Securing Your Network Using Shadowserver Reports
What do the Bad Guys See?
Who is Scanning your Network?

Reality of Today’s Risk!

- Miscreants are scanning your network. Assume they know your exposed risk.
- Miscreants have a list of vulnerable systems on your network.
- Organizations are scanning your network, gaining intelligence on your organization’s risk.
The Miscreant’s Network Visibility

What can others see when looking into your network from the outside?
What is your organization’s risk?
Would it be nice ....
Public Service Reporting
Network Reporting

Every day, Shadowserver sends custom remediation reports to more than 4600 vetted subscribers, including over 100 national governments and many Fortune 500 companies. These reports are detailed, targeted, relevant and free.

Much of the world uses these reports to receive rapid notification when computer networks globally are misconfigured, vulnerable, abusable, get compromised or become infected.

Everyone can get free daily reports about who/what is at risk in their own network/country.
Every day, Shadowserver sends free network reports to 4600+ organizations globally.

These emailed reports provide details of who is infected, violated, controlled and out of compliance in each organization.

If Shadowserver sees a problem on your network, then all Miscreants can exploit that problem.
Scanning each network from the “outside-in” is a small part of a proven Public Benefit Service:

- 15 years of **Trust** that includes operating malware sinkholes, honeynets, spam traps, domain confiscation, malware analysis, etc
- **Industry Unique Perspective** - providing a wide range of Network Reports which grow and evolve with each new investigation, botnet take down and cybercrime disruption action

What Goes Into the Daily Network Reports?

- Botnet Infiltration
- Honeynets
- CSP Feeds
- Malware Sinkholes
- Global Scans
- Malware Analytics
- SPAM/Phish Traps
- Takedown Operations
- Honeynets
- CSP Feeds
New Network Report types added by Community Action

- New network reports are added with each new category of incident
- Each network report type includes details of the source and recommended actions
- Over 111 network report types and growing!

https://www.shadowserver.org/what-we-do/network-reporting/
Brute Force Attack Report

This report identifies hosts that have been observed performing brute force attacks, using SISSDEN’s network of honeypots.

One of these honeypot type sensors is dedicated to detecting SSH and telnet attacks against network devices. These attacks typically involve brute-forcing credentials to obtain access.

Once access has been obtained, the devices are used for other attacks, which may involve installing malicious software that enables the device to function as part of a botnet. For example, the well-known Mirai botnets were used in this way to launch DDOS attacks.

Hacked devices may also be used to launch scans on other vulnerable Internet devices. In still other cases, using brute force to breach networking devices may enable a criminal to attempt financial theft. By inserting rogue DNS server entries into a home router’s network configuration, they can redirect user traffic to malicious webpages, making phishing attacks on the home network user.

When we detect brute force attacks, our system reports them to the owners of the network from which the attacks originate, or to the National CERTs responsible for that network.

This report was created as part of the EU Horizon 2020 SISSDEN Project.

ShadowServer
Publicly Disclosed Operations

- Goznum / Machette / Avalanche Y4 [& Live Ops] (2019)
- Gooligan Android / Avalanche Y1 / Mirai Botnet #14 (2016)
- AAEH/Beebone / XCodeGhost iOS / Dridex (2015)
- Gameover Zeus & Cryptolocker (2014)
- Conficker (2010 - 2008)

Criminal Actor, Botnet, and Malware Takedown data is all fed into Shadowserver’s Daily Network Reports to allow the organizations and victims to be notified and remediated.
The Miscreant’s Network Visibility

What can others see when looking into your network from the outside?
What is your organization’s risk?

Shadowserver’s daily Network Reporting is tuned by:
- ASNs for the organization
- CIDR Blocks
- Delegated IP Blocks (Cloud)
- Domains
How do Get Started?
# Subscribing to the Daily Network Reports


<table>
<thead>
<tr>
<th>Who Are you?</th>
<th>Your Network?</th>
<th>How do we Trust?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your name</td>
<td>Your ASNs and Customer ASNs</td>
<td>List of Emails to send the reports</td>
</tr>
<tr>
<td>Your organization</td>
<td>Your CIDR Blocks</td>
<td>List of references whom can vouch for you. Enter the name and contact</td>
</tr>
<tr>
<td>Your role within the organization</td>
<td>Your Domain Names</td>
<td>information for one or more individuals in your organization, ideally someone</td>
</tr>
<tr>
<td>Your email address</td>
<td></td>
<td>listed on the whois for your network space. This will help us verify your</td>
</tr>
<tr>
<td>Your phone number</td>
<td>If you are a national CERT, list your country.</td>
<td>identity.</td>
</tr>
<tr>
<td>Your PGP key (for an encrypted reply)</td>
<td>If you are doing this on behalf of another network, please explain.</td>
<td></td>
</tr>
</tbody>
</table>

---

[SHADOWSERVER](https://www.shadowserver.org)
Shadowserver cannot “grant” people access to the data.

Shadowserver staff will work with you to validate that you have the authority and responsibility over the ASNs, CIDR Blocks (IP addresses), and Domain names.

Sometimes it is best to start small, establish trust, then add to the list of what is reported.
General Theme - You only get free daily remediation reports for the networks or country(ies) that you can prove your authority (by ASNs, CIDRs, DNS Zones and national authorities).

Any organization may use any of the data that Shadowserver provides to them for free each day concerning their own network space, without any restrictions - we consider the data to be theirs, to do with as they want. We do not give Google’s data to Microsoft, or US data to the UK. We only give each network’s data to that network’s owner (plus their responsible national CERT/CSIRT and LE agencies).

Privacy & Terms has further details: https://www.shadowserver.org/privacy-and-terms/
Nationals CERTs with Legitimate Authority can request access to Country Data

Shadowserver offers National CSIRTs a clear view of what’s happening on their networks, providing personalized support to interpret the data and leverage its impact. Whether you’re responsible for a specific set of networks or every network in your region, together we can make a positive impact on Internet security.

