Compromised Website Report
A report on your network or constituency

@shadowserver
contact@shadowserver.org
Presentation Aims & Objectives

• Introduce compromised websites

• Highlight a sample compromised website report

• Describe key features of the report

• Demonstrate how a National CERT or network owner can action a compromised website report

• Offer general guidance on how to protect against compromised websites

• Provide a key list of Shadowserver online resources to enable report subscription and use
• A compromised website relates to a site whose code has been altered for malicious third party gain, such as
  • Installing malware on a device via Exploit Kits
  • Sending SPAM
  • DDoS attack
  • Injecting javascript to transmit user data without consent
  • Launch pop-up ads

• Anyone visiting a compromised website is also at risk of compromise or participation in some kind of attack

• Often the result of outdated versions of CMS, such as Joomla/Drupal/Wordpress (or plugins for these) and weak or keylogged FTP credentials
Compromised Website Report


- Report is available as a file in CSV format

- The report filename contains `compromised_website`

- All timestamps are in UTC

- Reports can be sent as e-mail attachments, downloaded via HTTP or obtained via a RESTful API

- For more documentation on API access, please visit the below URLs and send a request for access to contact@shadowserver.org
Compromised Website Report

This report is a list of all the websites we (or our collaborative partners) have been able to identify and verify to be compromised.

These websites might be used for sending spam, participating in DDoS attacks, redirecting users to exploit kits, etc. This information will be listed in the "category" field of the report.

A large subset of these compromises are caused by outdated versions of CMS, such as Joomla/Drupal/Wordpress (or plugins for these) and weak or keystroked FTP credentials.

As always, there is no guarantee that there are no additional infections or compromises on any IP that we report on. We have seen several different criminal groups abusing the same compromised system for different purposes; the same IP/domain that is hosting a spambot may also be used for infecting unsuspecting users. We recommend investigating systems with the assumption that there are more compromises on the systems than are reported.

### Key event fields

<table>
<thead>
<tr>
<th>timestamp</th>
<th>ip</th>
<th>port</th>
<th>hostname</th>
<th>tag</th>
<th>application</th>
<th>asn</th>
<th>geo</th>
<th>city</th>
<th>url</th>
<th>http_host</th>
<th>category</th>
<th>system</th>
<th>detected_since</th>
<th>server</th>
<th>cc_url</th>
</tr>
</thead>
<tbody>
<tr>
<td>18/04/2022</td>
<td>108.71.X.X</td>
<td>80</td>
<td>XXX</td>
<td>hacked-webserver-stealrat-t1</td>
<td>http</td>
<td>18450</td>
<td>US</td>
<td>missouri</td>
<td>wp-includes/returnV042.php*</td>
<td>0031a.com</td>
<td>spam</td>
<td>linux</td>
<td>2014-03-08</td>
<td>XXX</td>
<td>XXX</td>
</tr>
</tbody>
</table>
### Action a Compromised Website Report

<table>
<thead>
<tr>
<th>timestamp</th>
<th>ip</th>
<th>port</th>
<th>hostname</th>
<th>tag</th>
<th>application</th>
<th>asn</th>
<th>geo</th>
<th>city</th>
<th>url</th>
<th>http_host</th>
<th>category</th>
<th>system</th>
<th>detected_since</th>
<th>server</th>
<th>cc_url</th>
</tr>
</thead>
<tbody>
<tr>
<td>18/04/2022 00:00</td>
<td>108.71.X.X</td>
<td>80</td>
<td>XXX</td>
<td>hacked-webserver-stealrat-t1</td>
<td>http</td>
<td>18450</td>
<td>US</td>
<td>missouri</td>
<td>wp-includes/return/042.php&quot;</td>
<td>0031a.com</td>
<td>spam</td>
<td>linux</td>
<td>2014-03-08</td>
<td>XXX</td>
<td>XXX</td>
</tr>
</tbody>
</table>

**IP WHOIS 108.71.X.X**

- **NetRange:** 108.64.0.0 – 108.65.255.255
- **CIDR:** 108.64.0.0/11
- **NetName:** SBICS-SBIS
- **NetHandle:** NET-108-64-0-0-1
- **Parent:** NET188 (NET-108-0-0-0-0)
- **NetType:** Direct Allocation
- **OriginAS:** AS7132
- **Organization:** AT&T Corp. (AC-3200)
- **RegDate:** 2000-10-29
- **Updated:** 2018-03-05
- **Ref:** https://rdap.arin.net/registry/ip/108.64.0.0

**OrgName:** AT&T Corp.
- **OrgId:** AC-3200
- **Address:** 7277 164th Ave NE
- **Address:** Attn: IP Management
- **City:** Redmond
- **StateProv:** WA
- **PostalCode:** 98052
- **Country:** US
- **RegDate:** 2000-10-29
- **Updated:** 2021-06-26
- **Comment:** For policy abuse issues contact abuse@tt.net
- **Comment:** For all subpoena, Internet, court order related matters and emerg
- **Comment:** 11760 US Highway 1
- **Comment:** North Palm Beach, FL 33408
- **Comment:** Main Number: 800-635-6949
- **Comment:** Fax: 888-938-4715
- **Ref:** https://rdap.arin.net/registry/entity/AC-3200
Methodology for verification may differ depending on the threat identified. We provide the infection name and URL, but you would likely need to search more on the Web to fully understand how a reported attack works.

As always, there is no guarantee that there are no additional infections or compromises on any IP that we report on.

We have seen several different criminal groups abusing the same compromised system for different purposes.

We recommend investigating systems with the assumption that there are more compromises on the systems than are reported.

Contact us if you need help in better understanding our report!
• Follow security best practices when you make your website public

• Keep sites updated with the latest security patches

• Avoid untested plugins or themes

• Do not expose unnecessary services you do not need to

• Use firewalls to block access to website elements

• Use SSL only, do not allow for any website related passwords to be sent in plaintext
Compromised Website - REMEDIATE

- Recover access and reset passwords
- Backup the site and / or the server (e.g. a VPS) to preserve all content
- Update plugins and themes
- Remove unwanted files
- Clean out your sitemap
- Reinstall plugins and themes and WordPress core
- Clean out connected databases if necessary
Summary & Key Report Pages

Reports overview

• https://www.shadowserver.org/what-we-do/network-reporting/get-reports/
• https://www.shadowserver.org/what-we-do/network-reporting/

Report Updates

• https://www.shadowserver.org/news-insights/
• Twitter @shadowserver
• Mailing list access send request to contact@shadowserver.org and request access to public@shadowserver.org
• Or subscribe directly at https://mail.shadowserver.org/mailman/listinfo/public

Reports API

• Request access to contact@shadowserver.org
• https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/
• https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/