ccNSO

News Session #2

BOCRA

Domain Abuse

.bw ccTLD

27 MAY 2021

Outline

BOCRA

Introduction

Background on .bw

Common Abuse Trends

Phishing

Malware

Fraudulent Content - Defacements

Countermeasures & Challenges

Active Monitoring & Takedowns

Collaboration with CIRT

Awareness

Policy Review and Regulation

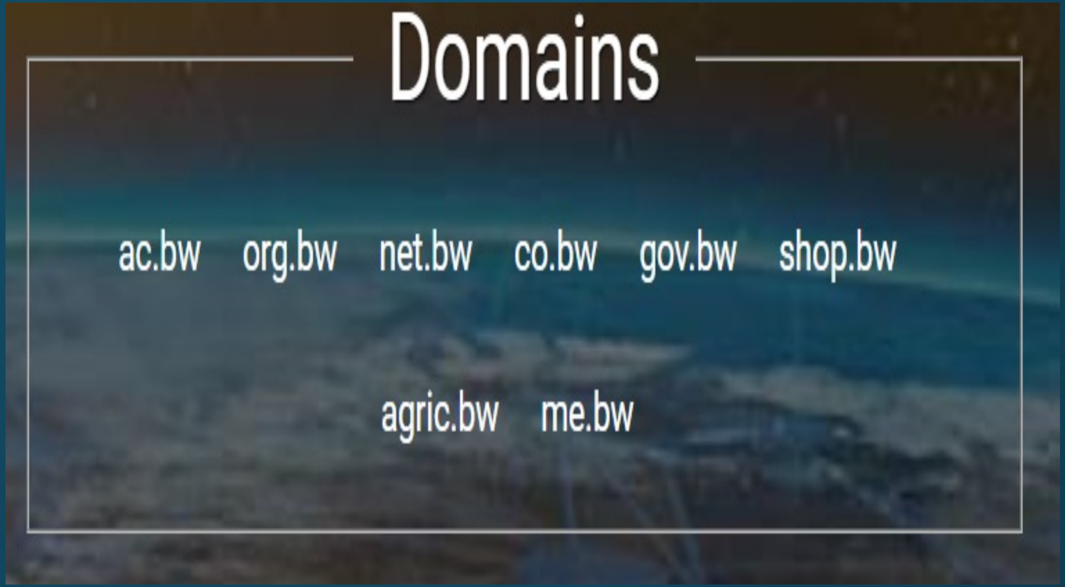
Summary

Lessons learnt & Recommendations

BOCRA

Background of .bw

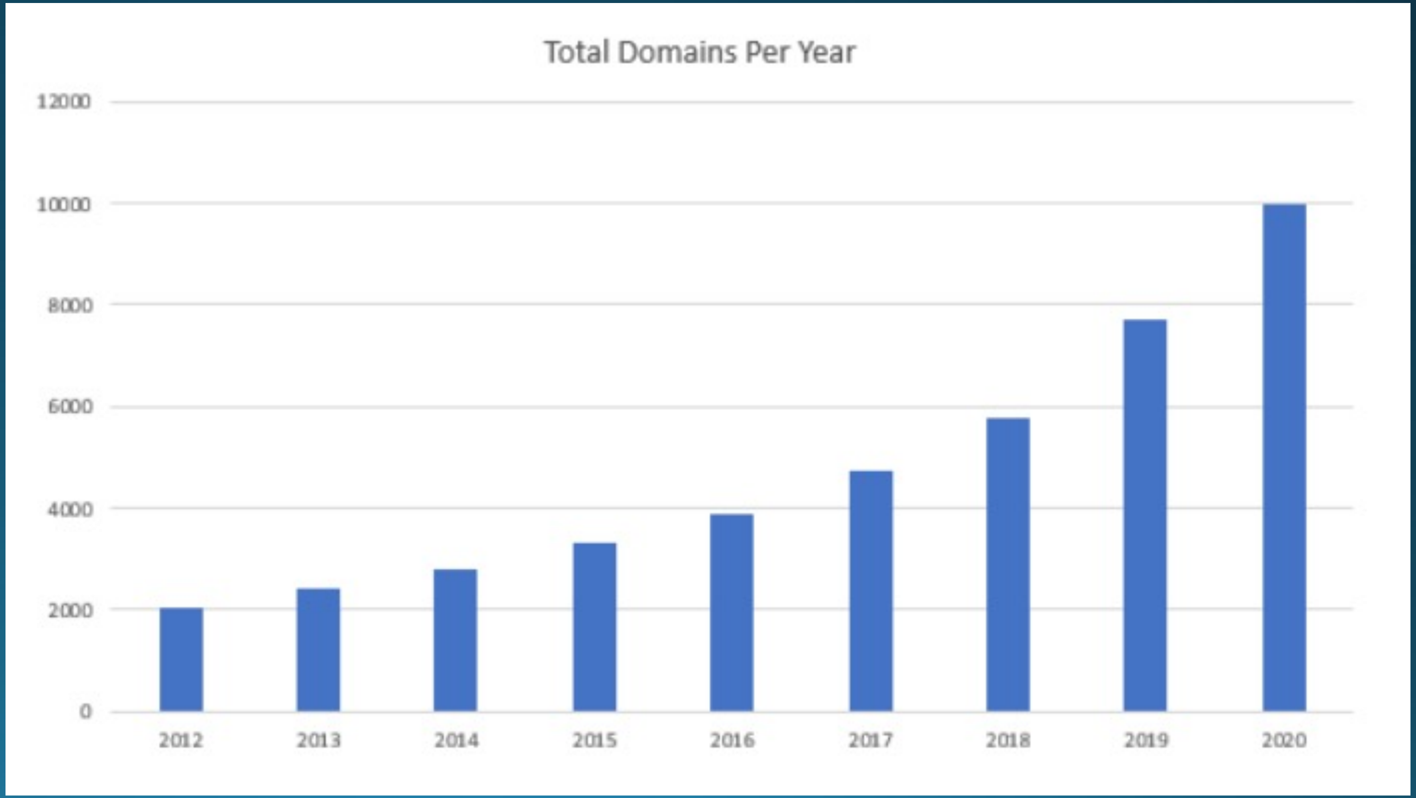
- redelegation process started in 2012 May and was completed in 2013.
- 10,000+ domains, co.bw leading the numbers
- 70+ accredited Registrars, 11 are International
- 3 – R model
- Operates on a Government model of governance (Regulator)