Celebrating Milestones (European CERT/CSIRT Report Coverage)
FEBRUARY 23, 2020

Celebrating a particularly significant long term milestone - our 107th National CERT/CSIRT recently signed up for Shadowserver’s free daily networking reporting service, which takes us to 136 countries and over 90% of the IPv4 Internet by IP space/ASN. This has finally changed our internal CERT reporting coverage map of Europe entirely green.

In the Service of National CERT’s (revisited)
APRIL 2, 2019

Shadowserver recently achieved the significant milestone of having our 100th National CERT/CSIRT sign up for our free daily network reports, so we thought that this would be a good moment to provide an update on our global network remediation coverage.

Privacy & Terms has further details: https://www.shadowserver.org/privacy-and-terms/
Leveraging the Network Reports
Why are their 19 Computer infected with MBROOT?

Shadowserver’s Daily Network Report arrives with a new report on Torpig botnet (also called Sinowal or Mebroot). It is now part of the “victim notification” of a malware takedown.

19 computers in the network are infected!

Those computer were immediately pull off the network. They were fully patched, had the latest antivirus versions, and several were running extra browser security tool.

The potential damage to the organization was prevented by Shadowserver’s Network Report. The infection vector was identified and extra network protections were put in place to protect the organization. All from a public benefit report!
How are we going to monitor the security of our network?

Large Carrier in Indonesia sees their security risk, but does not yet have a big security budget.

Subscribes to Shadowserver’s Daily Network Reports. That provides +70 reports of an “outside scan,” malware, botnets, and other vulnerabilities.

Small team uses these reports to track down systems and equipment in the report. One problem, leads to another problem, which leads to several vulnerabilities and security incidents for which the “contracted vendors” neglected to patch.

The Daily Network Reports cost effectively kick started the Mobile Operator’s Security Team - translating vast amounts of high-quality security data into actionable insights. These reports cleaned up the network and prevented major loss to the Carrier’s business.
Major US Carrier takes the Daily Network Reports specific reflection systems in their ASN.

Using Netflow and known spoofed triggered … compares that list to the Daily Report list.

Now Knows where the Spoofed traffic is originating!

- Flowspec to block.
- Contact Peer to Backtrace.
Shadowser’s Unique Source Data
Shadowserver’s Unique Sources

Network Scanning

We scan the entire IPv4 Internet on 45 ports every day, looking for misconfigured or abusable systems that could be used in attacks or otherwise exploited. Then we send targeted, relevant, remediation reports to more than 4600 vetted data consumers, including nearly a hundred national governments and many Fortune 500 companies, free of charge.

45

scans of all 4 billion IPv4 Internet addresses every day

Honeypots & Honeyclients

Shadowserver operates large-scale sensor networks of honeypots and honeyclients placed in strategic locations around the world. These sensors are constantly harvesting attack events and malware samples, either through passively being discovered by attackers or by actively seeking out attacks.

2750

Class C networks of honeypots in 90 countries
Shadowserver’s Unique Sources

Sandboxes
This is where raw malware data is transformed to actionable insight. With hundreds to thousands of custom physical and virtual sandboxes, Shadowserver analyzes the malware we’ve harvested, instruments behavior on live Internet connections, and generates detailed technical reports: attributing criminal infrastructures and identifying hidden investigative leads.

713,000
malware binaries executed every day

External Blacklists
Blacklists were formed to eliminate malicious email, but when sender addresses are spoofed, they can end up on a blacklist through no fault of their own — and once you’re blacklisted, it’s hard to get out. We publish blacklists to help you find out if (and where) you’ve been blacklisted.

110
blacklists shared every day
Shadowserver’s Unique Sources

Sinkholes
We use sinkholes to collect information about compromised or infected computers and the victims they affect globally; then we report on these activities so that the victims can be remediated. When collaborating with us, our partners gain access to one of the largest sinkhole infrastructures in the world.

4-5 million
unique IP addresses sinkholed per day, across 391 different malware family variants

Data-sharing relationships
Shadowserver has reciprocal data-sharing relationships with governments, industry partners, and law enforcement agencies across the world. The malware and sinkhole data they share with us further expands the scope of what we can achieve.

100+
international data-sharing partners
Who is Shadowserver?
The Shadowserver Foundation is a nonprofit security organization working altruistically behind the scenes to make the Internet more secure for everyone.

Our mission is to make the Internet more secure by bringing to light vulnerabilities, malicious activity and emerging threats.

We promote a culture of sharing, equip organizations to improve their security, support criminal investigations, help protect victims, and offer free remediation reports.

We’re driven by the vision of a secure, threat-free Internet.

As security professionals, we understand there will always be obstacles on that path. Yet as passionate altruists committed to doing the right thing for the right reasons, we strive to that end: conducting leading-edge research and innovation with transparency, impartiality, and unassailable ethical standards.

https://www.shadowserver.org
Shadowserver by (some of the) numbers

**4 BILLION**
IPv4 addresses scanned 45 times per day. 139 Million hosts respond

**713K**
Unique malware samples ingested & analyzed *every day* by our sandboxes

**4-5 MILLION**
IP addresses per day sinkholed across 400 different malware variants

**2750**
Class C networks hosting honeypots & spampots

**11.6 PETABYTES**
of malware & threat intel stored, growing at 1+ PB/year

**40 BILLION**
SSL certificates, indexed & searchable in our data & analysis clusters

4600 network owners & **106 National CSIRTs in 135 countries** rely on our free daily reports

Behind the scenes support for dozens of international Law Enforcement operations

*Daily proactive security is in jeopardy unless you act.*