looking for a partner to supply ransomware I have huge email lists and some select companies to infect via usb for more payoff.

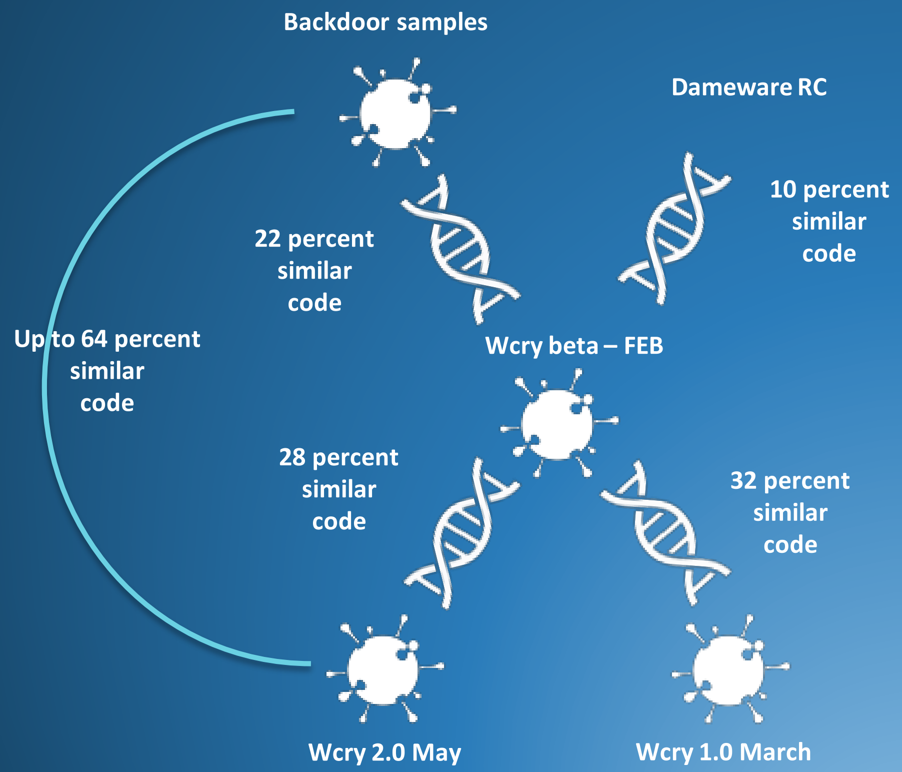
almost completed this on alpha but alpha bay has been down now for days and doesn’t seem to ever be on again

Pseudo Ransomware

Designed for speed & Destruction

	Cerber	Locky	Wcry	Petya’16	Pnetya	BadRabbit
Amount of file types	187	381	176	228	65	113

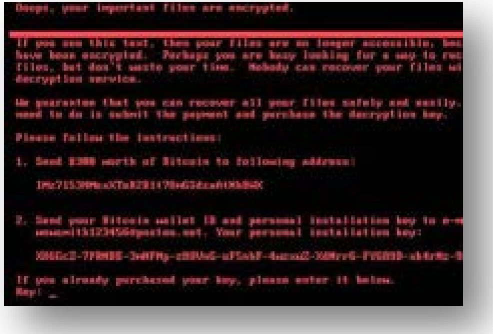
Pseudo Ransomware - Wcry



All three samples (Feb – May) were developed in same dev-environment:

