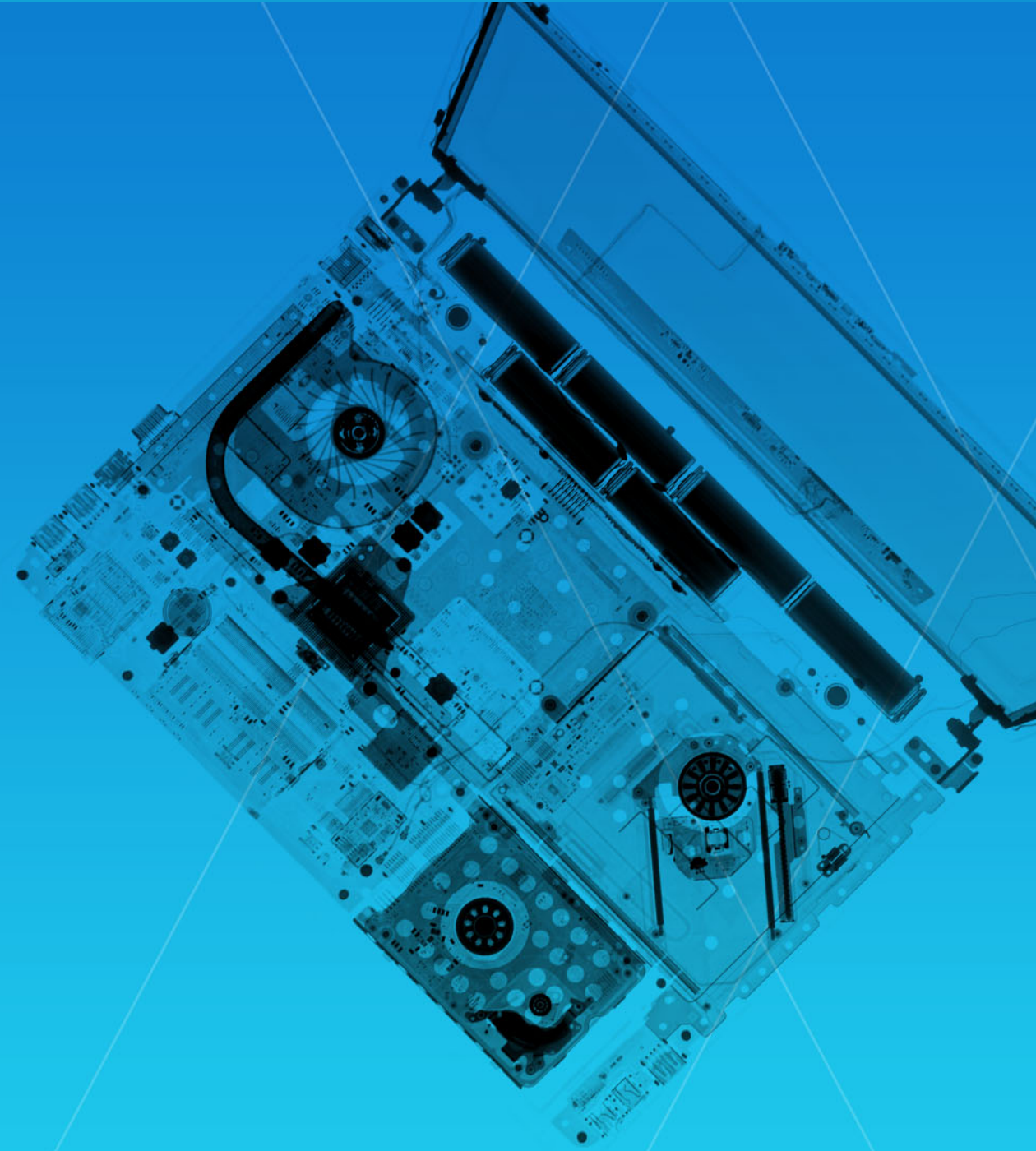




The Evolution of GandCrab Ransomware

Tamas Boczan

@tamas_boczan
Sr. Threat Analyst



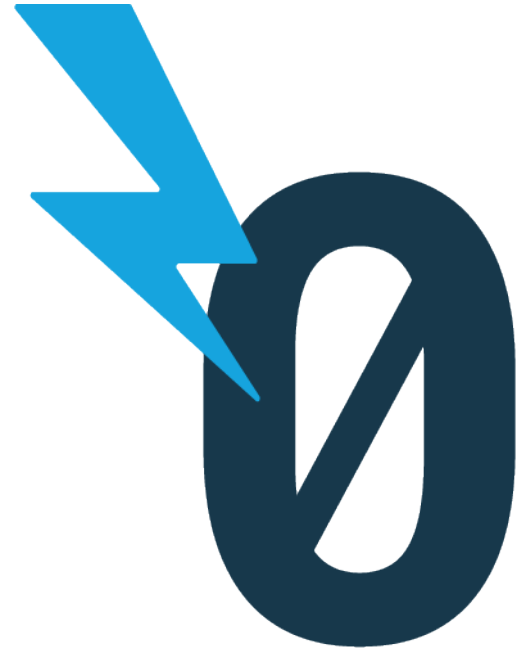
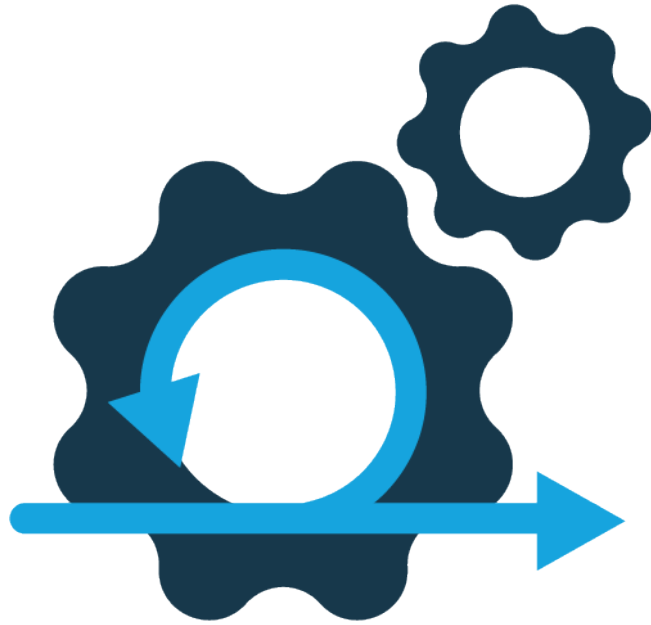
Why?



Why?



Why?



GandCrab  27.09.2018, 18:16



No More Ransom
■■■■■

Группа: [Seller](#)
Сообщений: 279
Регистрация: 18.12.2017
Пользователь №: 84 324
Деятельность: [вирусология](#)

Репутация: 52
(6% - хорошо)



**GandCrab v5
ransomware**

Panel for Affiliates



Dashboard

Ransoms list

Support

Transactions

Options

Administrator

2018-02-22 00:12:55
1 DASH = 678.461 \$

GandCrab (v2.1r)
All rights reserved © 2018

Ransoms list

Home / Ransoms list

Ransoms list (3662)

Countries: Countries
Advert: ww
HWID: HWID
Registration: Registration
Decrypt price: Decrypt price

