



San Francisco | March 4–8 | Moscone Center



SESSION ID: SEM-M03L

Emerging Threats

Ransomware: The Rise, Death and Resurrection of Digital Extortion

Raj Samani

Chief Scientist, McAfee Fellow
McAfee
@Raj_Samani

John Fokker

Head of Cyber Investigations
McAfee
@john_fokker

#RSAC

Speakers

**Raj Samani**

Chief Scientist, McAfee Fellow
McAfee

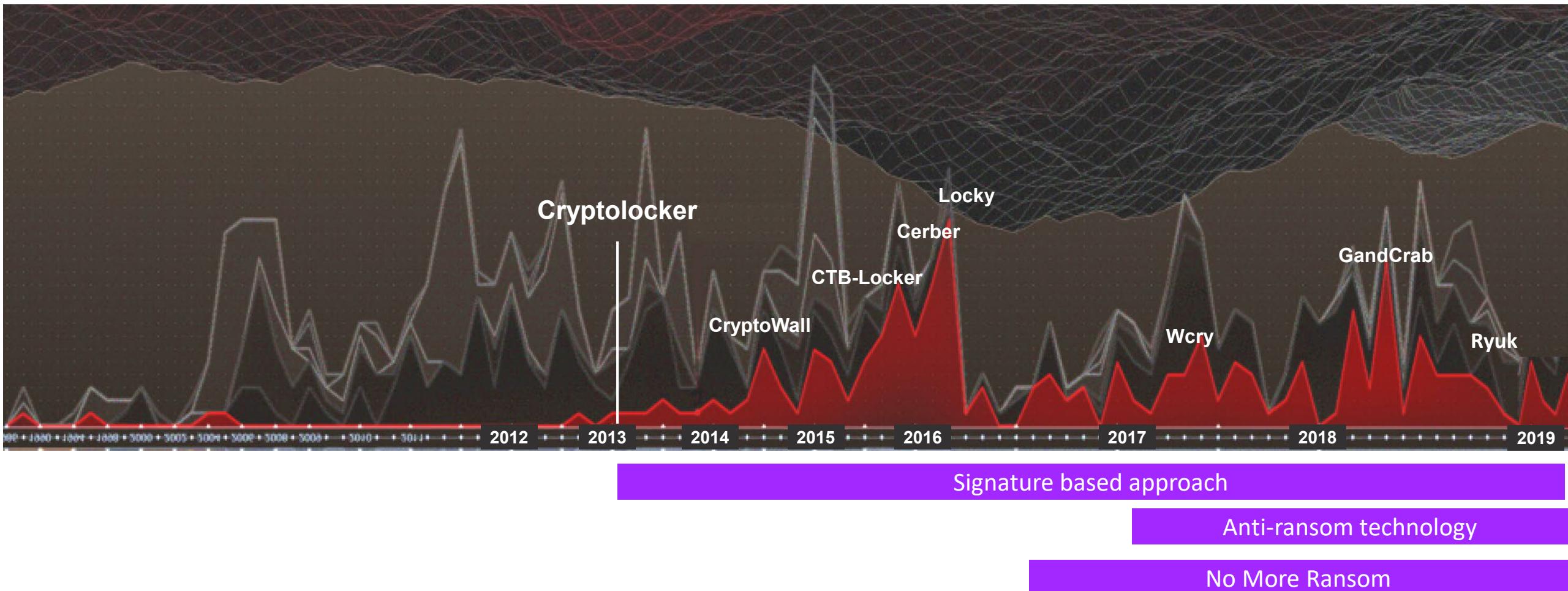
**John Fokker**

Lead Scientist, Senior Principal Engineer
McAfee

So what is on the Menu today?

- This session is primarily focused on Ransomware
 - The Rise, Death and Resurrection of Ransomware explained
 - Insights in one of our ransomware investigations
 - Prevention tips
 - Mitigation tips

The fall (Death): Decline in new ransomware families 2018



Ransomware Resurrected

From opportunistic to targeted

- RDP based attacks are increasingly favorable
- SAMSAM, Bitpaymer, Ryuk, GandCrab and now also Matrix ransomware

#379512 - NO REFUND FOR FRESH RDP!

