Responding to Cyber Security Attacks

@khannaanurag

#whoami

- Lead Investigator @ Symantec Incident Response
- Networking -> Security Researcher -> Web/Network Pen testing -> Security Architect -> Digital Forensics and Incident Response
- GSE # 97 + (GIAC and Others)
- MS - Digital Forensics & MBA- IT
- @khannaanurag 🐦

Disclaimer

- The views presented here are my own and may or may not be similar to those of the organization I work for

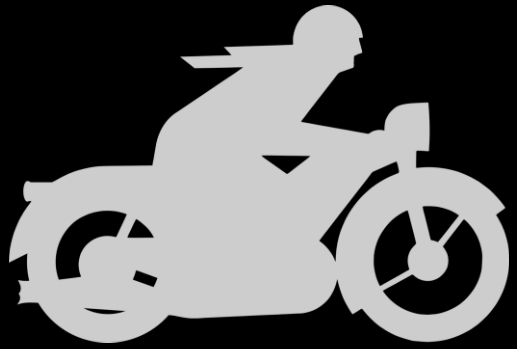
- I am not a Lawyer (IANAL)

Questions are more Powerful than Answers!

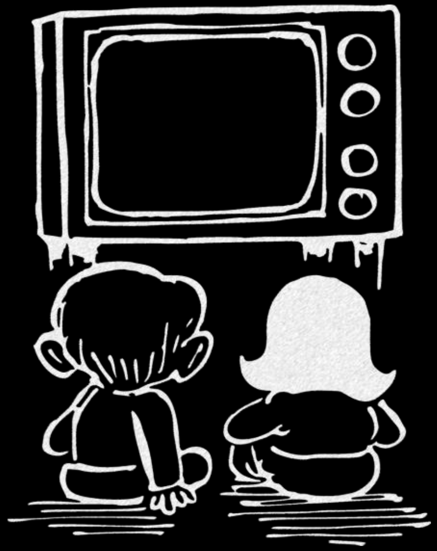
Mid size Logistics Firm.

Peter!