PC Key (Ru): PC Key (Ru)
Test file: Test file
Status: Status

Filter Reset

Country	IP address	Owner	HWID	Decrypt price / Discount	Registration	Encrypt datetime (last)	OS	AV	HDD	Views	Status
	46.154	ww	3989	800 /	2018-02-21 21:53:54		Windows 7 Ultimate (x64 bit)		C D	0	In processing
	85.103	ww	6ad6	800 /	2018-02-21 21:52:10		Windows 7 Ultimate (x64 bit)		C D	0	In processing
	88.244	ww	8a91	800 /	2018-02-21 21:43:08	2018-02-21 22:30:44	Windows 8.1 Connected Sin (x86 bit)	MsMpEng.exe	C	0	Encrypted
	46.155	ww	fce1b	800 /	2018-02-21 21:42:41		Windows 7 Home Basic (x64 bit)		C F	0	In processing
	176.42	ww	573fe	800 /	2018-02-21 21:41:18	2018-02-21 22:13:14	Windows 7 Ultimate (x64 bit)		C D	0	Encrypted
	95.12.1	ww	e9b2	800 /	2018-02-21 21:39:48		Windows 7 Ultimate (x64 bit)		C D	0	In processing
	95.5.9.1	ww	a363	800 /	2018-02-21 21:32:45	2018-02-21 21:42:48	Windows 7 Home Premium (x86 bit)		C D	0	Encrypted
		ww	ee4d	800 /	2018-02-21 21:30:59		Windows 7 Professional (x86 bit)	etrn.exe	C D	0	In processing
	78.168	ww	ed6f	800 /	2018-02-21 21:30:07		Windows 8.1 Pro (x64 bit)	etrn.exe,MsMpEng.exe	C D	0	In processing
	176.88	ww	b4cd	800 /	2018-02-21 21:28:22		Windows 7 Ultimate (x64 bit)	etrn.exe	C	0	In processing
	88.233	ww	91d4	800 /	2018-02-21 21:27:12		Windows 8 Single Language (x64 bit)	MsMpEng.exe	C D	0	In processing

- Email attachments
 - Javascript
 - Doc
 - Encrypted doc
- Drive-by download



Delivery: RDP, Exploits



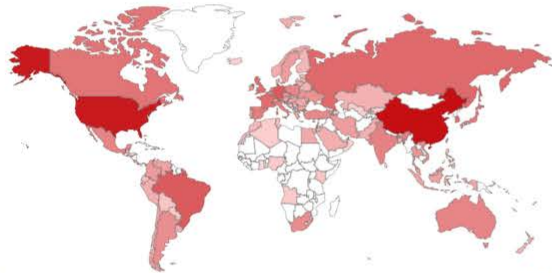
SHODAN Remote desktop [Explore](#) [Developer Pricing](#) [Enterprise Access](#) [Contact](#)

[Exploits](#) [Maps](#) [Images](#)

TOTAL RESULTS

2,558,684

TOP COUNTRIES



China	674,703
United States	542,059
Germany	114,138
Brazil	112,129
Russian Federation	72,462

TOP SERVICES

RDP	2,524,117
RDP (3388)	33,904
SMB	104

140.120.31.200

www.ee.nchu.edu.tw

National Chung Hsing University

Added on 2018-11-10 20:15:08 GMT

Taiwan, Taichung

[Details](#)

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x

132.232.22.150

Tencent cloud computing

Added on 2018-11-10 20:12:05 GMT

China

[Details](#)

self-signed

SSL Certificate

Remote

Issued By:

\x03\x

- Common Name:

Issued To:

- Common Name:

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters

Fingerprint: RFC2409/Oakley Group

2

18.222.229.92



Data collection

- System Info
- External IP
- AV?



Data collection

- System Info
- External IP
- AV?



Connect Home

- nslookup



Data collection

- System Info
- External IP
- AV?



Connect Home

- nslookup



Preparation

- Kill Processes



Data collection

- System Info
- External IP
- AV?



Connect Home

- nslookup



Preparation

- Kill Processes



Encryption

- AES
- *.GDCB



Data collection

- System Info
- External IP
- AV?



Connect Home

- nslookup



Preparation

- Kill Processes



Encryption

- AES
- *.GDCB



Post-Infection

- Shadow Copies



Data collection

- System Info
- External IP
- AV?