\$10
United States

Windows Server 2008 R2 Standard
Intel(R) Xeon(R) CPU E5-2407 0 @ 2.20GHz
Memory (RAM): -- | Cores: 4

Dwn. Speed: 6.52 Mbit/s | Up. Speed: 4.57 Mbit/s

Admin Rights: ✓
Direct IP: ✗
Antivirus: Unknown Blacklist: [Check](#)
proxyScore: [Check](#)

Domain: *.
ISP: City

Browsers:
[IE](#)
[Chrome](#)

Payment Systems:
[Not found](#)

Online Shops:
[Not found](#)

Poker Rooms:
[Not found](#)

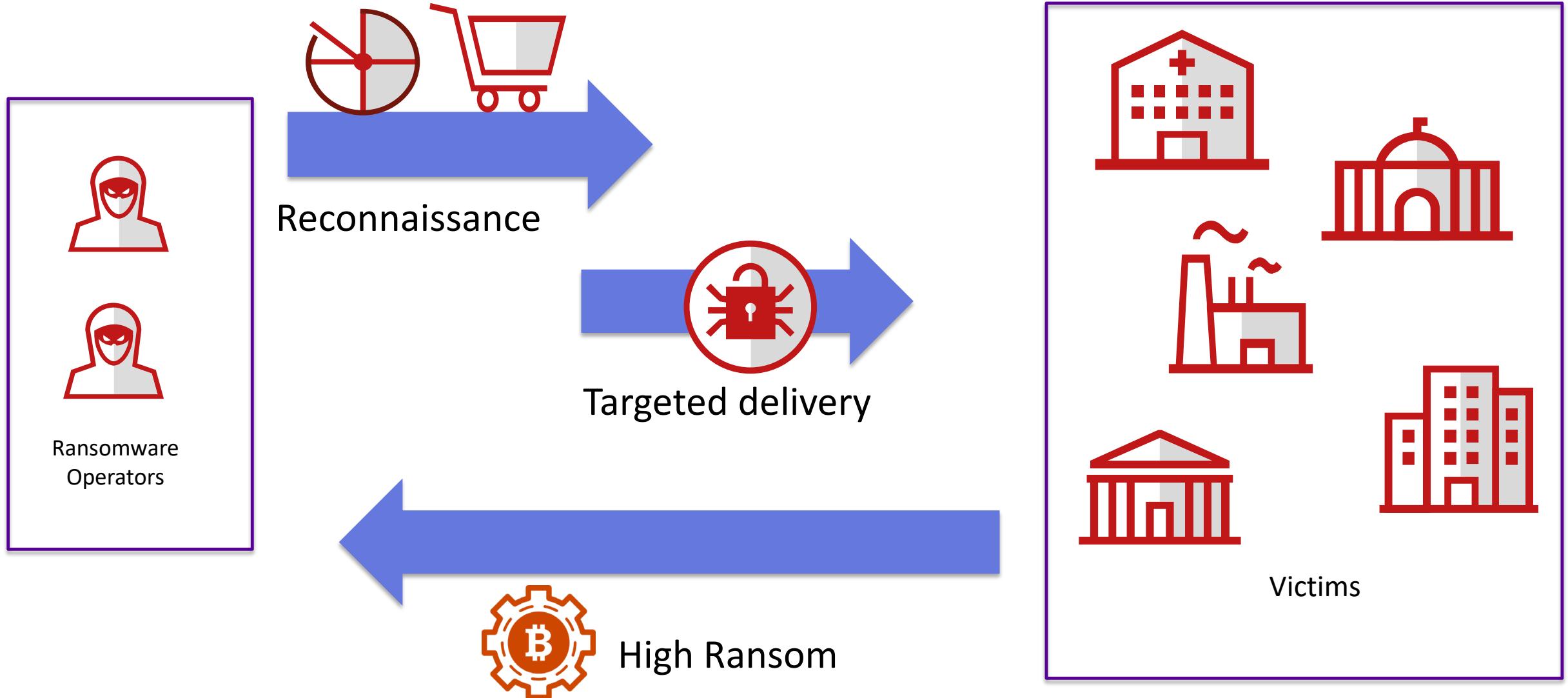
Dating:
[Not found](#)

Other Sites:
[Not found](#)

[Buy](#) [Close](#)



