# AIRMIC LIVE

## Responding to and costing a ransomware attack

25 November 2020

Kennedys

SubSure

# Sub*Sure*

Manufacturer for submarine parts

## What's happened?

- Hackers have accessed the IT infrastructure and detonated ransomware
- All internal and external systems are down
- All screens display a ransom note

***GREETINGS!***

CrazySnakes have left you a present AMIGOS

Pay 20 bitcoin to release your data

Bitcoin wallet:t38b1mmi93hs71bs0h2


# Insurers' 24/7 hotline

# Legal

## What is the legal team going to do for us?

- Investigate – What's happened?
- Notify ICO and Action Fraud
- Coordinate other vendors
- Advise on third party notification and general strategy
- Advise on exposures

"Do we go to our existing IT suppliers or a specialist forensics firm?

# IT Forensics

## What is the forensic team going to do for us?

- Close down vulnerability
- Assist with data restoration from backups
- Analyse scope and root cause of breach
- Look for evidence of exfiltration

# Do we communicate with the threat actors?

# PR Consultants

## What is the PR Team going to do for us?

- Manage media response (pro-active -V- reactive)
- Develop key messaging for customers and employees
- Assess stakeholder matrix
- Prepare press releases and social media announcements

# What do we say to customers and staff?

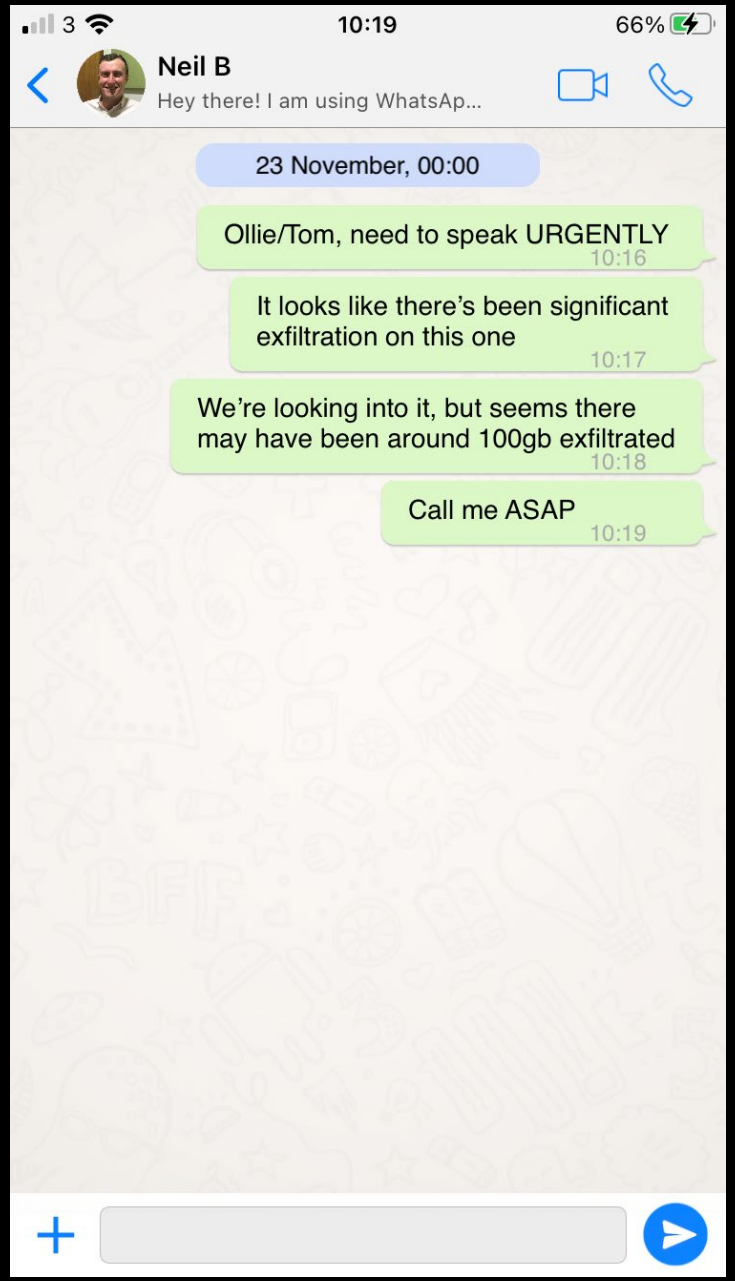
# Immediate messaging

## What are we saying to customers and employees?

- *“Experiencing some IT issues”*
- *“Working hard to restore functionality”*
- Reassuring messaging to key defence customers
- Employees – reassuring message and promise of updates