Domains

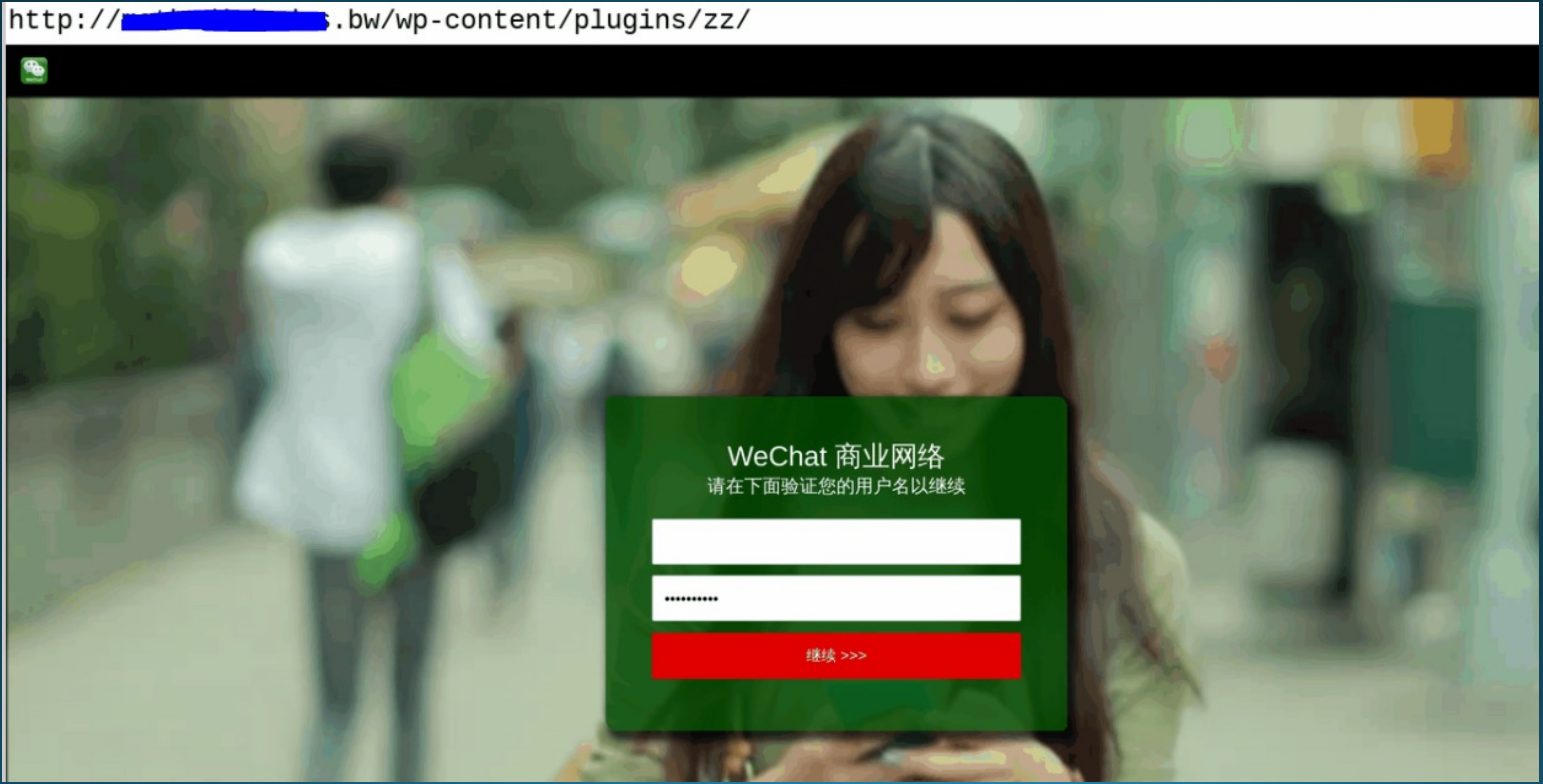
ac.bw org.bw net.bw co.bw gov.bw shop.bw

