


Compromised Website Report

A report on your network or constituency

 @shadowserver

 contact@shadowserver.org



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



Compromised Websites



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- Often the result of outdated versions of CMS, such as Joomla/Drupal/Wordpress (or plugins for these) and weak or keylogged FTP credentials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



- Compromised Website Report: <https://www.shadowserver.org/what-we-do/network-reporting/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
<https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/>
<https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/>

Compromised Website Report



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A large subset of these compromises are caused by outdated versions of CMS, such as Joomla/Drupal /Wordpress (or plugins for these) and weak or keylogged FTP credentials.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

<https://www.shadowserver.org/what-we-do/network-reporting/compromised-website-report/>



FIELDS

timestamp	Timestamp that the URL was last seen/verified to be compromised in UTC-0
ip	IP hosting the compromised website
port	Port the compromised website is served on
hostname	Reverse DNS of the IP of the compromised website
tag	Name of the malware family/type the website is compromised with/by
application	Layer 7 protocol (HTTP/HTTPS)
asn	ASN of the IP hosting the compromised URL
geo	Country of the IP hosting the compromised URL
region	State or province from the Geo
city	City from the Geo
url	URI path of the component indicating the website compromise
http_host	Domain/IP part of the URL
category	Type of maliciousness the compromised website is being used for
system	Operating system on the server hosting the compromised website (Windows/Linux)
detected_since	Timestamp that the URL was first seen/verified to be compromised in UTC-0
server	Server side software such as Apache/Nginx
cc_url	In the case that a C&C server is involved, the URL of that server

SAMPLE

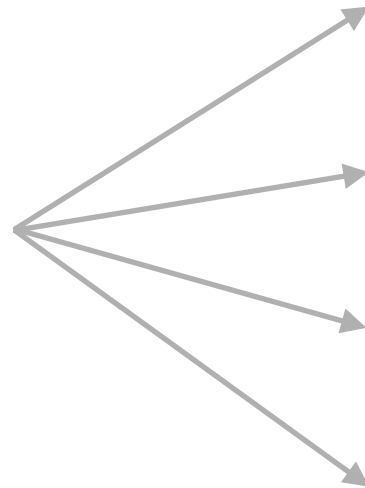
```
"timestamp", "ip", "port", "hostname", "tag", "application", "asn", "geo", "region", "city", "url",  
"2014-06-16 00:16:33", "23.80.185.68", 80, "23.80.185.68.rdns.as15003.net", "hacked-webserve:  
"2014-06-16 00:16:33", "108.171.205.43", 80, "hacked-webserver-stealrat-t1", "http", 18450, "t  
"2014-06-16 00:16:33", "108.171.205.43", 80, "hacked-webserver-stealrat-t1", "http", 18450, "t  
"2014-06-16 00:16:33", "108.171.205.43", 80, "hacked-webserver-stealrat-t1", "http", 18450, "t  
"2014-06-16 00:16:33", "123.196.112.160", 80, "hacked-webserver-stealrat-t1", "http", 4847, "t  
"2014-06-16 00:16:33", "108.171.205.43", 80, "hacked-webserver-stealrat-t1", "http", 18450, "t  
"2014-06-16 00:16:33", "74.220.202.17", 80, "hacked-webserver-stealrat-t1", "http", 46606, "t
```

Action a Compromised Website Report



timestamp	ip	port	hostname	tag	application	asn	geo	city	url	http_host	category	system	detected_since	server	cc_url
18/04/2022 00:00	108.71.X.X	80	XXX	hacked-webserver-stealrat-t1	http	18450	US	missouri	wp-includes/returnV04Z.php"	0031a.com	spam	linux	2014-03-08	XXX	XXX

Key event fields



FIELDS

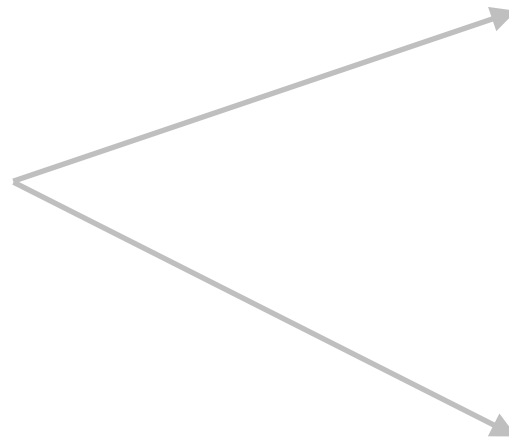
timestamp	Timestamp that the URL was last seen/verified to be compromised in UTC+0
ip	IP hosting the compromised website
port	Port the compromised website is served on
hostname	Reverse DNS of the IP of the compromised website
tag	Name of the malware family/type the website is compromised with/by
application	Layer 7 protocol (HTTP/HTTPS)
asn	ASN of the IP hosting the compromised URL
geo	Country of the IP hosting the compromised URL
region	State or province from the Geo
city	City from the Geo
url	URI path of the component indicating the website compromise
http_host	Domain/IP part of the URL
category	Type of maliciousness the compromised website is being used for
system	Operating system on the server hosting the compromised website (Windows/Linux)
detected_since	Timestamp that the URL was first seen/verified to be compromised in UTC+0
server	Server side software such as Apache/Nginx
cc_url	In the case that a C&C server is involved, the URL of that server

Action a Compromised Website Report



timestamp	ip	port	hostname	tag	application	asn	geo	city	url	http_host	category	system	detected _since	server	cc_url
18/04/2022 00:00	108.71.X.X	80	XXX	hacked-webserver- stealrat-t1	http	18450	US	missouri	wp-includes/ returnV04Z.php"	0031a.com	spam	linux	2014-03-08	XXX	XXX

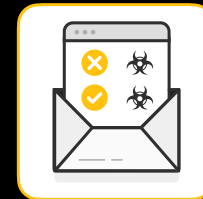
IP WHOIS
108.71.X.X



```
NetRange: 108.64.0.0 - 108.95.255.255
CIDR: 108.64.0.0/11
NetName: SBCIS-SBIS
NetHandle: NET-108-64-0-0-1
Parent: NET108 (NET-108-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS7132
Organization: AT&T Corp. (AC-3280)
RegDate: 2009-10-29
Updated: 2018-07-19
Ref: https://rdap.arin.net/registry/ip/108.64.0.0

OrgName: AT&T Corp.
OrgId: AC-3280
Address: 7277 164th Ave NE
Address: Attn: IP Management
City: Redmond
StateProv: WA
PostalCode: 98052
Country: US
RegDate: 2018-03-05
Updated: 2021-06-26
Comment: For policy abuse issues contact abuse@att.net
Comment: For all subpoena, Internet, court order related matters and emerge
Comment: 11760 US Highway 1
Comment: North Palm Beach, FL 33408
Comment: Main Number: 800-635-6840
Comment: Fax: 888-938-4715
Ref: https://rdap.arin.net/registry/entity/AC-3280
```

Verifying results



- 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!

Compromised Website - PROTECT

- 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/>
- <https://www.shadowserver.org/what-we-do/network-reporting/compromised-website-report/>

Report Updates

- <https://www.shadowserver.org/news-insights/>
- Twitter [@shadowserver](https://twitter.com/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/>





SHADOWSERVER

Lighting the way to a more secure Internet



@shadowserver



contact@shadowserver.org

SHADOWSERVER.ORG