# Two days in…

- Restoration going well – 60% of systems back online
- No wider media coverage
- BUT…


3
10:19
66%
Neil B
Hey there! I am using WhatsAp...
23 November, 00:00
Ollie/Tom, need to speak URGENTLY
10:16
It looks like there's been significant exfiltration on this one
10:17
We're looking into it, but seems there may have been around 100gb exfiltrated
10:18
Call me ASAP
10:19

3 12:40 80%

# Tweet

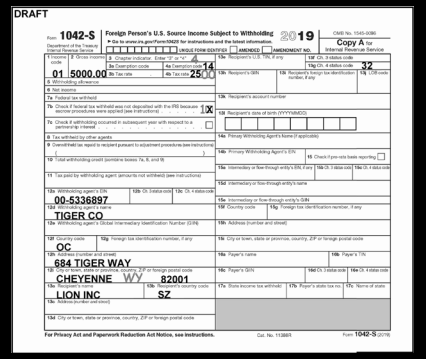
CrazySnakes$🐍

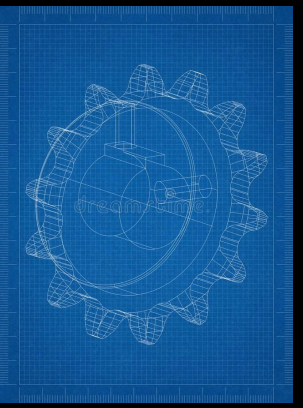
@CrazySnakes

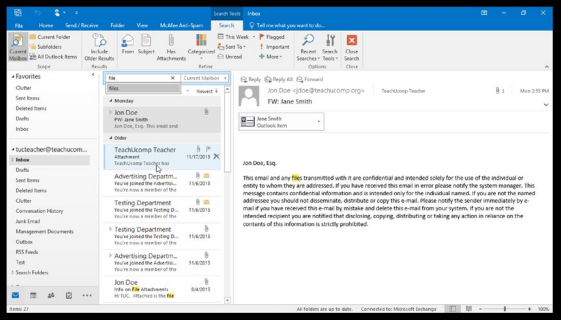
!Hacked! SUBSURE - www.subsure.com

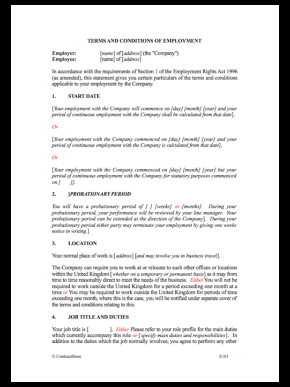
***We got the lot. Here's 5gb for FREE!!! - https://mega.nz/hins682gy5fyj53

