

Negotiating With Cyber Criminals

Moty Cristal

**..no need to talk
about the obvious..**

Ransomware market soars 2,500% amid high-profile attacks, rise of cryptocurrencies

Published: Oct 11, 2017 9:00 a.m. ET



2019 will be the year of Ransomware Rising



A new business will fall victim to ransomware every 14 seconds in 2019 — and every 11 seconds by 2021. According to Cybersecurity Ventures predictions.



Over half of all SMBs are willing to pay a ransom to recover breached or stolen data.

55%

All SMBs

74%

Large SMBs

39%

39% Large SMBs say they would pay ransom at "almost any price"

**..but rather on what
we still don't know..!**

Levels of Cyber-extortion

- ✓ Malware (no negotiation..)
- ✓ Ransomware (..some negotiations..)
- ✓ **Cyber Extortion (..crisis negotiations..)**

Ransomware

Your computer has been infected!



Your documents, photos, databases and other important files encrypted



To decrypt your files you need to buy our special software - *r1s03p-Decryptor*



You can do it right now. Follow the instructions below. But remember that you do not have much time

r1s03p-Decryptor costs

You have **2 days, 07:08:58**

* If you do not pay on time, the price will be doubled

* Time ends on Jun 1, 02:35:03

Current price 5.7320014 BTC
≈ 50,000 USD

After time ends **11.4640028 BTC**
≈ 100,000 USD

Bitcoin address: 39DcSuSKqqS6gAmcTdU9cnni7bo1A6CKrwy

* Amount in BTC will be recalculated in 31 minutes with an actual rate.



MONEY

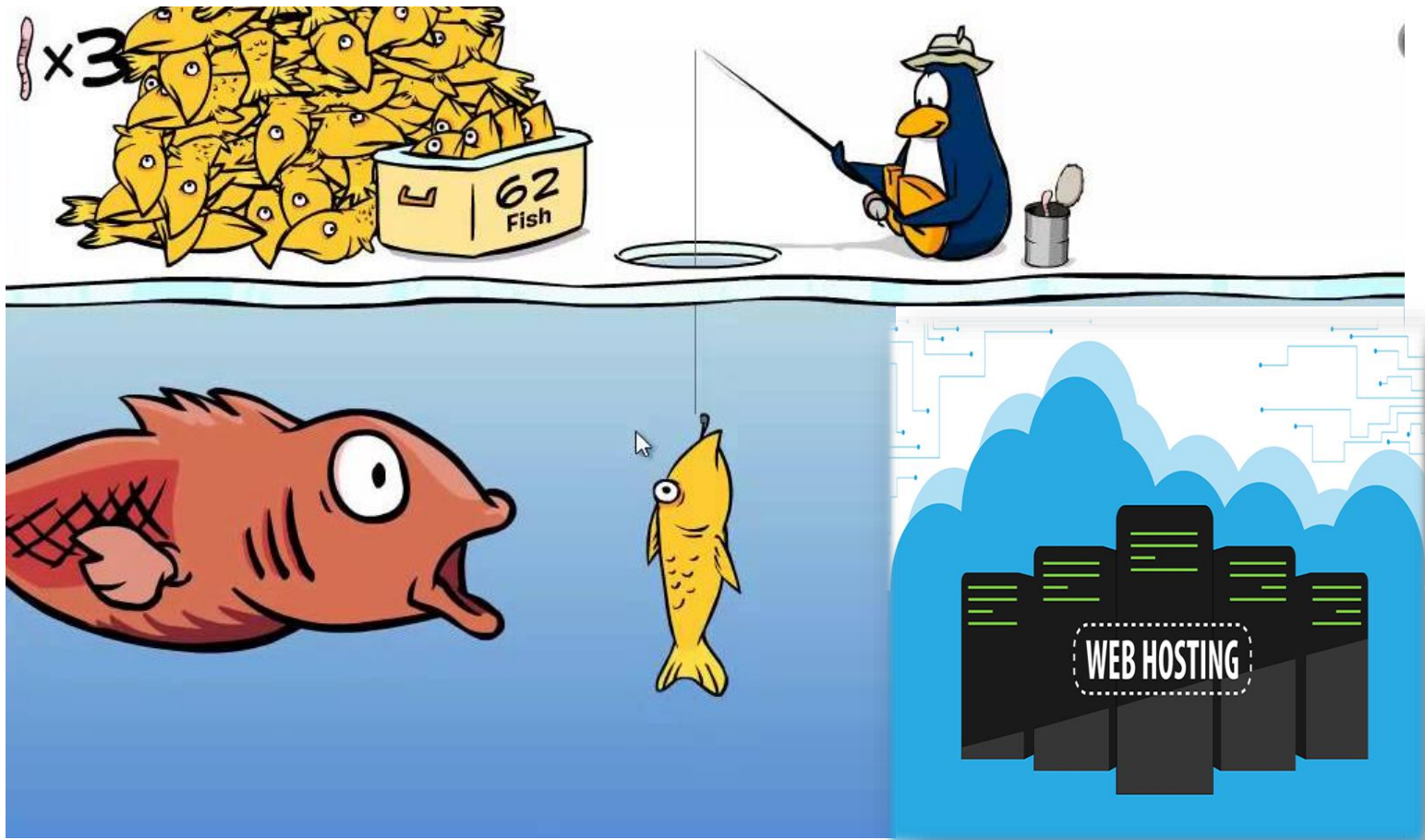
YES

NO

Logic of Simple Ransomware: Traffic



Complex Ransomware: Catch a Big Fish



Negotiating Ransomware: 3 Steps



Step 1: Call a professional to access backup.