Rise : targeted Ransomware



Rise : Ransomware-as-a-Service are growing stronger

New Fallout Exploit Kit Drops GandCrab Ransomware or Redirects to PUPs

By Lawrence Abrams

September 6, 2018 06:24 PM 0



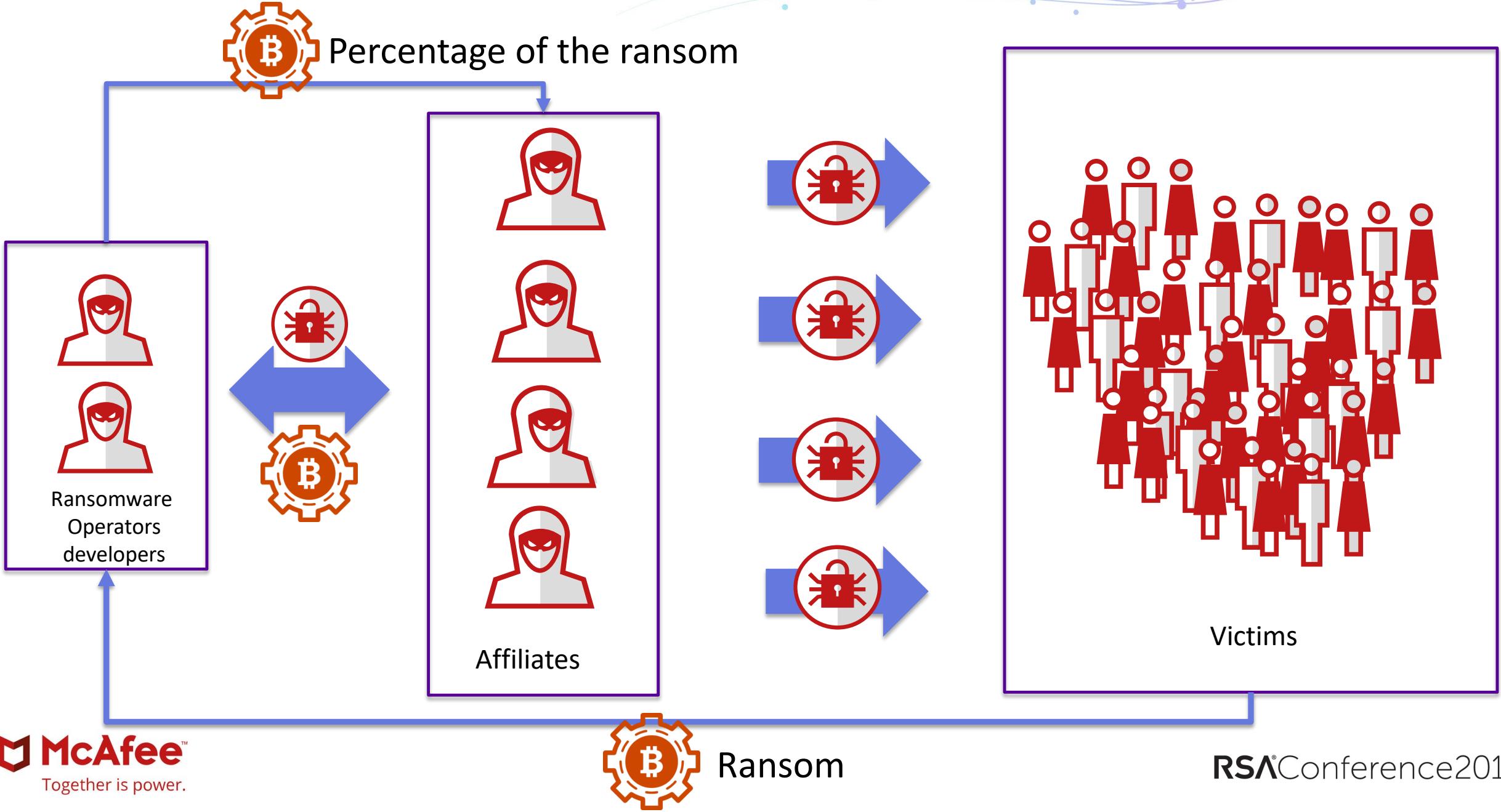
байт

Группа: По Сообщений Регистрации Пользовате

мотров: 25 691

A new exploit kit called Fallout is being used to distribute the GandCrab ransomware, malware downloading Trojans, and other potentially unwanted programs (PUPs).

Rise : Ransomware-as-a-Service (RaaS) Model



Gandcrab

09/27/2018 6:16 PM

Sent # 128



No More Ransom



Group: Seller

Messages: 279

Registration: 12/18/2017

User No: 84 324

Activity: Virology

Reputation: 52

(6% is good)



Despite all the storms and storms, our crab steadfastly and proudly walks like a cruiser along the fairway.

Undoubtedly, I would like to thank you, dear adverts. It is your job that helps us go forward, look for unique solutions and be the flagship in our niche.

