# Κινυ

Trends in Hacker Business Models Lessons from Negotiating with Extortionists Winston Krone, Kivu Consulting

July 24, 2019

#### Automated Attacks

- No ability to negotiate
- Amounts low
- Decryption relatively easy

IMPORTANT Microsoft Internet Explorer	
3 test - 0 - 1 2 1 Death + Fourtes @ 3. 3 6 - 1 1 12 3	ALL YOUR
Copeoments and Setting(User/Desites)(ECRIPT_INSTRUCTIONS.tex)	Lois *
To help protect your security, bitamet Explorer has restricted this file from showing active content that could access your computer. Out here for options	×
WARNING we have encrypted your files with CryptoLocker viru	To recover data you need decryptor. To get the decryptor you should:
we have encrypted your mes with cryptococker virt	Send 1 test image or text file In the letter include your personal ID (let
our important files (including those on the network disks, USB, etc.): photos, videos, documents, etc. were encrypted with hyptoLocker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.	
aution: Removing of CryptoLocker will not restore access to your encrypted files.	
	After we send you instruction how to p We can decrypt one file in quality the et
Click here to pay for files recovery	
Frequently Asked Questions	Only net can de     Do not trust anyone
ane	Do not attempt to remove the pr
Start 🔄 Mickitan - Mons 👔 DECENTE JASTRUCT 🍙 Crystalader 🛛 😡 🤣	• Attempts to self-decrypting files
	<ul> <li>Decoders other users are not co</li> </ul>
🔲 HOW TO DECRYPT FILES.txt - Notepad 🚽 🗖 🔀	
File Edit Format View Help	10
þecoding Files 1 Bitcoin, tomorrow 2 Bitcoin 🛛 🔿	Diana in Bolt Brand
translation at the expense of Bitcoin	Phoenix ROM BIOS PLUS Version
1Nez7W9ashFL4BA7vHuA5aoaad9XtqHKCF	Copyright 1985-1988 Phoenix 1
Here are our recommendations: If you have no Bitcoin address register	Copyright 1990-2010 Dell Inc
https://blockchain.info/wallet	All Rights Reserved
pay at the Bitcoin address above	and a second second
after payment you will receive a program that	Rell Sustem Poursedan B210
automatically decrypts all your files	Dell System PowerEdge R210
mail support Satan-Stn@india.com or Satan- Stn@bitmessage.ch	www.dell.com
	Your hard drive is securely
	igaint.org with code
	Carry March 1997 - Carl & Party
	the same of the second s

#### Se YOUR FILES ARE ENCRYPTED!

#### IMPORTANT DATA HAS BEEN ENCRYPTED.

net. ok at the beginning of this document).

assign the price for decryption all files

ay for decrypt and after payment you will receive a decryptor and instructions idence that we have the decoder. Attention

crypt your files net

- gram or run the anti-virus tools
- will result in the loss of your data
- patible with your data, because each user's unique encryption key

1.10 1.3.4 Technologies Ltd.

encrypted. To buy password send an email to gem3370s

#### Automated Attacks

- Bragging rights
- Nuisance attacks

## **MKLIUKANG@INDIA.COM** ububurudub ububububujub olobah!"

#### Automated Attacks

- Business model of efficiency
- Self-policed by reviews

John		com>			
to me 💌					
	for your payment! for attachment is your e	mail:	com		
Google are	blocking 7zip now (I ca	an't attach file in email), downlo	bad link:		
https://ut					
	F all antyviruses and u all files to C:\ProgramD		dministrator (it's important) the	n load dma_private.key and	click "UNLOCK FILES" button.
	encrypted workstations of sure what to do see	s repeat process on every mac attached images.	hine.		
Regards,					
4 Attachme	ents				
	Open				
S = 9	Run as administrator	Construction of the second sec			
	Pin to Taskbar Pin to Start Menu	Support Statements			
	Remove from this list	The second secon			
	Properties			A	

- Size of ransom negates amount reduction negotiation
- Negotiate to get Decryption Assistance

to me 💌
and can ypu provide how much % of files you couldnt decrypt and what antivirus u r using on the server I am emailing the guyz who makes infection.
to attacker about 20% of files did not decrypt.
They are in C: directory in random folders.
Thank you for looking into it.
to me 💌
it looks like if antivirs block crypter crypter kill av and rerun and create a different password. If you can give me a bitcoin address i can send you 0.6 bitcoin which is %20 of the payment.

