Outline

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
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)
Abuse Trends
Malware Category
Trojan

Hash
811897693b91a1c304f251...

Risk
1

Email Address
b9195c22a8458341df83de...

Show in Table

Data Powered By Bitdefender

Entity

Reputation
threat-found

Tags
Fraudulent Content

SHODAN

Domain

Shodan Link
Domain View

Malware URLs

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

<table>
<thead>
<tr>
<th>Date added (UTC)</th>
<th>URL</th>
<th>Status</th>
<th>Tags</th>
<th>Reporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-01-18 12:07:41</td>
<td><a href="https://example.ac.bw/ru/update.bin">https://example.ac.bw/ru/update.bin</a></td>
<td>Offline</td>
<td>Dreambot, Encoded, Module</td>
<td>Anonymous</td>
</tr>
<tr>
<td>2019-12-20 09:25:32</td>
<td><a href="https://example.ac.bw/ru/update.bin">https://example.ac.bw/ru/update.bin</a></td>
<td>Offline</td>
<td>Dreambot, Module</td>
<td>Anonymous</td>
</tr>
</tbody>
</table>
Hosting server weakness
Countermeasures
Active Monitoring & Takedowns

Summary

Takedown Information

- **Resolved**
- **Automated**

**Attack URL**  
https://[co.bw/bw/31cip5wj91kuam5s10viy3g373dce75d92181ca956e737b3cb66db98].p...  
**Malicious**

**Attack Type**  
Phishing URL

Site Status Graph

- **Active**
- **Benign**
- **N/A**

https://[co.bw/bw/31cip5wj91kuam5s10viy3g373dce75d92181ca956e737b3cb66db98].php?sessionID=ci5ib3dzZ1AbnRsd29ybGQuY29t

Takedown Status

- 29. Jan
- 30. Jan
- 31. Jan
- 1. Feb
- 2. Feb
- 3. Feb
- 4. Feb
- 5. Feb
- 6. Feb
- 7. Feb
- 8. Feb
- 9. Feb

© 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

<table>
<thead>
<tr>
<th>CVSS Score</th>
<th>5.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality Impact</td>
<td>Partial (There is considerable informational disclosure.)</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>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.)</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>Partial (There is reduced performance or interruptions in resource availability.)</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)</td>
</tr>
<tr>
<td>Authentication</td>
<td>Not required (Authentication is not required to exploit the vulnerability.)</td>
</tr>
<tr>
<td>Gained Access</td>
<td>None</td>
</tr>
<tr>
<td>Vulnerability Type(s)</td>
<td>Bypass a restriction or similar</td>
</tr>
<tr>
<td>CWE ID</td>
<td>264</td>
</tr>
</tbody>
</table>
End user Awareness

Deceptive site ahead

Attackers on `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

[Details]

Back to safety

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..

<table>
<thead>
<tr>
<th>Registrar</th>
<th>BW Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Status</td>
<td>ok <a href="https://icann.org/epp#ok">https://icann.org/epp#ok</a></td>
</tr>
</tbody>
</table>

### Registrant Contact

<table>
<thead>
<tr>
<th>Registry Registrant ID</th>
<th>Yqs6Z-HGq0Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrant Name</td>
<td>Redacted</td>
</tr>
<tr>
<td>Registrant Street</td>
<td>Redacted</td>
</tr>
<tr>
<td>Registrant City</td>
<td>Redacted</td>
</tr>
<tr>
<td>Registrant State/Province</td>
<td>Redacted</td>
</tr>
<tr>
<td>Registrant Country/Province</td>
<td>GB</td>
</tr>
<tr>
<td>Registrant Phone</td>
<td>Redacted</td>
</tr>
<tr>
<td>Registrant Email</td>
<td>Redacted</td>
</tr>
</tbody>
</table>

### Admin Contact

<table>
<thead>
<tr>
<th>Registry Admin ID</th>
<th>w8afB-c99YH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Name</td>
<td>Redacted</td>
</tr>
<tr>
<td>Admin Street</td>
<td>Redacted</td>
</tr>
<tr>
<td>Admin City</td>
<td>Redacted</td>
</tr>
<tr>
<td>Admin State/Province</td>
<td>Redacted</td>
</tr>
<tr>
<td>Admin Country</td>
<td>GB</td>
</tr>
<tr>
<td>Admin Phone</td>
<td>Redacted</td>
</tr>
<tr>
<td>Admin Email</td>
<td>Redacted</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>angelamatlapeng.me.bw</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry Domain ID</td>
<td>54267-bwnic</td>
</tr>
<tr>
<td>Registry WHOIS Server</td>
<td>whois.nic.net.bw</td>
</tr>
<tr>
<td>Updated Date</td>
<td>2020-08-20T19:27:39.349Z</td>
</tr>
<tr>
<td>Creation Date</td>
<td>2020-08-05T09:51:17.349Z</td>
</tr>
<tr>
<td>Registry Expiry Date</td>
<td>2021-08-05T09:51:17.396Z</td>
</tr>
<tr>
<td>Registrar Registration Expiration Date</td>
<td>2021-08-05T09:51:17.396Z</td>
</tr>
</tbody>
</table>

### Registrar

<table>
<thead>
<tr>
<th>Registrar</th>
<th>BOCRA Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Status</td>
<td>ok <a href="https://icann.org/epp#ok">https://icann.org/epp#ok</a></td>
</tr>
</tbody>
</table>

## Registrant Contact

<table>
<thead>
<tr>
<th>Registry Registrant ID</th>
<th>Sdkvn-UMpqZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrant Name</td>
<td>BOCRA</td>
</tr>
<tr>
<td>Registrant Organization</td>
<td>BOCRA</td>
</tr>
<tr>
<td>Registrant Street</td>
<td>Independence Avenue</td>
</tr>
<tr>
<td>Registrant City</td>
<td>Gaborone</td>
</tr>
<tr>
<td>Registrant Country</td>
<td>BW</td>
</tr>
<tr>
<td>Registrant Phone</td>
<td>+267.3685557</td>
</tr>
</tbody>
</table>
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.
Thank You!

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

Your Gateway to the World!