

# Shadowserver reports for share and investigation

“While we collect a lot of different data, it does not become useful unless that information is shared.”

*<https://www.shadowserver.org/wiki/pmwiki.php/Services/Reports>*



# shadowSERVER

Hide ↓ Home

Edit

HomePage

Shadowserver

**Mission**

Updated

Terms of Service

New

Privacy

Standards and Guidelines

Organizations

Blog

Calendar

Future Goals

Jobs and Contributions

Press

Security Organizations

News Articles

Blogs and Forums

Misc

Presentations

Chronological

Operations Status

Knowledge Base

Technology in Use

Botnets

Botnet Detection

## Mission

### Introduction

The Shadowserver Foundation is continually seeking to provide timely and relevant information to the security community at large. We also seek to increase our level of research and investigation into the activity we discover. As such, we list our goals and plans for the next six to twelve months:

### Goals

- Investigate and contribute to new technologies in botnet control.
- Develop and deploy new methods for harvesting malware and studying its behavior.
- Develop and utilize additional techniques for gathering and analyzing botnet data and network flows.
- Work more closely with ISPs, Hosting and DNS providers in the identification and mitigation of botnets and malware propagation.
- Increase our collaboration with other key security organizations and researchers to share discoveries and analysis.
- Develop and release whitepapers and reports based on our research.
- Further develop our website to provide information and reports to the interested public.
- Participate in future security conferences and workgroups.
- Increase our communication with the public through irc, mailing lists, and the website.



Report	Alternative Report Name	Description	Source	Interval
<a href="#">ASN Summary Report</a>		Top 25 ASN's summarized by number of Command and Control systems that were within that ASN, by the highest closed C&C's, and lowest closed of C&C's	Summary from all data sources	Weekly (Sunday)
<a href="#">Botnet URL Report</a>		Any URL that was seen in a botnet channel is reported. The URL could be an update, complaint, or information related to the criminals. Everything is included in case there is something of value in the URL	Botnet Monitoring	24-Hours
<a href="#">Compromised Host Report</a>		Specific hosts that were seen to be compromised from a botnet. These are usually seen when another infected system reports on each host that had been compromised	Botnet Monitoring	24-Hours
<a href="#">Compromised Website Report</a>		Websites that were seen to be compromised, and hence are likely to be abused for various types of attacks.	Tracking systems	24-Hours
<a href="#">Click-Fraud Report</a>		This is used as a source of fraud and possible revenue when a botnet is used to select links that are used for tracking or monetary purposes. The specific URL's are targeted are listed	Botnet Monitoring	24-Hours
<a href="#">Command and Control Report</a>		A list of all the currently known active C&C's	Tracking System	7-Days
Conficker-Drone	RETIRED: All data has been rolled into the "Sinkhole" report	Any host connecting to any of the Conficker Working Group Sinkholes	Conficker Sinkholes	24-Hours
<a href="#">DDoS Report</a>		Any attack is reported whether the recipient is the target or the source of the attack	Botnet Monitoring	24-Hours
<a href="#">DNS Open Resolvers Report</a>		Any host (IP) that appears to be running an openly recursive DNS server.	Service Scan	24-Hours