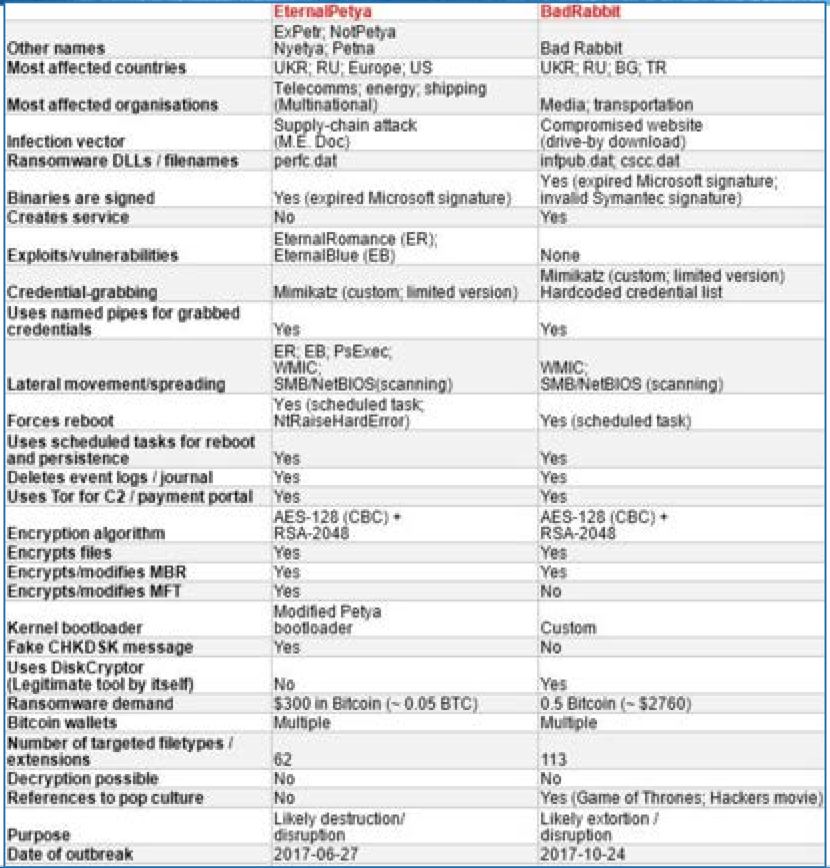
Visual Studio 2003 release 07.10

Pseudo Ransomware: NotPetya vs Badrabbit



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, bec
have been encrypted.  Perhaps you are busy looking for a way to rec
files, but don't waste your time.  Nobody can recover your files wi
decryption service.

We guarantee that you can recover all your files safely and easily.
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-m
   wowsmith123456@posteo.net. Your personal installation key:

   [illegible]

