

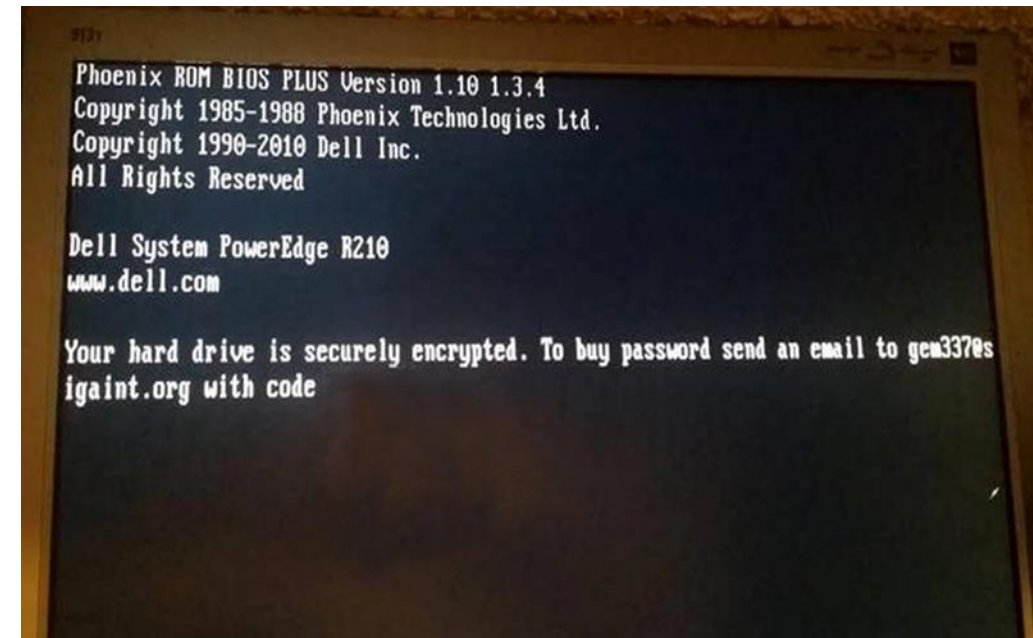
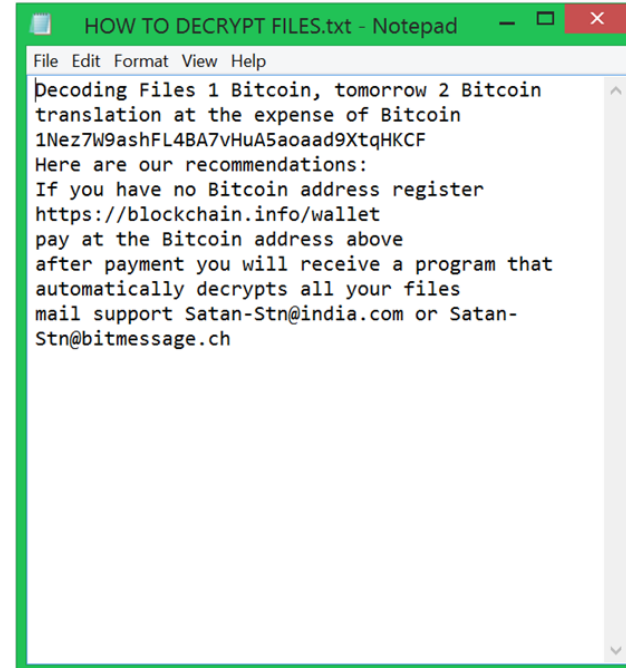


Trends in Hacker Business Models
Lessons from Negotiating with Extortionists
Winston Krone, Kivu Consulting

July 24, 2019

Automated Attacks

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



Automated Attacks

- Bragging rights
- Nuisance attacks

MKLIUKANG@INDIA.COM



Automated Attacks

- Business model of efficiency
- Self-policed by reviews

John [REDACTED].com>
to me [REDACTED]

Thank you for your payment!
Password for attachment is your email: [REDACTED].com

Google are blocking 7zip now (I can't attach file in email), download link:
[https://\[REDACTED\]](https://[REDACTED])

- 1.) Turn OFF all antyviruses and uninstall it.
- 2.) Extract all files to C:\ProgramData and run svchostd.exe as administrator (it's important) then load dma_private.key and click "UNLOCK FILES" button.

If you have encrypted workstations repeat process on every machine.
If you are not sure what to do see attached images.