Pick Your Seat



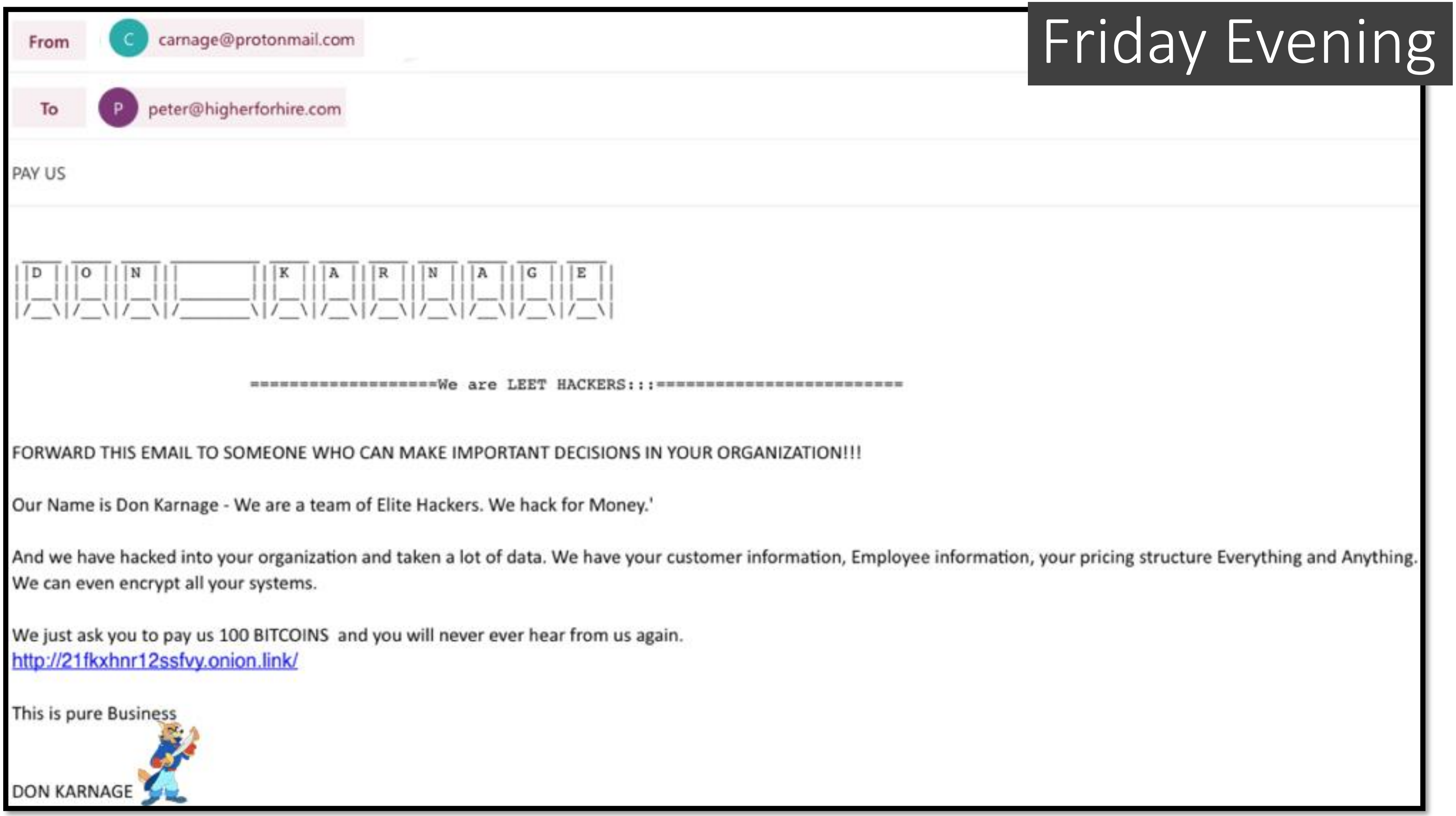
Doer



Spectator

Relax

Friday Evening



From C carnage@protonmail.com

To P peter@higherforhire.com

PAY US

```
 ____ ____ ____ _________ ____ ____ ____ ____ ____ ____ ____
||D ||||O ||||N ||||       ||||K ||||A ||||R ||||N ||||A ||||G ||||E ||
||__||||__||||__||||_______||||__||||__||||__||||__||||__||||__||||__||
|/__\||/__\||/__\||/_______\||/__\||/__\||/__\||/__\||/__\||/__\||/__\|
```

```
===================We are LEET HACKERS:::=========================
```

FORWARD THIS EMAIL TO SOMEONE WHO CAN MAKE IMPORTANT DECISIONS IN YOUR ORGANIZATION!!!

Our Name is Don Karnage - We are a team of Elite Hackers. We hack for Money.'

And we have hacked into your organization and taken a lot of data. We have your customer information, Employee information, your pricing structure Everything and Anything. We can even encrypt all your systems.

We just ask you to pay us 100 BITCOINS and you will never ever hear from us again.
http://21fkxhnr12ssfvy.onion.link/

This is pure Business

DON KARNAGE

Options

Call CEO

Ignore - Noise

Security Operations

Questions

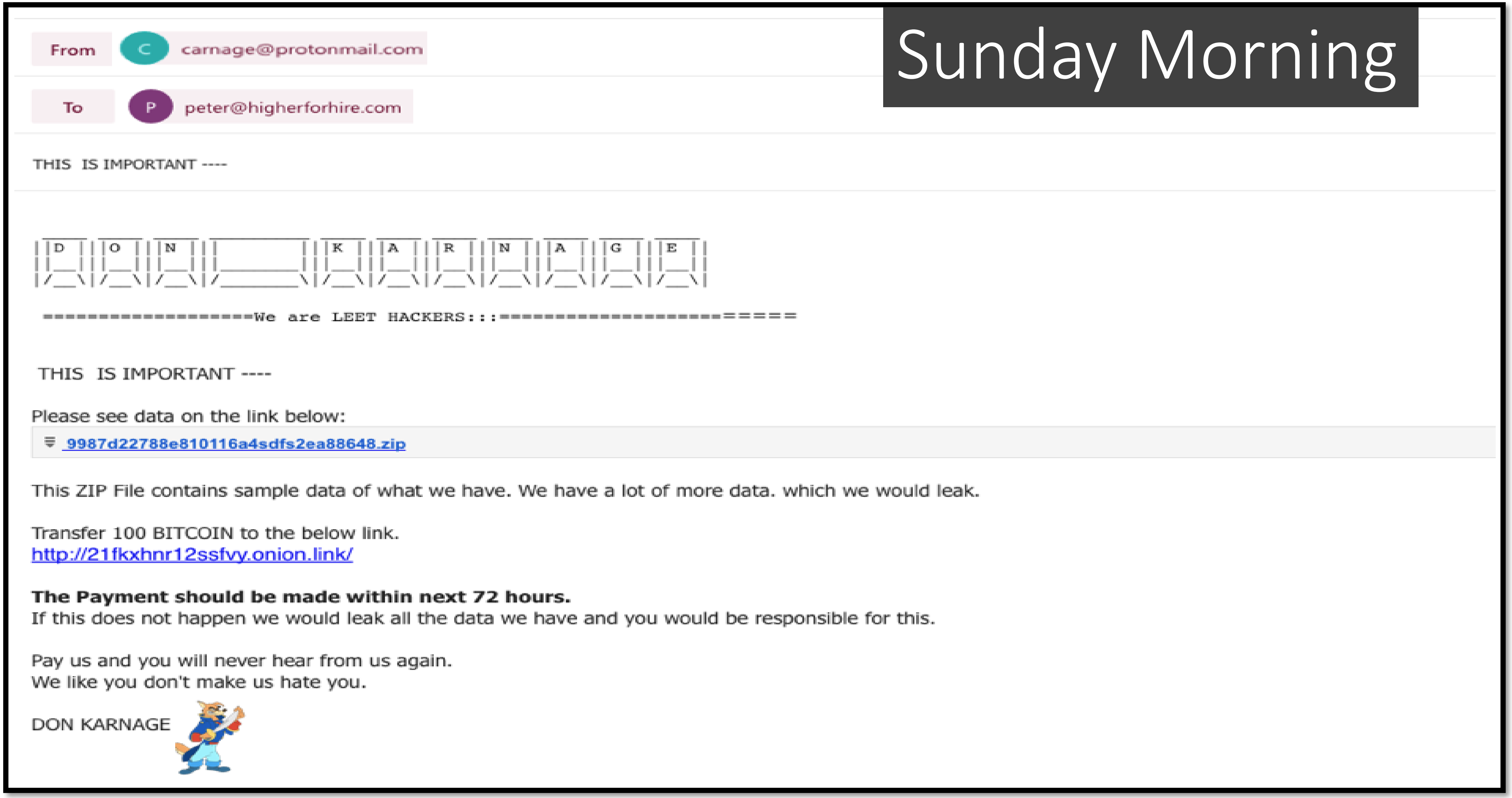
- Is this worth the effort?

