Breach Workshop
Data Center Breach

Nadi, Fiji
Adli Wahid adli@apnic.net
2020

FIRST

Copyright

Self Introduction

Adli Wahid
Senior Internet Security Specialist @ APNIC

Previously
- Bank of Tokyo Mitsubishi-UFJ (MUFG-CERT)
- Malaysia Computer Emergency Response Team (MYCERT)

Let's connect!
- Twitter: @adliwahid
- LinkedIn: Adli Wahid
- Unsplash: https://www.unsplash.com/adliwahid

Why are we doing this?

What is it like to have a security incident?

Apply what we learn/know

Key words from the plenary session:

- Dry Run
- Prepare
- Learn from case study/experience
- Recovery speed
- Deal with exceptions

Dealing with an Incident

All the ‘technical stuff’

And also

- Coordination
- Priorities
- Communication
- Recovery
- Collaboration
- Context (i.e. legal, reputation, safety)

Workshop Progress

Table Top: General Rules of Engagement

You will be wearing multiple hats

No right or wrong answer but need may need to elaborate

Ask moderator/facilitator to clarify if needed

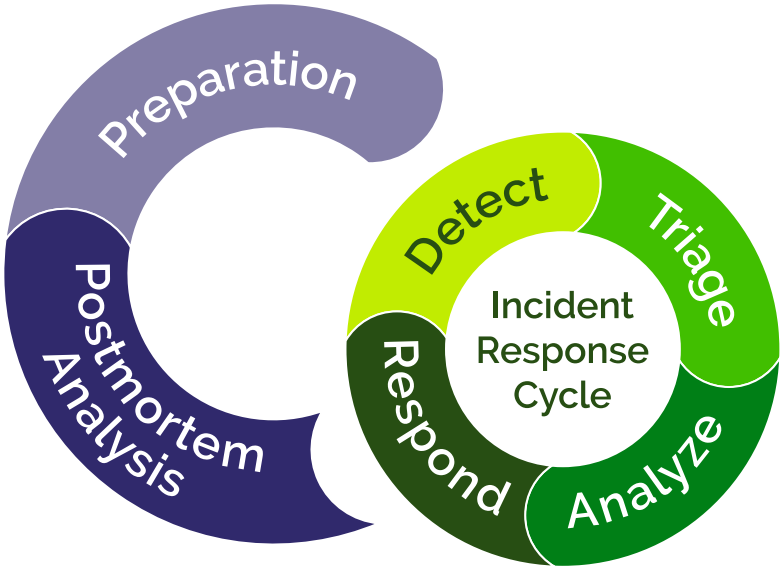
Additional Notes

This is based on a real incident (2017)

Incident response framework:
Fast forward to an incident

Before we start let's have a look at the...

Incident Management



Welcome to the Kingdom of Mahi-Mahi

- Small Island Nation in the Pacific
- 150k population
- Main source on income is Tourism, Fish, and Tech industry
- Mahi-mahi CERT was just established 6 months ago. Thinking about joining PacSON and APCERT
- National election is around the corner
- Central bank recently made it illegal for citizens to own or use bitcoin and other forms of crypto-currency

Rocket Science Hosting

- The premier web hosting company in Mahi-Mahi
- Earlier in the year, awarded contract to host all government websites & applications
- They also have non-government, private sector customers – banks, hotels, and other SMEs
- Currently have 20 staff, including 5 non-tech administrative staff (legal, Marketing, HR)
- CEO is a family member of the current Prime Minister

Day 1:
Screenshot
sent to CEO

Warning!!
Your documents and important files have been encrypted
If you modify any file, it may cause damage
To decrypt your file please go to the following website:

Please download and install TOR browser
7fv4vg4n26cxl337.onion/purchase?mid=XXFJWEUXDKDJWEJXJW
7fv4vg4n26cxl337.onion.to/purchase?mid=XXFJWEUXDKDJWEJXJW
fv4vg4n26cxl337.onion.nu/purchase?mid=XXFJWEUXDKDJWEJXJW
7fv4vg4n26cl337.hiddenservice.net//purchase?mid=XXFJWEUXDKDJWEJXJW
7fv4vg4n26cl337.gbe0.top/purchase?mid=XXFJWEUXDKDJWEJXJW

Please download and install TOR browser
Machine ID: XXFJWEUXDKDJWEJXJW

7fv4vg4n26cxl337.onion/purchase?mid=XXFJWEUXDKDJWEJXJW

Your files are still encrypted and will be deleted in 72 Hours

Here are your options:

1. Pay via bitcoin – to buy decryption key you will need some bitcoins.
   Bitcoin is a currency, just like dollars and euros but entirely on Internet
2. Get a wallet – you need wallet to hold your coins. We suggest https://blockchain.info
3. Buy Some Bitcoins – depending on your country you can buy bitcoins using various ways (paypal, credit card, cash). We suggest https://localbitcoins.com because you can buy directly from people
4. Payment: You need 1 bitcoin (BTC) for this machine and send them to: 12hBxZl3373LgT3SjCsSl337tVefPBWCPt. The process can take up to 24 hours for us to check the payment. Then you will receive the key and link to the decryption program

Date: 6 November 2019 07:30
From: Sysadmin On Duty
To: Sysadmin Group
Cc: CEO
Subject: Systems Encrypted

Dear all,

We have a problem. We found ransom notes on 55 servers.
Some folders (i.e. /var/www/) and files are encrypted.
All of those are government related websites.

