

# An Impactful Security BCP

An easy technique that every  
Operator would benefit NOW



# The Simple things Make a Big Difference

**Security Best Common Practices (BCPs) are not hard, they are not expensive. They take time, persistence, and consistency.**

- ▶ You do not need to pay to subscribe to any “security threat service.”
- ▶ You do not need to buy expensive scanning services.
- ▶ You have access to the most advanced “surface area” security service to let you know what the “bad guy” threat actors can see.

All of this is free and a public service that provides daily reports on your ASN, IP Blocks, and Domain Names. The reports are delivered via email or APIs.

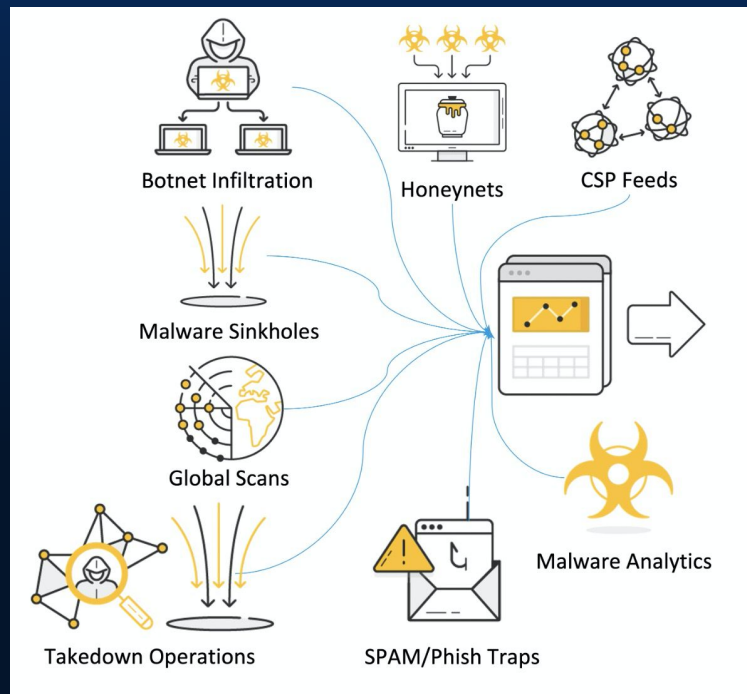
# Subscribing to the Daily Network Reports

Shadowserver.org Provides Organizations with an “Outside In” view of their network as a Public Service

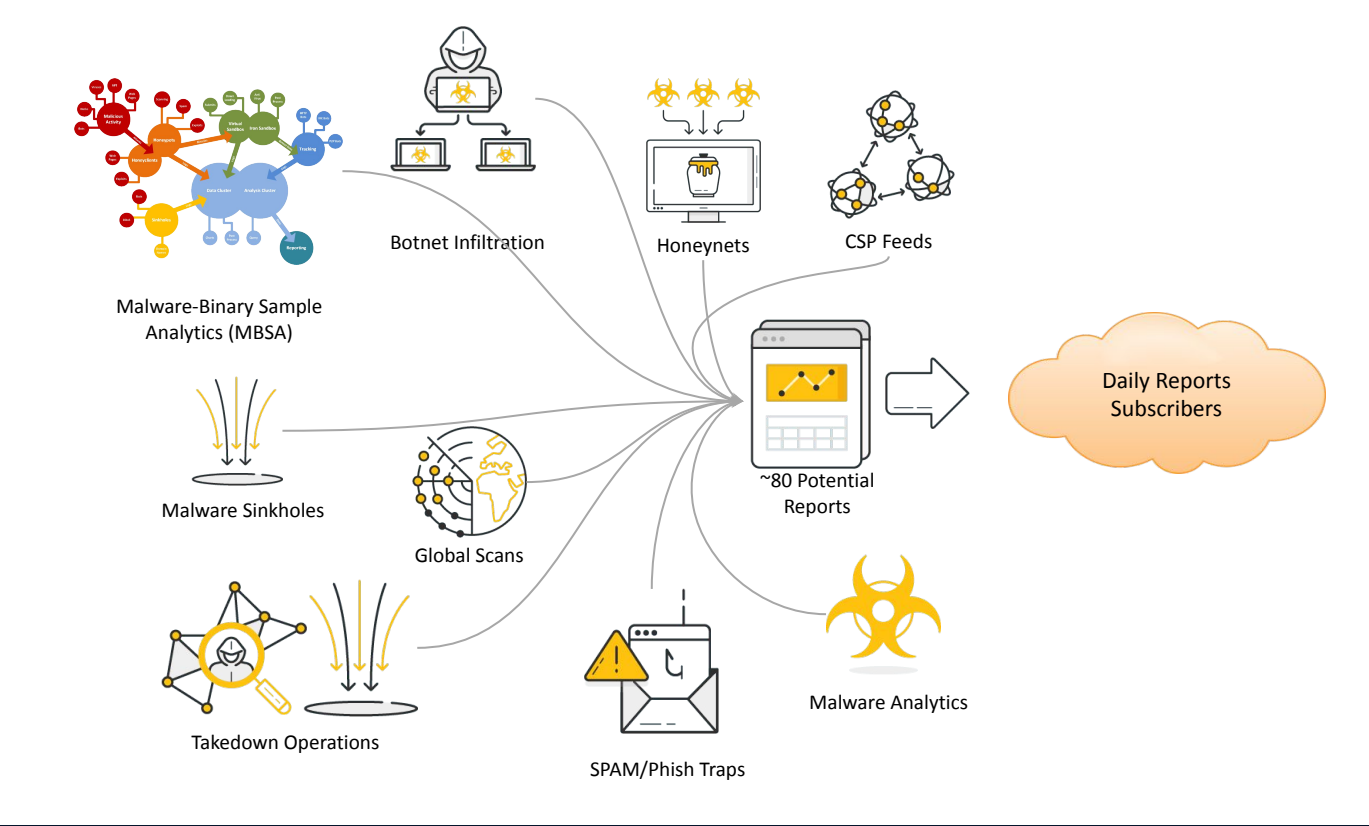
- Critical tool for any organization security toolkit.
- Find and Close Risk before they are exploited!

