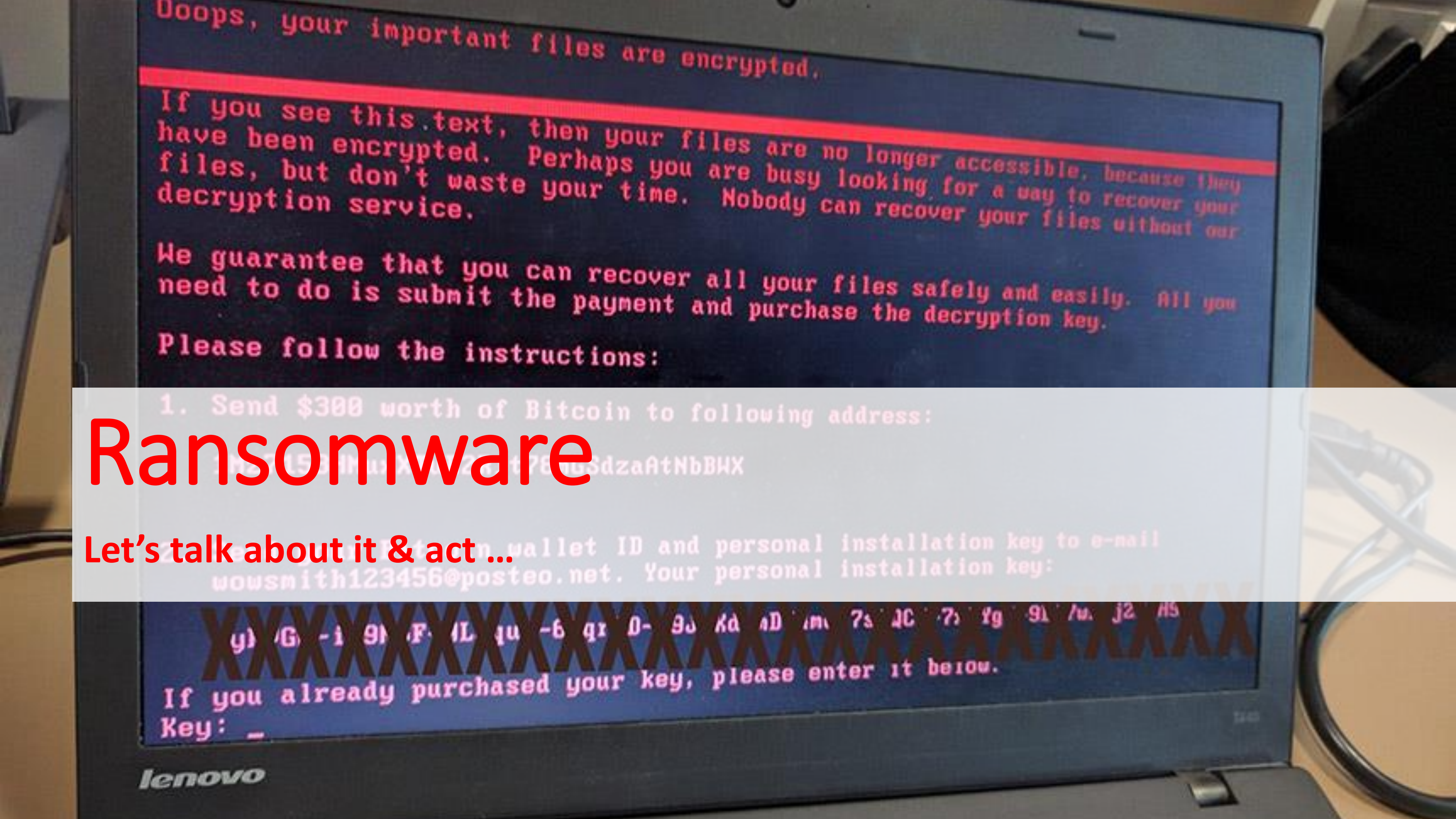
Ransomware

Let’s talk about it & act …



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   [redacted]

If you already purchased your key, please enter it below.
Key: _
```

About Me
Didier Van Hoye aka @WorkingHardInIT

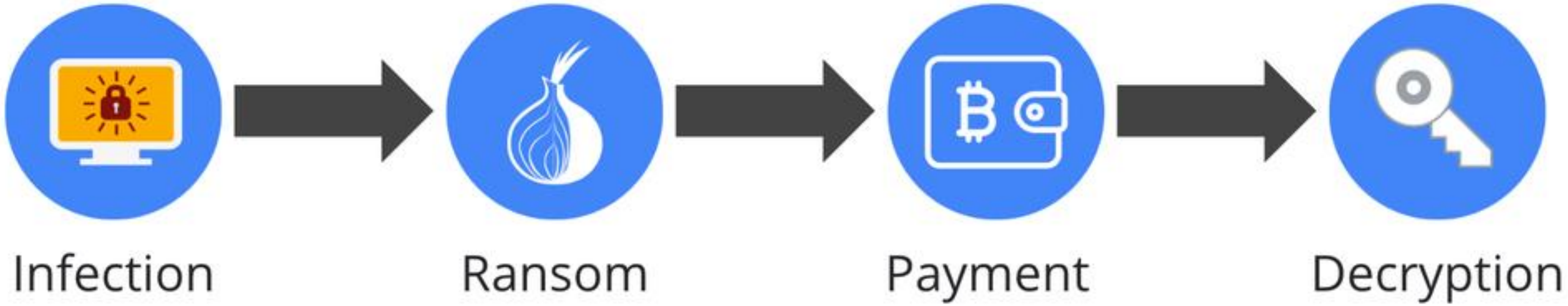
Technical Architect & Technology Strategist

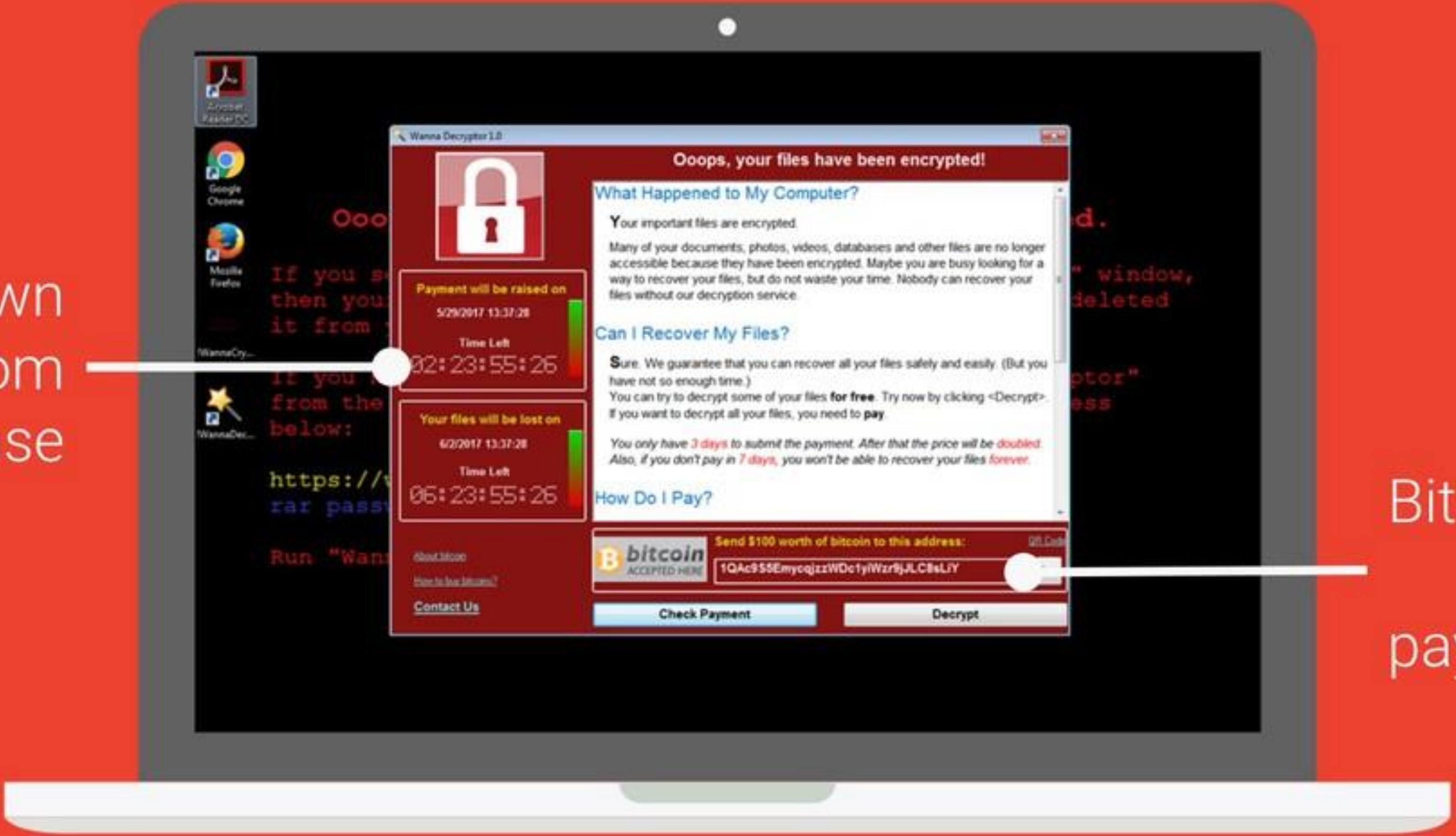
- Microsoft MVP Cloud & Datacenter Management
- MEET Member
- DELL Community Rockstar
- Veeam Vanguard

http://blog.workinghardinit.work