- Generic Emails –
  - security@higherforhire.com info@higherforhire.com

- Invoke-IR?

- What else?

Sunday Morning



From carnage@protonmail.com

To peter@higherforhire.com

THIS IS IMPORTANT ----

```
 ____ ____ ____ _________ ____ ____ ____ ____ ____ ____ ____
||D |||O |||N |||       |||K |||A |||R |||N |||A |||G |||E ||
||__|||__|||__|||_______|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/_______\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|

 ===================We are LEET HACKERS:::============================
```

THIS IS IMPORTANT ----

Please see data on the link below:

9987d22788e810116a4sdfs2ea88648.zip

This ZIP File contains sample data of what we have. We have a lot of more data. which we would leak.

Transfer 100 BITCOIN to the below link.
http://21fkxhnr12ssfvy.onion.link/

The Payment should be made within next 72 hours.
If this does not happen we would leak all the data we have and you would be responsible for this.

Pay us and you will never hear from us again.
We like you don't make us hate you.

DON KARNAGE

So far… First threat email

Options

Click

Exec Response

FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
IB625 [redacted] 38A
B2
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
SERIES 2006
LINCOLN
5
FIVE DOLLARS

Pay

Call LEA

More Questions

- Is data current ? Public ?
- Inform?
  - Govt., Law Enforcement, Regulators, Partners, Investors
- External Help ?

Monday

- Data is internal and Current
- Law Enforcement has been informed
- Incident Response has been invoked

So far… ✉ First threat email → ✉ Second threat email

Options

Public Relations

Pay

Internal Relations

Questions

- Take Down request?
- Law Enforcement

Wednesday

- CRM system is identified as breached
- Active C2 identified
- Possible APT in the environment

So far…

First threat email → Second threat email → Suspected breach - IR invoked

Should We?

- Take CRM offline & kill the C2
- Kill the internet
- Ahhhh… Pay

Questions

Technology

- Evidence Collection
- Evidence Analysis
- Swift Response
- Endpoint Tools IOC Sweeping

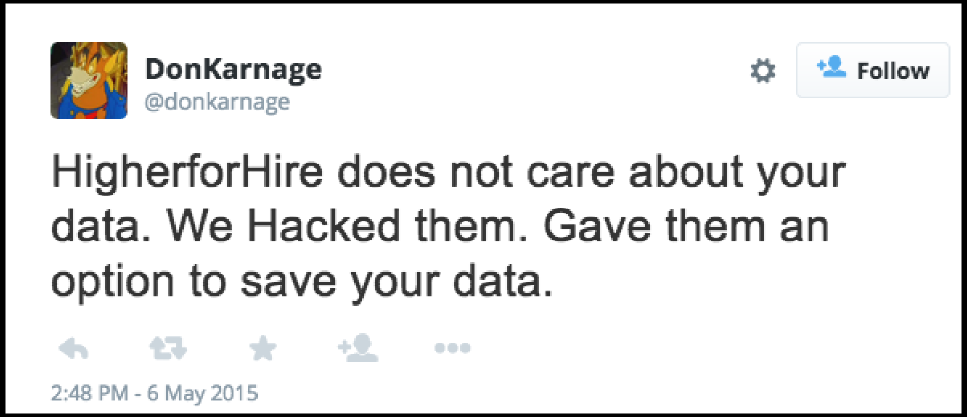
People

- 24x7
- Reachable
- Skilled
- Motivated

Resources

- Money
- Office
- Access
- Support
- Opsec

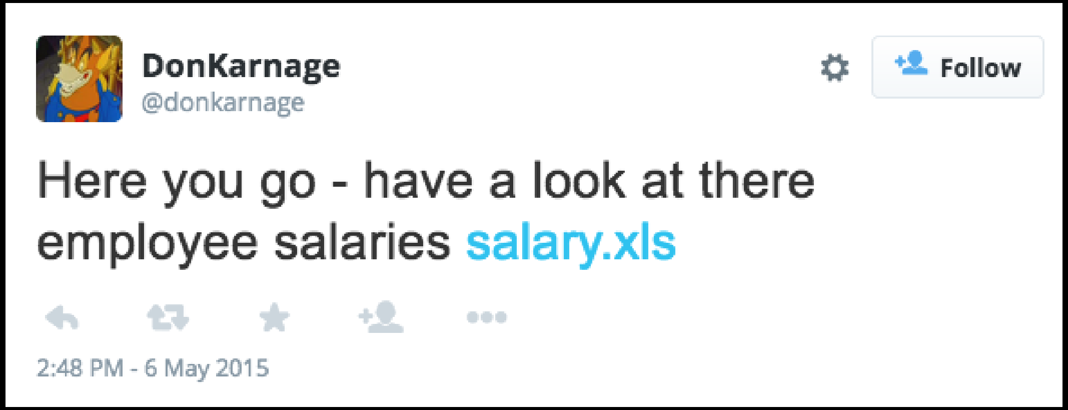
Sometime in Future



DonKarnage
@donkarnage

HigherforHire does not care about your data. We Hacked them. Gave them an option to save your data.