Sign up here:

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



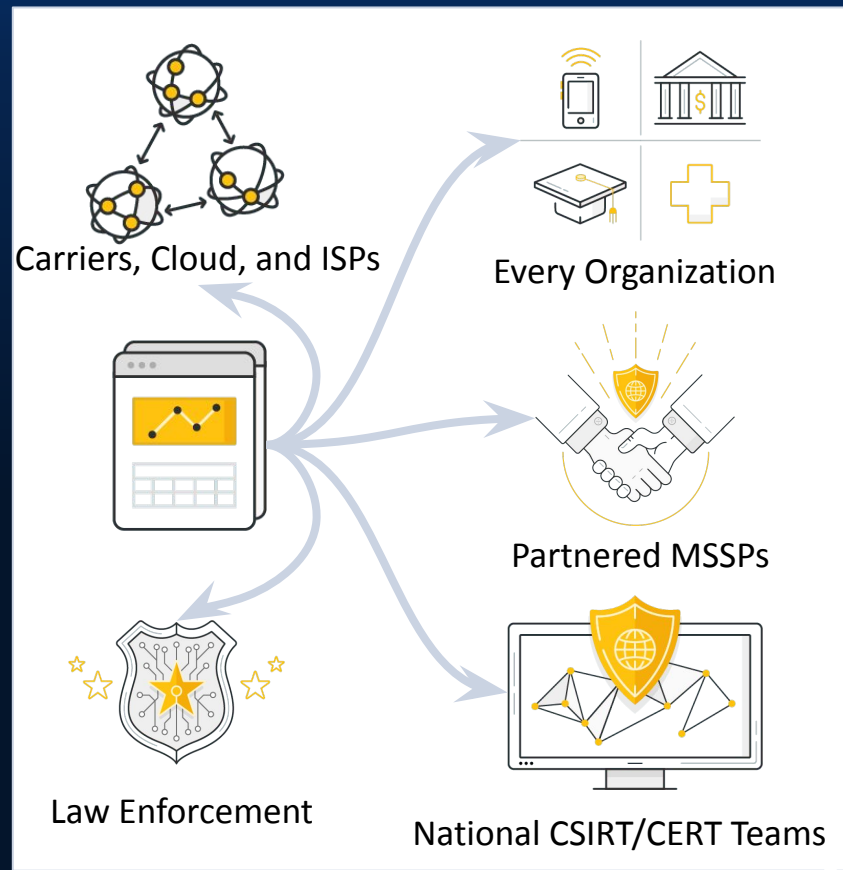
# Would it be nice ....



