As part of its Shared Cybersecurity Services (SCS) portfolio, the Cybersecurity and Infrastructure Security Agency (CISA) leverages the IT security company Infoblox to provide domain mitigation (also sometimes called domain “takedowns”) & phishing analysis services. These services help lessen the impact of cyber threats, including website spoofing, phishing, malicious name services and sites hosting malicious name servers, stolen content, and malware command and control. CISA offers these services to:

- Federal Civilian Agencies; including agencies from executive, legislative, and judicial branches
- State Fusion Centers

Eligible users can request these services directly from Infoblox, who, in turn, validates the request and the threat. If validation is successful, Infoblox will attempt to mitigate the impact of the malicious site, leveraging its relationships with internet service providers (ISPs), registrars, and web hosting providers across the internet. Additionally, Infoblox analyzes phishing emails it receives for malicious domains, includes them in their own threat feeds, and shares the bad domains with the Anti-Phishing Working Group (APWG). These domain mitigation and phishing analysis offerings do not require any additional contracts or authorizations to use.

**DOMAIN MITIGATION SERVICES**

<table>
<thead>
<tr>
<th>Malicious Activity</th>
<th>Explanation</th>
<th>Infoblox Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing sites</td>
<td>Criminal websites that attempt to steal user credentials by claiming to be a legitimate entity</td>
<td>Work with the affected host to remove content</td>
</tr>
<tr>
<td>Malicious name server</td>
<td>Server that provides Authoritative Domain Name Services only for malicious domain names</td>
<td>Work with service providers to remove the criminally controlled infrastructure</td>
</tr>
<tr>
<td>Stolen credentials or other content</td>
<td>Stolen agency proprietary information (e.g., credentials, PII, credit card data), usually hosted in a forum or a fraudulent host account</td>
<td>Work with the affected host to remove the stolen content</td>
</tr>
<tr>
<td>Malware file hosting location</td>
<td>Malware existing on a publicly available site</td>
<td>Confirm the existence of malware at the location and work to get the malicious files removed from the host</td>
</tr>
<tr>
<td>Malware command &amp; control (C2)</td>
<td>A host location identified as a C2 server for malware campaigns</td>
<td>Independently verify the threat and work with the host to remove it</td>
</tr>
</tbody>
</table>
WHAT DOMAIN MITIGATION CANNOT DO

Table 2: Limitations on Infoblox domain mitigation services

<table>
<thead>
<tr>
<th>Limitation</th>
<th>Explanation</th>
<th>Alternatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniform Domain-Name Dispute-Resolution</td>
<td>Requesting transfer of legitimate domain may infringe upon customer initiative</td>
<td>Uniform Domain-Name Dispute-Resolution Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Engage legal counsel</td>
</tr>
<tr>
<td>Suspension of innocent domains</td>
<td>3rd party “nuisance” domain names infringe upon brand but don’t map to an offending web presence or relate to email campaigns or malware</td>
<td>Registrar may suspend domains if activity violates terms of service</td>
</tr>
</tbody>
</table>

INITIATING DOMAIN MITIGATION REQUESTS

An eligible user should initiate a domain mitigation service request when it experiences or suspects any of the following:

- Sites spoofing legitimate websites
- Sites hosting malicious content
- Sites hosting C2 servers
- Sites used to maliciously capture user credentials
- Sites hosting stolen agency data (e.g., stolen credentials)
- Sites engaging in similarly malicious activity

If the request meets the above conditions, an organization should proceed as follows:

1. Request Domain Mitigation Services from Infoblox. Organizations should send a request to deactivatenow@infoblox.com and courtesy copy CISA at CISAServiceDesk@cisa.dhs.gov. The request should contain as much supporting information as is available (e.g., location of observed activity, context, techniques, characteristics, and other known information). Mitigations can be requested for any domain and need not be limited to sites believed to be impersonating agency properties.

   Upon receipt of request, Infoblox will:
   - Validate the specifics of the organization’s request
   - Work with its partners—such as ISPs and other service providers—to remove the malicious content
   - Keep the request open for 30 days following the mitigation
   - Monitor the affected hosts/targets for reoccurrence
   - Provide updates to the requesting agency, including final close-out notification, as it takes mitigating actions

2. Report the suspected website or incident to CISA. Organizations should follow the federal notification guidelines outlined at https://www.us-cert.gov/incident-notification-guidelines. Reports can be submitted to CISA via:

   - Agencies should err on the side of caution and request domain mitigation services for sites spoofing legitimate websites if they suspect those sites to also be engaged in malicious activity. Infoblox will verify maliciousness of any requested site before performing the mitigation.

   - The specifics of each individual process and the order in which steps are carried out, and any additional steps and requirements, will depend on agency internal policies and procedures.
Alert stakeholders and potential users, as appropriate. Organizations should follow their internal incident response procedures to execute their pre-defined communications plan and work with their internal stakeholders.

Notify law enforcement regarding any criminal activity and legal counsel regarding any improper use of trademarks or agency seals. Organizations should alert appropriate law enforcement entities if malicious website activities might constitute a crime. Federal Civilian Agencies should also notify their Office of General Counsel if malicious website activities involve agency trademarks, logos, marks, or seals.³

If necessary, request Federal Bureau of Investigation (FBI) support. If previous steps are unsuccessful, the FBI may be able to compel a web operator/hosting provider to remove the malicious/spoofing website. To contact the FBI, see https://www.fbi.gov/contact-us.

PHISHING ANALYSIS

Through a partnership with the Anti-Phishing Working Group (APWG) and CISA, Infoblox analyzes phishing emails sent to CISA’s public phishing reporting email: phishing-report@us-cert.gov. Infoblox also incorporates the publicly available data on malicious domains and URLs gleaned from those emails into its proprietary threat feeds, which are available for free to eligible users through the SCS program. The process is as follows:

- An organization forwards a phishing email to phishing-report@us-cert.gov.
- The email is forwarded to Infoblox for anonymization and analysis.
- If the domains are malicious, Infoblox will share them with the APWG and incorporate them into their own threat feeds.

Recommendation: Save time and effort and fight phishing by augmenting your existing spam and abuse reporting process. Automate your reports to phishing-report@us-cert.gov. The more phishing attempts we block and mitigate, the safer all federal users and systems become.

COSTS

SCS program services, including Infoblox domain mitigations, are provided to eligible users at no cost. Infoblox also integrates the results of its phishing analysis into its proprietary threat feeds, which are available to eligible SCS users at no additional cost.

CONTACTS

- For questions about SCS, contact the CISA SCS Team at CISA.CTIS.SCS_Info@cisa.dhs.gov.
- To request domain mitigation services or obtain additional information, contact Infoblox at deactivatenow@infoblox.com. Please courtesy copy CISA at CISAServiceDesk@cisa.dhs.gov when requesting domain mitigation services.
- To report phishing, forward emails to phishing-report@us-cert.gov.
- To report a cybersecurity incident, please utilize the CISA Incident Reporting System: https://us-cert.cisa.gov/forms/report.
- To contact the FBI, see https://www.fbi.gov/contact-us.

³ Malicious actors often attempt to spoof federal websites or impersonate federal agencies, officials, or services by depicting official government seals and logos without permission to appear legitimate to unsuspecting users. This activity may constitute trademark infringement and/or related intellectual property rights violations or violate federal statutes that protect agency seals and insignia.