If you already purchased your key, please enter it below.
Key: _
```

Picture by @Bartblaze



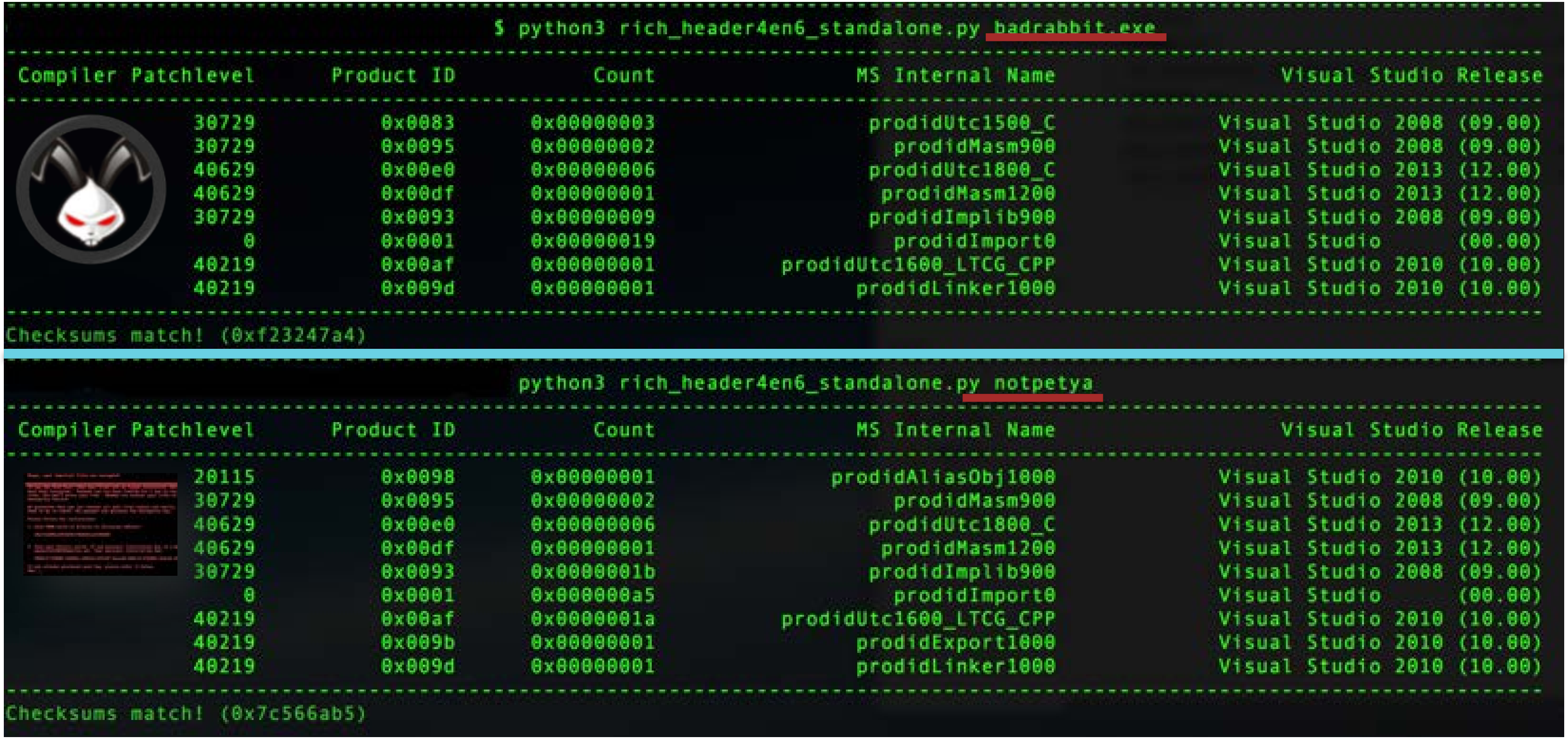
	EternalPetya	BadRabbit
Other names	ExPetr; NotPetya Nyetya; Petna	Bad Rabbit
Most affected countries	UKR; RU; Europe; US	UKR; RU; BG; TR
Most affected organisations	Telecomms; energy; shipping (Multinational)	Media; transportation
Infection vector	Supply-chain attack (M.E. Doc)	Compromised website (drive-by download)
Ransomware DLLs / filenames	perfc.dat	infpub.dat; cscc.dat
Binaries are signed	Yes (expired Microsoft signature)	Yes (expired Microsoft signature; invalid Symantec signature)
Creates service	No	Yes
Exploits/vulnerabilities	EternalRomance (ER); EternalBlue (EB)	None
Credential-grabbing	Mimikatz (custom; limited version)	Mimikatz (custom; limited version) Hardcoded credential list
Uses named pipes for grabbed credentials	Yes	Yes

Lateral movement/spreading	ER; EB; PsExec;
	WMIC;
	SMB/NetBIOS(scanning)
		WMIC;
		SMB/NetBIOS (scanning)

Forces reboot	Yes (scheduled task; NtRaiseHardError)	Yes (scheduled task)
Uses scheduled tasks for reboot and persistence	Yes	Yes
Deletes event logs / journal	Yes	Yes
Uses Tor for C2 / payment portal	Yes	Yes
Encryption algorithm	AES-128 (CBC) + RSA-2048	AES-128 (CBC) + RSA-2048
Encrypts files	Yes	Yes
Encrypts/modifies MBR	Yes	Yes
Encrypts/modifies MFT	Yes	No
Kernel bootloader	Modified Petya bootloader	Custom
Fake CHKDSK message	Yes	No
Uses DiskCryptor (Legitimate tool by itself)	No	Yes
Ransomware demand	$300 in Bitcoin (~ 0.05 BTC)	0.5 Bitcoin (~ $2760)
Bitcoin wallets	Multiple	Multiple
Number of targeted filetypes / extensions	62	113
Decryption possible	No	No
References to pop culture	No	Yes (Game of Thrones; Hackers movie)
Purpose	Likely destruction/ disruption	Likely extortion / disruption
Date of outbreak	2017-06-27	2017-10-24

McAfee

Pseudo Ransomware: NotPetya vs Badrabbit



