

CYBER SECURITY INCIDENT RESPONSE

AN ISLAND STATE CASE STUDY APNIC 52



OUTLINE

- Introduction / Background
- CERT Vanuatu
- Types of Incidents
- Methods Use to Mitigate
- Final Remarks

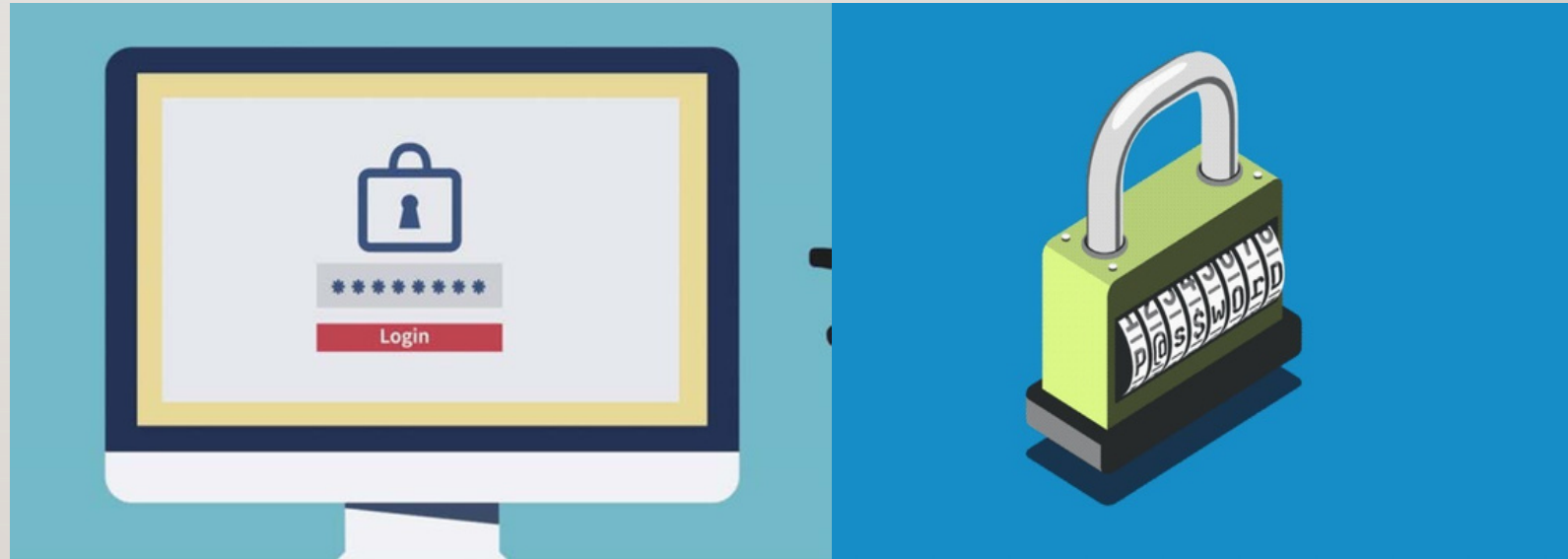


WHAT IS CYBER SECURITY?

- Cyber security is the practice of defending:

- Computers,
- Servers,
- Mobile devices,
- Electronic systems,
- Networks, and
- Data

from malicious attacks.



BACKGROUND -VANUATU'S PAST & CURRENT CYBER SECURITY CONTEXT

PAST Context:

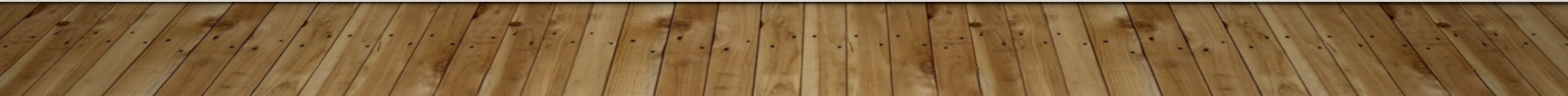
Nationally, we had no clue at all about cyber security nor cyber-attacks i.e. all cyber-attacks were ordinary traditional computer issues that were addressed by systems and hardware technicians.