Our monthly income with you is more than 1 million dollars. And this figure will constantly grow. We invest most of our revenue into development — new exploits, new methods, integration with other services, and so on.

When we updated the crab for version 4, we thought that this would be the most global update of its entire existence and the coming months. But no. I dare to assure you that the new update is comparable in scale to the 4th version, and somewhere even surpasses.

I present you the 5 version of GandCrab.

What's new?

1. Added a PowerShell script builder in admin panel. Many people appreciate him because he allows him to pass where even the most top-notch LoadPE of crypts passes, and the ordinary one cannot even crawl to a cannon shot.

The PowerShell script allows you to pass antivirus protection like butter, while not leaving traces in the system. Thus, everyone can now independently build and use.

How to prepare a crab?



Breaking GandCrab's shell

Pulling it apart, building dection

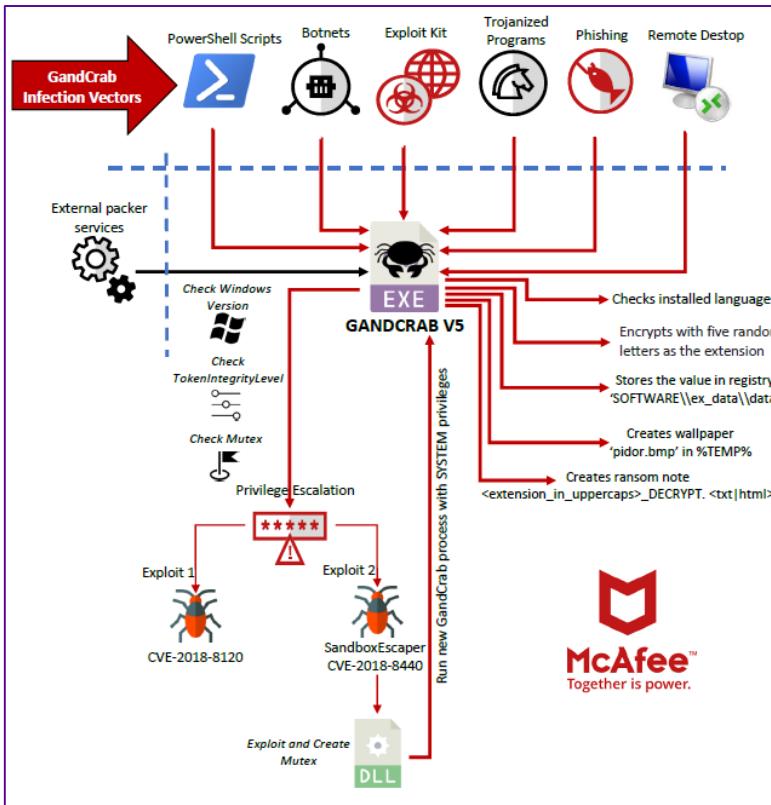
```

xor    eax, eax
mov    [ebp-1BCh], ax
push   0
lea    eax, [ebp-2Ch]
push   eax
lea    eax, [ebp-260h]
push   eax
push   0
push   0
push   dword ptr [ebp-274h]
push   0
push   0
lea    eax, [ebp-104h]
push   eax
lea    eax, [ebp-254h]
push   eax
call   ds:StartXpsPrintJob
mov    [ebp-264h], eax
cmp    dword ptr [ebp-2Ch], 0
jz    short loc_4085A7
mov    eax, [ebp-2Ch]
mov    eax, [eax]
push   dword ptr [ebp-2Ch]
call   dword ptr [eax+14h]

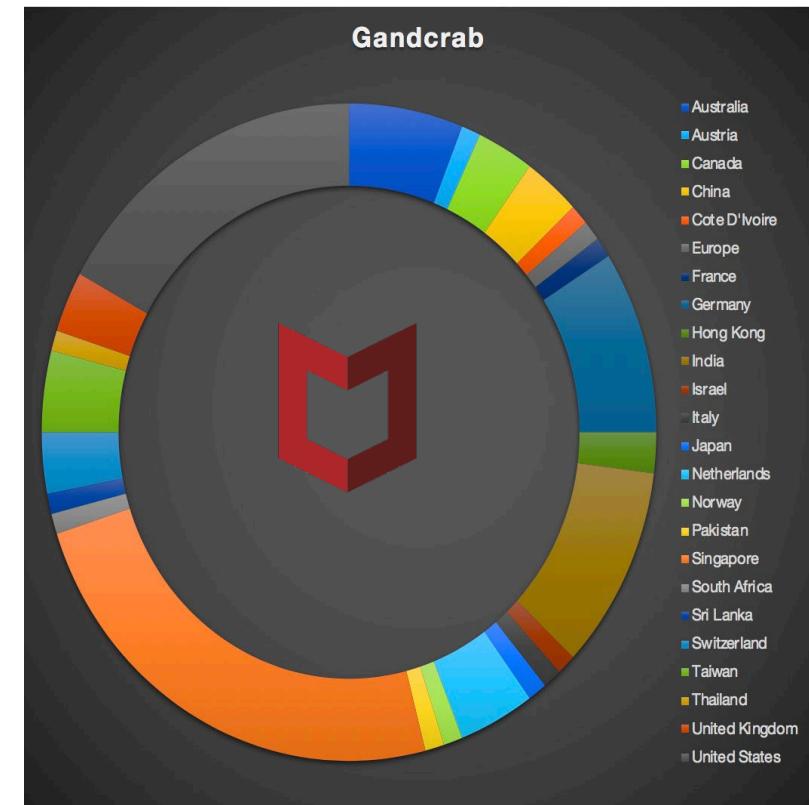
loc_4085A7:           ; CODE XREF: .text:0040859A↑j
call   ds:CoUninitialize
2710h
push   dword ptr [ebp-268h]
call   ds:WaitForSingleObject
cmp    dword ptr [ebp-264h], 0
jl    short loc_4085CC
xor   eax, eax
inc   eax
jmp   short loc_4085CE