agric.bw me.bw



Abuse Trends

Phishing Attacks



http://[redacted].bw/wp-content/plugins/zz/

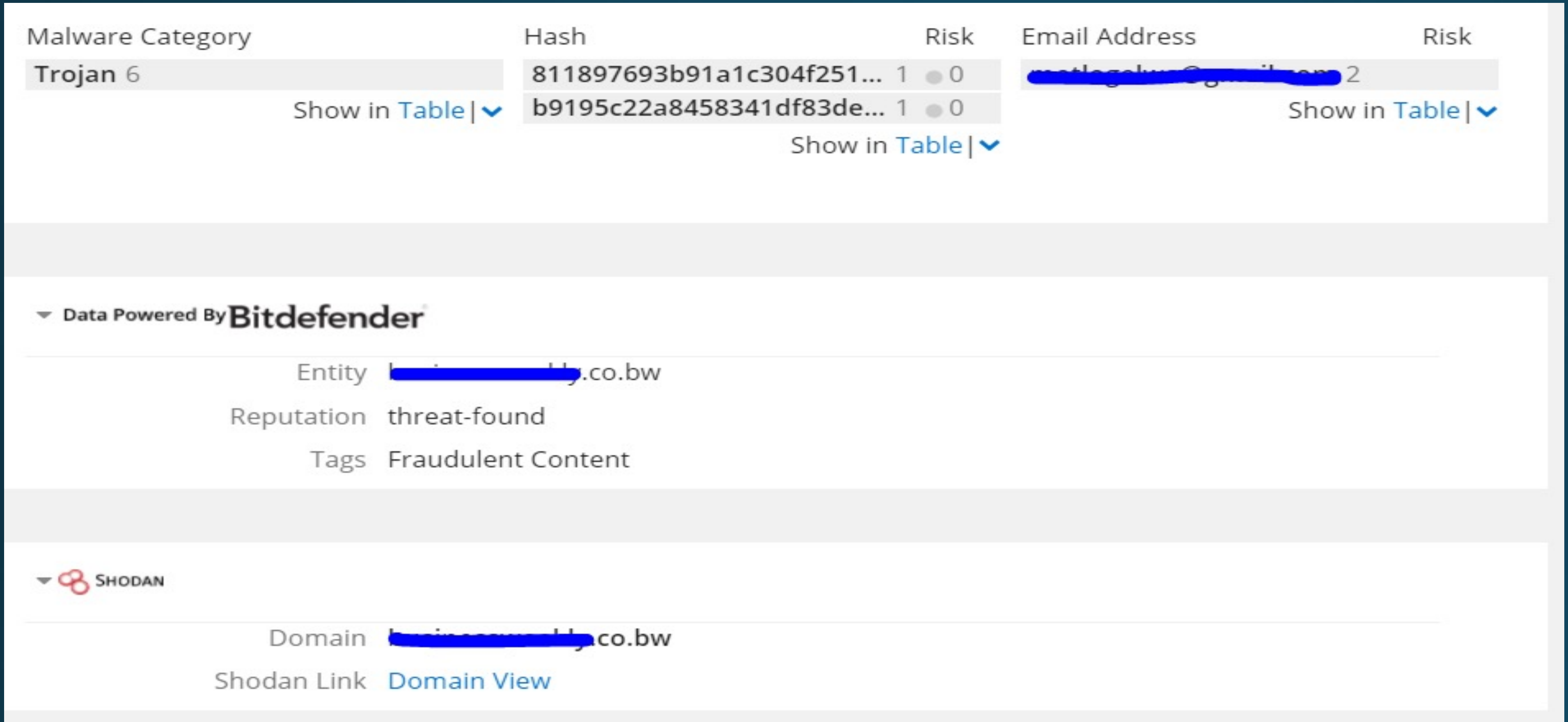
WeChat 商业网络

请在下面验证您的用户名以继续

•••••••••••

BOCRA

Malware



Malware Category	
Trojan	6

Show in Table |

Hash	Risk	
811897693b91a1c304f251...	1	● 0
b9195c22a8458341df83de...	1	● 0

Show in Table |

Email Address	Risk
[redacted]	2

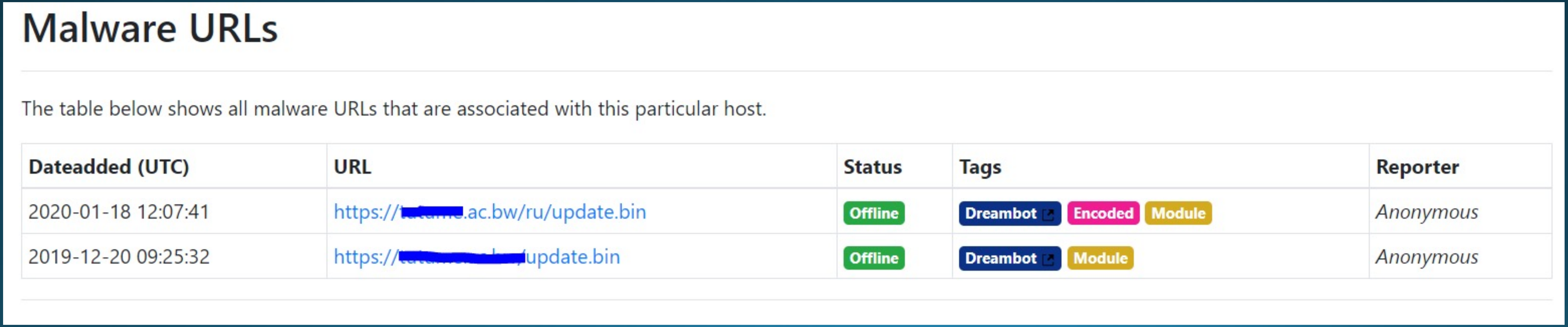
Show in Table |

Data Powered By Bitdefender

Entity	[redacted].co.bw
Reputation	threat-found
Tags	Fraudulent Content

SHODAN

Domain	[redacted]co.bw
Shodan Link	Domain View

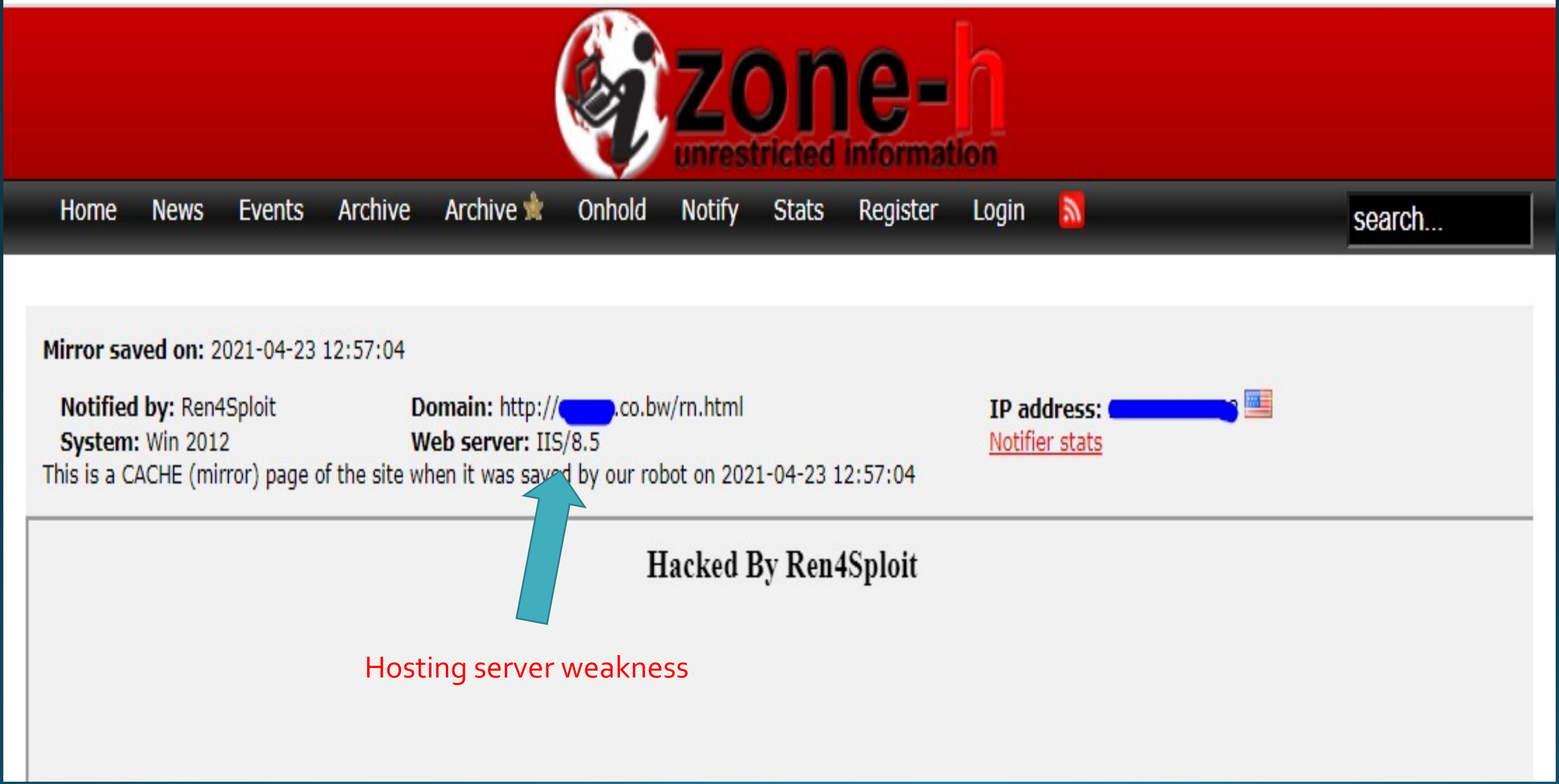


Malware URLs

The table below shows all malware URLs that are associated with this particular host.

Dateadded (UTC)	URL	Status	Tags	Reporter