Connect Home

- nslookup



Preparation

- Kill Processes



Encryption

- AES
- *.GDCB



Post-Infection

- Shadow Copies



Data collection

- System Info
- External IP
- AV?
- **Kernel-AV**



Connect Home

- nslookup



Preparation

- Kill Processes



Encryption

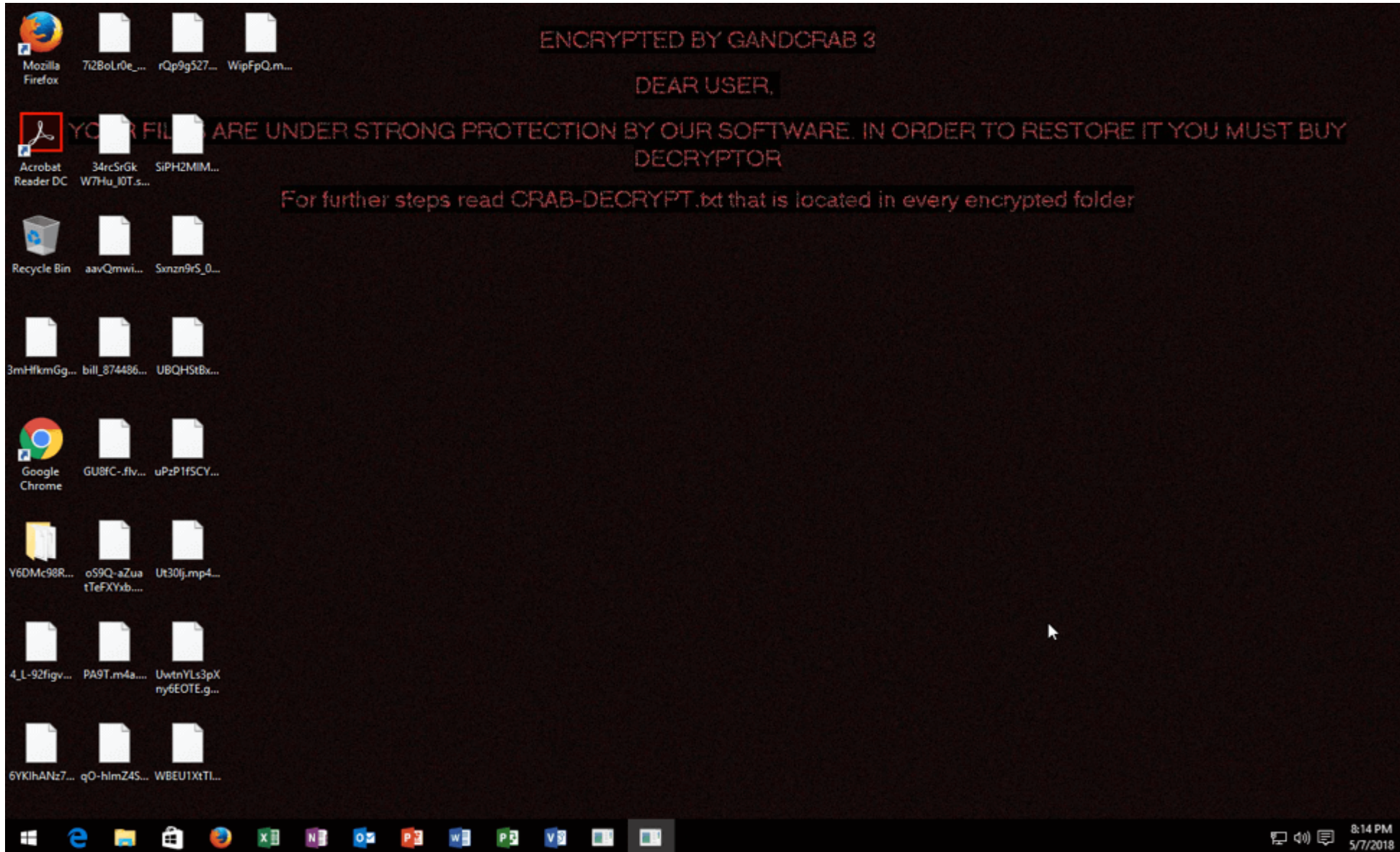
- AES
- ***.CRAB**



Post-Infection

- Shadow Copies

7 weeks later: v3



Post-Infection

- Shadow Copies
- **Wallpaper**



Data collection

- System Info
- ~~External IP~~
- AV?