```

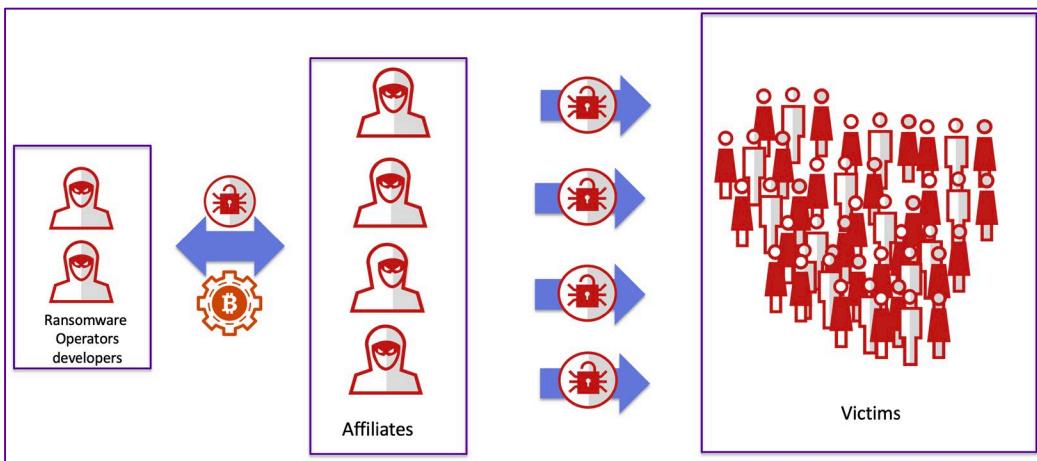
Understanding the details



Finding victims



Accounting is crucial for successful RaaS criminals



The Big Picture

- Hunting for Samples
 - Yara rules
 - Custom software
 - More than 280 samples
 - Hunting Detections
 - Building an overview