# What Goes Into the Daily Network Reports?



- ▶ 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*

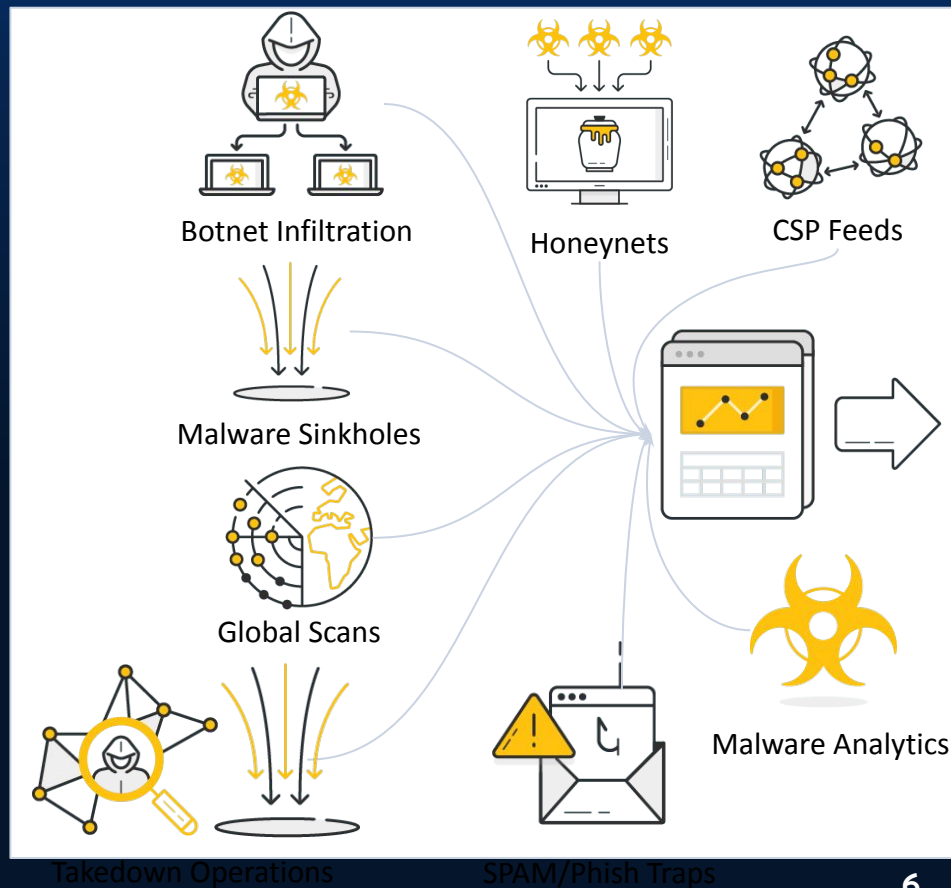


# What Goes Into the Daily Network Reports?



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



# Network Reports Highlight Actionable Risk



## 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 76 network report types and growing!

### OUR 76 REPORT TYPES

#### DNS Open Resolvers Report

This report identifies DNS servers that have the potential to be used in DNS amplification attacks by criminals that wish to perform denial of service attacks. Sourced from Service Scan. Updated every 24 hours.

#### Accessible XDMCP Service

This report identifies hosts that have the X Display Manager service running and accessible on the Internet. It's a Service Scan and is updated every 24 hours.

#### ASN Summary Report

In this report, we summarize the total activity over all time for the top 25 ASNs related to Command and Controls for botnets. This is a summary from all data sources. Updated weekly (Sunday).

#### Botnet URL Report

This report identifies URLs captured from botnet communications. 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. This data is sourced from Botnet monitoring. Updated every 24 hours.

#### Sinkhole HTTP Drone Report

This report identifies all the IPs that joined the sinkhole server that did not join via a referral URL. Sourced from Sinkholes. Updated every 24 hours.

# Network Report Details (example)



## 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 type was created as part of the EU Horizon 2020 SISSDEN Project.