```
-----------------------------------------------------------------------------------------------------------------
                                $ python3 rich_header4en6_standalone.py badrabbit.exe
-----------------------------------------------------------------------------------------------------------------
 Compiler Patchlevel        Product ID          Count                MS Internal Name            Visual Studio Release
-----------------------------------------------------------------------------------------------------------------
                   30729        0x0083     0x00000003                 prodidUtc1500_C      Visual Studio 2008 (09.00)
                   30729        0x0095     0x00000002                  prodidMasm900       Visual Studio 2008 (09.00)
                   40629        0x00e0     0x00000006                 prodidUtc1800_C      Visual Studio 2013 (12.00)
                   40629        0x00df     0x00000001                 prodidMasm1200       Visual Studio 2013 (12.00)
                   30729        0x0093     0x00000009                 prodidImplib900      Visual Studio 2008 (09.00)
                       0        0x0001     0x00000019                  prodidImport0       Visual Studio      (00.00)
                   40219        0x00af     0x00000001          prodidUtc1600_LTCG_CPP      Visual Studio 2010 (10.00)
                   40219        0x009d     0x00000001                prodidLinker1000      Visual Studio 2010 (10.00)
-----------------------------------------------------------------------------------------------------------------
Checksums match! (0xf23247a4)
```

```
-----------------------------------------------------------------------------------------------------------------
                                  python3 rich_header4en6_standalone.py notpetya
-----------------------------------------------------------------------------------------------------------------
 Compiler Patchlevel        Product ID          Count                MS Internal Name            Visual Studio Release
-----------------------------------------------------------------------------------------------------------------