D	VERSION	ID	Sub_ID	HASH
92-06-19	VERSION: 5.04	140	SUBID: 720	8ec87fd3ea777fa8d5160dc957e6683e
92-06-19	VERSION: 5.04	140	SUBID: 763	9916e107b3d501c60d4baaf1b8f8a77a
11-07-03	VERSION: 4.3	163	SUBID: 535	03915be56034b6ad7f66b5fce1974f5e
11-07-03	VERSION: 4.3	163	SUBID: 535	5abcf4fea45e090ecd476cb5a56dfabc
18-06-29	VERSION: 4.0	117	SUBID: 397	8d604e3c567aab3c8cfa2d2c424c09c4
18-06-30	VERSION: 4.0	9	SUBID: 9	cbdb4aebb984096ee54c9eb2b1c128c
18-06-30	VERSION: 4.0	15	SUBID: 15	9be5102484d60f074499a8fd4403819c
18-06-30	VERSION: 4.0	15	SUBID: 15	77a7573a20dbf141a0ff1e5fade2eae0
18-07-03	VERSION: 4.0	41	SUBID: 62	19aa2a0f61f8b928b44de28d16f31174
18-07-03	VERSION: 4.1	9	SUBID: 9	946aa4b8273be8d4984e14d6c8c9d3b4
18-07-03	VERSION: 4.1	15	SUBID: 15	86613ae664b74c3a464f473408352635
18-07-03	VERSION: 4.1	44	SUBID: 83	3eed6f11720e53756db16de1b9a8d561
18-07-03	VERSION: 4.1	106	SUBID: 363	b6d06a87b35d15a1b3d9d76aced96f4e
18-07-03	VERSION: 4.1	114	SUBID: 383	7fd94b59280d80bcfd1b3970c4189ed
18-07-04	VERSION: 4.1	15	SUBID: 15	fd602a6ae269d8fbcb32b2c996678825b7
18-07-04	VERSION: 4.1	95	SUBID: 331	2212fac7fcded7f06042d0a0ca67898f
18-07-04	VERSION: 4.1	100	SUBID: 411	903f8718a1c3c12042fc44bac6a4c786
18-07-04	VERSION: 4.1	106	SUBID: 363	c24b3cf9336e7e994625d223fa7b5f4f
18-07-04	VERSION: 4.1	122	SUBID: 403	340117038ae2ef8d07c90c614d652934
18-07-05	VERSION: 4.1	110	SUBID: 374	9a680a7ff23746d92f4bb274c50be4a5
18-07-05	VERSION: 4.1.1	41	SUBID: 62	24fdd71ded0b9ffcefe3387002f7d361
18-07-05	VERSION: 4.1.1	73	SUBID: 414	ef50f5c2d6d8d10d8adc1efb840518d0
18-07-05	VERSION: 4.1.1	99	SUBID: 386	cce23a33a5a78b24ef7f5ced7d715d95
18-07-05	VERSION: 4.1.1	99	SUBID: 386	f876735f6d4f076dfb148c63c4ba5a3a
18-07-05	VERSION: 4.1.1	99	SUBID: 386	9b785e93d9ce42f6213d2c2a1ecc8293
18-07-05	VERSION: 4.1.1	99	SUBID: 417	c6b0fbf5190d3850b212c53e6ed56886
18-07-05	VERSION: 4.1.1	99	SUBID: 417	9c973702f8b40793c3ab60329dad7263
18-07-05	VERSION: 4.1.1	99	SUBID: 417	62fd133df8be543900aab64b707896b
18-07-05	VERSION: 4.1.1	124	SUBID: 413	a74c335c0ee5958929b99cb14726cd9a
18-07-05	VERSION: 4.1.1	128	SUBID: 423	e8e19525aa73d1714f15552d166aaa84
18-07-06	VERSION: 4.1.1	111	SUBID: 375	6b8872624f0427deaf8df292038e657a
18-07-13	VERSION: 4.1.2	41	SUBID: 62	75f215c1f086c47ee45392bd188909d0
18-07-13	VERSION: 4.1.2	57	SUBID: 133	0301296543c91492d49847ae636857a4
18-07-13	VERSION: 4.1.2	57	SUBID: 133	2aad5ce883a44154e7d7a9d982bb286c
18-07-13	VERSION: 4.1.3	57	SUBID: 133	3cef3301e48135dc3159181aa500bfe8
18-07-19	VERSION: 4.1.2	15	SUBID: 15	5c3bed3feaea533d2eb537850aa7079c
18-07-19	VERSION: 4.1.2	15	SUBID: 15	b8381b2b78d8e4088aca4f3c1535fea2
18-07-19	VERSION: 4.1.2	41	SUBID: 62	2d617c60478949d900cf37d3dfaf527a
18-07-19	VERSION: 4.1.2	79	SUBID: 250	9ec04ede383aa5a6774696a361d515b
18-07-19	VERSION: 4.2	41	SUBID: 438	2f09d9e81aa3c7ff0437625f976510ca
18-07-19	VERSION: 4.2	41	SUBID: 62	38a803baf56ec45e8b7db3ce610afac2
18-07-19	VERSION: 4.2	79	SUBID: 250	0b216cdb07d901c41514a7baabfb0f55
18-07-19	VERSION: 4.2	95	SUBID: 332	0d97b152305de1324901dbebe644506
18-07-19	VERSION: 4.2	99	SUBID: 448	2c79b1c6565616109cd38bd13e1b6019
18-07-19	VERSION: 4.2	99	SUBID: 448	4893880bcc579d21085eacea2f6d2b8e
18-07-19	VERSION: 4.2	131	SUBID: 432	9f59740a5d45cf545e2fd591b9ba0428
18-07-19	VERSION: 4.2	136	SUBID: 443	3b74163ebab14e3736424a4d83077bf7
18-07-21	VERSION: 4.2.1	126	SUBID: 152	5f1620416207265666860414_01_000000

Connecting the dots..