@workinghardinit

The ransomware business model





Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Payment will be raised on
5/29/2017 13:37:28
Time Left
02:23:55:26

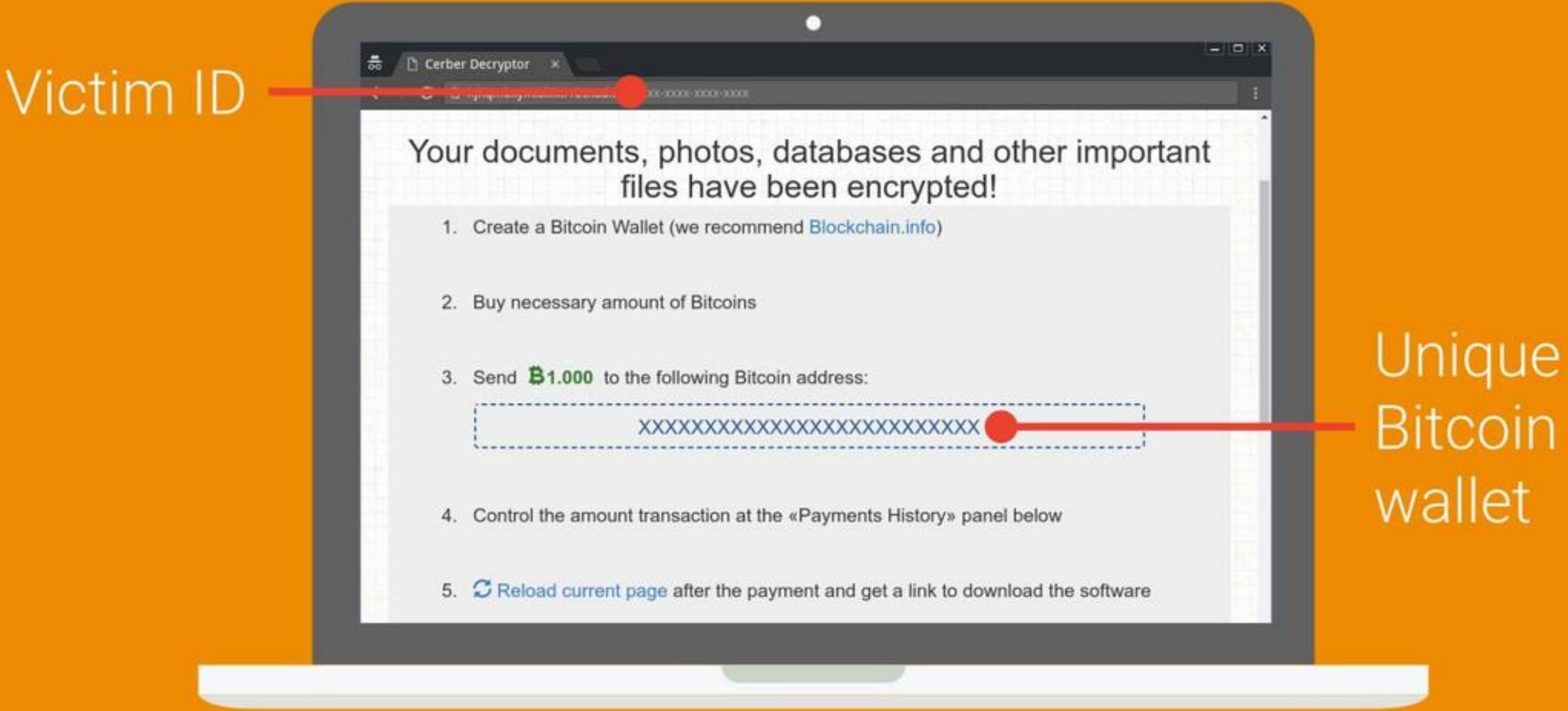
Your files will be lost on
6/2/2017 13:37:28
Time Left
06:23:55:26

Send $100 worth of bitcoin to this address:
1QAc9S5EmycqjzzWDc1yiWzr9jJLC8sLiY

Countdown to ransom increase

Bitcoin wallet or payment URL

Victim is shown **ransom note**



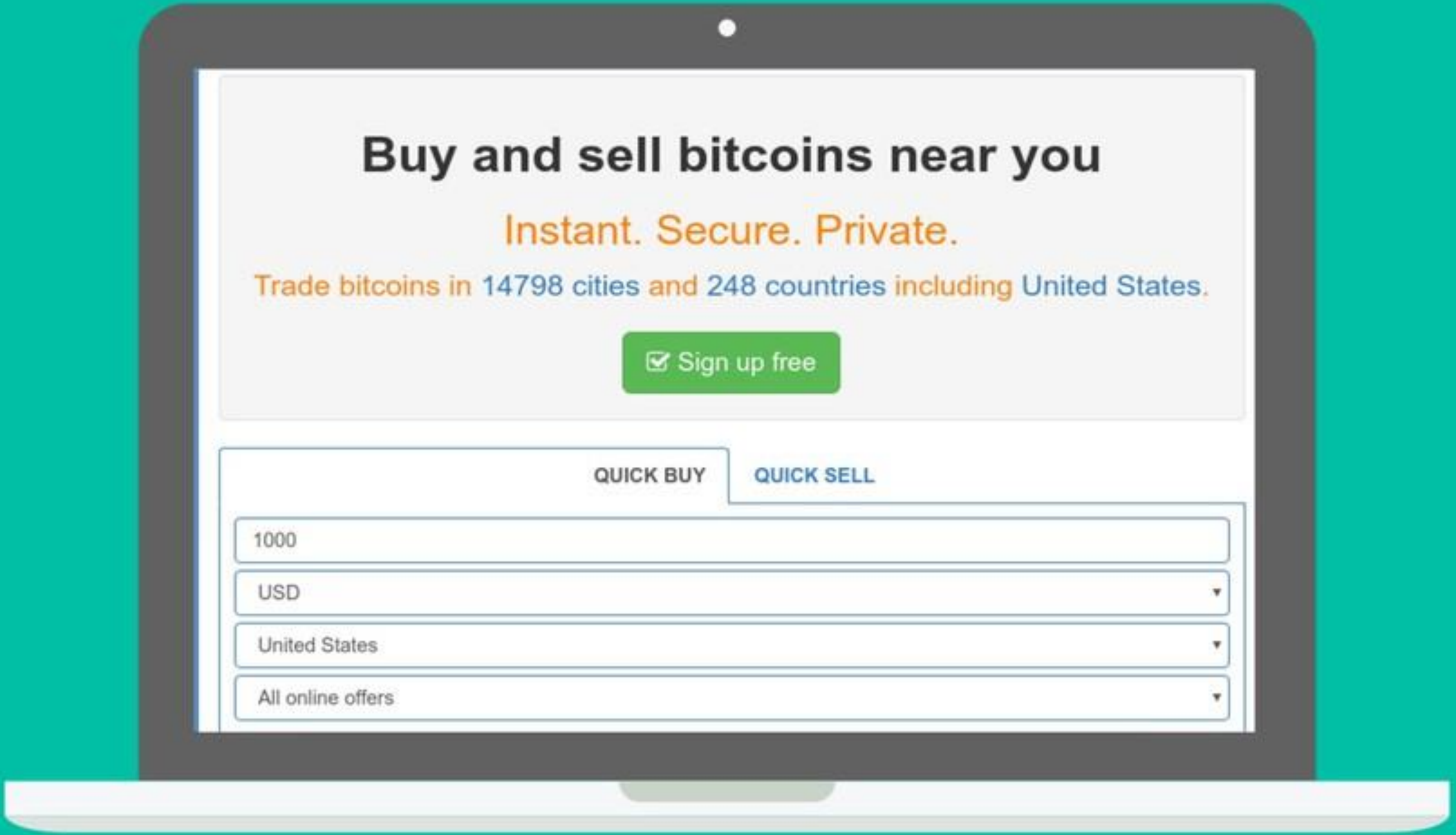
Your documents, photos, databases and other important files have been encrypted!

1. Create a Bitcoin Wallet (we recommend Blockchain.info)
2. Buy necessary amount of Bitcoins
3. Send Ƀ1.000 to the following Bitcoin address:

   XXXXXXXXXXXXXXXXXXXXXXXXXXXX

4. Control the amount transaction at the «Payments History» panel below
5. Reload current page after the payment and get a link to download the software

Victim visits **payment site** via Tor



Buy and sell bitcoins near you

Instant. Secure. Private.

Trade bitcoins in 14798 cities and 248 countries including United States.