12:39 • 02/10/2020







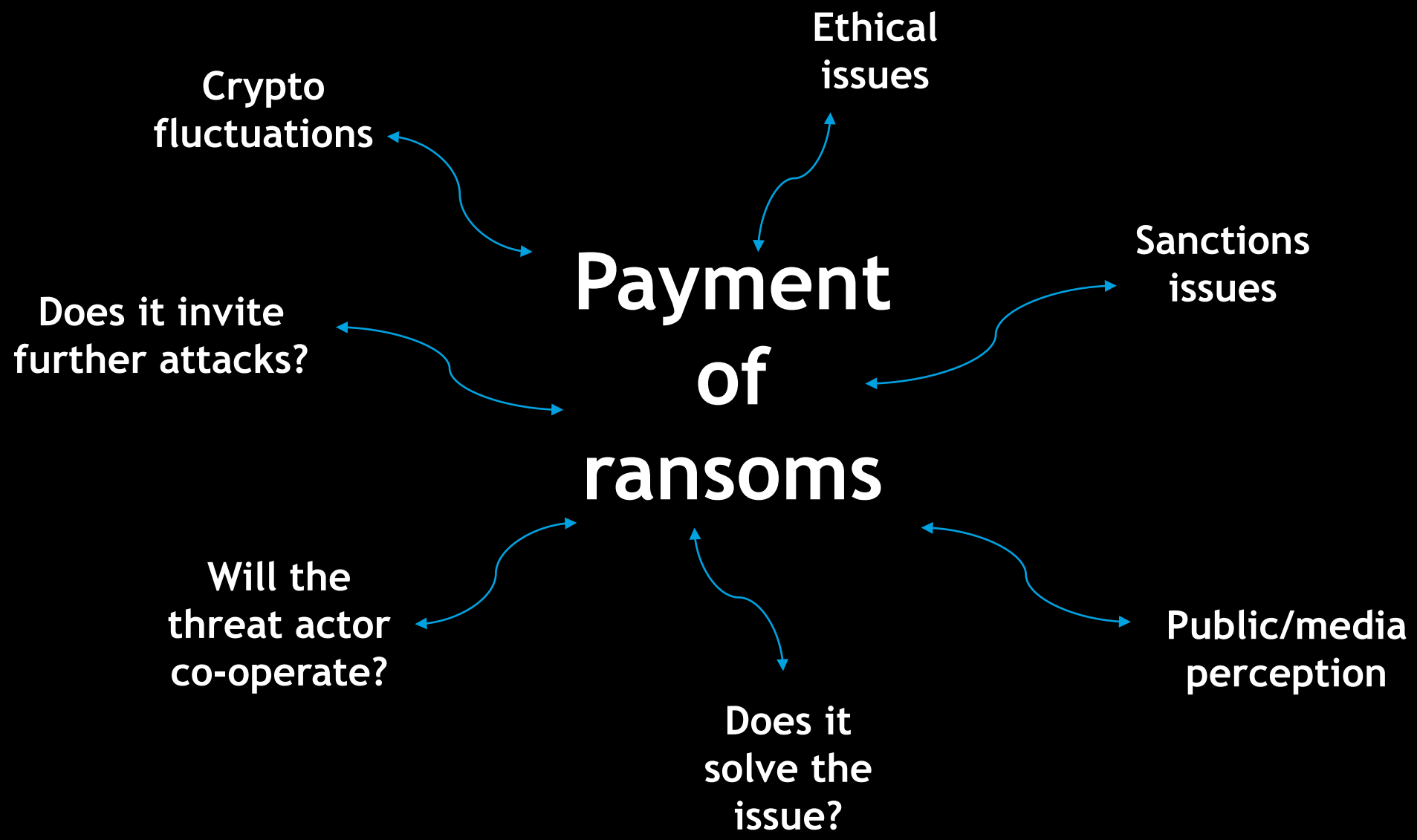

LIVE
BREAKING NEWS
MAJOR DEFENCE DATA LEAK
14:38
THOUSANDS OF SUBSURE DOCUMENTS RELEASED BY ATTACKERS

# What do we say to the media, customers and staff?

# Key Messaging

- Confirm attack and data loss
- Focus on the fact it’s a criminal act
- We are investigating with a team of experts and engaging with the Police and regulators
- We will be communicating with any affected individuals and customers
- Cannot comment further at this time
- Follow up with an immediate message to customers and staff

# Should we pay the ransom?


Payment of ransoms
Ethical issues
Crypto fluctuations
Sanctions issues
Does it invite further attacks?
Will the threat actor co-operate?
Does it solve the issue?
Public/media perception

# “How much is this going to cost us?

SubSure CEO

# Potential exposures

- Fees of response team - £200,000+
- Ransom payment – 20 BTC = £280,000
- Third party/customer/employee claims – 
- Business interruption and lost contracts
- Regulator fines
- Hidden notification costs

£1m+

# Key Contacts

**Tom Pelham**
Partner
Kennedys
07818 573 330
Tom.Pelham@kennedyslaw.com

**Ollie Dent**
Partner
Kennedys
07584 391 370
Ollie.Dent@kennedyslaw.com


**Want to know more?**