From samples to affiliates to victims

D	VERSION	ID	Sub_ID	HASH
1992-06-19	VERSION: 5.04	140	SUBID: 720	8ec87fd3ea777fa8d5160dc957e6683e
1992-06-19	VERSION: 5.04	140	SUBID: 763	9916e107b3d501c60d4baaf1b8f8a77a
2011-07-03	VERSION: 4.3	163	SUBID: 535	03915be56034b6ad7f66b5fce1974f5e
2011-07-03	VERSION: 4.3	163	SUBID: 535	5abc74fea45e090ecd76cb5a56dafb
2018-06-29	VERSION: 4.0	117	SUBID: 397	8d604e3c567aab3c8cfa2d2c424c09c4
2018-06-30	VERSION: 4.0	9	SUBID: 9	cbdb4eabb984096ee54c9eb2b1c128c
2018-06-30	VERSION: 4.0	15	SUBID: 15	9be5102484d60f074499a8fd4403819c
2018-06-30	VERSION: 4.0	15	SUBID: 15	77a7573a20dbf141a0ff1e5fade2eae0
2018-06-30	VERSION: 4.0	41	SUBID: 62	19aa2a0f61f8b928b44de28d16f31174
2018-07-03	VERSION: 4.1	9	SUBID: 9	946aa4ab273be8d4984e14d6c89d3b4
2018-07-03	VERSION: 4.1	15	SUBID: 15	86613ae664b74c3a464f473408352635
2018-07-03	VERSION: 4.1	44	SUBID: 83	3eed6f11720e53756d16de1b9a8d561
2018-07-03	VERSION: 4.1	106	SUBID: 363	b6d06a87b35d15a1b3d9d76a6d96f4e
2018-07-03	VERSION: 4.1	114	SUBID: 383	7fd94b59280d80bcfd1b3970c4189ed
2018-07-04	VERSION: 4.1	15	SUBID: 15	fd602a6ae269d8fbcb32c996678825b7
2018-07-04	VERSION: 4.1	95	SUBID: 331	2212fac7fcded7f06042d0a0ca67898f
2018-07-04	VERSION: 4.1	100	SUBID: 411	903f8718a1c3c12042fc44bac6a4c786
2018-07-04	VERSION: 4.1	106	SUBID: 363	c24b3cf9336e7e994625d223fa7b5f4f
2018-07-04	VERSION: 4.1	122	SUBID: 403	340117038ae2ef8d07c90c614d652934
2018-07-05	VERSION: 4.1	110	SUBID: 374	9a680a7f2374d92f4bb274c50be4a5
2018-07-05	VERSION: 4.1.1	41	SUBID: 62	24ffd71ded0b9ffccfe3387002f7d361
2018-07-05	VERSION: 4.1.1	73	SUBID: 414	ef50f5c2d6d8d10d8ad1c1efb4a0518d0
2018-07-05	VERSION: 4.1.1	99	SUBID: 386	cce23a33a5a78b24ef7f5ced7d715d95
2018-07-05	VERSION: 4.1.1	99	SUBID: 386	f876735f6d4f076dfb148c63c4ba5a3a
2018-07-05	VERSION: 4.1.1	99	SUBID: 386	9b785e93d9ce42f6213d2c2a1ecc8293
2018-07-05	VERSION: 4.1.1	99	SUBID: 417	c6b0fbf5190d3850b212c53e6ed56886
2018-07-05	VERSION: 4.1.1	99	SUBID: 417	9c973702ff8b40793c3ab60329dad7263
2018-07-05	VERSION: 4.1.1	99	SUBID: 417	62fd133df8be543900aab64b707896b
2018-07-05	VERSION: 4.1.1	124	SUBID: 413	a74c335c0ee5958929b99cb14726cd9a
2018-07-05	VERSION: 4.1.1	128	SUBID: 423	e8e19525aa73d1714f15552d166aaa84
2018-07-06	VERSION: 4.1.1	111	SUBID: 375	6b8872624f0427deaf8df292038e657a
2018-07-13	VERSION: 4.1.2	41	SUBID: 62	75f215c1f086c47ee45392bd188909d0
2018-07-13	VERSION: 4.1.2	57	SUBID: 133	0301296543c91492d49847ae636857a4
2018-07-13	VERSION: 4.1.2	57	SUBID: 133	2aad5ce883a44154e7d7a9d982bb286c
2018-07-13	VERSION: 4.1.3	57	SUBID: 133	3cef3301e48135dc3159181aa500bf8
2018-07-19	VERSION: 4.1.2	15	SUBID: 15	5c3bed3feaea533d2eb537850aa7079c
2018-07-19	VERSION: 4.1.2	15	SUBID: 15	b8381b2b78d8e4088aca4f3c1535fea2
2018-07-19	VERSION: 4.1.2	41	SUBID: 62	2d617c60478949d900cf37d3dfa527a
2018-07-19	VERSION: 4.1.2	79	SUBID: 250	9ec04ede383aa5a6774696a361d515b
2018-07-19	VERSION: 4.2	41	SUBID: 438	2f09d9e81aa3c7ff0437625f976510ca
2018-07-19	VERSION: 4.2	41	SUBID: 62	38a803baf56ec45e8b7db3ce610fac2
2018-07-19	VERSION: 4.2	79	SUBID: 250	0b216cdb07d901c41514a7baabfb055
2018-07-19	VERSION: 4.2	95	SUBID: 332	0d97b152305de1324901dbebe644506
2018-07-19	VERSION: 4.2	99	SUBID: 448	2c79b1c6565616109cd38bd13e1b6019
2018-07-19	VERSION: 4.2	99	SUBID: 448	4893880bce579d21085aceaa2f6d2b8e
2018-07-19	VERSION: 4.2	131	SUBID: 432	9f59740a5d45cf545e2fd591b9ba0428
2018-07-19	VERSION: 4.2	136	SUBID: 443	3b74163ebab14e3736424a4d83077bf7
2018-07-21	VERSION: 4.2.1	128	SUBID: 452	45120a1c37836c6c0244d6c018a06c2