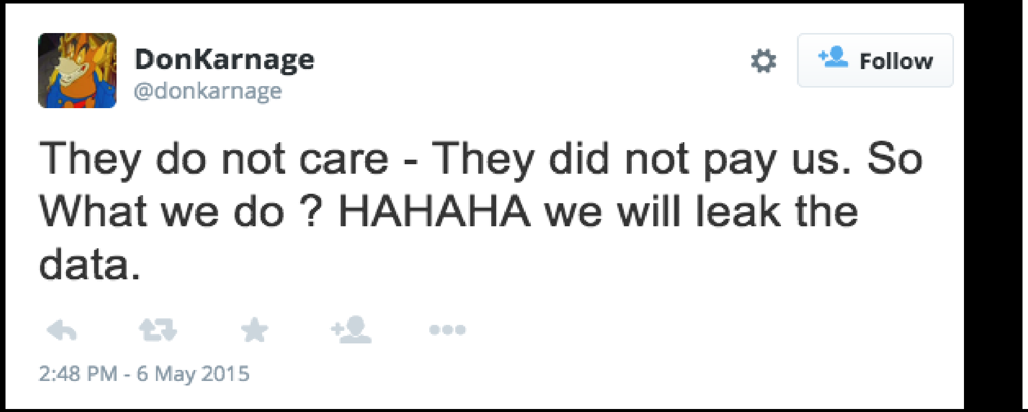
2:48 PM - 6 May 2015



DonKarnage
@donkarnage

Here you go - have a look at there employee salaries salary.xls

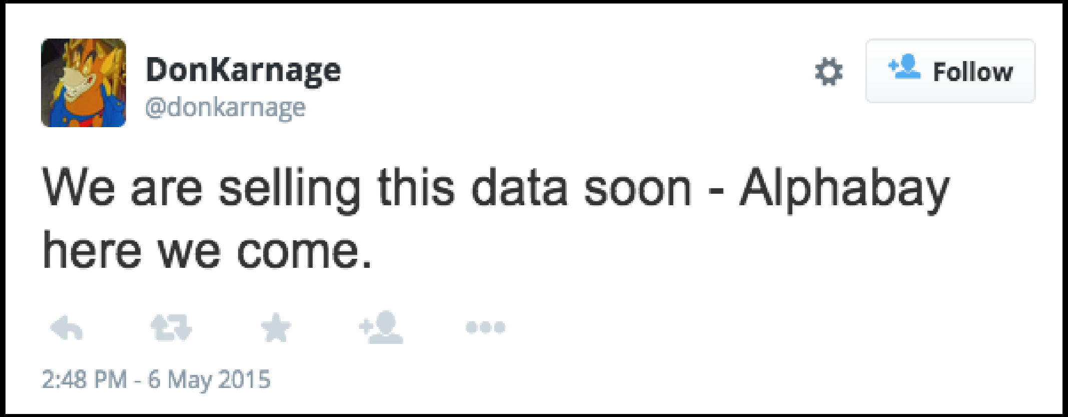
2:48 PM - 6 May 2015



DonKarnage
@donkarnage

They do not care - They did not pay us. So What we do ? HAHAHA we will leak the data.

2:48 PM - 6 May 2015



DonKarnage
@donkarnage

We are selling this data soon - Alphabay here we come.

2:48 PM - 6 May 2015

So far… First threat email → Second threat email → Suspected breach - IR invoked → C2 identified

BREAKING NEWS

Stock Crashed – Employees Quitting

PR nightmare

Brace for More data leak?

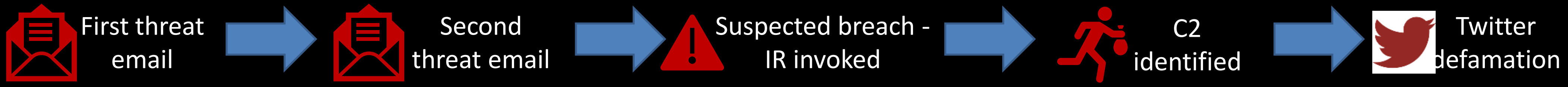
Questions

- Invoke PR response?
- How do you brace for data leak?