Step 2: Call a professional to search for a key.

Step 3: Call a professional to negotiate.

Negotiating Ransomware: Available Keys?

NO MORE RANSOM!

★ English ▼

Crypto Sheriff

Ransomware: Q&A

Prevention Advice

Decryption Tools

Report a Crime

Partners

About the Project



New decryptor for **Pewcrypt** available, please click [here](#).

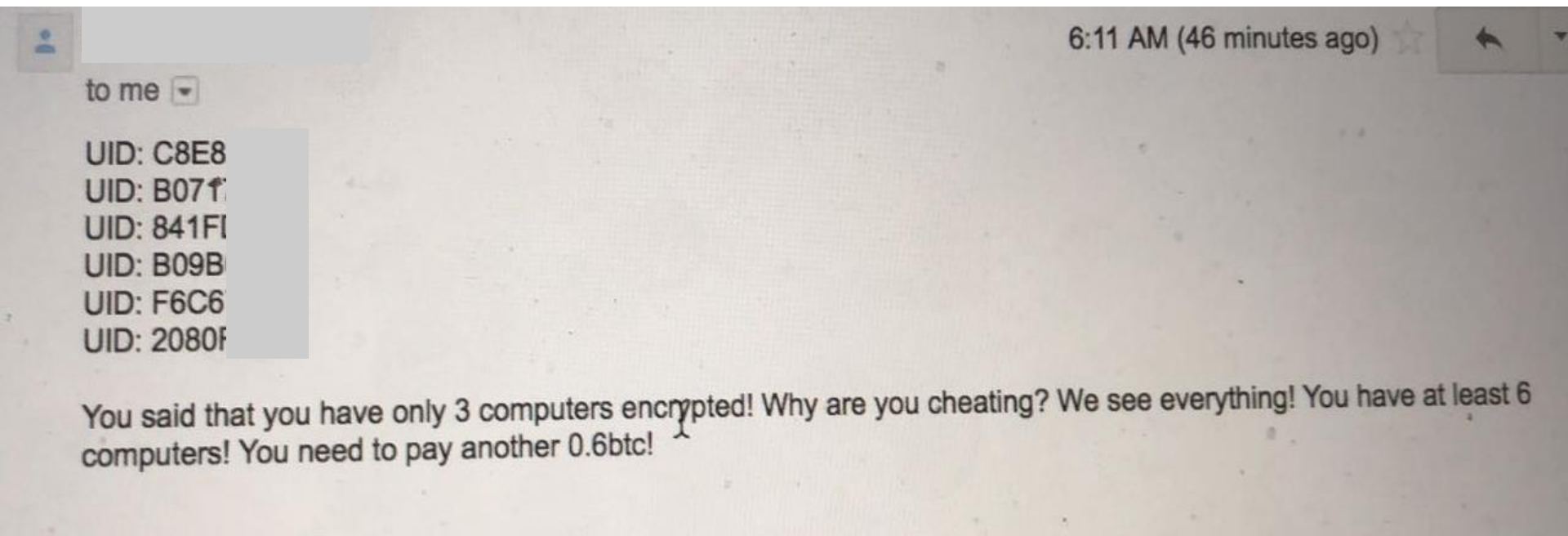


NEED HELP unlocking your digital life
without paying your attackers*?

YES

NO

Negotiating Ransomware: Never Lie



Negotiating Ransomware: Ask for a Discount!

воскресенье, 18 декабря 2016 15:16 Sam

писал(а):

Oh my I see that a bitcoin is quit expensive. I can probably get 1 if I'm lucky. Will that work? Where would I send it? How do you help to recover my files? Thanks for your advise

Sam.

----- Forwarded message -----

From

Date: Sun, Dec 18, 2016 at 4:59 AM

Subject: Отв: Отв: Help!

