SHADOWSERVER

Lighting the way to a more secure Internet

Overview of 'Free Public Benefit' Network Security Reports

🐦 @shadowserver

✉ contact@shadowserver.org

SHADOWSERVER.ORG
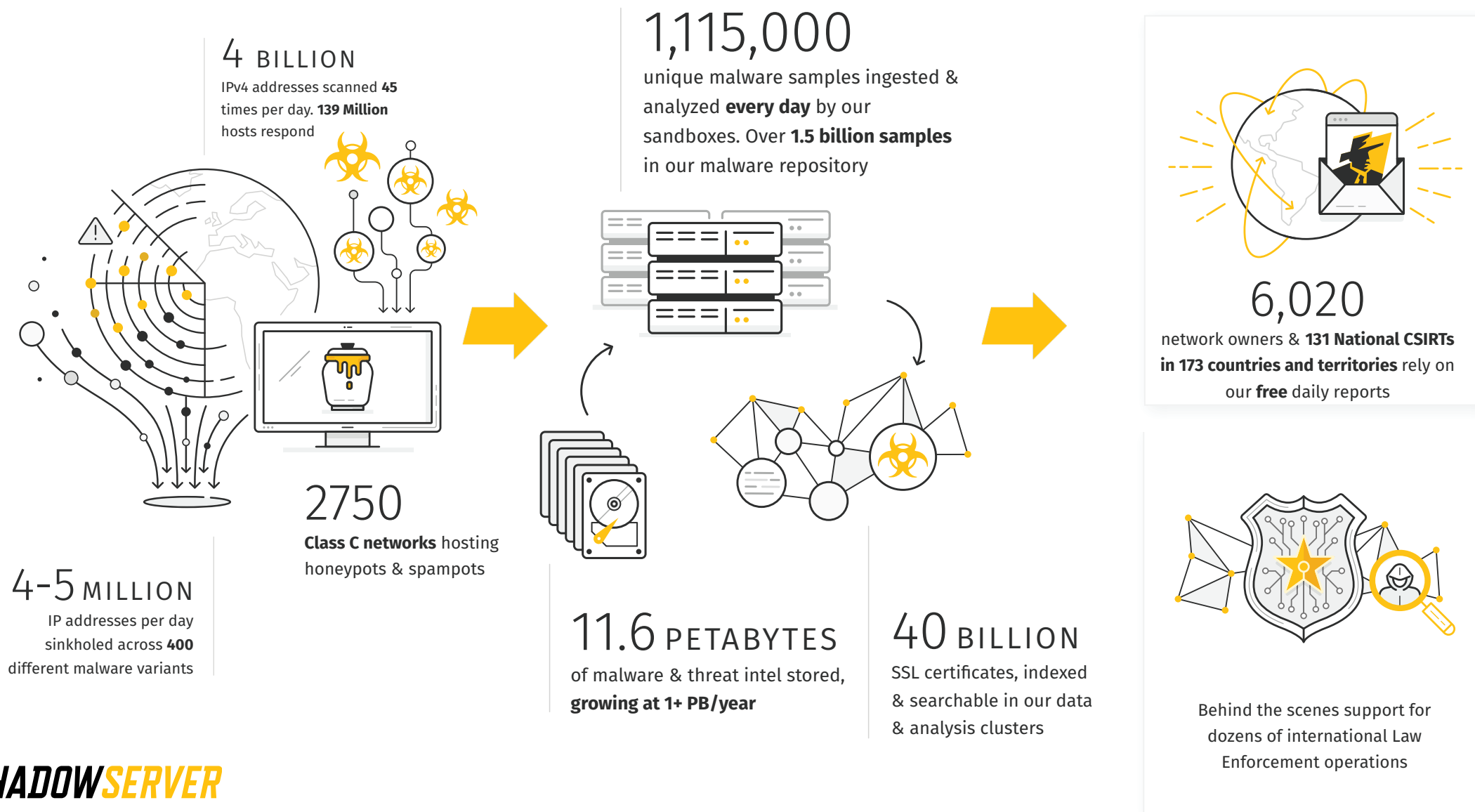
Presentation Aims & Objectives

- To provide an overview of The Shadowserver Foundation

- To provide an overview of Shadowserver reports and how to subscribe

- To demonstrate the benefit of Shadowserver reports as

  - a National CERT/CSIRT

  - an ISP

  - an enterprise

  - a government agency

  - a financial institution

What is The Shadowserver Foundation ?

- A not-for-profit organisation (NPO) working to make the Internet more secure for everyone

- **Unique insight into network security**, a **global vantage point** and **proven partnerships** with:
    - *National Computer Security Incident Response Teams (nCSIRTs)*
    - *Law Enforcement*
    - *Industry and security researchers world-wide*

- **Shares information with Internet defenders at no cost** to mitigate vulnerabilities, detect malicious activity and counter emerging threats.