1000

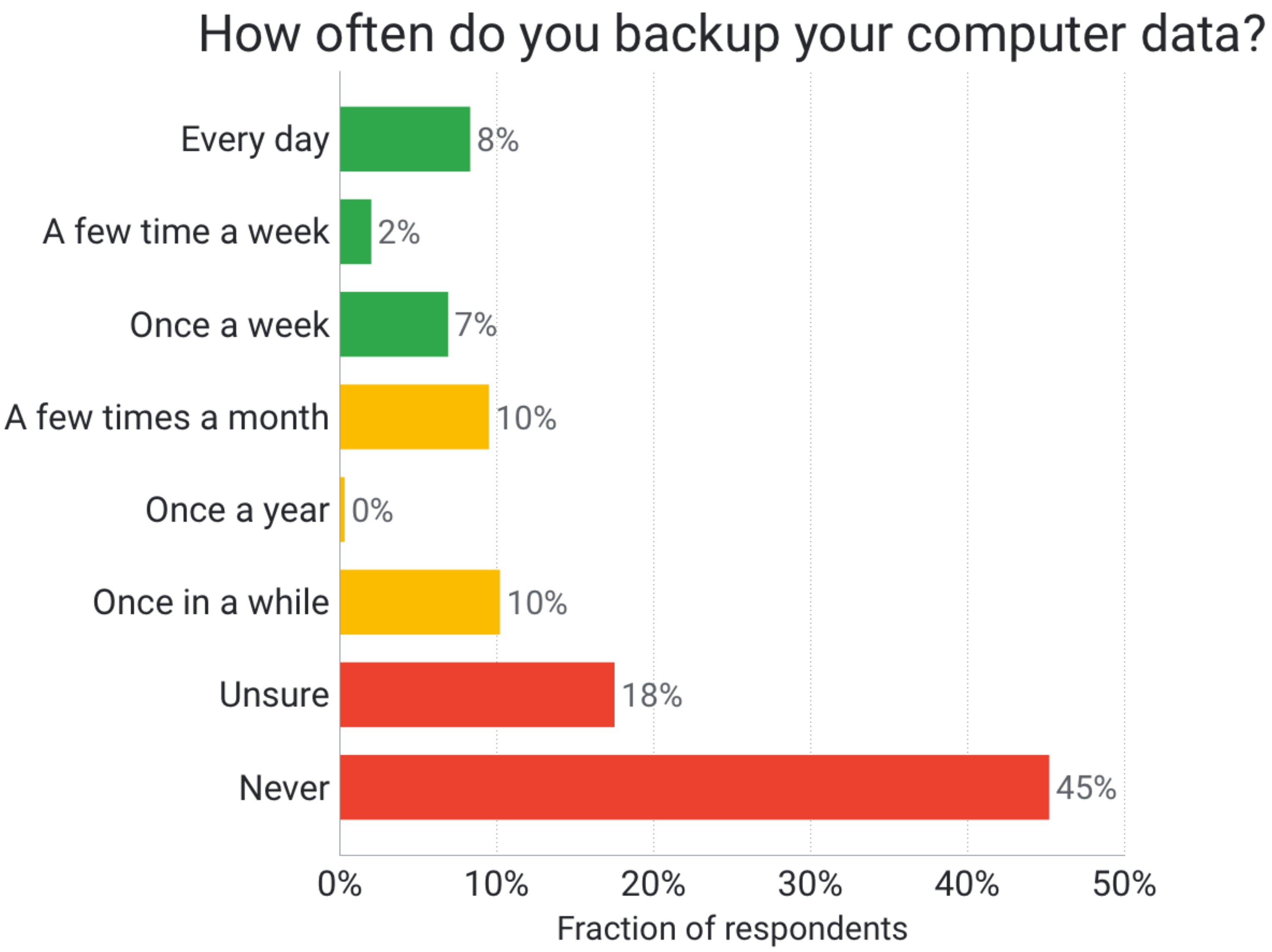
USD

United States

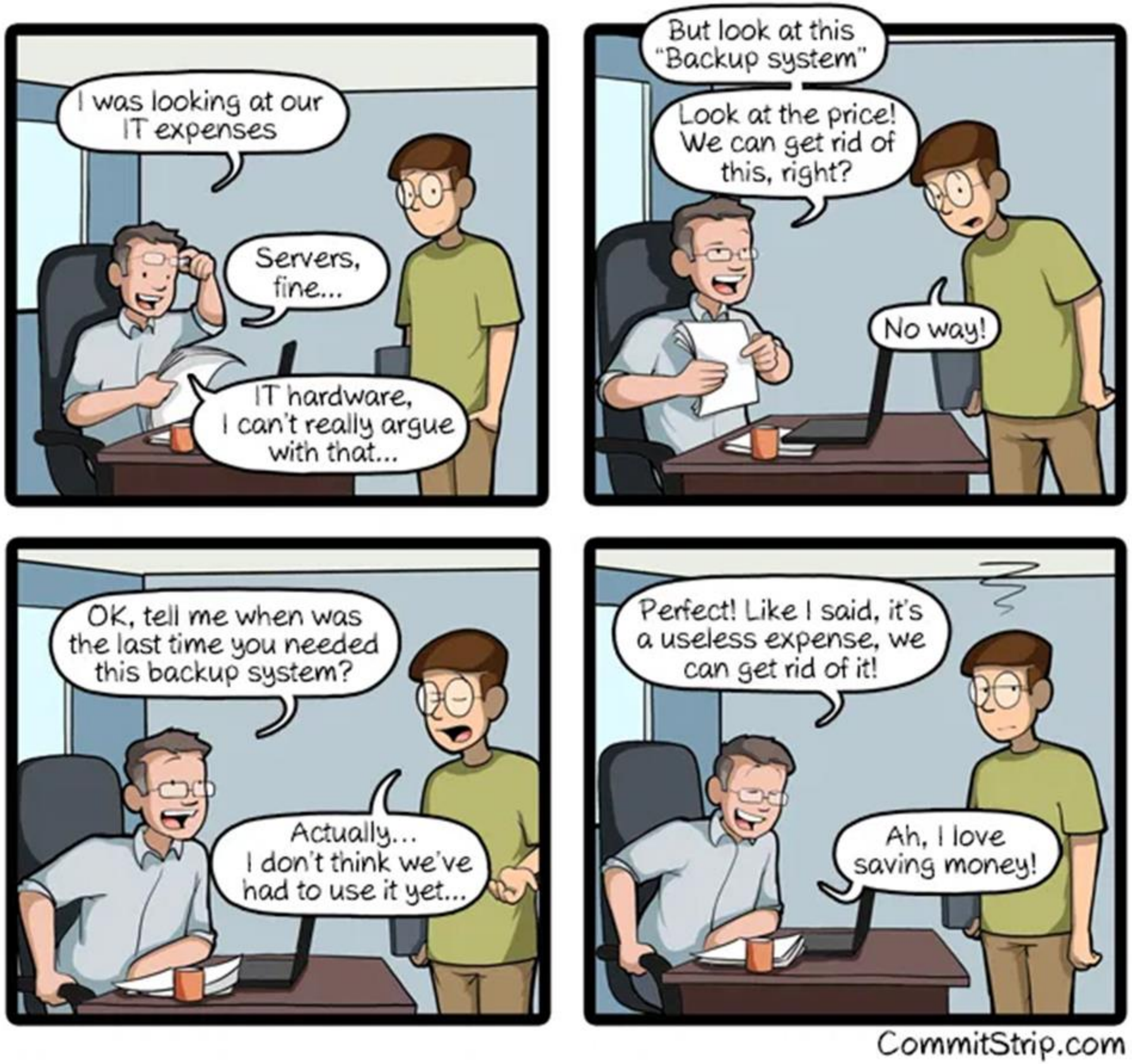
All online offers

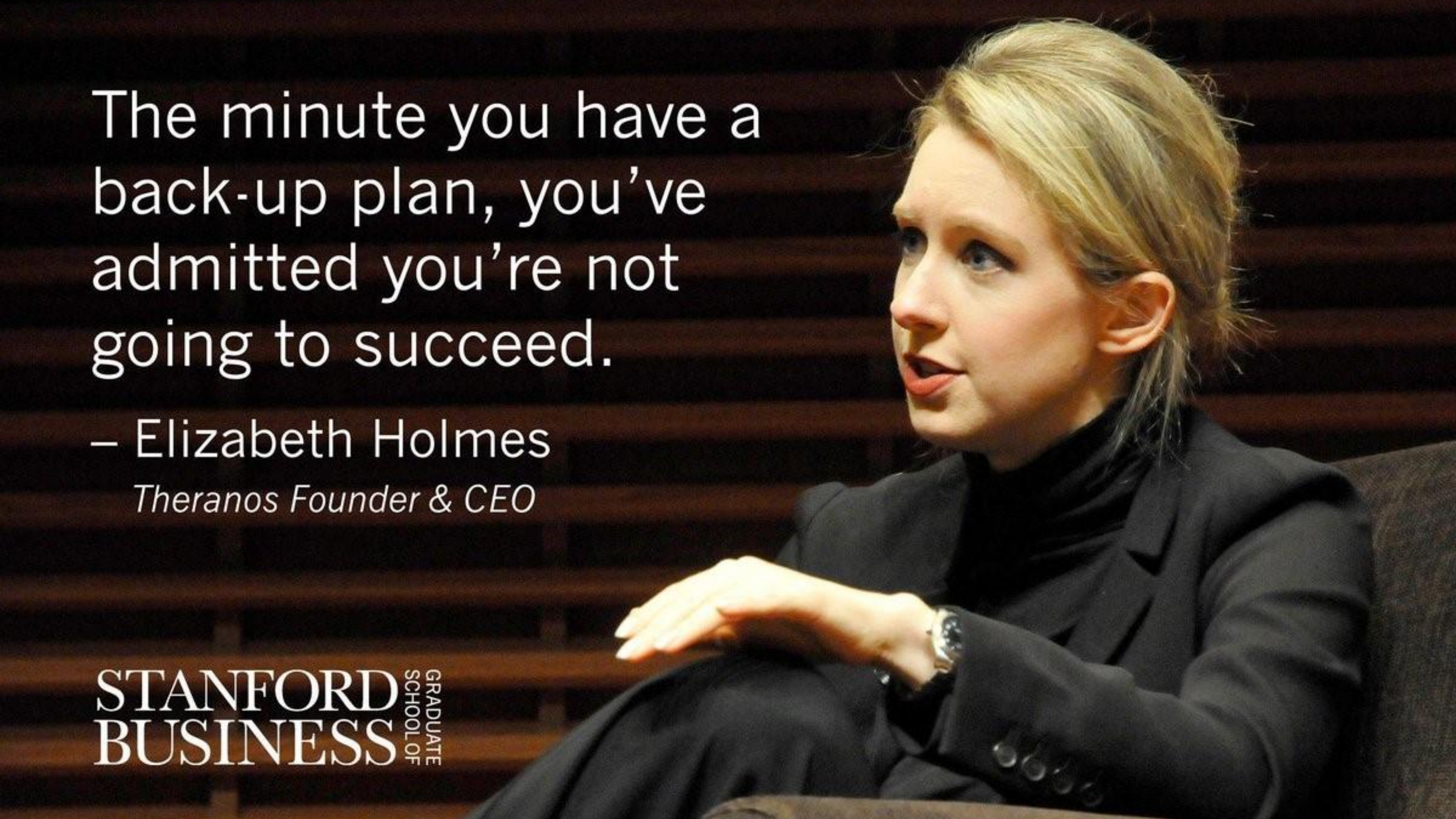
Victim buys bitcoin at ***exchange***

Is this you?


How often do you backup your computer data?
Every day
8%
A few time a week
2%
Once a week
7%
A few times a month
10%
Once a year
0%
Once in a while
10%
Unsure
18%
Never
45%
0%
10%
20%
30%
40%
50%
Fraction of respondents

Is this your boss or customer?


I was looking at our IT expenses
Servers, fine...
IT hardware, I can't really argue with that...
But look at this "Backup system"
Look at the price! We can get rid of this, right?
No way!
OK, tell me when was the last time you needed this backup system?
Actually... I don't think we've had to use it yet...
Perfect! Like I said, it's a useless expense, we can get rid of it!
Ah, I love saving money!
CommitStrip.com



The minute you have a back-up plan, you've admitted you're not going to succeed.

– Elizabeth Holmes

Theranos Founder & CEO

STANFORD
GRADUATE SCHOOL OF
BUSINESS

Ransomware # Peaks 2016-2017

- In total number Ransomware is peaking … but often limited to file shared and knowledge worker data, relatively easy to recover from at small scale.
- A bit more challenging and disrupting on a larger scale
- Paying did or did not lead to a satisfactory result

Ransomware # Decrease: 2018-2020

- The become less spray and pray but more sophisticated
- More targeted attacks,
- Highly sophisticated: weeks to months of reconnaissance. Professional services desk, blunt negotiations, see it as a sustainable business (be reliable).
- Also seen: “socialy responsible” ethics, “educational goals”.