### FIELDS

timestamp	Time that the attack was performed in UTC+0
ip	The IP address performing the attack
port	The source port used in the attack
asn	ASN announcing the attacking IP
geo	Country where the attacking IP resides
region	State / Province / Administrative region where the attacking IP resides
city	ASN of where the attacking IP resides
hostname	PTR record of the attacking IP
dest_ip	Country where the device in question resides
dest_port	Destination port used in the attack

### SAMPLE

```
"timestamp","ip","port","asn","geo","region","city","hostname","dest_ip","dest_port",":de
"2017-04-27 00:00:06","185.38.148.3",4428,200039,"UK","BRISTOL","BRISTOL","3.148.38.185.4
"2017-04-27 00:00:55","200.175.184.148",16503,18881,"BR","DISTRITO FEDERAL","BRASILIA",":
"2017-04-27 00:01:45","186.52.245.178",32941,6057,"UY","MONTEVIDEO","MONTEVIDEO","r186-5
"2017-04-27 00:05:45","77.126.141.114",56133,9116,"IL","HAMERKAZ","KEFAR SAVAN",":158.255
"2017-04-27 00:07:34","212.3.34.144",53558,39155,"ES","GRANADA","FUENTE CAMACHO","212-3-
"2017-04-27 00:09:55","180.169.17.83",58809,4812,"CN","SHANGHAI","SHANGHAI",":37.235.56.
"2017-04-27 00:13:31","197.46.62.186",56735,8452,"EG","AL QAHIRAH","CAIRO","host-197.46.
"2017-04-27 00:14:56","84.172.148.54",3316,3320,"DE","BADEN-WURTEMBERG","SCHRIESHEIM",":
"2017-04-27 00:16:29","171.231.155.225",56158,7552,"VN","BINH DINH","QUI NHON",":5.28.63
```



# Example of the Daily - SNMP

timestamp	ip	protocol	port	hostname	sysdesc
2022-05-19 09:38:06		udp	161		Cisco IOS Software Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M) Version 12.2(54)SG RELEASE SOFTWARE (fc3)Te
2022-05-19 09:49:18		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 10:03:53		udp	161		Cisco NX-OS(tm) n3000 Software (n3000-uk9) Version 6.0(2)U6(6) RELEASE SOFTWARE Copyright (c) 2002-2012 by Cisco Systems Inc.
2022-05-19 10:20:07		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 10:44:14		udp	161		Cisco IOS Software Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M) Version 12.2(54)SG RELEASE SOFTWARE (fc3)Te
2022-05-19 11:15:39		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 11:58:20		udp	161		Cisco IOS XR Software (NCS-5500) Version 7.1.2 Copyright (c) 2013-2020 by Cisco Systems Inc.
2022-05-19 14:07:19		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 14:33:17		udp	161		Cisco IOS Software C3560E Software (C3560E-UNIVERSALK9-M) Version 12.2(55)SE1 RELEASE SOFTWARE (fc1)Technical Support: htt
2022-05-19 15:05:26		udp	161		Cisco IOS Software Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M) Version 12.2(54)SG RELEASE SOFTWARE (fc3)Te
2022-05-19 15:12:21		udp	161		Cisco IOS Software Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICESK9-M) Version 12.2(54)SG RELEASE SOFTWARE (fc3)Te

Each of these devices have SNMP ports open to the Internet.

They are exposed for abuse.

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

# Example of the Daily - SNMP

sysname	asn	geo	region	city	version	naics	sic	sector	device_vendor	device_type	device_model	d
		US	OREGON	PORTLAND	2	517919		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		US	MASSACHUSETTS	CAMBRIDGE	2	517919		Communications, Service Provider, and Hosting Service				
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		US	WASHINGTON	SEATTLE	2	517919		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting Service	Cisco		IOS	
		AR	CAPITAL FEDERAL	BUENOS AIRES	2	517919		Communications, Service Provider, and Hosting Service				
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting S				
		JP	TOKYO	TOKYO	2	518210		Communications, Service Provider, and Hosting S				
		US	WASHINGTON	SEATTLE	2	517919		Communications, Service Provider, and Hosting S				
		US	WASHINGTON	SEATTLE	2	517919		Communications, Service Provider, and Hosting S				