- Size of ransom negates amount reduction negotiation
- Negotiate to get Decryption Assistance



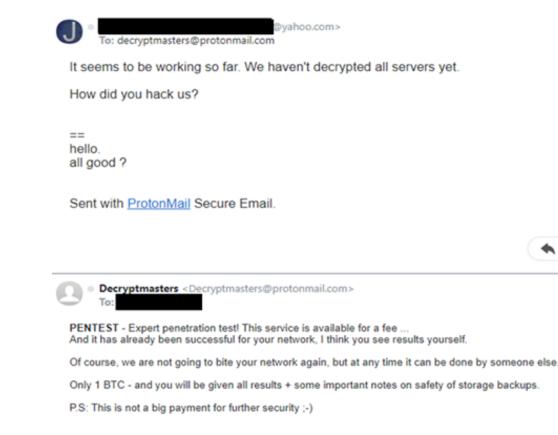
- Keep attacker focused, interested, sober
- 2017 2018 RaaS leads to amateur attackers

From:	
Sent:	
To:	
Subject: RE	: BTC
Dear	
it`s really v	ery strange! We must have Your keys! Absolutely!
But someth	ing wrong with information You gave.
1. What was use?	s the remote access (RDP) IP address? And which login name did You
-	ht button on the original encrypted file and choose Properties. See the date nd send it please.
Best regard	s!

ome 👻	tur bull yolu didhit if yolu cam i to my child and love m to steak house for
et i was waithing you to provide me a bilicos address. 4 hour but you didn't 7 you c ally send you money today i buy a samsung geleery lab 2 to my child and love solution mounted and tommy folloger year and shut and goes to steak house for ner so today i lost 1000 and 1 so money gees but allaf i can fir you is i can send	numbul you didnt if you can i to my child and lowe yo to steak house for
elly send you money today i boy a samsung galaxy tab 2 to my child and love solution mounted and tommy follger year and shot and goes to steak house for per so today i lost 1000 und 1 so money gees hut and under in the year is i can send	to my child and love to to steak house for
sphereo mesuritied and tommy folliger years and short and goes to steak house for new so follow i lost \$200 and 1 so money goes had what i can for you is i can send	es to offenale house for
	can for you is i can send you
other decryption key from your processor there is 43 server inteched and you r to	ver inflected and you r the 2

III All of your files are encrypted III To decrypt them send e-mail to this address: greg.philipson@aol.com. If we don't answer in 24h., send e-mail to this address: leeming.derick@aol.com If there is no response from our mail, you can install the Jabber client and write to us in support of waitheisenberg@xmpp.jp

- Keep attacker focused, interested, sober
- 2017 2018 RaaS leads to amateur attackers



Sent with ProtonMail Secure Email.

- RaaS attackers need us to provide technical assistance
- Incompetence biggest problem
- Attackers annoy RaaS Admin who revoke their licenses mid-attack
- Dark web forum searches for missing attackers

to me 💌
and can ypu provide how much % of files you couldnt decrypt and what antivirus u r using on the server I am emailing the guyz who makes infection.
to attacker about 20% of files did not decrypt.
They are in C: directory in random folders.
Thank you for looking into it.
to me 💌
it looks like if antivirs block crypter crypter kill av and rerun and create a different password. If you can give me a bitcoin address i can send you 0.6 bitcoin which is %20 of the payment.

#### My subscription was suspended, why?

Because you have infringed many times our TOE, for example: (a) by sending your unique RANION exe to online AVs; (b) by publishing our product on clearnet websites; (c) by flooding our mailbox with many junk emails without having purchased a package with "support"; etc.