Later

- All data was posted on darknet offering an exclusive sale

So far…

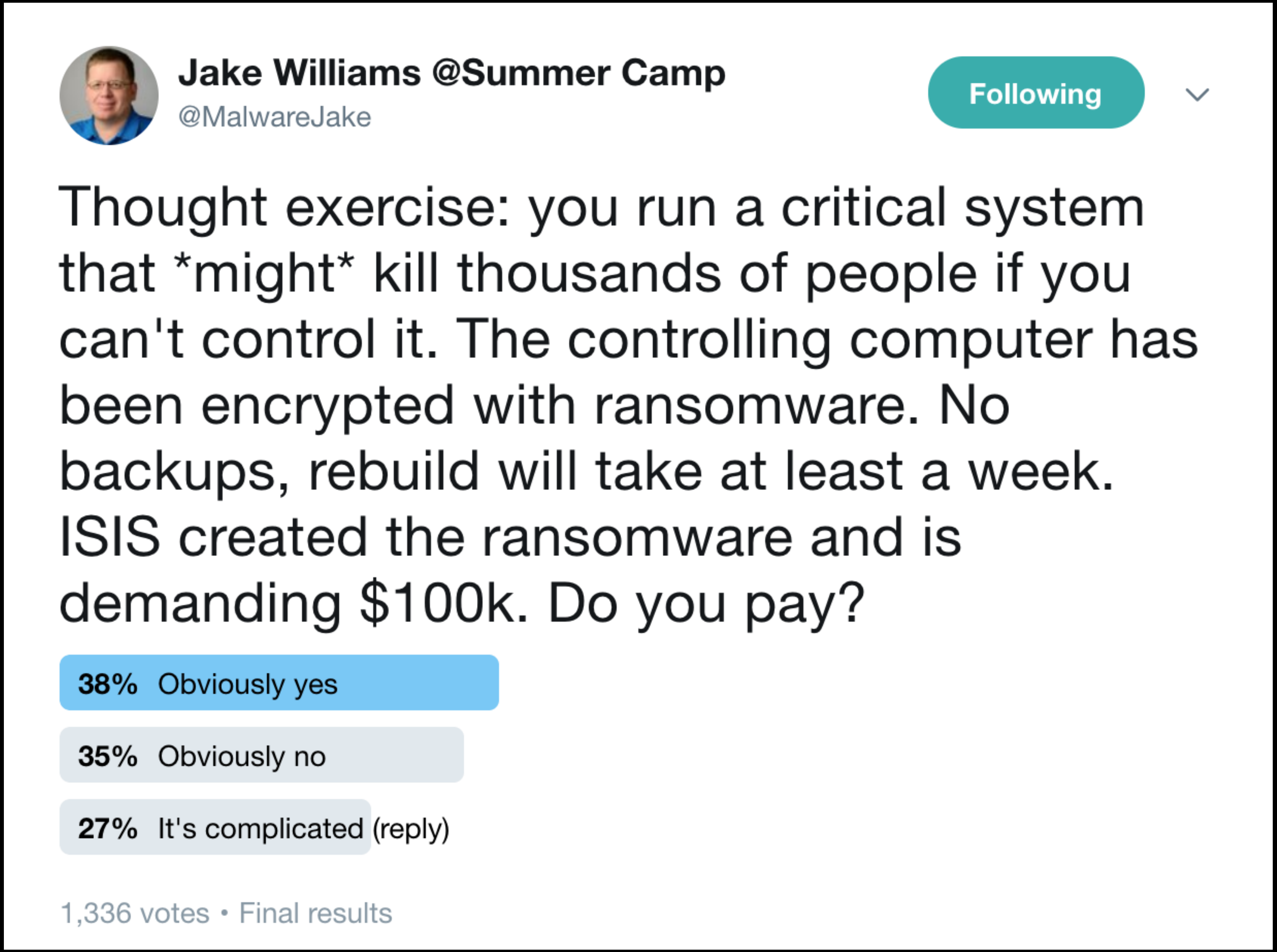


First threat email → Second threat email → Suspected breach - IR invoked → C2 identified → Twitter defamation

This is our chance of redemption.

Questions

- Buy data now How?
- Brace for data leak?



Jake Williams @Summer Camp
@MalwareJake

Thought exercise: you run a critical system that *might* kill thousands of people if you can't control it. The controlling computer has been encrypted with ransomware. No backups, rebuild will take at least a week. ISIS created the ransomware and is demanding $100k. Do you pay?