Botnet-Drone	RETIRED: All data has been rolled into the "New Style" report	Any host (IP) that was seen joining a known Command and Control system.	Botnet Monitoring (IRC and HTTP)	24-Hours
<a href="#">Drone Report/Botnet-Drone</a>		Any host (IP) that was seen joining a known Command and Control system.	Botnet Monitoring (IRC and HTTP) and Sinkholes	24-Hours
<a href="#">Geographical Summary Report</a>		Top 25 Countries summarized by number of Command and Control systems that were within that country, by the highest closed C&C's, and lowest closed of C&C's	Summary from all data sources	Weekly (Sunday)
<a href="#">Honeypot URL Report</a>	Daily Nepenthes Digest Report	This is a report of the source URL's of where malware was downloaded from by the Honeypot systems	Honeypots	24-Hours
<a href="#">IRC Port Summary Report</a>		Summary of the ports used by Command and Controls and sorted three ways. By the most seen, the highest rate of being shutdown, and the lowest rate of being shutdown.	Summary from all data sources	Weekly (Sunday)
<a href="#">Microsoft Sinkhole Report</a>		IP's accessing Microsofts Sinkholes and shared with Shadowserver for remediation	Sinkhole	24-Hours
<a href="#">Netcore/Netis Router Vulnerability Scan Report</a>		Any host (IP) that appears to have an openly accessible backdoor on a Netcore/Netis router.	Service Scan	24-Hours
<a href="#">NTP Monitor Report</a>		Any host (IP) that appears to have an openly accessible NTP service running that responds to Mode 7 requests.	Service Scan	24-Hours
<a href="#">NTP Version Report</a>		Any host (IP) that appears to have an openly accessible NTP service running that responds to Mode 6 requests.	Service Scan	24-Hours
<a href="#">Open Proxy Report</a>		Drones are used frequently as proxies or jump points either directly or sold to other criminals.	Search Engine Scraping, Botnets, Other	24-Hours



<a href="#">Open CharGen Report</a>		Any host (IP) that appears to have an openly accessible chargen service running.	Service Scan	24-Hours
<a href="#">Open IPMI Report</a>		Any host (IP) that appears to have an openly accessible IPMU service running that responds to an IPMI ping.	Service Scan	24-Hours
<a href="#">Open NetBIOS Report</a>		Any host (IP) that appears to have an openly accessible NetBIOS service running.	Service Scan	24-Hours
<a href="#">Open QOTD Report</a>		Any host (IP) that appears to have an openly accessible Quote Of The Day service running.	Service Scan	24-Hours
<a href="#">Open SNMP Report</a>		Any host (IP) that appears to have an openly accessible SNMP service running.	Service Scan	24-Hours
<a href="#">Open SSDP Report</a>		Any host (IP) that appears to have an openly accessible Simple Service Discovery Protocol service running.	Service Scan	24-Hours
<a href="#">Proxy Report</a>		Drones are used frequently as proxies or jump points either directly or sold to other criminals.	Botnet Monitoring	24-Hours
<a href="#">Scan Report</a>		Vulnerability scanning is a standard part of any botnet arsenal. We report on these as a warning that specific network blocks are being targeted	Botnet Monitoring	24-Hours
<a href="#">Sandbox URL Report</a>	Daily HTTP Report	These are the URL's that were accessed by malware. There are two versions of this report, an unfiltered version, and a filtered version.	Sandbox	24-Hours
<a href="#">Sandbox Connection Report</a>		This is a summarization of all the network traffic that the sandbox has seen for the specific interval.	Sandbox	24-Hours
<a href="#">Sandbox IRC Report</a>	Daily Digest Report	A list of all the new IRC Command and Control systems that were found after analyzing malware	Sandbox	24-Hours
<a href="#">Sandbox SMTP Report</a>	Daily SMTP Report	A list of e-mail addresses that was used by malware during a sandbox run.	Sandbox	24-Hours
<a href="#">Sinkhole HTTP Drone Report</a>		All the IP's that joined the sinkhole server that did not join via a referral URL	Sinkhole	24-Hours
<a href="#">Sinkhole HTTP Referer Report</a>		A list of referral URL's that pushed systems to the sinkhole server	Sinkhole	24-Hours
<a href="#">Spam-URL Report</a>		A list of the URL's and relays for Spam that was received.	Spam/E-Mail	24-Hours