2020-01-18 12:07:41	https://[redacted].ac.bw/ru/update.bin	Offline	Dreambot Encoded Module	*Anonymous*
2019-12-20 09:25:32	https://[redacted]update.bin	Offline	Dreambot Module	*Anonymous*

Defacements



Mirror saved on: 2021-04-23 12:57:04

Notified by: Ren4Sploit
System: Win 2012

Domain: http://[redacted].co.bw/rn.html
Web server: IIS/8.5

IP address: [redacted]
Notifier stats

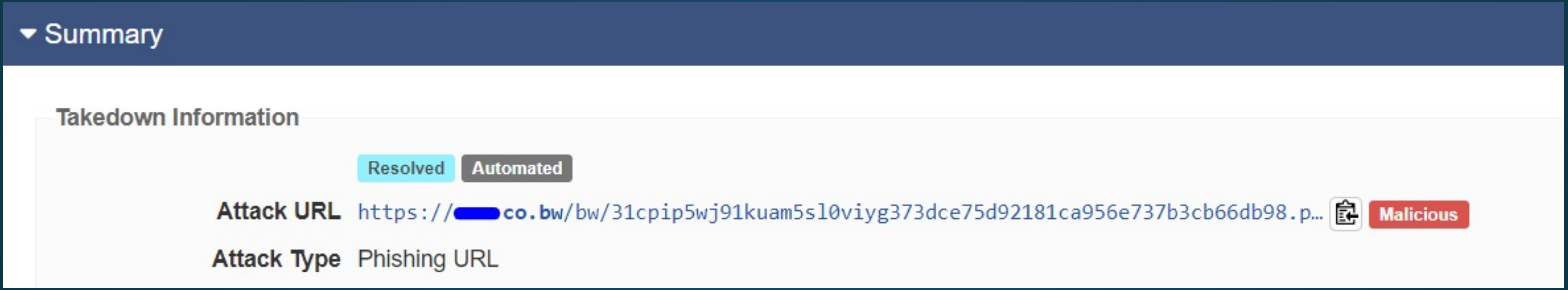
This is a CACHE (mirror) page of the site when it was saved by our robot on 2021-04-23 12:57:04

Hacked By Ren4Sploit

Hosting server weakness

Countermeasures

Active Monitoring & Takedowns



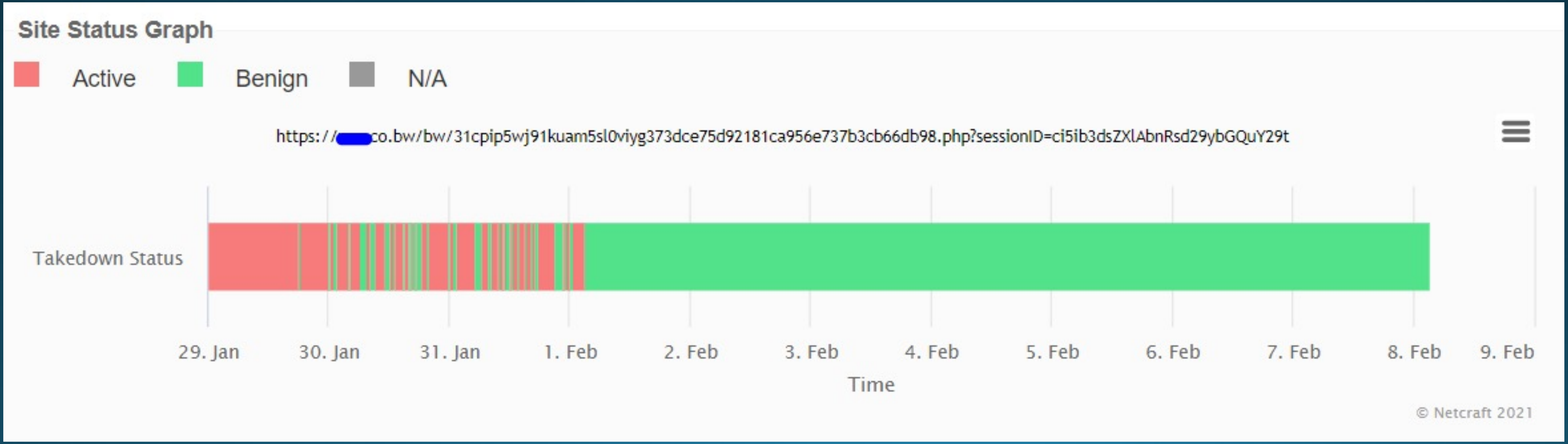
▾ Summary

Takedown Information

Resolved Automated

Attack URL https://[redacted]co.bw/bw/31cpip5wj91kuam5sl0viyg373dce75d92181ca956e737b3cb66db98.p... Malicious