BACKGROUND -VANUATU'S PAST & CURRENT CYBER SECURITY CONTEXT

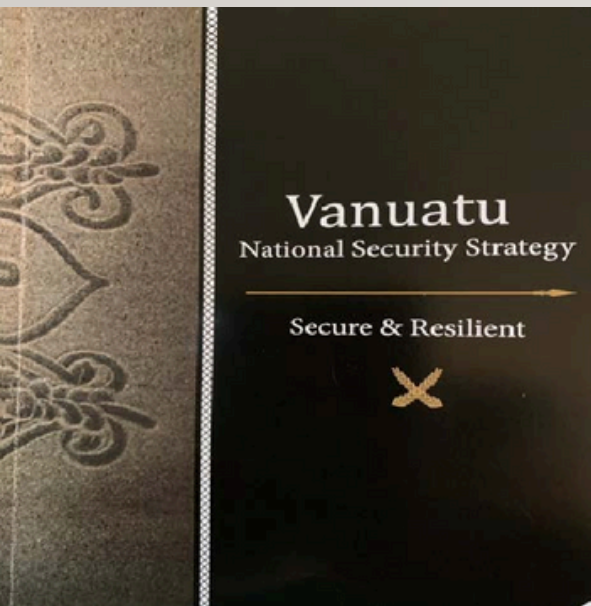
CURRENT Context:

Nationally, we are educating our citizens, business houses on what Cyber Security is and why it is important.

We can now distinguish between a traditional hardware / software problem on a computer versus a cyber-attack on a computer system.



vThe Vanuatu National Cyber Security Strategy of 2030 and



TYPES OF CYBER-ATTACKS/THREATS

- Malware Attacks (e.g. Virus)
- Social Engineering Attacks
- Phishing Attacks
- Insider Threats
- Misinformation
- Pornography
- Identity-related Crime
(e.g. Fake IDs)



CASE STUDY

2nd March 2021: 14:00hrs

- q Compromise event entered into our GBN and Systems.
- q Malware Attack with stealth behavior with remote access capabilities

3rd March 2021: 04:00hrs

- q All Government online web presence were taken down and defaced


CASE STUDY

3rd March 2021: 06:00hrs

Detection Phase:

- q Systems and Security Team (CERTVU and OGCIO) have identified that our systems were compromised and all *.gov.vu websites are down and defaced

zone-h.org/archive/ip=103.7.197.89?hz=2



Home News Events Archive Archive ★ Onhold Notify Stats Register Login search...

[ENABLE FILTERS]

Total notifications: 19 of which 1 single ip and 18 mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★ Domain	OS	View
2021/03/03	s49_hack		M			★ police.gov.vu/index.HTM	Linux	mirror
2021/03/03	s49_hack	H	M			★ ombudsman.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M			★ immigration.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M			★ moh.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M			★ malffb.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M	R		★ doe.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M			★ fisheries.gov.vu	Linux	mirror
2021/03/03	s49_hack		M			★ mol.gov.vu/index.HTM	Linux	mirror
2021/03/03	s49_hack	H	M			★ revenue.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M			★ forestry.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M			★ parliament.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M			★ cert.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M			★ ictdays.gov.vu	Linux	mirror
2021/03/03	s49_hack	H	M			★ covid19.gov.vu	Linux	mirror
2021/03/02	s49_hack	H	M	R		★ customs.inlandrevenue.gov.vu	Linux	mirror
2021/03/02	s49_hack	H	M	R		★ psc.gov.vu	Linux	mirror
2021/03/02	s49_hack	H	M			www.univ.edu.vu	Linux	mirror
2021/03/02	s49_hack	H	M	R		★ vnso.gov.vu	Linux	mirror
2021/03/02	s49_hack	H	R			★ www.gov.vu	Linux	mirror

1

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

CASE STUDY

3rd March 2021: 06:00hrs

Detection Phase:

- q Systems and Security Team (CERTVU and OGCIO) have identified that our systems were compromised and all *.gov.vu websites are down and defaced