Fighting back,

Private sector and Law Enforcement together

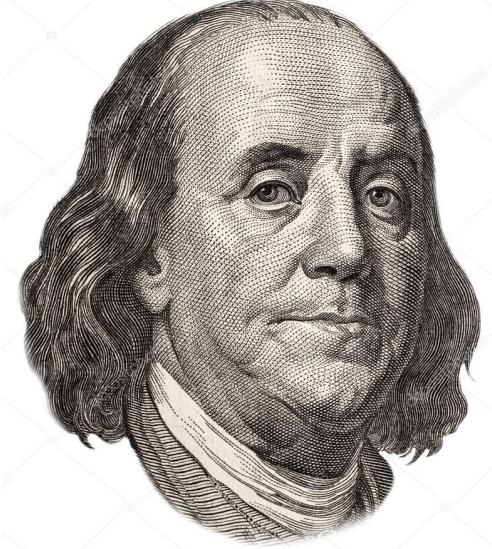
- Public-private initiative
- Nr.1 portal for decryption tools
- Thousands computers unlocked
- More than 22 million USD saved



Prevention Tips

"An ounce of prevention is worth a pound of cure"

- Back-up! Back-up! Back-up!
- Use robust Endpoint security software
- Network segmenting
- Robust identity management
- Keep all the software on your computer up to date
- Show file extensions
- Consider setting up a software restriction Policy (SRP)



Mitigation Tips

- **Don't turn off or reboot the computer**
- **Disconnect it immediately from the internet or other network connections, when infected**
- **Create a memory dump**
- **DO NOT delete any files (inc. Ransom notes)**
- **Take pictures for evidence**
- **Make copy of the encrypted drive**
- **Try to recover files with forensic tools like PhotoRec**

- **Don't pay, but check NoMoreRansom.org for a possible decryptor**
- **If you decide to pay except the risk of losing everything and seek professional advice**

Apply What You Have Learned Today

- After this talk you should have:
 - A better understanding of the Ransomware threat landscape
 - Identify the different types of Ransomware
- Next week you should:
 - Identify your Ransomware security posture
- In the first three months you should:
 - Set-up a plan and to roll-out the necessary prevention methods
 - Develop a ransomware mitigation strategy

Key take-aways

- Back-ups
- Don't pay

RSA® Conference 2019

Thank you!!



@Raj_Samani



@john_fokker