Attack Type Phishing URL



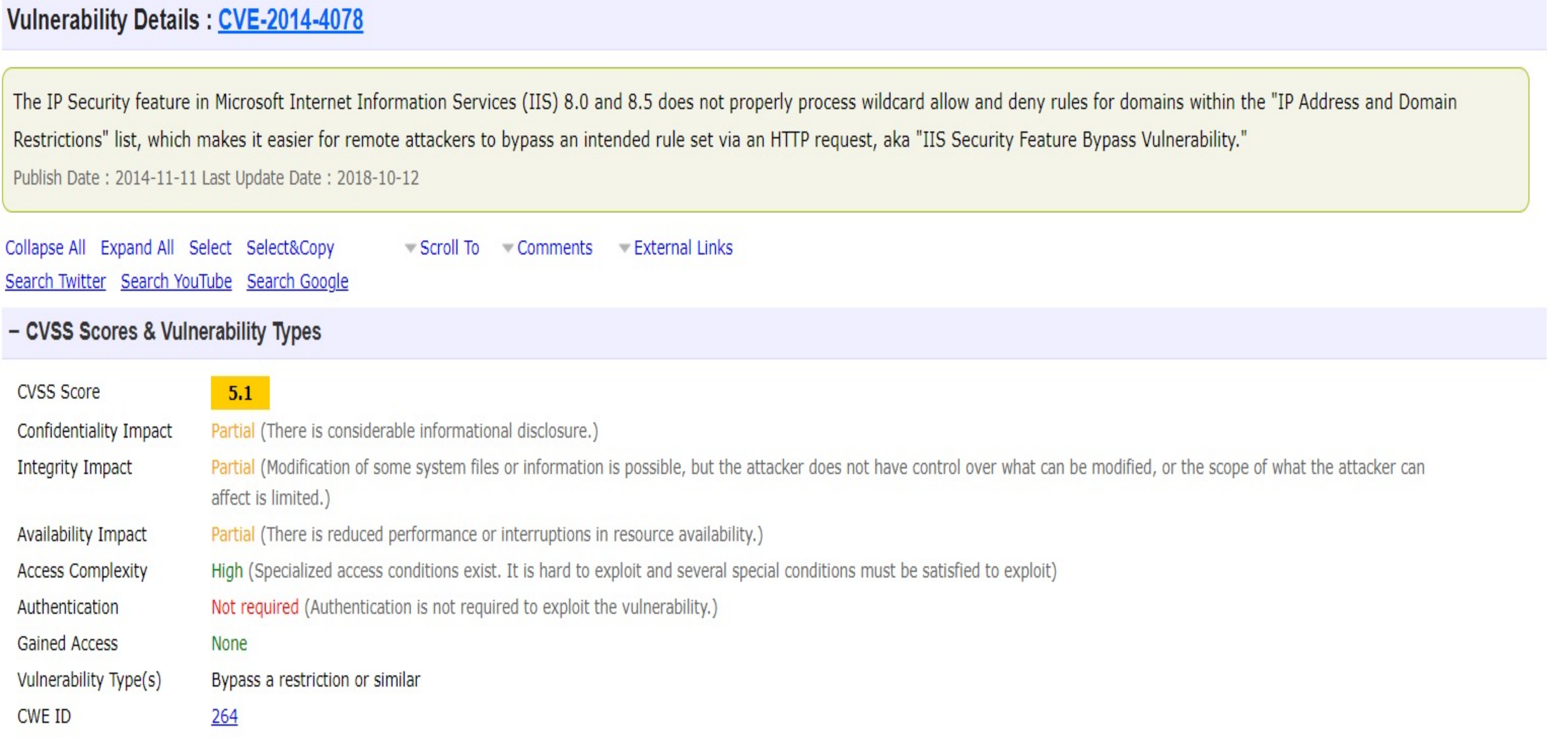
Site Status Graph

🟥 Active 🟩 Benign ▨ N/A

https://[redacted]co.bw/bw/31cpip5wj91kuam5sl0viyg373dce75d92181ca956e737b3cb66db98.php?sessionID=ci5ib3dsZXlAbnRsd29ybGQuY29t