Attack Type/Method

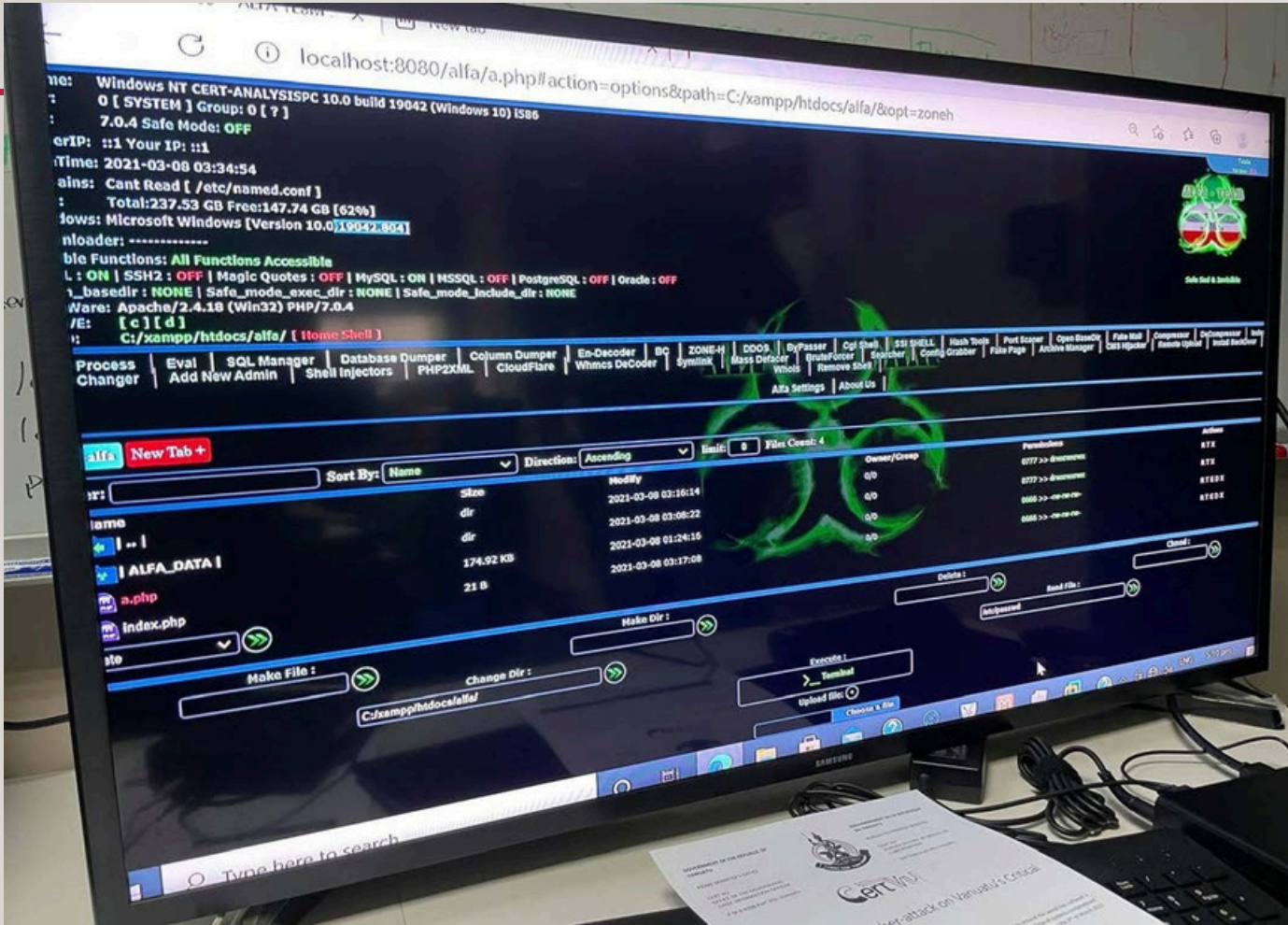
q **Malware Payload:**

**-ALFA Team's Web
Shell Malware Tool
q-"a.php" file**

**-directory: ..\....
Reg\.....\uploads\a.php**

CASE STUDY

3rd March
2021:
08:00hrs



Attack Type/Method

qMalware Payload:

-ALFA Team's Web Shell Malware Tool

-directory: ..\....
Reg\.....\uploads\a.php

CASE STUDY

3rd March 2021: 08:00hrs (official working hours begin)

Concurrent Events:

Planning

- q All proactive communications and collaboration between OGCIO's Systems and CERTVU team are executing the Cyber incident Triage phase remotely and online using Social Media chat groups;

CASE STUDY

3rd March 2021: 08:00hrs (official working hours begin)

Concurrent Events:

Developing a Incident Press Report (For superiors & Media)

- q All proactive communications and collaboration between OGCIO's Systems, CERTVU team and the CIO/DCIO
- q Seek approval for a Media Press Report to critical organizations/agencies affected

CASE STUDY

3rd March 2021: 08:30hrs
(official working hours begin)

Concurrent Events:

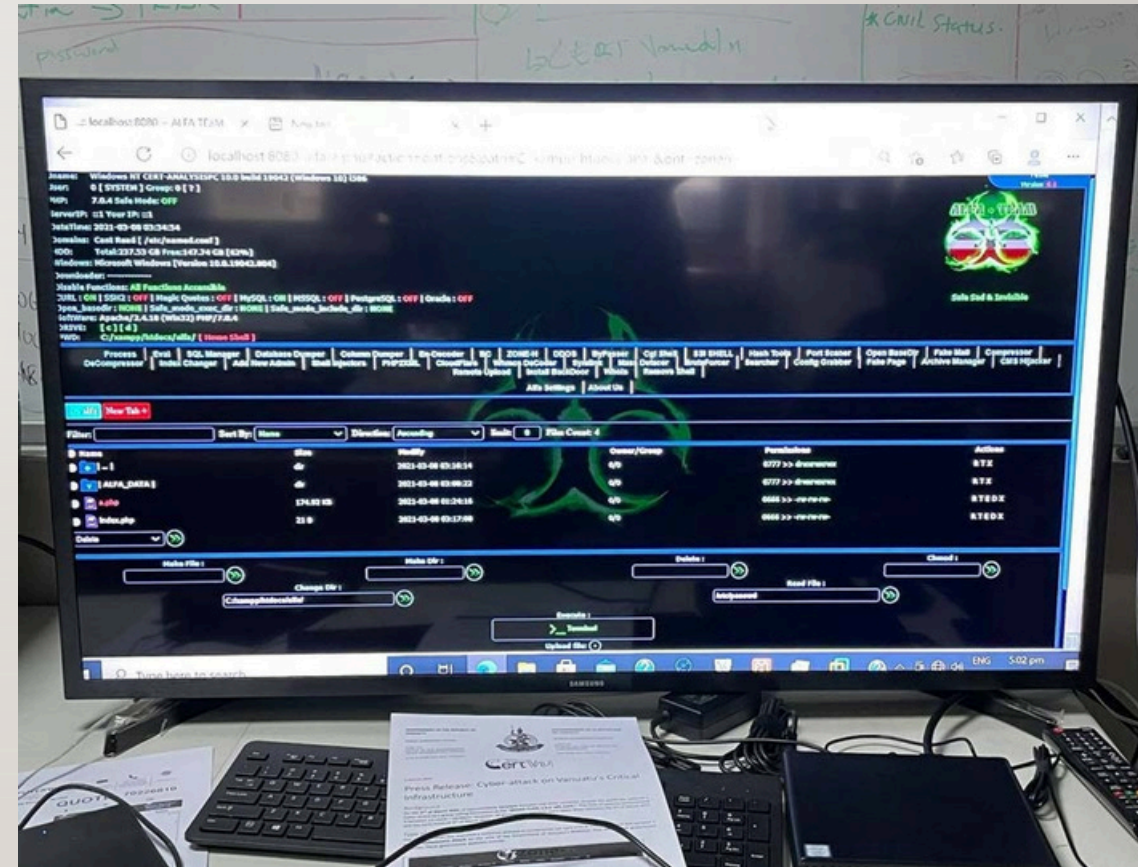
What we knew:

Point of Entry –How?

q **V***Reg –gov dept.**

Web App platform

q **Via –the Upload
feature.**



CASE STUDY

3rd March 2021: 08:30hrs (official working hours begin)

Concurrent Events:

What we knew:

Point of Entry –How?