- Better at covering their tracks in subsequent releases
- Wipers are mixed in amongst them

ZPMC
MAERSK

Background: NotPetya

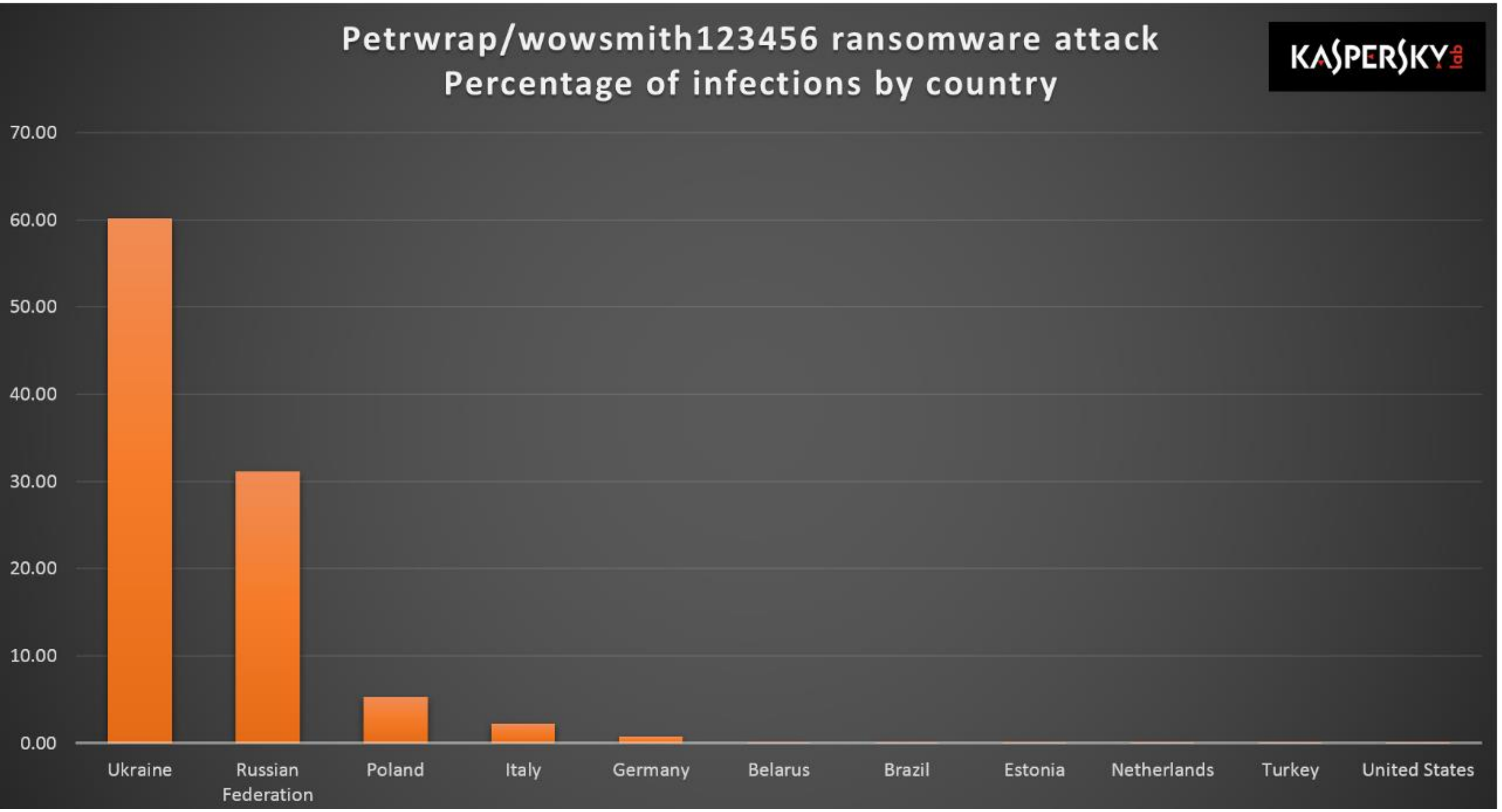
- First appeared June 27, 2017
- Destructive "wiper" malware that looks/acts like "ransomware"
  - Wipers don't just encrypt data – they destroy it
- Based on known ransomware dubbed "Petya" (Russian)
- Believed to be nation-state backed operation
- Primary target: Govt. of Ukraine and Ukraine civil society

Background: NotPetya

- Initially spread as a software update for M.E.Docs, Ukrainian Accounting software package
    - Distributed as signed software updates from compromised firm
- Destructive “wiper” malware designed to look/act like ransomware
    - Based on known malicious software dubbed “Petya” with Russian origins – but probably created by a separate group
    - Believed to be nation-state backed operation
- Primary target: Ukraine

6
3

NotPetya Infections by Country



- Infected more than 1 million computers
- 2,000 companies in Ukraine hit by NotPetya
- Extensive “spill over” outside Ukraine including Russia, Poland, Italy, Germany
- FedEx, Maersk, Merck & Mondelez all heavily impacted

What happened? (1/3)

- Part of long running tensions between Russia and Ukraine
  - Extensive use of cyber operations to disrupt Ukrainian government and civil society
- Companies were not targets of campaign or actors, but innocent bystanders of regional tension between Russia and Ukraine

What happened? (2/3)