© Netcraft 2021

Collaboration with bwCIRT in Incident Response



Vulnerability Details : CVE-2014-4078

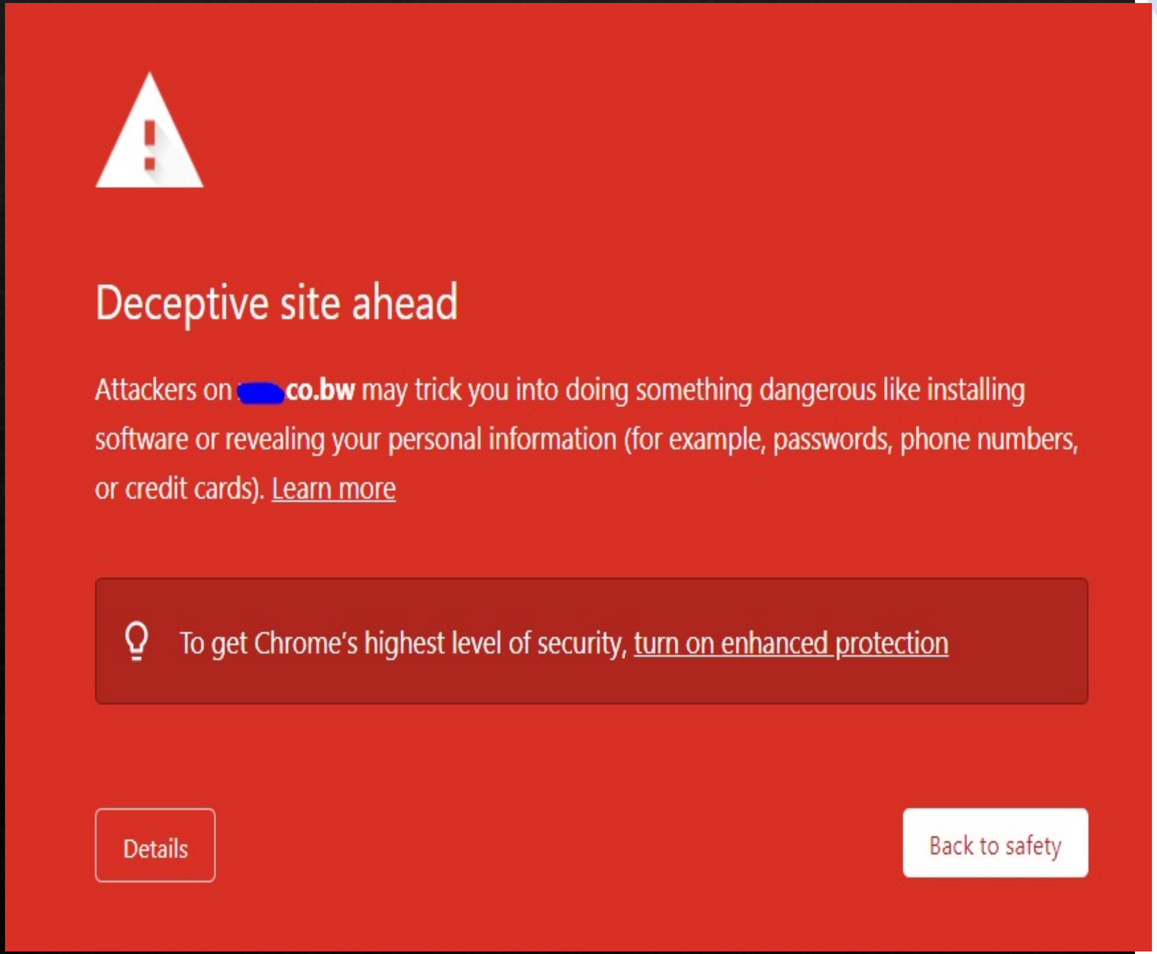
The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

Publish Date : 2014-11-11 Last Update Date : 2018-10-12

– CVSS Scores & Vulnerability Types

CVSS Score	5.1
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Bypass a restriction or similar
CWE ID	264

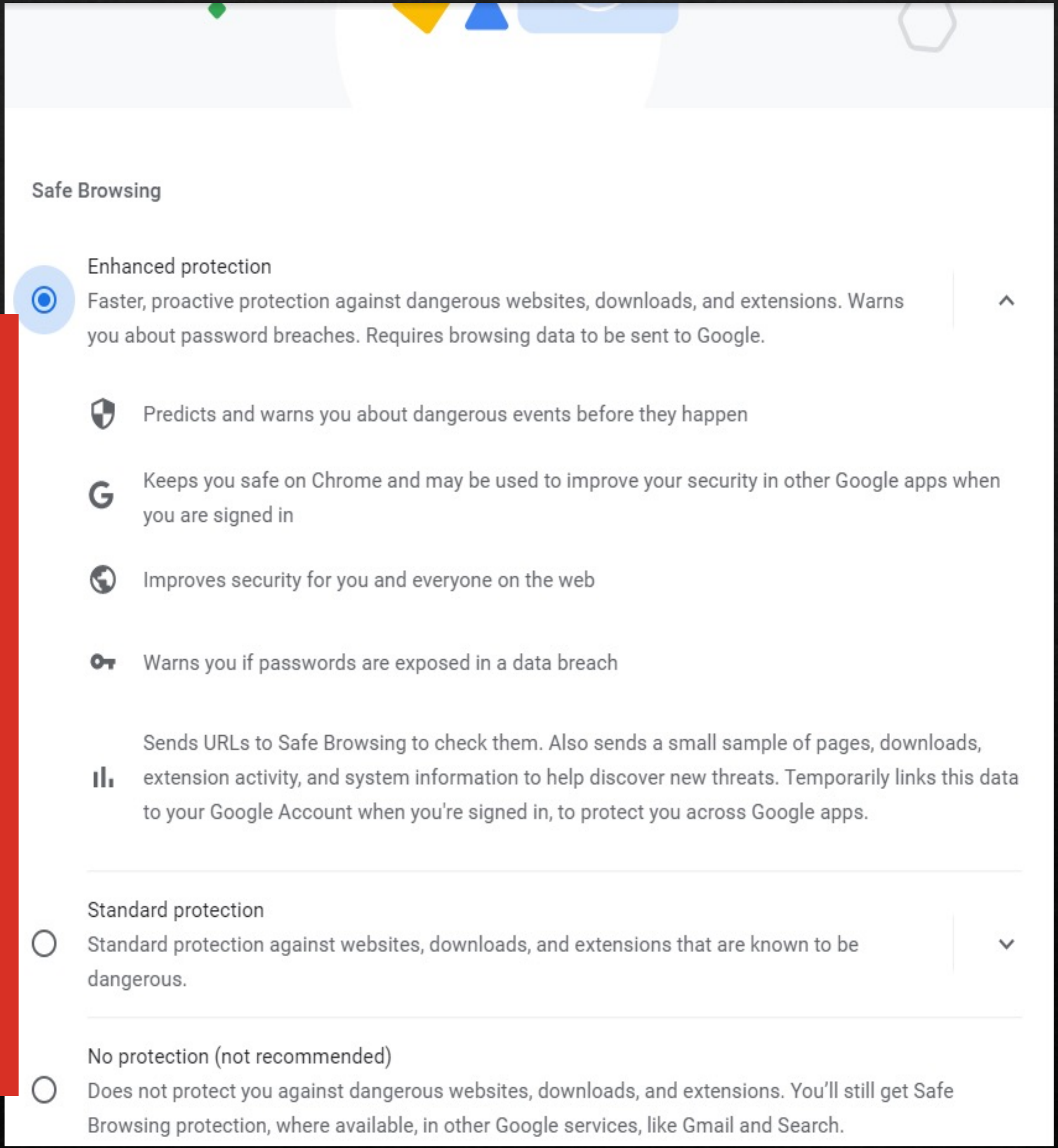
End user Awareness



Deceptive site ahead

Attackers on [redacted]**co.bw** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

To get Chrome's highest level of security, turn on enhanced protection



Safe Browsing

● Enhanced protection
Faster, proactive protection against dangerous websites, downloads, and extensions. Warns you about password breaches. Requires browsing data to be sent to Google.