Regards,
[REDACTED]

4 Attachments



The attachments include a Windows context menu for a file named 'S...', where the 'Run as administrator' option is highlighted with a red box. The other three attachments are screenshots of a red-themed software interface. Each screenshot shows a padlock icon in the top left corner and an 'UNLOCK FILES' button in the bottom right corner, with red arrows pointing to the button. The interface also contains various text fields and instructions.

Negotiate for Assistance

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

```
attacker [redacted] com>
to me [dropdown]
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.
...

investigator [redacted] com>
to attacker [redacted]
about 20% of files did not decrypt.
They are in C: directory in random folders.
Thank you for looking into it.
...

attacker [redacted] com>
to me [dropdown]
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.
```

Negotiate for Assistance

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

investigator [redacted] com>
to [redacted]
Hi. It won't allow me to decrypt all PC. An error pops up.

DP Decryptor
Decrypt all PC or Choose 1 file and decrypt it

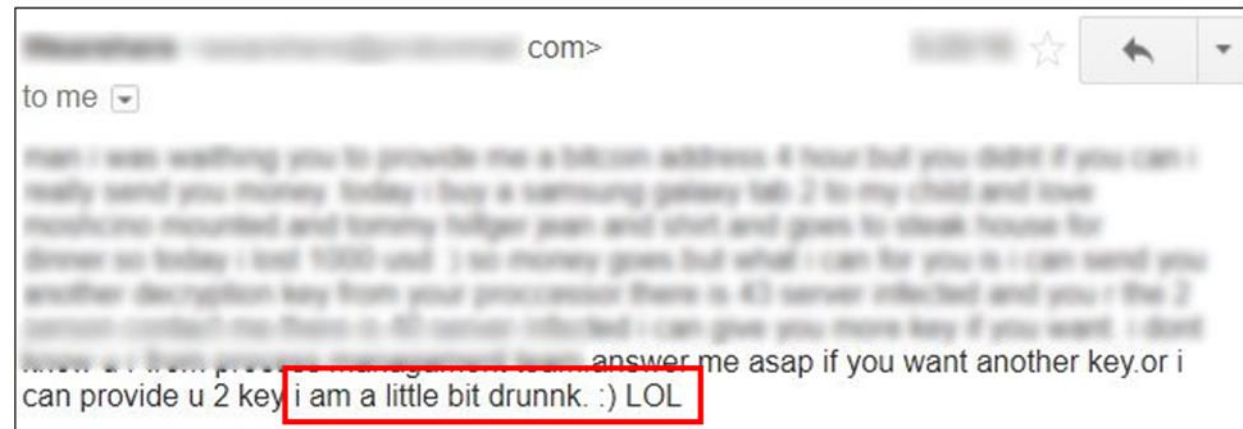
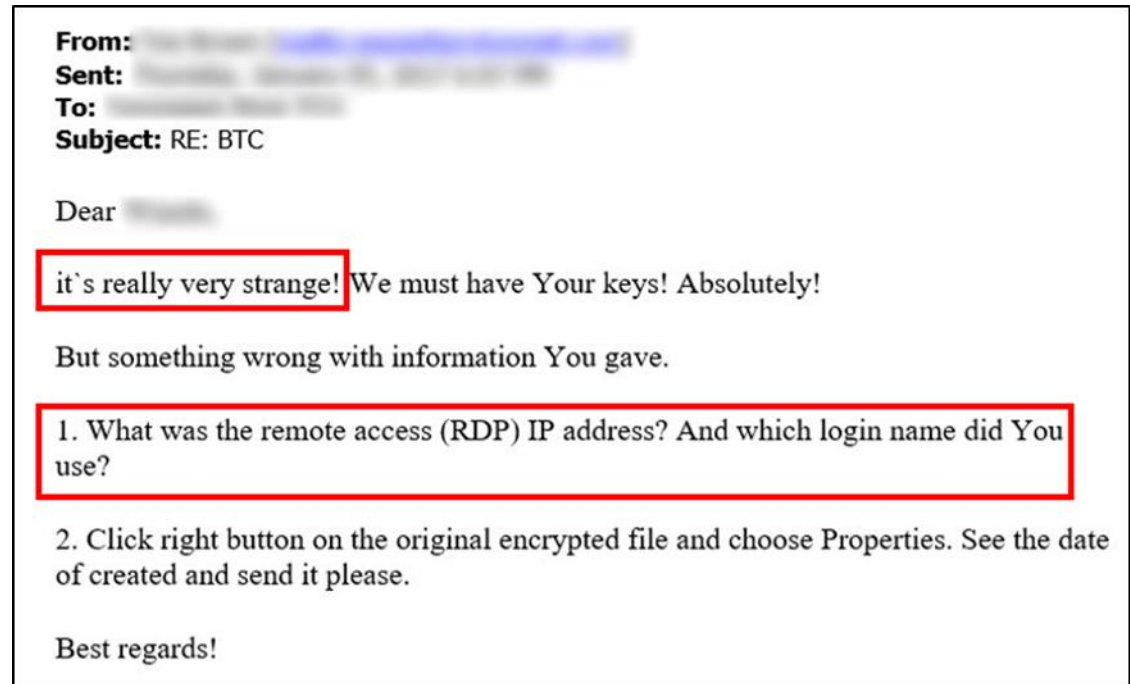
Access error: The key for decrypting a single file.
OK