38% Obviously yes

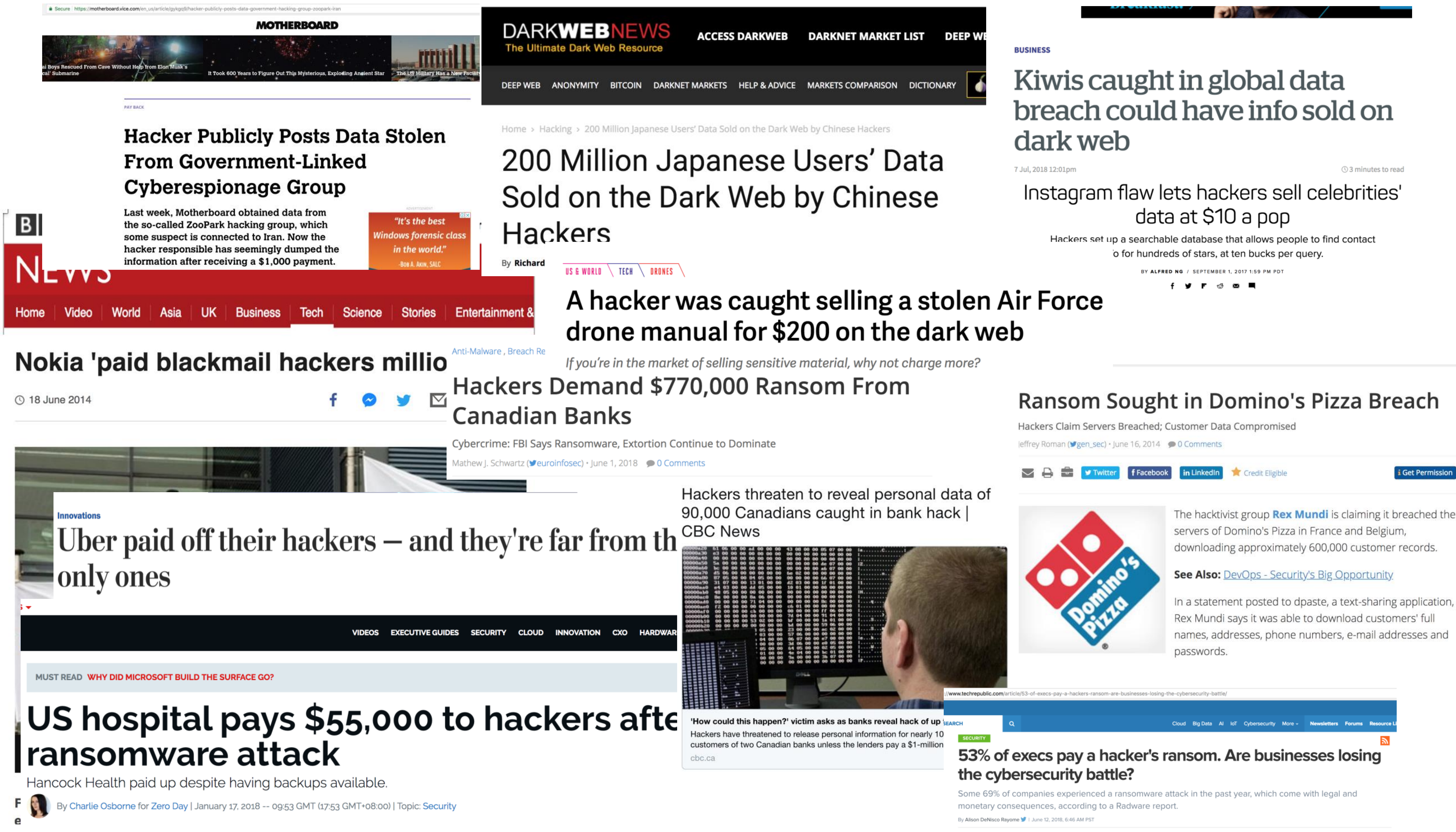
35% Obviously no

27% It's complicated (reply)

1,336 votes • Final results

I wish I had known things can go downhill so quickly, I would have done things differently….

Are you prepared to handle something like this?



Secure https://motherboard.vice.com/en_us/article/gykgq9/hacker-publicly-posts-data-government-hacking-group-zoopark-iran

MOTHERBOARD

PAY BACK

Hacker Publicly Posts Data Stolen From Government-Linked Cyberespionage Group

Last week, Motherboard obtained data from the so-called ZooPark hacking group, which some suspect is connected to Iran. Now the hacker responsible has seemingly dumped the information after receiving a $1,000 payment.

DARKWEBNEWS
The Ultimate Dark Web Resource

Home › Hacking › 200 Million Japanese Users' Data Sold on the Dark Web by Chinese Hackers

200 Million Japanese Users' Data Sold on the Dark Web by Chinese Hackers

By Richard

BUSINESS

Kiwis caught in global data breach could have info sold on dark web

7 Jul, 2018 12:01pm · 3 minutes to read

Instagram flaw lets hackers sell celebrities' data at $10 a pop

Hackers set up a searchable database that allows people to find contact 'o for hundreds of stars, at ten bucks per query.

BY ALFRED NG / SEPTEMBER 1, 2017 1:59 PM PDT

BBC NEWS

Nokia 'paid blackmail hackers millio

18 June 2014

US & WORLD \ TECH \ DRONES

A hacker was caught selling a stolen Air Force drone manual for $200 on the dark web

If you're in the market of selling sensitive material, why not charge more?

Anti-Malware , Breach Re

Hackers Demand $770,000 Ransom From Canadian Banks

Cybercrime: FBI Says Ransomware, Extortion Continue to Dominate

Mathew J. Schwartz (euroinfosec) • June 1, 2018 · 0 Comments

Ransom Sought in Domino's Pizza Breach

Hackers Claim Servers Breached; Customer Data Compromised

Jeffrey Roman (gen_sec) • June 16, 2014 · 0 Comments

The hacktivist group Rex Mundi is claiming it breached the servers of Domino's Pizza in France and Belgium, downloading approximately 600,000 customer records.

See Also: DevOps - Security's Big Opportunity

In a statement posted to dpaste, a text-sharing application, Rex Mundi says it was able to download customers' full names, addresses, phone numbers, e-mail addresses and passwords.