Connect Home

- nslookup



Preparation

- Kill Processes



Encryption

- ~~AES~~
- Salsa
- *.KRAB
- SMB shares



Post-Infection

- Shadow Copies
- Wallpaper
- Self-removal



Data collection

- System Info
- AV?



Connect Home

- **WPress hacks**
- **URL generation**



Preparation

- Kill Processes



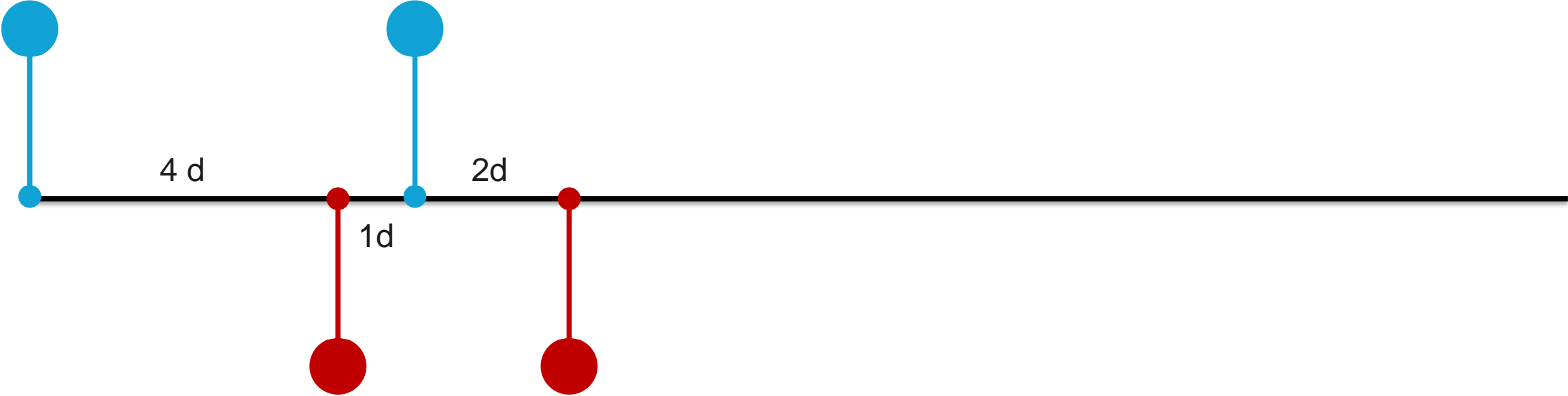
Encryption

- Salsa
- *.KRAB
- SMB shares



Post-Infection

- Shadow Copies
- Wallpaper
- Self-removal





- BSOD, no RCE
- Full disclosure, not used
- Why?
 - Retaliation
 - Overestimated impact
- Probably just fuzzed it



Data collection

- System Info
- AV?



Connect Home

- WPress hacks
- URL generation



Preparation

- Kill Processes
- **Escalate**



Encryption

- Salsa
- ***.{Random}**
- SMB shares



Post-Infection

- Shadow Copies
- Wallpaper
- Self-removal



Data collection

- System Info
- AV?



Connect Home

- WPress hacks
- URL generation



Preparation

- Kill Processes
- Escalate



Encryption

- Salsa
- *.{Random}
- SMB shares



Post-Infection

- Shadow Copies
- Wallpaper
- Self-removal

Gandcrab

(\ /) _ (\$ _ \$) _ (\ /)
●●●●●●



Seller

424 posts

Joined

12/18/17 (ID: 84324)

Activity

virology



We are leaving for a well-deserved retirement .



We personally earned more than **150 million** dollars per year.



For the year of working with us, people have earned more than **\$ 2 billion**

What We Learned: Developer's Profile

- > RaaS marketing skills
- Project organization:
 - > react quickly
 - < poor quality
- Exploit development capability:
 - > implement exploits based on POCs
 - > find simple exploit via fuzzing
 - < can't develop more complex RCE exploit
 - < can't guess impact of an exploit



The Evolution of GandCrab Ransomware

Tamas Boczan

@tamas_boczan
Sr. Threat Analyst