attacker [redacted]
to me [redacted]
<https://www.sendspace.com> [redacted]

Fixed invalid key was.
Repeat all the same steps

Negotiate for Assistance


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



Negotiate for Assistance

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

!!! All of your files are encrypted !!!
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

 <[redacted]@yahoo.com>
To: decryptmasters@protonmail.com

It seems to be working so far. We haven't decrypted all servers yet.

How did you hack us?

==
hello.
all good ?

Sent with [ProtonMail](#) Secure Email.



 <Decryptmasters@protonmail.com>
To: [redacted]

PENTEST - Expert penetration test! This service is available for a fee ...
And it has already been successful for your network, I think you see results yourself.

Of course, we are not going to bite your network again, but at any time it can be done by someone else.

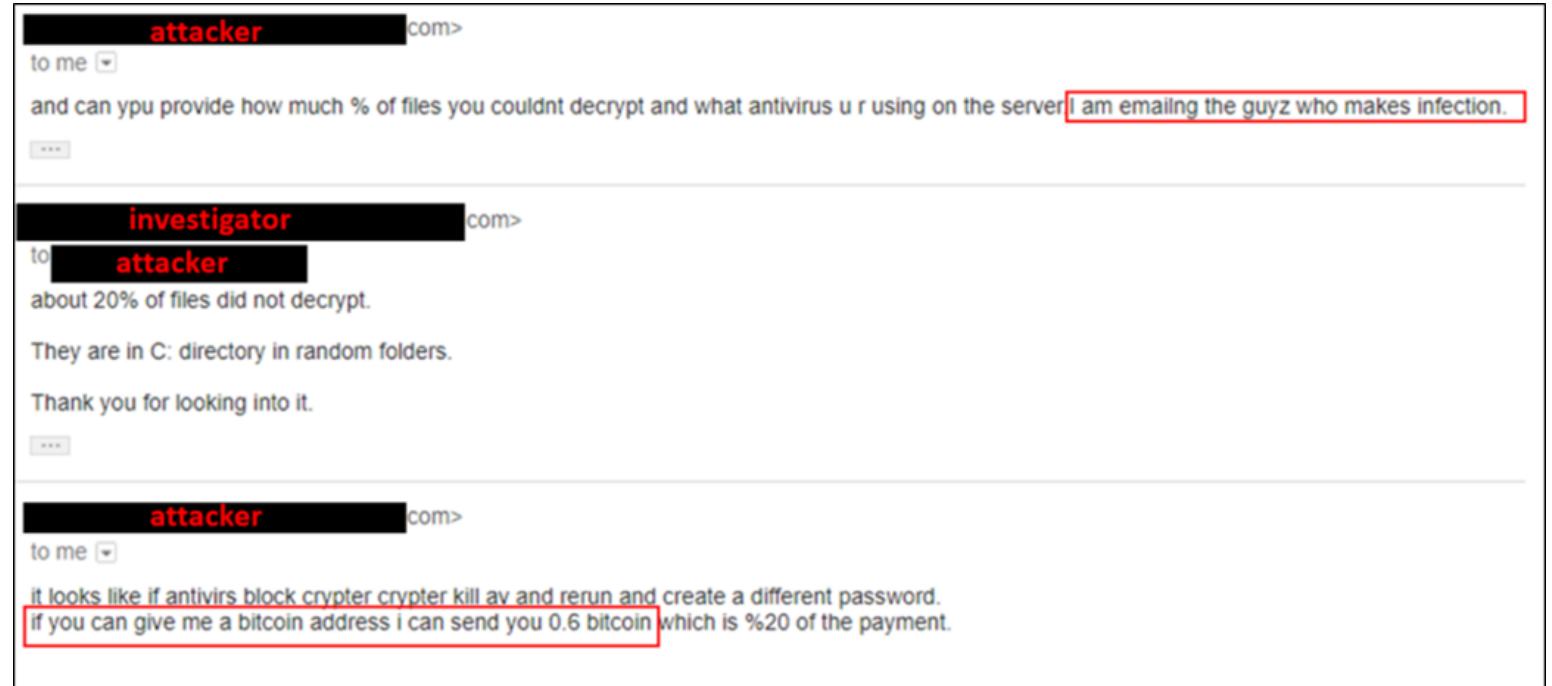
Only 1 BTC - and you will be given all results + some important notes on safety of storage backups.