- Predicts and warns you about dangerous events before they happen
- Keeps you safe on Chrome and may be used to improve your security in other Google apps when you are signed in
- Improves security for you and everyone on the web
- Warns you if passwords are exposed in a data breach
- Sends URLs to Safe Browsing to check them. Also sends a small sample of pages, downloads, extension activity, and system information to help discover new threats. Temporarily links this data to your Google Account when you're signed in, to protect you across Google apps.

○ Standard protection
Standard protection against websites, downloads, and extensions that are known to be dangerous.

○ No protection (not recommended)
Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search.

Policy Review and Regulation

- Regular checks for compliance e.g., KYC for Registrars and Registrants core registration information.

- Review and update policies according to need of the market and DNS community through a consultative approach eg WHOIS policy and Requester Form used for redacted info.

- The Clean Internet Initiative: The ccTLD and the bwCIRT recently developed Minimum Security Guidelines for websites and Emails.

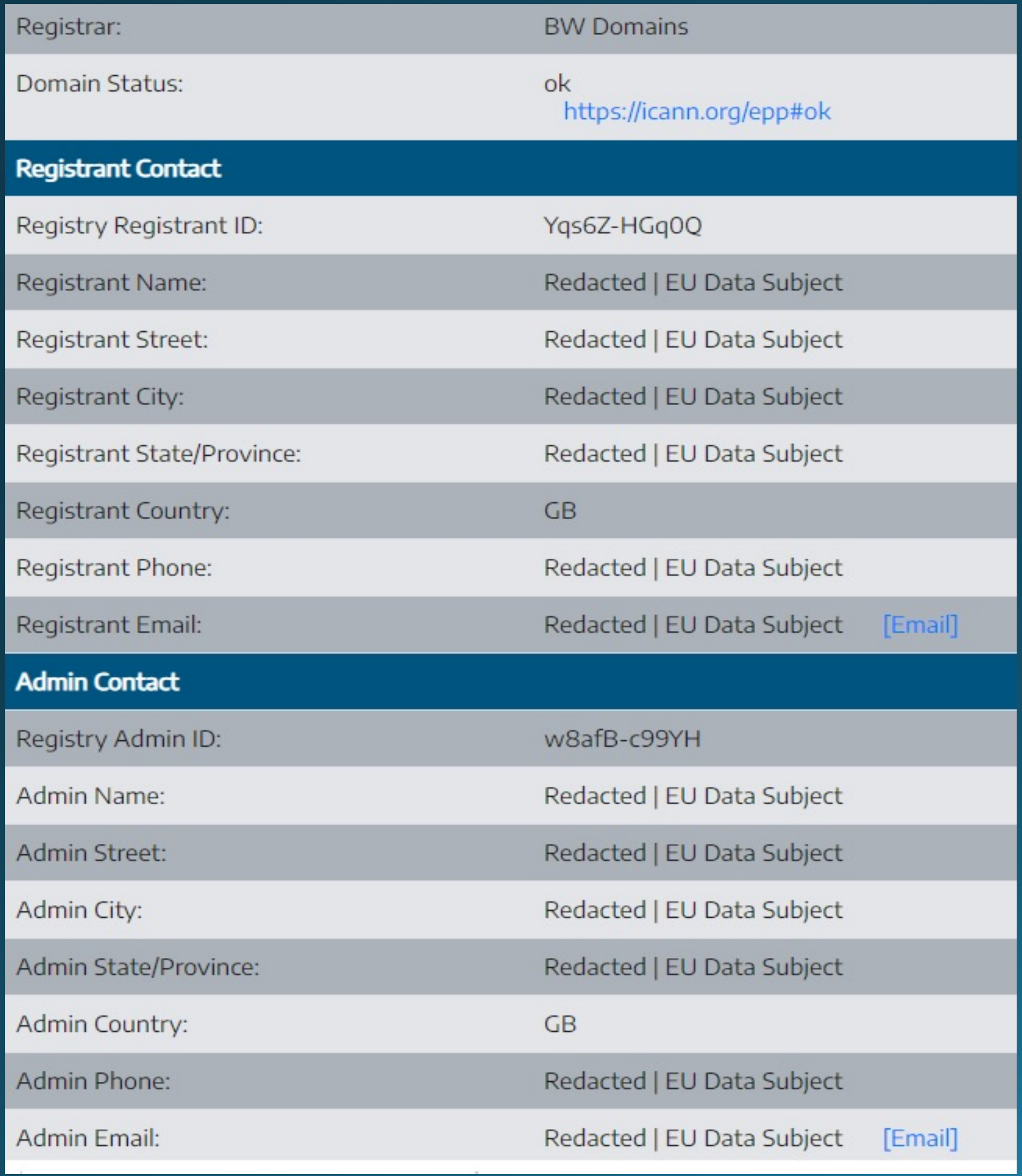
- From the Regulator’s side:
  - BOCRA recently developed a penalty framework that will be used as a guide imposing civil penalties in line with the CRA Act focusing on consumer protection.