- Massively costly to affected firms
  - $400 million in direct, indirect costs at FedEx
  - $184m for Mondelez with $84m in direct costs and ~$100 million in lost revenue
  - Maersk: $300 million dollar
  - Merck unable to produce GARDASIL vaccine ➔ emergency borrowing from US Govt. stockpile

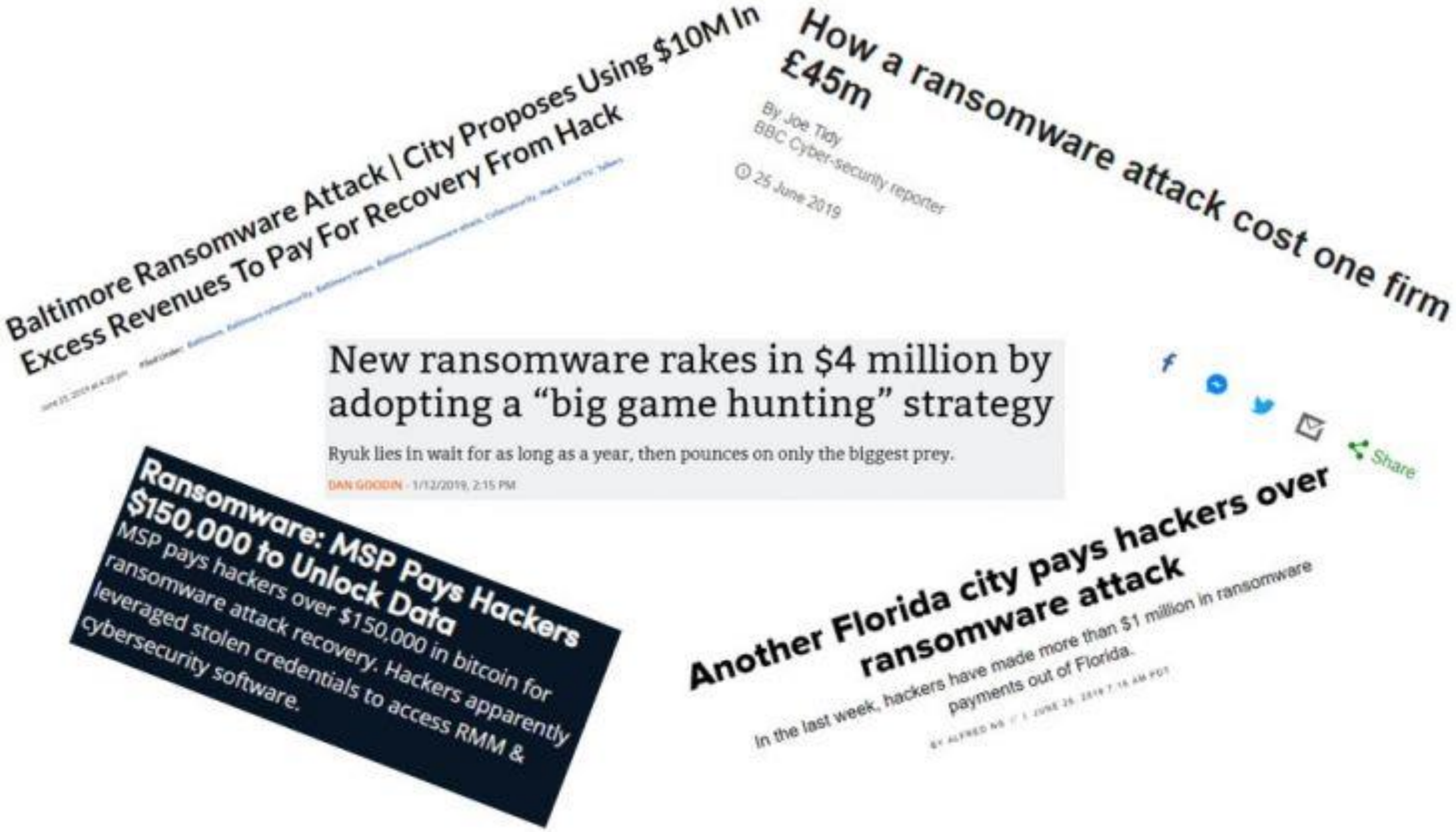
What happened? (3/3)

Affected companies were hit because:

- They were in the Ukraine or Ukraine-based OR…
- They used the M.E. Docs software internally – either corporate wide or as part of a subsidiary/acquisition OR…
- **They did not patch with MS17-010 patch and remained vulnerable to exploit by EternalBlue and/or Eternal Romance Windows exploits**

SamSam, MegaCortex, LockerGoga, Dharma, BitPaymer, Ruyk, …

Ransomware shuts down production at Flemish multinational | VRT ...



Baltimore Ransomware Attack | City Proposes Using $10M In Excess Revenues To Pay For Recovery From Hack

June 25, 2019 at 4:20 pm Filed Under: [illegible]

How a ransomware attack cost one firm £45m

By Joe Tidy
BBC Cyber-security reporter

25 June 2019

New ransomware rakes in $4 million by adopting a "big game hunting" strategy

Ryuk lies in wait for as long as a year, then pounces on only the biggest prey.

DAN GOODIN - 1/12/2019, 2:15 PM

Share

Ransomware: MSP Pays Hackers $150,000 to Unlock Data

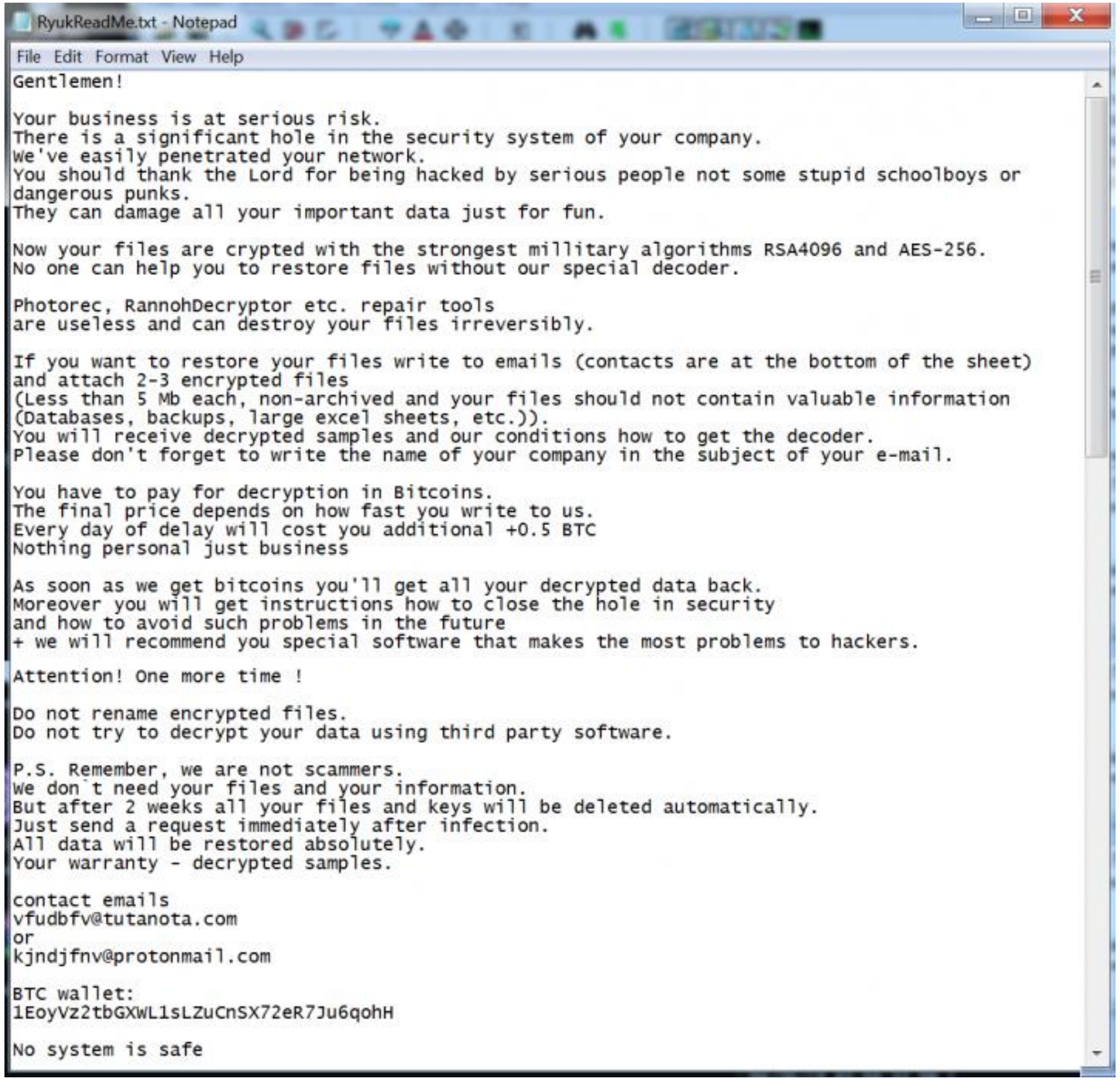
MSP pays hackers over $150,000 in bitcoin for ransomware attack recovery. Hackers apparently leveraged stolen credentials to access RMM & cybersecurity software.