                   20115        0x0098     0x00000001             prodidAliasObj1000       Visual Studio 2010 (10.00)
                   30729        0x0095     0x00000002                  prodidMasm900       Visual Studio 2008 (09.00)
                   40629        0x00e0     0x00000006                 prodidUtc1800_C      Visual Studio 2013 (12.00)
                   40629        0x00df     0x00000001                 prodidMasm1200       Visual Studio 2013 (12.00)
                   30729        0x0093     0x0000001b                 prodidImplib900      Visual Studio 2008 (09.00)
                       0        0x0001     0x000000a5                  prodidImport0       Visual Studio      (00.00)
                   40219        0x00af     0x0000001a          prodidUtc1600_LTCG_CPP      Visual Studio 2010 (10.00)
                   40219        0x009b     0x00000001                prodidExport1000      Visual Studio 2010 (10.00)
                   40219        0x009d     0x00000001                prodidLinker1000      Visual Studio 2010 (10.00)
-----------------------------------------------------------------------------------------------------------------
Checksums match! (0x7c566ab5)
```

OPERATION BAKOVIA

How Private & Public can succeed

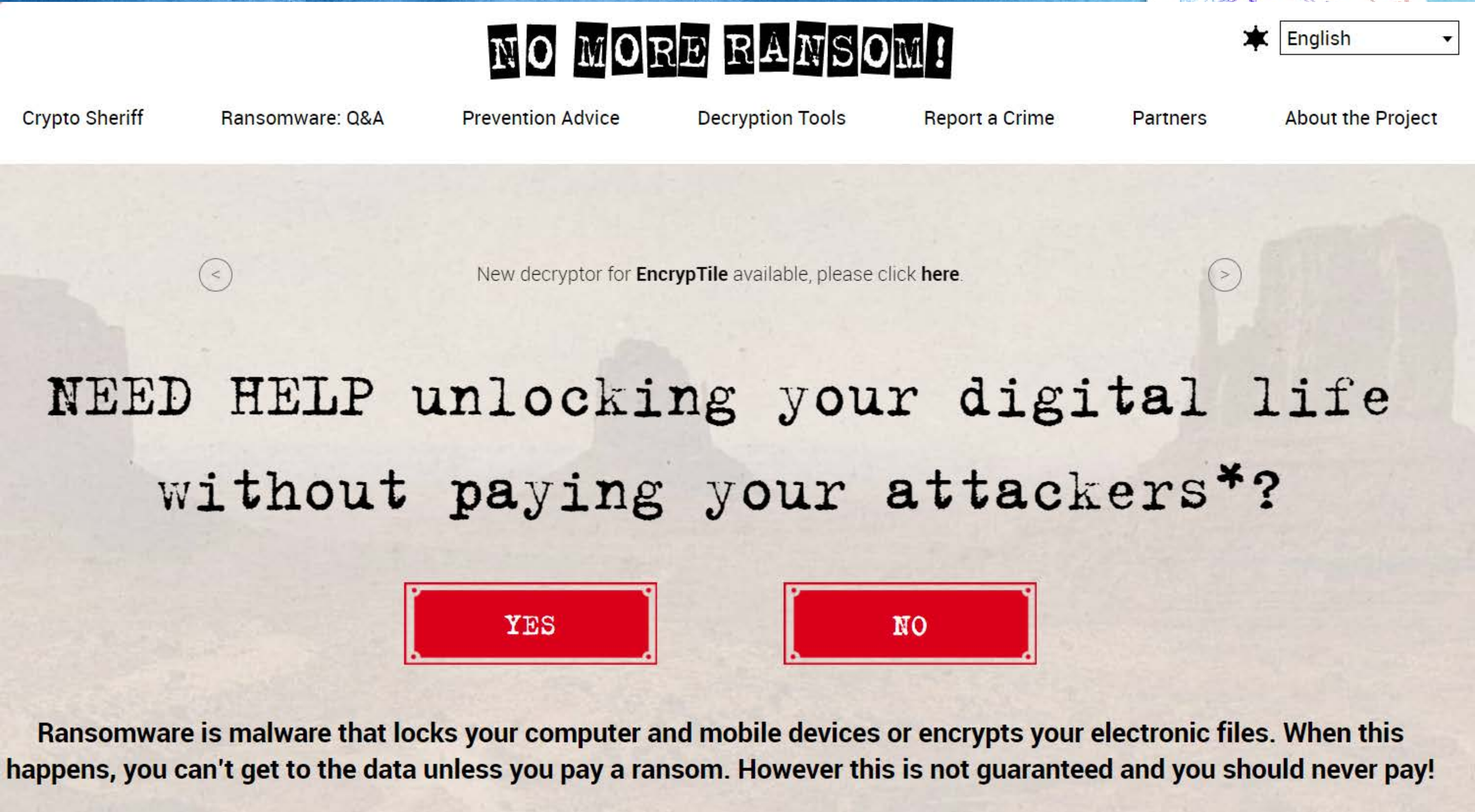
Video

https://www.youtube.com/watch?v=iP9Kr5T9FFs

The Bad: Lifestyle of Ransomware Actors

30% of ransomware were pseudo?

Easy money fast, easy and safe



New decryptor for **EncrypTile** available, please click **here**.

NEED HELP unlocking your digital life without paying your attackers*?

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

NO MORE RANSOM!

JULY 25, 2016

Founders

Kaspersky Lab,
Dutch police, Europol,
and McAfee

Tools

5 from Kaspersky Lab
2 from McAfee

Language

English

JULY 25, 2017

Partners

35 law enforcement agencies

74 private and public sector companies

Tools

54 decryptors provided by 9 partners covering 104 strains of ransomware

More than 28,000 devices successfully decrypted, saving more than $8.5 million for victims

Languages

26 available languages