I think we need a meeting. More updates soon!

T.C

Date: 6 November 2019 0800
From: Sysadmin2
To: Sysadmin Group
Cc: CEO
Subject: Update (Was Re: Systems Encrypted)

Update – I'll be brief. 100 servers encrypted all are government customers. Backups are also encrypted. Looks like ransomware attack. More than 300 websites & applications are involved. Attacker is asking 1BTC per server.

Please advise.

Group Discussion

rocket science hosting

Role: Internal Staff & CEO

Potential Questions

1. What is the impact of this incident?
2. What should be done?
3. Who should be in charge?
4. What are the tasks that should be prioritize?
5. Do we need to contact anyone else?

Date: 6 November 2019 1000
From: Sys Admin – Prime Ministers Office
To: CEO Rocket Science Hosting
Subject: Government website down

We noticed that our e-government portal has been inaccessible since 0200 on 6/11/2019.

This is disrupting a lot of services and access to the public. Kindly advise!

Sysadmin PMO

Group Tasks

rocket science hosting

Write a note to affected customers

Prepare for a meeting with Government

Day 2

Mahi Mahi Daily News

6 November 2019 (11:59 PM)

Rocket Science Hosting Held at Ransom Might be Political related

We have learned that Rocket Science Hosting, the premiere hosting company in Mahi Mahi is under attack. An un-named source said that 250 servers are held are ransom and the unknown attacker is demanding 2 million USD. It is also learned that this might be politically related as the CEO is a family member of the current Prime Minister.

The CEO of Rocket Science Hosting is unavailable for comments, despite multiple attempts by our reporter communicate with the company.

Group Tasks

rocket science hosting

Prepare a written media release to be distributed to the media

Give an update to customers on the current progress

Prepare the CEO for a phone interview with the Mahi Mahi Daily News Reporter

What else should we do?

Time to vote!

Date: 7 November 2019 0900
From: Mahi-Mahi CERT
To: Security @ RocketScience Hosting
Subject: Ransomware Analysis

Dear Security Administrator,
Our team was not able to decrypt the ransomware you shared with us. We have also asked other partners and international CERTs to assist us. An AV company told us that malware is a variant of an known ransomware. As per our previous advisory on ransomware, we strongly advise that you do not pay the attacker.
We also suspect that attackers were able to compromise the server via a vulnerable Joomla installation, then install a webshell. Also since all of your installations are using 2.6 kernel, there's possibility of a local privilege escalation that enables attacker to become root.
Let us know if you need us to do anything else.

Have a safe day!

Date: 7 November 2019
From: Ransomware Crew @ secure_email_provider
To: CEO Rocket Science Hosting
Subject: Wanna Negotiate?

Hi,

We notice 100 of your servers are encrypted. Price is 1BTC per server.
We know you are government backed and can raise the money.
Please pay as soon as possible.

Time is running out!

Group Task: Meeting with Government, National CERT and other customers

Role: Rocket Science Team vs Stakeholders

- Ask for help to government to raise funds.
- Get advise about negotiating with attacker.
- Ask for exception in using BTC to pay attacker.

Group Discussion

rocket science hosting

Role: Rocket Science Internal meeting

- Pending issues:
- Security & Technical Updates
- Other plans
- Pending items?
- Final Decision – Pay or Not Pay

Pay or not pay?

Day 3:
Pay

Date: 7 November 2019
From: Ransomware Crew @ secure_email_provider
To: CEO Rocket Science Hosting
Subject: Re: Wanna Negotiate?

Dear CEO,

We accept your offer to pay us 50 BTC in 2 installation.
Please make the first payment of 25 BIT coins.