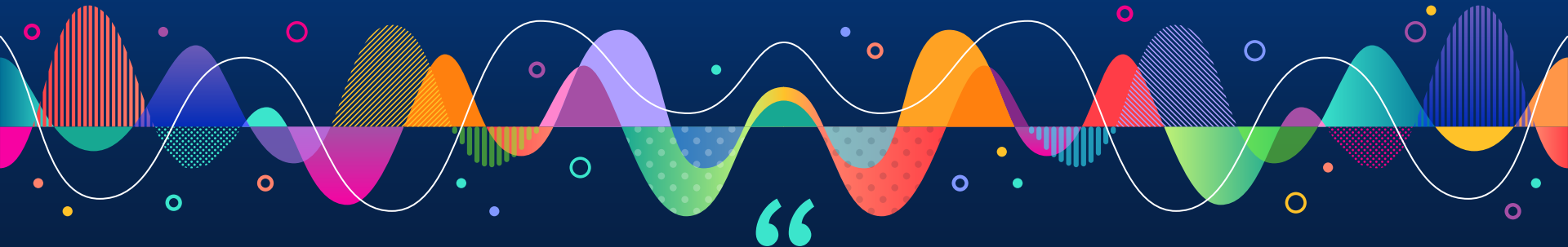
device_sector	tag	community
enterprise	snmp	public
enterprise	snmp	public
	snmp	public
enterprise	snmp	public
enterprise	snmp	public
enterprise	snmp	public
	snmp	public
enterprise	snmp	public
enterprise	snmp	public
enterprise	snmp	public
enterprise	snmp	public
enterprise	snmp	public

The Shadowserver reports using geolocation to provide the region and city.

Notice the “public” SNMP Community

# Example of the Daily - SNMP





“

# How Network are Leveraging Shadowserver's Daily Network Reports to Reduce Their Risk to Attack

# Hardware Vendor's Network

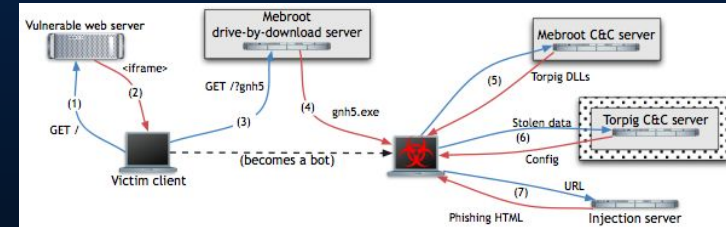


## Why are their 19 Computer infected with MBROOT?

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 immediatly 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!**

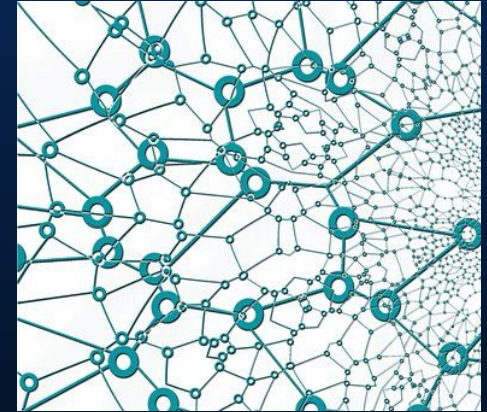
# Mobile Telecom Operator Example

## 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.



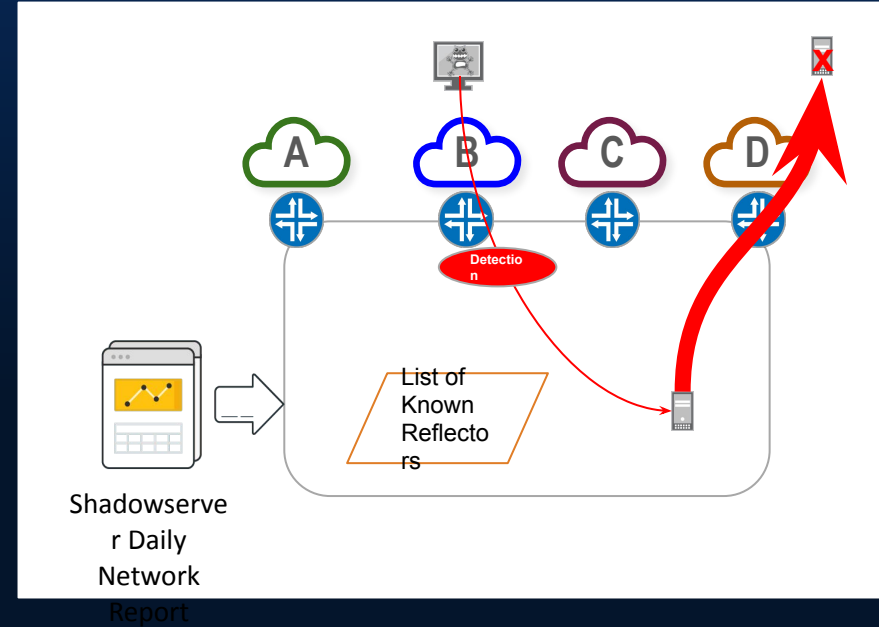
**The Daily Network Reports cost effectively kick started the Mobile Operator's Security Team - translating vast amounts of high-quality security data into actionable insights. These reports cleaned up the network and prevented major loss to the Carrier's business.**