- 2014-10-03-botnet\_drone-armenia-geo.csv
- 2014-10-03-compromised\_website-armenia-geo.csv
- 2014-10-03-dns\_openresolver-armenia-geo.csv
- 2014-10-03-microsoft\_sinkhole-armenia-geo.csv
- 2014-10-03-scan\_chargen-armenia-geo.csv
- 2014-10-03-scan\_ipmi-armenia-geo.csv
- 2014-10-03-scan\_netbios-armenia-geo.csv
- 2014-10-03-scan\_ntp-armenia-geo.csv
- 2014-10-03-scan\_ntpmonitor-armenia-geo.csv
- 2014-10-03-scan\_qotd-armenia-geo.csv
- 2014-10-03-scan\_snmp-armenia-geo.csv
- 2014-10-03-scan\_ssdp-armenia-geo.csv
- 2014-10-03-sinkhole\_http\_drone-armenia-geo.csv

# Shadowserver reports delivery

- email with attachments - zipped csv files
- link for retrieval
- direct download

```
"timestamp", "ip", "asn", "geo", "region", "city", "port", "protocol", "hostname", "min_amplification", "dns_version", "p0f_genre", "p0f_detail"
```

```
"2013-10-10
```

```
00:05:10", "208.70.149.107", "36252", "US", "Illinois", "Chicago", "53", "udp",  
"107.149.70.208.static.ipv4.dnsptr.net", "4.6190", "PalmOS DNS v1.0", ,
```

```
"2013-10-10 00:05:10", "204.245.210.223", "2914", "US", "Oregon", "Warren",  
"53", "udp", "", "1.3810", "", ,
```

```
"2013-10-10 00:05:10", "40.135.0.109", "7029", "US", "Nebraska", "Pawnee  
City", "53", "udp", "h109.0.135.40.static.ip.windstream.net", "1.3810",  
"SERVFAIL", ,
```

```
"2013-10-10 00:05:10", "76.74.186.178", "13768", "CA", "British Columbia",  
"Richmond", "53", "udp", "ns2.domainhostingservers.com", "3.4762",  
"9.2.4", ,
```

```
"2013-10-10 00:05:10", "31.42.105.195", "51003", "RU", "-", "-", "53",  
"udp", "", "1.3810", "dnsmasq-2.63", ,
```



- retrieve report or extract from mail
- convert and import data into database
- generate specific reports by requests
  - filter by IP,ASN, attack, etc
  - export data for offline inspection
  - allow authorized users to work with their respective data

DNS-open-resolvers	
timestamp	2014-10-03
ip	195.250.64.74
asn	1234
geo	AM
region	YEREVAN
city	YEREVAN
port	53
protocol	udp
hostname	test.daemon.am
min_amplification	4.6190
dns_version	bind
p0f_genre	
p0f_detail	

Sinkhole-HTTP-Drone	
timestamp	2014-01-01 11:23:45
ip	195.250.64.74
asn	1234
geo	AM
url	GET /search?q=2611 HTTP1/0
type	downadup
http_agent	KUKU v4.00 alpha
tor	
src_port	29313
p0f_genre	Windows
p0f_detail	2000 SP4, XP SP!+
hostname	<b>test.daemon.am</b>
dst_port	80
http_host	www.lukki6dndas.info
http_referer	
http_referer_asn	
http_referer_geo	
dst_ip	87.106.250.34
dst_asn	8660
dst_geo	DX

REPORTS [db.table]	
id	12345
record_id	md5
field_name	asn
field_value	1234
report_type	sinkhole-http-drone
report_source	file://
comments	n/a

summary report for authorized ASN  
from 2014-10-02 to 2014-10-03

	botnet_drone	compromised website	scan ipmi	scan ntp
2014-10-02	34	5	2	67
2014-10-03	56	2	1	123

summary report for each ASN  
from 2014-10-02 to 2014-10-03

	botnet_drone	compromised website	scan ipmi	scan ntp
AS1234	90	5	2	190
AS5678	156	2	1	45



# Users Table Structure

ASN  
PGP  
IP  
email  
phone  
[etc]

users [db.table]	
id	12345
username	<i>testuser</i>
attribute	Password
value	notSecuRe+1
comments	n/a

**Thank You!**