To: Sam

1.5 Bitcoin to agree on the price?

Payment instructions: 1. Go to <http>

2. Register (sign up) 3. You need to buy Bitcoins from people. (You can pay with any method, which is convenient to you) 4. Send purchased Bitcoins to our address listed below. If you have any questions, you can contact support this service, or email us. Our Bitcoin wallet



FORRESTER®

Paying A Ransom Is A Business Decision

+972-544-694-345

Levels of Cyber-extortion

- ✓ Malware (no negotiation..)
- ✓ Ransomware (..some negotiations..)
- ✓ **Cyber Extortion (..crisis negotiations..)**

Cyber-extortion Negotiations

**..when your data is “held hostage”, and it’s
beyond ransomware..**

Real World Vs. Cyberspace


Similarities	Differences
Damage/Risk Level	No Operational Alternative
Complex Ecosystem	No Professional Management
	No Guarantee
	Practice of Payment

Cyber-Extortion

- 1. Targeted Attack**
- 2. Level of Sophistication**
- 3. Level and Scope of Communication**

Cyber Extortion: Different Types of Losses

- ③ Direct financial losses
- ③ Indirect financial losses: Brand, Legal
- ③ **Damage to company's structure and internal relationships**



Our demand is a single, non negotiable payment of 500 Bitcoins, without any further sanctions from our side. So far we only extracted data without damaging or trading it. This could be either a real-world penetration testing, or an event that will damage your brands in an irreversible way. Just think what a leak of all that on the relevant forums, an article on _____ and other places could do.

10:19

Cyber Extortion: Types of Motivation

Our demand is a single, non negotiable payment of 500 Bitcoins, without any further sanctions from our side. So far we only extracted data without damaging or trading it. This could be either a real-world penetration testing, or an event that will damage your brands in an irreversible way. Just think what a leak of all that on the relevant forums, an article on _____ and other places could do.

10:19

Money

Cyber Extortion: Types of Motivation

Revenge

**AM AND EM MUST SHUT DOWN
IMMEDIATELY PERMANENTLY**

We are the Impact Team.

We have taken over all systems in your entire office and production domains, all customer information databases, source code repositories, financial records, emails

**Shutting down AM and EM will cost you, but non-compliance will cost you more:
We will release all customer records, profiles with all the customers' secret sexual fantasies, nude pictures, and conversations and matching credit card transactions, real names and addresses, and employee documents and emails.
Avid Life Media will be liable for fraud and extreme harm to millions of users.**

Avid Life Media runs Ashley Madison, the internet's #1 cheating site, for people who are married or in a relationship to have an affair. ALM also runs Established Men, a prostitution/human trafficking website for rich men to pay for sex, as well as cougar life, a dating website for cougars, man crunch, a site for gay dating, swappernet for swingers, and the big and the beautiful, for overweight dating.

Trevor, ALM's CTO once said "Protection of personal information" was his biggest "critical success factors" and "I would hate to see our systems hacked and/or the leak of personal information"

Cyber Extortion: Purpose of Negotiations

- ③ Negotiating for a better deal
- ③ Negotiating for intelligence
- ③ Negotiating for time
- ③ Negotiating for operational advantage

Step 1: Profiling

This is not a traditional business deal where you can do that, and we are not the kind of people who need just some kind of money quickly. I don't know what you have read about us, but this is not a regular hacking group. 15:34

Step 2: Assess the Cost of No Deal

Tell the board to be thankful to receive our terms thru you, and not thru our well polished "reminding system" that we decided not to turn on yet.

12:05

Step 3: Build Relationship



Step 4: Move toward a Deal

The way I see it:

1. 6 payments via SEPA
2. Once the first is paid you share with me the inventory of what you have from us
3. Each payment we go deeper on your advise regarding our security
4. If opportunities emerge during this 6 months period, we will discuss them separately.
5. Please indicate what guarantee you give me
6. Let's nail price in USD or EUR for our accounting system.
7. Don't you ever rest?

11:25 ✓✓

Step 5: Expect No Guarantee

See? I saved you some time and gave you the info before the first payment. This is actually a repetition of what we already showed

18:51

Good. Thanks. Now, once we complete the deal, all this will be dumped to the Sea with this number or yours?

18:54 ✓✓

Not so far, but you can be assured that no other party except you and our team will know about it. We know what it does to a company when all the are starting to spread rumors about a breach

18:55

Cyber Extortion: Negotiators' Objectives

1. Diagnose the crisis;
2. Engage constructively with attackers;
3. Assess the cost of no-deal;
4. Support the technological effort;
5. Improve the terms of the deal;

...in order to support a better decision making..

Negotiations: Working Assumptions

- ③ **You are one member of a larger team.!**
- ③ **Remember that the other side knows much more than you do..!**
- ③ **Remember that in cyberspace reality moves much faster than in the real world!**

Negotiations: Professional Tips

- ③ Professional engagement as early as possible;
- ③ Respect, respect, respect;
- ③ Identification of motives and psycho profile;
- ③ Look for behavioral patterns;
- ③ Expand the conversation and build relations;

Cyber Crisis: Professional Management



Bottom Line

Professional crisis negotiation, as well as crisis management is a fundamental component in dealing with cyber extortion and ransomware attacks, as well as preparing IT teams to act as first responders.



Thank you

Moty.cristal@interventisglobal.com

+972-544-694-345