Innovations

Uber paid off their hackers — and they're far from th only ones

Hackers threaten to reveal personal data of 90,000 Canadians caught in bank hack | CBC News

'How could this happen?' victim asks as banks reveal hack of up
Hackers have threatened to release personal information for nearly 10
customers of two Canadian banks unless the lenders pay a $1-million
cbc.ca

MUST READ WHY DID MICROSOFT BUILD THE SURFACE GO?

US hospital pays $55,000 to hackers afte ransomware attack

Hancock Health paid up despite having backups available.

By Charlie Osborne for Zero Day | January 17, 2018 -- 09:53 GMT (17:53 GMT+08:00) | Topic: Security

://www.techrepublic.com/article/53-of-execs-pay-a-hackers-ransom-are-businesses-losing-the-cybersecurity-battle/

SECURITY

53% of execs pay a hacker's ransom. Are businesses losing the cybersecurity battle?

Some 69% of companies experienced a ransomware attack in the past year, which come with legal and monetary consequences, according to a Radware report.

By Alison DeNisco Rayome | June 12, 2018, 6:46 AM PST

When it Strikes

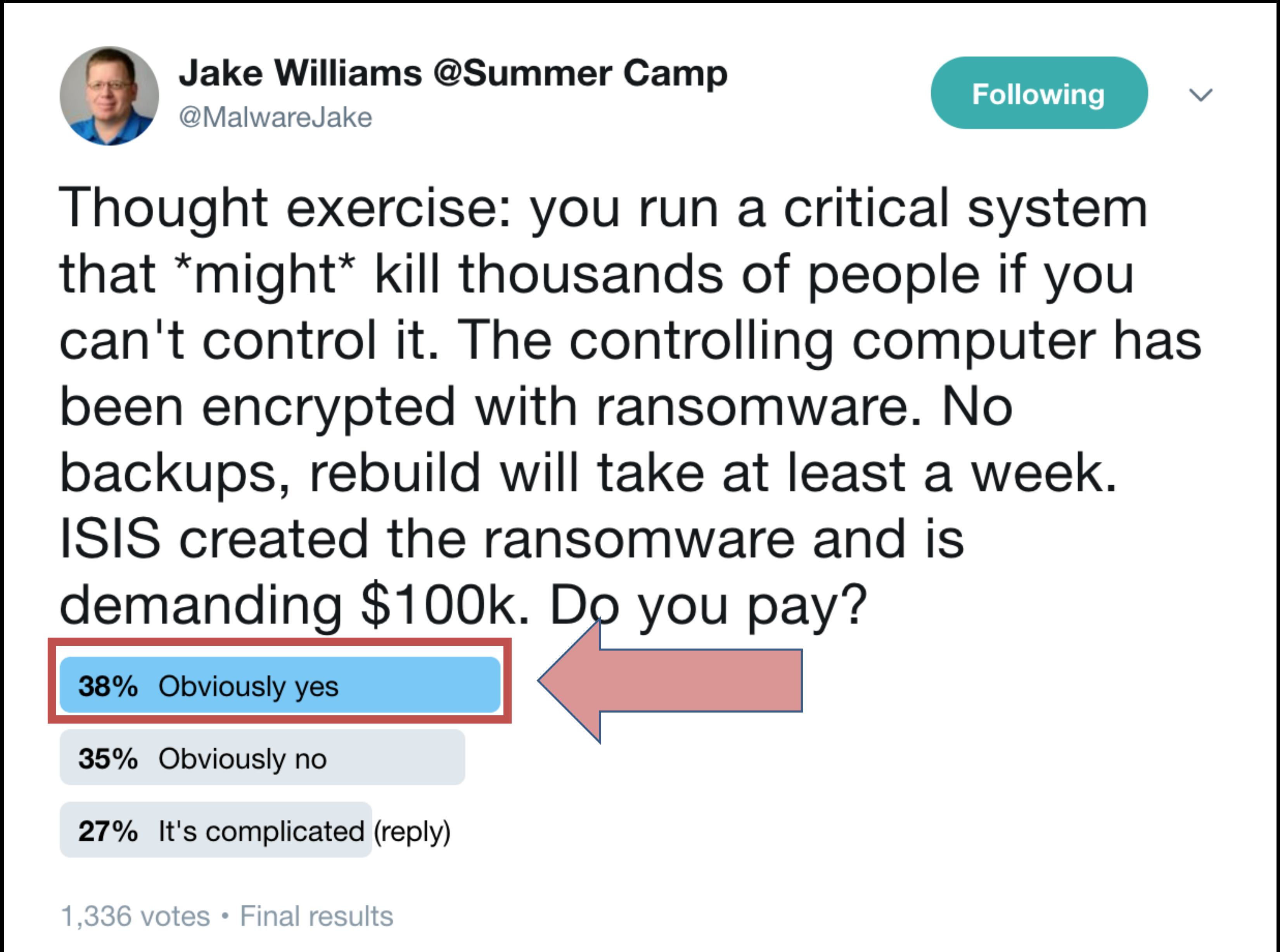
Step1 - Call a technical Expert

Step2 - Call a Lawyer

Step3 - Get a Crisis PR Firm

Questions!

How many percent of the people were in favor of paying the ransom in the survey that was done over twitter?



Jake Williams @Summer Camp
@MalwareJake

Thought exercise: you run a critical system that *might* kill thousands of people if you can't control it. The controlling computer has been encrypted with ransomware. No backups, rebuild will take at least a week. ISIS created the ransomware and is demanding $100k. Do you pay?