- q **V***Reg –gov dept.**
- Web App platform**
- q **Via –the Upload feature.**

Redundant Backdoor

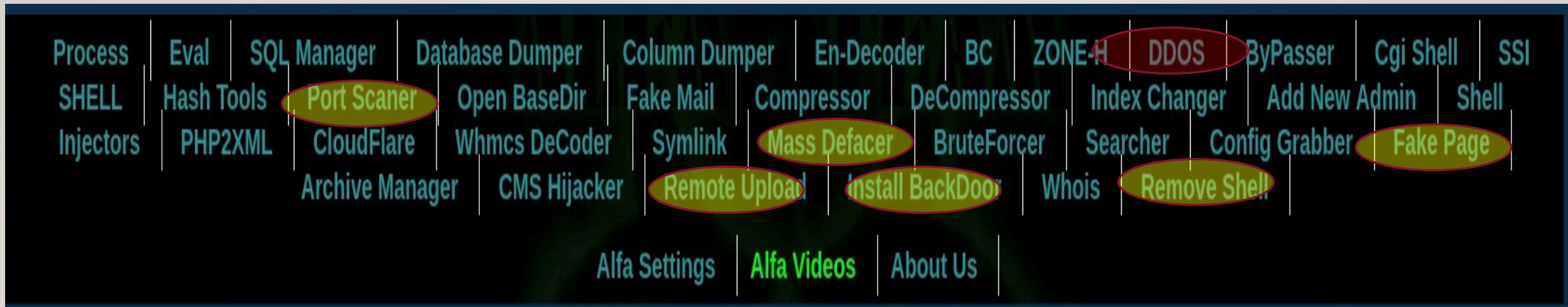
- q **Via the another gov Website**
- q **a “a.php” file was place in the web directory as well.**

CASE STUDY

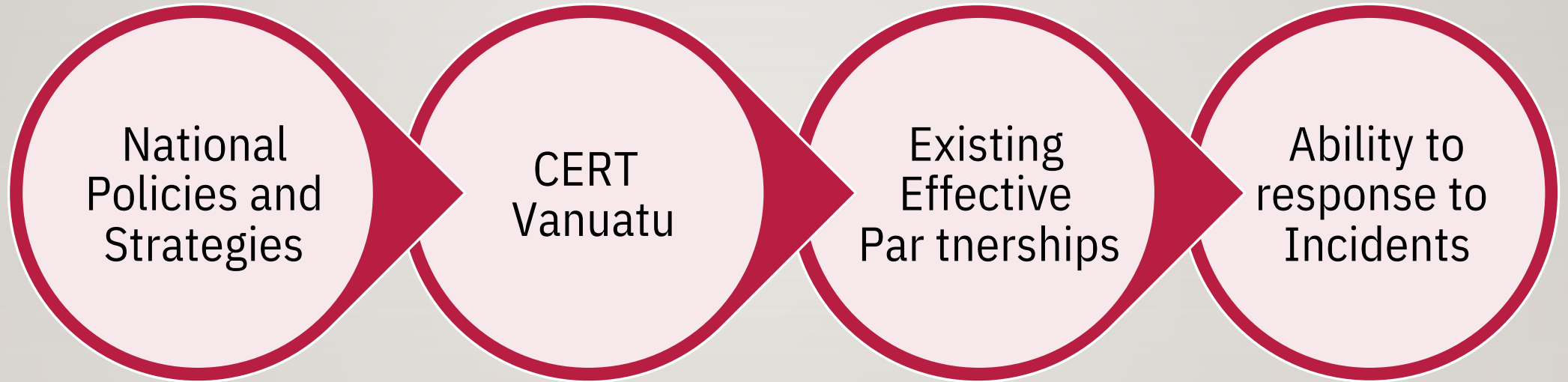
3rd March 2021: 08:30hrs

Malware Web shell was identified.

- q Removed, back-door payload was sandboxed, removed, blocked
- q All critical GBN systems were restored back online.



LESSON LEARNT



FINAL REMARKS