- An unparalleled combination of position, **trusted information** and **15 years of proven community partnerships** enables Shadowserver to **perform a critical role in Internet security** - **the world's largest provider of free cyber threat intelligence.**

Shadowserver by (some of the) numbers

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

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

2750
Class C networks hosting honeypots & spampots

1,115,000
unique malware samples ingested & analyzed **every day** by our sandboxes. Over **1.5 billion samples** in our malware repository

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

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

6,020
network owners & **131 National CSIRTs in 173 countries and territories** rely on our **free** daily reports

Behind the scenes support for dozens of international Law Enforcement operations
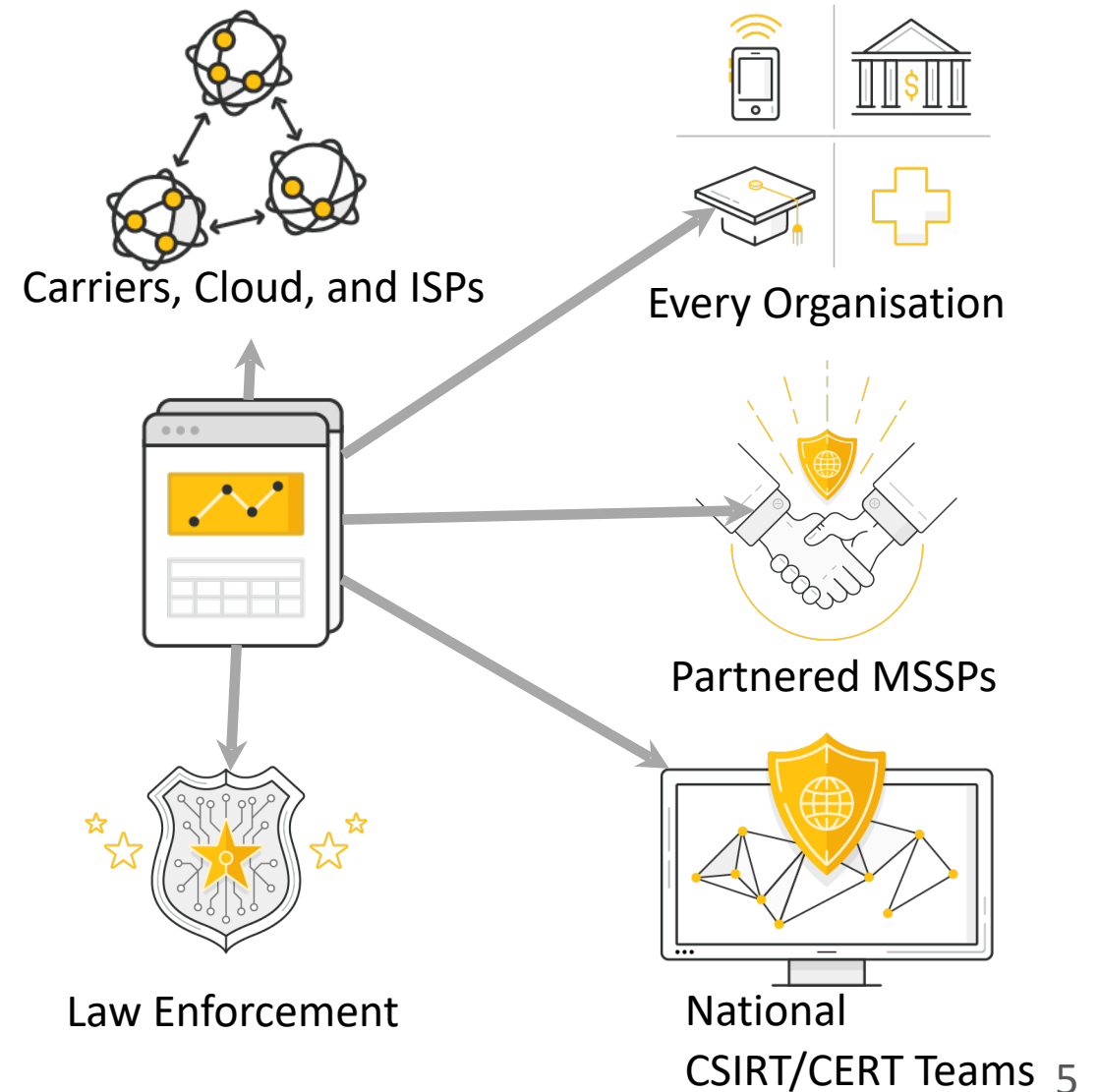
SHADOW SERVER

What Goes Into the Daily Network Reports?