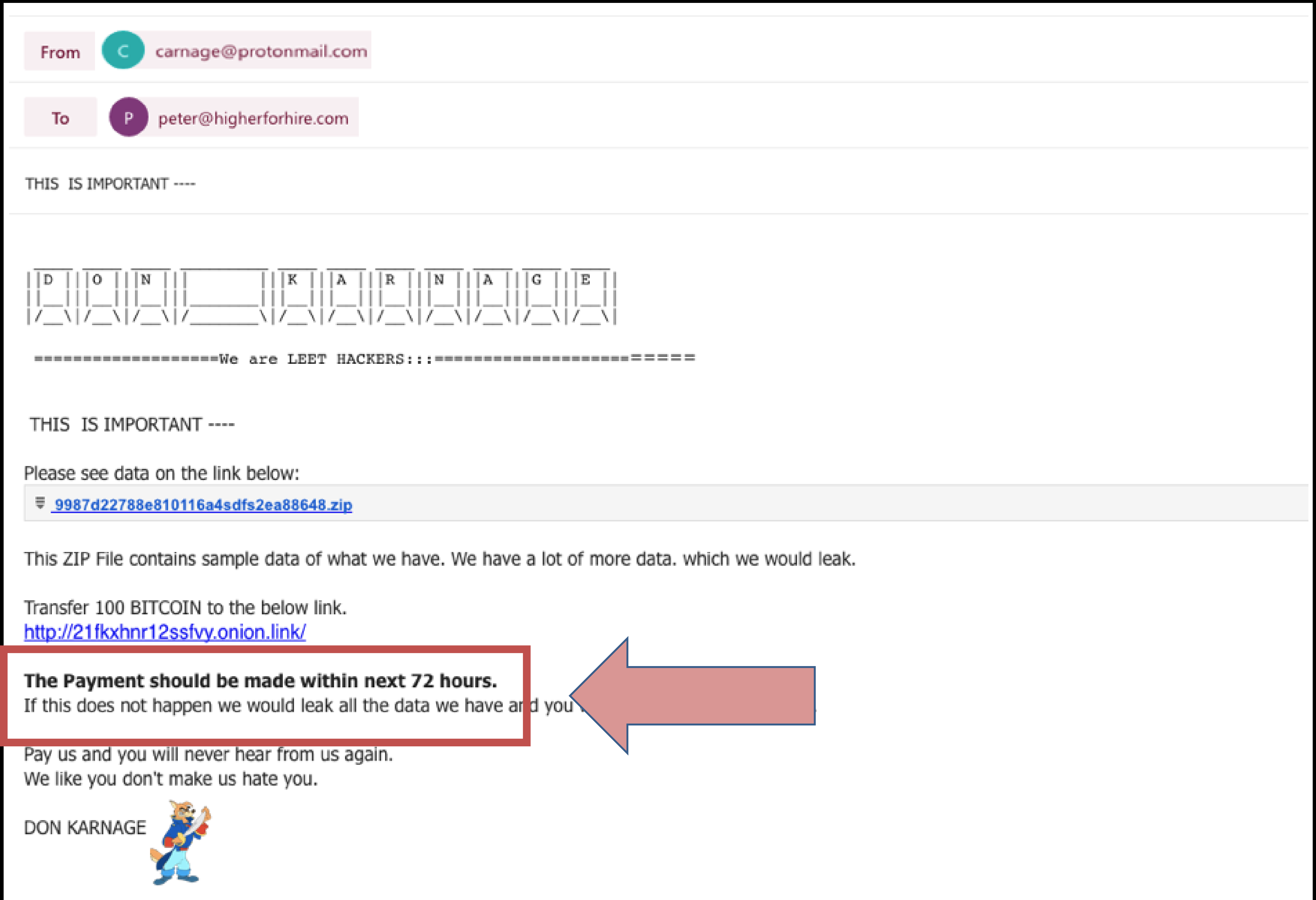
38% Obviously yes

35% Obviously no

27% It's complicated (reply)

1,336 votes • Final results

How much time did the attacker give Higher-for-Hire in the second email to pay ransom?



From carnage@protonmail.com

To peter@higherforhire.com

THIS IS IMPORTANT ----

```
 ____ ____ ____ _________ ____ ____ ____ ____ ____ ____ ____
||D ||||O ||||N ||||       ||||K ||||A ||||R ||||N ||||A ||||G ||||E ||
||__||||__||||__||||_______||||__||||__||||__||||__||||__||||__||||__||
|/__\||/__\||/__\||/_______\||/__\||/__\||/__\||/__\||/__\||/__\||/__\|

 ===================We are LEET HACKERS:::=========================
```

THIS IS IMPORTANT ----

Please see data on the link below:

9987d22788e810116a4sdfs2ea88648.zip

This ZIP File contains sample data of what we have. We have a lot of more data. which we would leak.

Transfer 100 BITCOIN to the below link.
http://21fkxhnr12ssfvy.onion.link/

The Payment should be made within next 72 hours.
If this does not happen we would leak all the data we have and you

Pay us and you will never hear from us again.
We like you don't make us hate you.

DON KARNAGE