P.S: This is not a big payment for further security ;-)

Sent with [ProtonMail](#) Secure Email.

Negotiate for Assistance

- 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



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  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

Re: Decrypt this 

Inbox x



 @ 

to me 

dude, stop crying. I can explain again I am not the author of the software did not know what it would be like this.

Amateur Attackers



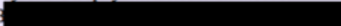


- Rarely hostile
- Incompetence biggest problem

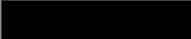
Time Played: 4 days 18 hours 34 minutes 39 seconds

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	
 2017 Thank you. Do I pay this bitcoin address? 1HCF 	Download two decrypted files: <a data-bbox="1753 491 2091 515" href="https://expirebox.com/download/4b ">https://expirebox.com/download/4b 
 2017 Okay I just sent you payment for all affected PC's	Yes

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

Ryuk

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

[REDACTED]@gmail.com> Wed, Jun 12, 2019 at 6:24 AM
To: [REDACTED]@protonmail.com

Thank you

I do not have money for 48 bitcoin. Can I pay for only some of the computers?

[Quoted text hidden]

[REDACTED]@protonmail.com> Wed, Jun 12, 2019 at 6:58 AM
Reply-To: [REDACTED]@protonmail.com
To: [REDACTED]@gmail.com>

how much?

[REDACTED]@gmail.com> Wed, Jun 12, 2019 at 7:00 AM
To: [REDACTED]@protonmail.com

I can get the money together for 30 bitcoin today. If I have to get more it will take me like 5 or 6 days.

On Wed, Jun 12, 2019 at 6:58 AM <downnasimen@protonmail.com> wrote:


| how much?

[REDACTED]@protonmail.com> Wed, Jun 12, 2019 at 7:30 AM
Reply-To: [REDACTED]@protonmail.com
To: [REDACTED]@gmail.com>








ok 30 btc

[REDACTED]@gmail.com> Wed, Jun 12, 2019 at 7:40 AM

Target_Defray

From: [REDACTED]@protonmail.com >  Sent [REDACTED] 2019 (a month ago) ☆


To: [REDACTED]

[Show details](#)       

We do not have bitcoins yet. We are still discussing with our team. Will you accept a lower price?

Sent with [ProtonMail](#) Secure Email.

----- Original Message -----
On Saturday, [REDACTED] 2019 3:16 PM, [REDACTED]@protonmail.com> wrote:




 From: [REDACTED]@protonmail.com >  [REDACTED] 2019 (a month ago) ☆

To: [REDACTED]

[Show details](#)       








We know who are you (74M+ assets, ~3k employees).
We offer you some discount if payment will happen fast (-40000.00 USD).
The minimum payment for the next 5 days is 700000.00 USD.
This is our final offer.

Target_Defray

From [REDACTED]@protonmail.com >  Sent [REDACTED] 2019 (a month ago) ☆

To: [REDACTED]

[Show details](#)

Sir thank you for working with us on price. We really appreciate it. We have discussed with management and we are willing to raise price to \$550,000. Do you accept our offer? If yes we will start getting bitcoins.

Sent with [ProtonMail](#) Secure Email.

----- Original Message -----

On Saturday [REDACTED] 2019 6:21 PM, [REDACTED]@protonmail.com> wrote:



From [REDACTED]@protonmail.com >  [REDACTED] 2019 (a month ago) ☆

To: [REDACTED]

[Show details](#)

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.

Questions?

Winston Krone, Esq., Global Managing Director

Kivu Europe

E: wkrone@kivuconsulting.com

San Francisco - New York - Washington, DC

Denver – Toronto – Amsterdam - London

www.kivuconsulting.com