#### Amateur Attackers

- Rarely hostile
- But when keys fail or the tool doesn't work, attackers can't troubleshoot

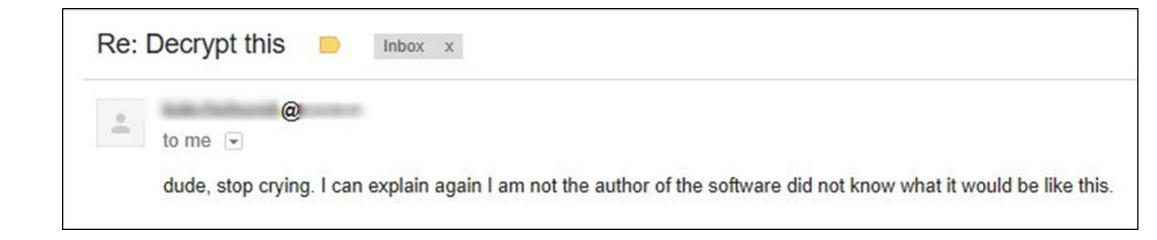
My supervisor says that you try to f 🄬 us when you ask passwords from

- 10.0.12.221 10.0.12.13

So he want 0.5 bitcoins more for this 2 servers

Please send 0.5 btc to the same address

My supervisor said not waste time with this case because you hold us for idiots and ask most critical servers including HYPER-V host with more then 10 VM



#### Amateur Attackers

- Rarely hostile
- Incompetence biggest problem

Time Played: 4 days 18 hours 34 minutes 39 seconds				
Please wait for decrypt files				
Upload File For Decryption				
Files Available To Decrypt: 0				
Your comments	Our Answer			
2017 I uploaded two files for decryption	Download two decrypted files: https://expirebox.com/download			
2017 Thank you. Do I pay this bitcoin address? 1HCB	/4b			
2017 Okay I just sent you payment for all affected PC's				

16:58 -- THESE GUYS TAKE BTC BUT DO NOT GIVE KEYS ! FRAUDS ! THESE GUYS TAKE BTC BUT DO NOT GIVE KEYS ! FRAUDS ! FRAUDS !THESE GUYS TAKE BTC BUT DO NOT GIVE KEYS ! FRAUDS !

### Ryuk

- 2018 Game Changer
- Unwilling to reduce demand
- Not motivated by building a brand
- Using APT tactics/ tools
- Can spend months doing reconnaissance so know network details of victim and their ability to pay large ransoms

@protonmail.com @protonmail.com



balance of shadow universe

### New Ryuk Operatives

- Starting Jan 2019
- New Ryuk groups willing to negotiate
- Less aware/ realistic about victim's ability to pay

To: diamana and a grotonmail.com>	Wed, Jun 12, 2019 at 6:24 AM
Thank you	
I do not have money for 48 bitcoin. Can I pay for only some of the computer [Quoted text hidden]	rs?
Reply-To:@protonmail.com To:@gmail.com>	Wed, Jun 12, 2019 at 6:58 AM
how much?	
@gmail.com> To:	Wed, Jun 12, 2019 at 7:00 AM
I can get the money together for 30 bitcoin today. If I have to get more it will	l take me like 5 or 6 days.
On Wed, Jun 12, 2019 at 6:58 AM <downnasimen@protonmail.com> wrote how much?</downnasimen@protonmail.com>	
@protonmail.com> Reply-To:@protonmail.com To@gmail.com>	Wed, Jun 12, 2019 at 7:30 AM
ok 30 btc	
@amail.com>	Mad lun 12 2010 at 7.40 MM

### Target\_Defray



#### Target\_Defray

From: @protonmail.com> - 🔒		month a	igo) ☆		
To:					
Show details	<b>Υ</b> ~ <b>Β</b> ~	• • •	*) «h	~	~
Sir thank you for working with us on price. We really appreciate it. We have discussed with management Do you accept our offer? If yes we will start getting bitcoins. Sent with <u>ProtonMail</u> Secure Email. Original Message On Saturday, 2019 6:21 PM, @protonmail.com> wrote:	nt and we are willi	ng to raise	price to \$5	50,000.	
SFrom @protonmail.com> ▼		121	/2019 (a	month a	4100
To:			2013 (a	monara	igo) ia
Show details	<b>▼</b> ~ ■~	• •	<ul><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li></ul>	*	~

As we said this amount (640000.00 USD, only 90K more than 550000.00 USD) was ultimately final and 100000.00 USD is a very good discount for a such grand firm. It is the best deal we can offer.



#### Winston Krone, Esq., Global Managing Director Kivu Europe

E: <u>wkrone@kivuconsulting.com</u>

San Francisco - New York - Washington, DC Denver – Toronto – Amsterdam - London www.kivuconsulting.com