Another Florida city pays hackers over ransomware attack

In the last week, hackers have made more than $1 million in ransomware payments out of Florida.

BY ALFRED NG // JUNE 26, 2019 7:16 AM PDT

Serious bad boy right now …Ruyk



```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or
dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don`t need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
vfudbfv@tutanota.com
or
kjndjfnv@protonmail.com

BTC wallet:
1EoyVz2tbGXWL1sLZuCnSX72eR7Ju6qohH

No system is safe
```

Beyond the 3-2-1 rule – Airgap (1/3)

Tapes!

- Tape?! Yes, they have a great cost/TB ratio, they have longevity, and they get the job done. Now, many of us have a love-hate relationship with tapes,
- But in ransomware times, the off-site and off-line aspect of tapes have made it popular again.
- Both physical ones and Virtual Tape Libraries

Beyond the 3-2-1 rule - Airgap (2/3)

Disk

- rotate them out

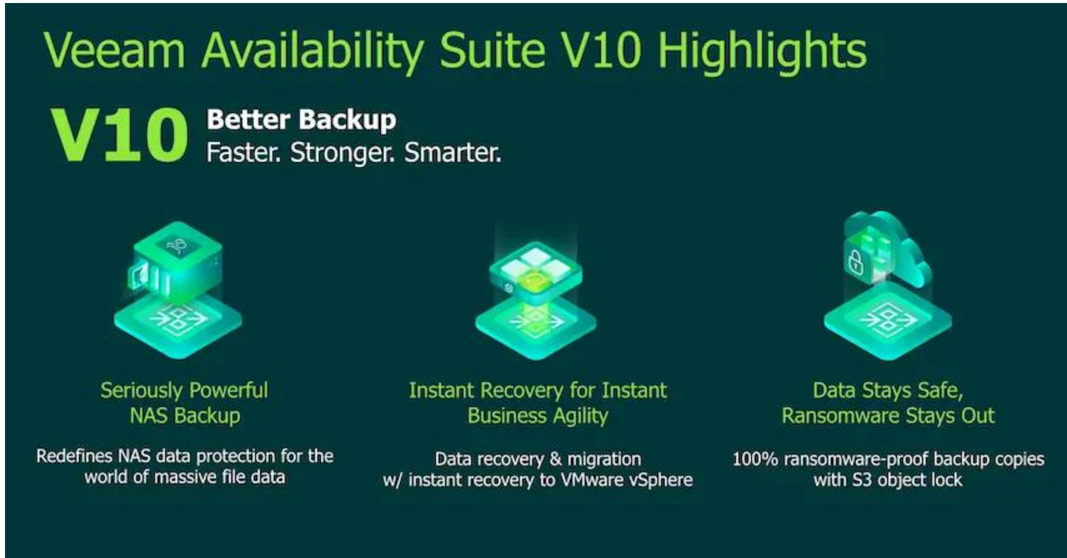
Disk-based WORM

- WORM is an option that is not only available via tape. There are other options based on disk storage, and there are disk-based solutions that offer WORM. One such example is Silent Brick that offers disk-based backup and archive with WORM capabilities.

Beyond the 3-2-1 rule - airgap (3/3)

Immutable storage integrations with backups (VTL/Direct)

- Amazon S3 Object Lock in compliance mode offers exactly this for the duration of the retention period. Please note that S3 immutable storage does not mean you are tied to the public cloud of the hyper scalers. As long as you find object storage that can deliver S3 buckets with immutability implemented, you are good to go.



Veeam Availability Suite V10 Highlights

V10 **Better Backup**
Faster. Stronger. Smarter.

Seriously Powerful
NAS Backup

Redefines NAS data protection for the
world of massive file data

Instant Recovery for Instant
Business Agility

Data recovery & migration
w/ instant recovery to VMware vSphere

Data Stays Safe,
Ransomware Stays Out

100% ransomware-proof backup copies
with S3 object lock

Prevent?

- Protect privileged credentials
  - Tiered AD model
  - Tiered credential model
  - Authorization Groups and policies
  - Jump hosts
- MFA for critical systems
- Protect against lateral movement
- End point protection
- Accept you can defend but must do so in depth and will fail at some point in time: delaying and detection are key

Recover!

- Restore your data.
- You must have multiple options. You must have implemented the 3-2-1 rule + airgaped copies
- Your off site, air gapped copy cannot be too old. You need to have fairly recent backups in there to have a decent RPO that is meaningful to the business. But old enough to not be contaminated too badly

I was looking at our IT expenses
Servers, fine...
IT hardware, I can't really argue with that...
But look at this "Backup system"
Look at the price! We can get rid of this, right?
No way!
OK, tell me when was the last time you needed this backup system?
Actually... I don't think we've had to use it yet...
Perfect! Like I said, it's a useless expense, we can get rid of it!
Ah, I love saving money!
CommitStrip.com

PAY?!

- You can but see https://blog.workinghardinit.work/2018/07/10/the-lure-of-having-a-ransomware-fund/

Why are ransoms in Bitcoin?

- **Anonymous**: Creating bitcoin wallets, does not require any form of ID. This makes it ideal for conducting cybercrimes.
- **Fully Automatable**: All aspects of ransom payments, from wallet creation to payment monitoring to moving money to cashing it out are automated,
- **Irrefutable**: Bitcoin transactions are irrefutable, which guarantees that once the ransom is paid, the money will not be charged back
- **Usable**: Bitcoin is the only crypto currency with enough people who want to buy it to make it usable. No other currency would so easily allow cybercriminals to cash out at the scale they need.

Why use so many Bitcoin wallets?

- Cybercriminals make use of the fact that creating and monitoring Bitcoin wallets can be done automatically.
- It assists them in figuring out which victims have paid. Ransomware creates one wallet for each infection, so it is easy to tie a specific payment to a given ransomware infection and a given victim.

Why does ransomware use TOR?

- TOR makes it difficult for law enforcement authorities to locate ransom websites and shut them down.
- Makes it hard to leverage one of the most effective tactics against botnets: shutting down the control site.
- TOR also makes it harder to crawl the sites to get ransom wallet addresses, as the sites require that the crawler supports the TOR protocol.

Interactive discussion, Q&A