Challenges

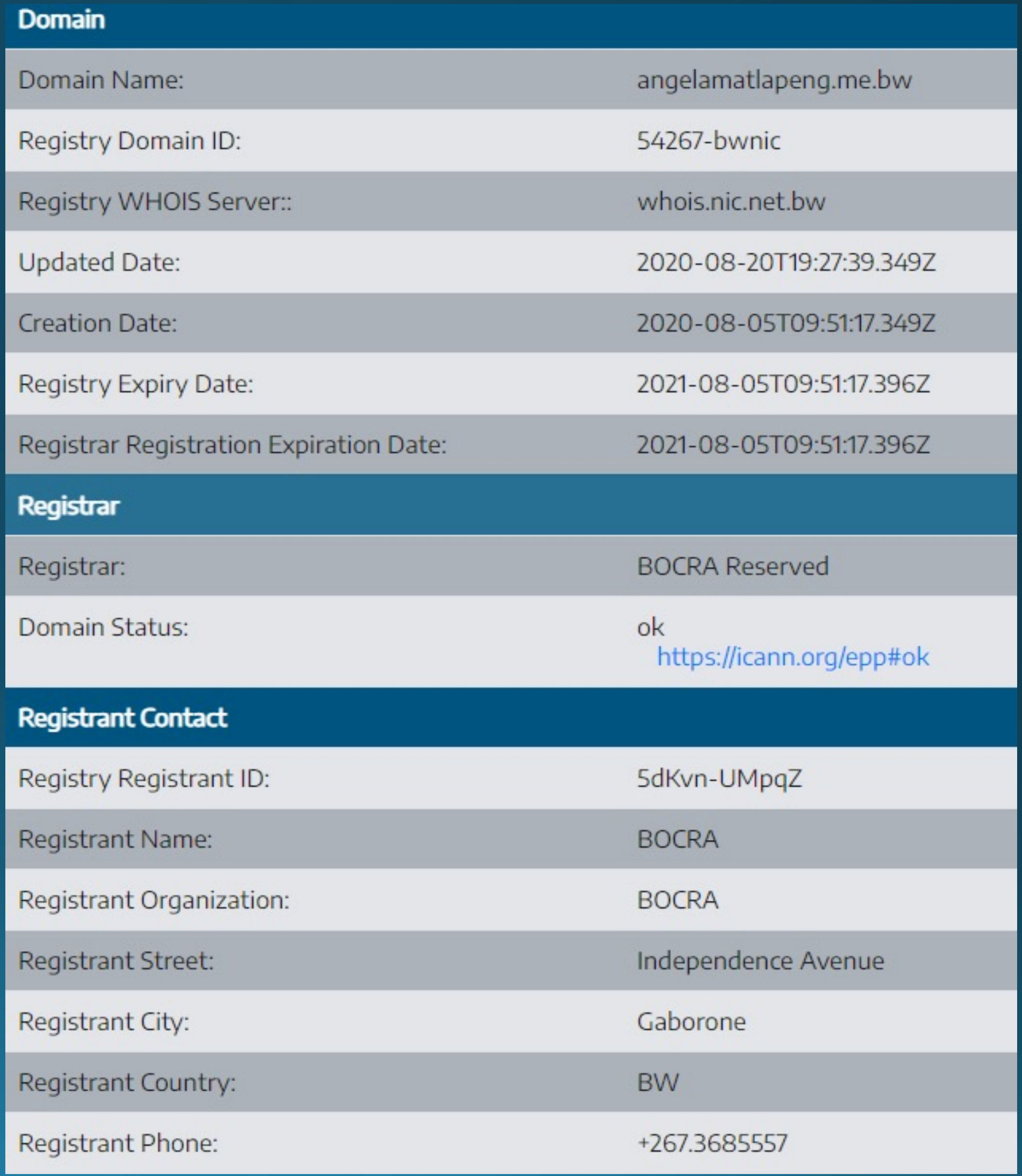
Challenges we face..

- Not knowing and understanding one’s abuse landscape.
- Inaccurate WHOIS data delays and complicates investigation.
- Additional work for the ccTLD to process redacted WHOIS information requests, this with a potential to delay incident response.
- Discrepancies when registering domains – content mismatch to domain e.g., registering a commercial company under .org.bw.

Challenges we face cont..



Registrar:	BW Domains
Domain Status:	ok https://icann.org/epp#ok
Registrant Contact	
Registry Registrant ID:	Yqs6Z-HGq0Q
Registrant Name:	Redacted | EU Data Subject
Registrant Street:	Redacted | EU Data Subject
Registrant City:	Redacted | EU Data Subject
Registrant State/Province:	Redacted | EU Data Subject
Registrant Country:	GB
Registrant Phone:	Redacted | EU Data Subject
Registrant Email:	Redacted | EU Data Subject [Email]
Admin Contact	
Registry Admin ID:	w8afB-c99YH
Admin Name:	Redacted | EU Data Subject
Admin Street:	Redacted | EU Data Subject
Admin City:	Redacted | EU Data Subject
Admin State/Province:	Redacted | EU Data Subject
Admin Country:	GB
Admin Phone:	Redacted | EU Data Subject
Admin Email:	Redacted | EU Data Subject [Email]



Domain	
Domain Name:	angelamatlapeng.me.bw
Registry Domain ID:	54267-bwnic
Registry WHOIS Server::	whois.nic.net.bw
Updated Date:	2020-08-20T19:27:39.349Z
Creation Date:	2020-08-05T09:51:17.349Z
Registry Expiry Date:	2021-08-05T09:51:17.396Z
Registrar Registration Expiration Date:	2021-08-05T09:51:17.396Z
Registrar	
Registrar:	BOCRA Reserved
Domain Status:	ok https://icann.org/epp#ok
Registrant Contact	
Registry Registrant ID:	5dKvn-UMpqZ
Registrant Name:	BOCRA
Registrant Organization:	BOCRA
Registrant Street:	Independence Avenue
Registrant City:	Gaborone
Registrant Country:	BW
Registrant Phone:	+267.3685557

Summary

In Summary..

- DNS abuse and exploits contribute to many threats on the cyberspace.
- Have both proactive and reactive measures in place to detect and curb abuse.
- Implement DNSSEC for integrity and authenticity of DNS data
- Join ICANN's Domain Abuse Activity Reporting (DAAR) Project
- Registries should have an Abuse contact field to assist CSIRTs and law enforcement especially if your WHOIS data is redacted.
- Collaborate with CIRTs in your country as they may have better visibility on abuse

- For Consumers:
  - Engage end users on cyber hygiene and awareness activities.
  - Encourage Registrants to trademark or patent their brands/companies

BOCRA

Thank You!

- Angela Matlapeng
- bwNIC
- matlapeng@bocra.org.bw
- https://nic.net.bw
- https://www.bocra.org.bw

switch to .bw

Your Gateway to the World!