Day 3:
Not Pay

All files deleted
on 100 servers

Group Task

rocket science hosting

Prepare update to customers based on your decision (Pay or Not Pay)

Wrap up – Group Discussion

rocket science hosting

KINGDOM OF MAHI MAHI

CERT

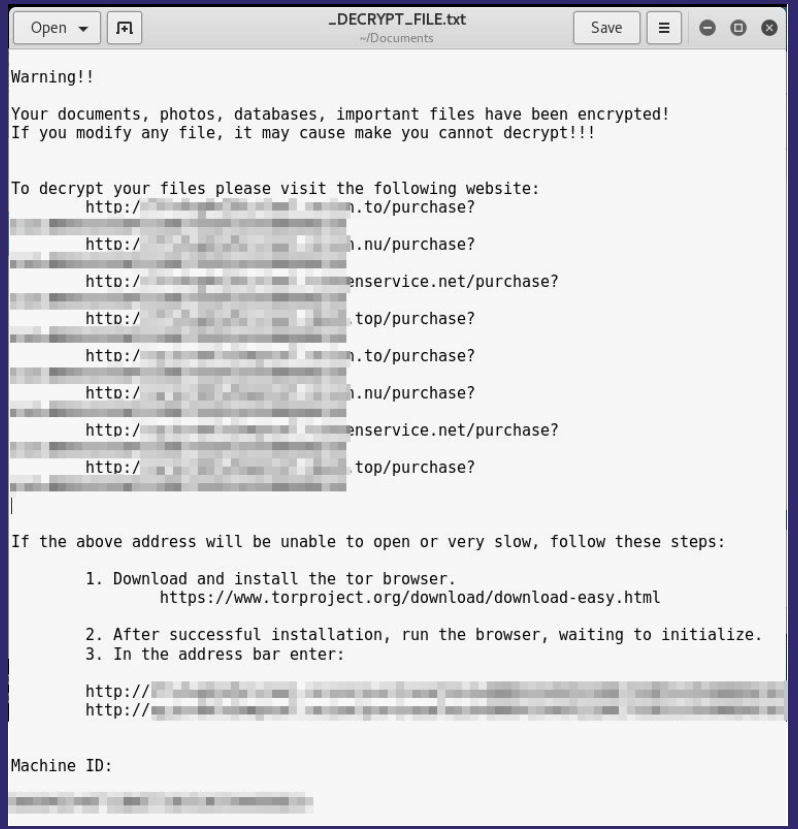
Mahi Mahi Daily News

Prepare update to customers based on your decision (Pay or Not Pay)

Background of TTX

Real Incident

- Nayana Web Hosting in KR
- Ransomware is called Erebus: Only known to infect Windows Previously
- 153 Linux servers: More than 3000 websites
- Initially asked for 550 BTC
- Incident Started on June 10th: Sent notices on customer portal (public) on the 12th
- Negotiated and paid on 14th: 397 BTC
- Tried to raised funds by selling shares to company that wanted to acquire them



Notice on June 12 2017

We will inform you about the current situation.
Currently, all employees of Internet Nayana Co., Ltd. are in the process of responding to customers who have requested a consultation.

Using the backup file you send
Restoration settings are in progress on a new server that does not have ransomware.
We are also changing index pages that have been tampered with ransomware to parking pages.

We are working to secure loans and funds to recover ransomware costs.
We are discussing with the Korea Hosting Domain Association which companies that can manage the consignment and takeover of web hosting and server hosting that are not infected with ransomware.

We are doing our best to protect your interests.

We are in ongoing negotiations with the hackers and announce the full text of our response.

Notice on 12th part 2

My boss tell me, your buy many machine, give you good price 550 BTC
If you do not havce enough money, you need make a loan

You company have 40+ employees,
every employees's annual salary $30,000
all employees 30,000*40 = $1,200,000
all server 550BTC = $1,620,000

If you can't pay that, you should go bankrupt.
But you need to face your childs, wife, customers and employees.
Also your will lost your reputation, business.
You will get many more lawsuits.

We will post notice from time to time about the current situation.

Note on 14th

Last contact with a hacker last night.

Hello, I'm CEO.
Now I'm broke.
Everything I've worked hard for 20 years is expected to disappear by 12 o'clock tomorrow.
I don't know how satisfied you are
I can't make money
All my money in a hurry
It's Hanwha 400 million won (123bit) I can't negotiate better with you.
I wish you had the 550bit you wanted. If I have that money I
Trust me and trust me
I could save many people's data
Is now exposed to news and media
Nobody wants to buy a company
There is no money available anymore.
Who would lend me money knowing this company's situation?

Take-aways from today

References

- http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=127928
- http://www.ajudaily.com/view/20170612145809915
- https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/
- https://www.bleepingcomputer.com/news/security/south-korean-web-hosting-provider-pays-1-million-in-ransomware-demand/
- https://www.zdnet.com/article/korean-web-host-hands-over-1-billion-won-to-ransomware-crooks/

Analysis

- https://asec.ahnlab.com/1068
- https://medium.com/@jongmin.kim/%EC%9B%B9-%ED%98%B8%EC%8A%A4%ED%8C%85-%EC%97%85%EC%B2%B4%EB%A5%BC-%EA%B0%90%EC%97%BC%EC%8B%9C%ED%82%A8-erebus-%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4%EC%97%90-%EA%B4%80%ED%95%9C-%EC%A1%B0%EC%82%AC-4f4574f1aca0