# Tracking Spoofed Traffic Into the Network

- 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



# How to Sign Up and Get Started with Shadowserver's Daily Reports



# Subscribing to the Daily Network Reports



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

## Who Are you?

Your name

Your organization

Your role within the organization

Your email address

Your phone number

Your PGP key (for an encrypted reply)

## Your Network?

Your ASNs and Customer ASNs

Your CIDR Blocks

Your Domain Names

If you are a national CERT, list your country.

If you are doing this on behalf of a another network, please explain.

## How do we Trust?

List of Emails to send the reports

List of references whom can vouch for you. Enter the name and contact information for one or more individuals in your organization, ideally someone listed on the whois for your network space. This will help us verify your identity.

# How will Shadowserver Validate Trust?



***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.

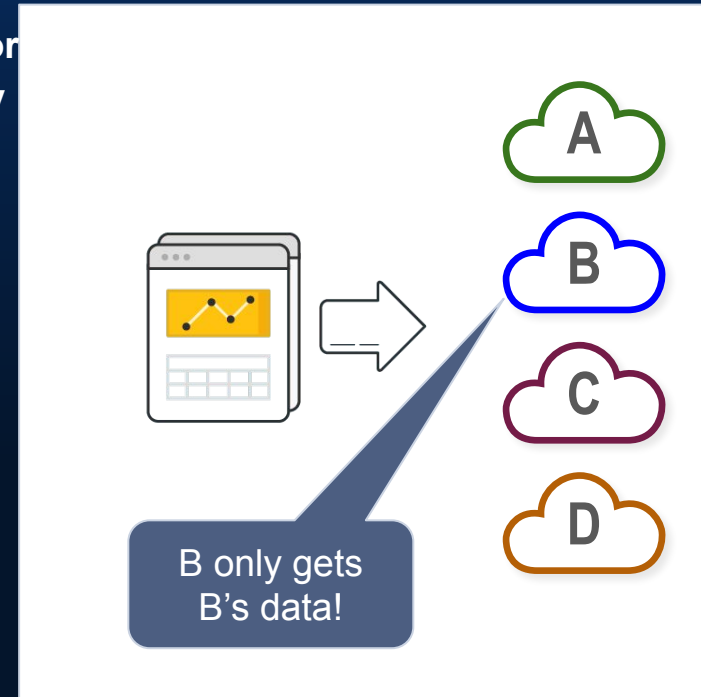


# Shadowserver's Data Sharing Principles



**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/>

# Shadowserver's Data Sharing Principles



## 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

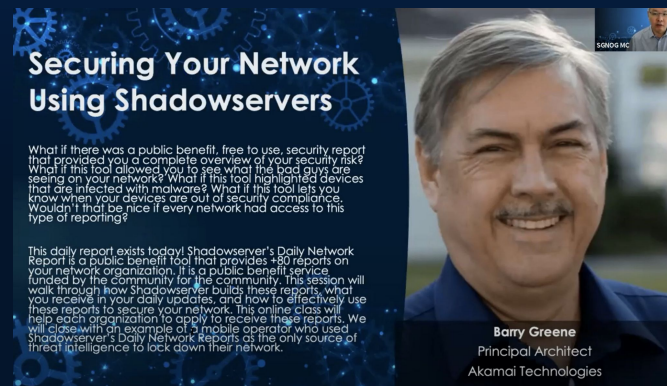
Shadowserver recently achieved the significant milestone of having our 100th National CERT/CSIRT sign up for our free daily network reports, so we thought that this would be a good moment to provide an update on our global network remediation coverage.

Privacy & Terms has further details: <https://www.shadowserver.org/privacy-and-terms/>

# Watch the Webinar - Leveraging Shadowserver

Securing Your Network Using Shadowserver's Daily Network Reports is a webinar that walks organizations through how these daily reports are used by organizations large and small - all as a public benefit.

- ALL Organizations can have all your domains, IP addresses, and devices monitor by Shadowserver.
- Only you get this data.
- It is a list of vulnerabilities and risk that the bad threat actors also see.



**Securing Your Network Using Shadowservers**

What if there was a public benefit, free to use, security report that provided you a complete overview of your security risk? What if this tool allowed you to see what the bad guys are seeing on your network? What if this tool highlighted devices that are infected with malware? What if this tool lets you know when your devices are out of security compliance. Wouldn't that be nice if every network had access to this type of reporting?

This daily report exists today! Shadowserver's Daily Network Report is a public benefit tool that provides +80 reports on your network organization. It is a public benefit service funded by the community for the community. This session will walk through how Shadowserver builds these reports, what you receive in your daily updates, and how to effectively use these reports to secure your network. This online class will help each organization to apply to receive these reports. We will close with an example of a mobile operator who used Shadowserver's Daily Network Reports as the only source of threat intelligence to lock down their network.

**Barry Greene**  
Principal Architect  
Akamai Technologies

# “Plug in” and “Review” Key CSIRT/CERT Teams

The National CERT Teams from many countries send out alerts to their constituents. Most allow anyone to sign up for the email alerts. This is an easy “alert to action tool” to find out immediate risk. They are critical during a time of cyber-crisis. These organizations will have classified/TLP: RED intelligence they can now share, BUT WILL SHARE THE MEANS TO MINIMIZE THE RISK TO THE CLASSIFIED THREAT! Here is a small list to get started. A larger list can be found by looking at all the members from FIRST (Forum of Incident Response and Security Teams).

- [Australian Cyber Security Centre \(ACSC\)](#) – All of ACSC’s alerts can be viewed here: [View all alerts](#). They are broken down by end-user role, making it easier to gain their constituent’s attention. Sign up from their alerts [Get alerts on new threats Alert Service](#) page.
- [Canadian Centre for Cyber Security \(CCCS\)](#) – their advisories are listed on [Alerts and advisories](#) and sign up for the alerts are via RSS and Twitter.
- [CERT New Zealand \(CERT-NZ\)](#) – Use CERT-NZ’s “Subscribe do updates” on their homepage and/or follow them on social media. The list of alerts is sorted by Individuals, Businesses, and IT Specialists.
- [European Union Agency for Cybersecurity, ENISA](#) - ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. All ENISA’s Advisory, Guidelines and Security Tools are posted to their [Newsroom](#)
- [UK National Cyber Security Centre – NCSC.GOV.UK](#) – NCSC’s Security Alerts are on their [News page](#). You can sign up for weekly reports and the immediate email alerts here – <https://ncsc-production.microsoftcrmporals.com/subscribe/>
- [National Cyber Security Centre New Zealand](#) - <https://www.ncsc.govt.nz/newsroom/>
- [CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY \(CISA\)](#) -.You can subscribe to all the CISA updates and Advisories here: Email Updates. A full list of the advisories is on the [National Cyber Awareness System](#).

# Consequence of not paying attention?

## Feb 2022 new alerts on network infrastructure!

- ▶ *Three years ago, the Department of Homeland Security (DHS) released an alert on how cyber adversaries obtained hashed password values and other sensitive information from network infrastructure configuration files.*
- ▶ *Once the hashes were obtained, the adversaries were able to compromise network devices.*
- ▶ *That alert showed the results of what happens when cyber adversaries compromise device configurations that have insecure, reversible hashes: they are able to extract sensitive information and compromise networks [1].*

[https://media.defense.gov/2022/Feb/17/2002940795/-1/-1/1/CSI\\_CISCO\\_PASSWORD\\_TYPES\\_BEST\\_PRACTICES\\_20220217.PDF](https://media.defense.gov/2022/Feb/17/2002940795/-1/-1/1/CSI_CISCO_PASSWORD_TYPES_BEST_PRACTICES_20220217.PDF)

## NSA Issues Guidance for Selecting Strong Cisco Password Types

Poorly protected passwords in device configuration files present a risk of compromise, agency says.



Jai Vijayan  
Contributing Writer

February 17, 2022



National Security Agency | Cybersecurity Information Sheet

### Cisco Password Types: Best Practices

Three years ago, the Department of Homeland Security (DHS) released an alert on how cyber adversaries obtained hashed password values and other sensitive information from network infrastructure configuration files. Once the hashes were obtained, the adversaries were able to compromise network devices. That alert showed the results of what happens when cyber adversaries compromise device configurations that have insecure, reversible hashes: they are able to extract sensitive information and compromise networks [1].

The rise in the number of compromises of network infrastructures in recent years is a reminder that authentication to network devices is an important consideration.

Network devices could be compromised due to:

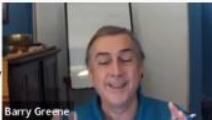
- Poor password choice (vulnerable to brute force password spraying),
- Router configuration files (which contain hashed passwords) sent via unencrypted email, or
- Reused passwords (where passwords recovered from a compromised device can then be used to compromise other devices).

#### NSA recommends using:

- Multi-factor authentication when feasible
- Type 8 for passwords
- Type 6 for VPN keys
- Strong, unique passwords
- Privilege levels for least privilege

# Watch the APRICOT 2022 Session ....

Russian State-Sponsored Actors Targeting Network Infrastructure




**[Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices \(TA18-106A\) April 20, 2018](#)**

Update: On April 19, 2018, an industry partner notified NCCIC and the FBI of malicious cyber activity that aligns with the techniques, tactics, and procedures (TTPs) and network indicators listed in this Alert. Specifically, the industry partner reported the actors redirected DNS queries to their own infrastructure by creating GRE tunnels and obtained sensitive information, which include the configuration files of networked devices.

NCCIC encourages organizations to use the detection and prevention guidelines outlined in this Alert to help defend against this activity. For instance, administrators should inspect the presence of protocol 47 traffic flowing to or from unexpected addresses, or unexplained presence of GRE tunnel creation, modification, or destruction in log files.

Systems Affected

- Generic Routing Encapsulation (GRE) Enabled Devices
- Cisco Smart Install (SMI) Enabled Devices
- Simple Network Management Protocol (SNMP) Enabled Network Devices

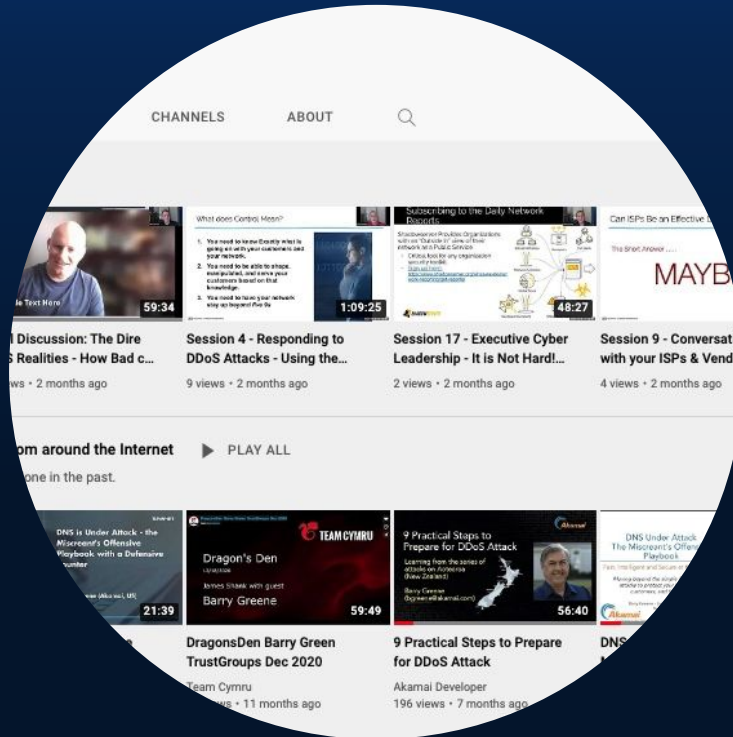
 Barry Greene - CC-Attribution-ShareAlike (BY-SA) 2022-02-24 13:15:28

**[Session 4.1 - Protecting Routers, Switches, and Network Devices \(APRICOT 2022 - Day 4\)](#)**



# Subscribe to Senki's Youtube Channel

Long list of current and past Network Security tutorials and presentations.



Several new videos each month with current Security & Resilience briefings and tutorials

[https://www.youtube.com/channel/UCikUeU1\\_i9K7q6Qk5P85XvA](https://www.youtube.com/channel/UCikUeU1_i9K7q6Qk5P85XvA)

# What's Next?

- ▷ Connect: to Barry Greene

[bgreene@akamai.com](mailto:bgreene@akamai.com) or [bgreene@senki.org](mailto:bgreene@senki.org)

Linkedin - [www.linkedin.com/in/barrygreene/](https://www.linkedin.com/in/barrygreene/)

Whatsapp & Signal - +1 408 218 4669

- ▷ Ask Questions .....



Slides: Email to [bgreene@senki.org](mailto:bgreene@senki.org) for the Links