- Every day, Shadowserver sends free network reports to 6000+ organisations globally

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

- *If Shadowserver sees a problem on your network, then it is likely all bad actors can see and exploit that problem*

Carriers, Cloud, and ISPs

Every Organisation

Partnered MSSPs

Law Enforcement

National CSIRT/CERT Teams

What can others see when looking into your network from the outside?

What is your organisation's risk?

Shadowserver's daily Network Reporting is tuned by:

- ASNs for the organisation
- CIDR Blocks (including IPv6)
- Delegated IP Blocks (Cloud)
- Domains (including entire TLDs)
- Geo-location (for National CSIRTs)
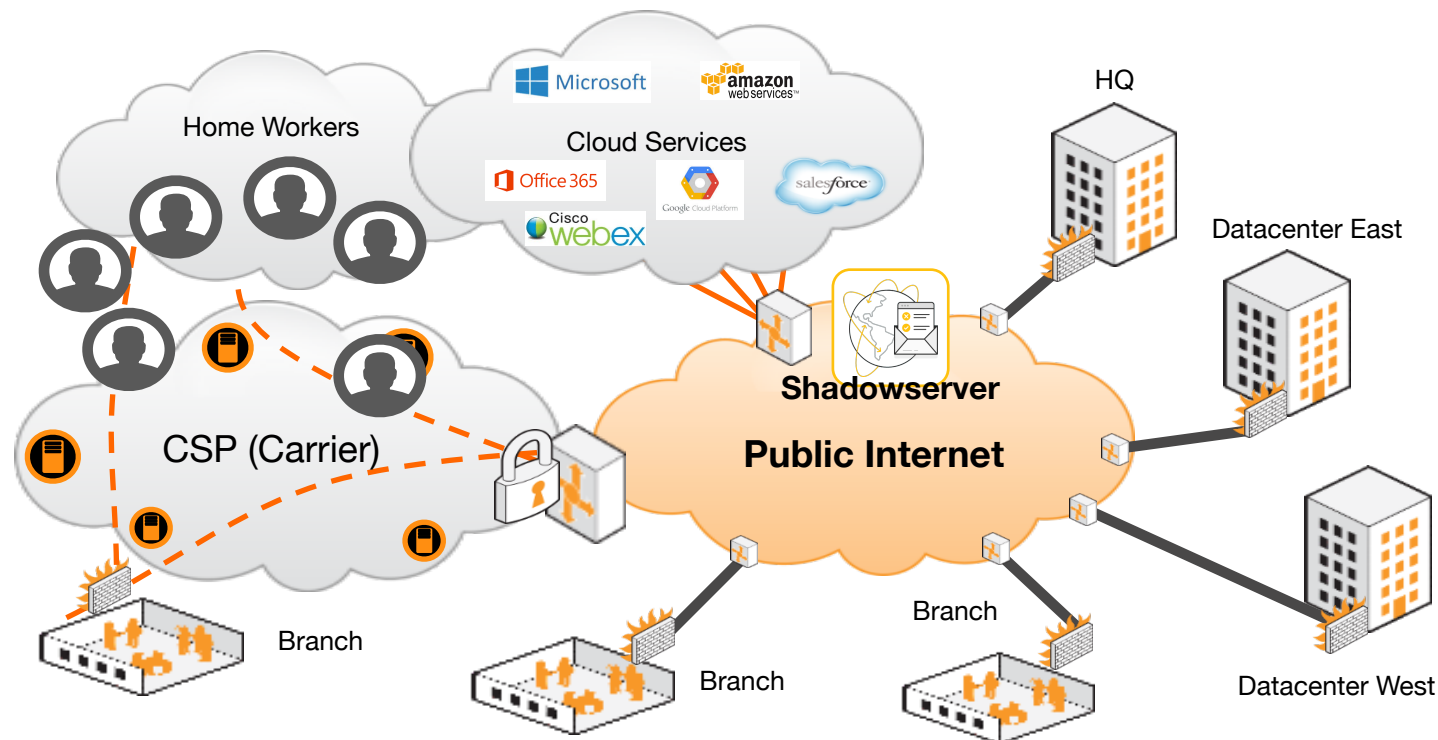
Network Reports Highlight Actionable Risk

New Network Report types are 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 70 network report types and growing!

- Includes optional reports for population type scans (like SSL certificate inventory, exposed SSH services etc)

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

Accessible ADB Report	This report identifies hosts that have the Android Debug Bridge (ADB) running, bound to a network port (5555/tcp) and accessible on the Internet. It's a Service Scan, and it's updated every 24 hours.
Accessible AFP Report	This report identifies hosts that have the Apple Filing Protocol (AFP) running and accessible on the Internet. It's a Service Scan, and it's updated every 24 hours.
Accessible Apple Remote Desktop (ARD) Report	This report identifies hosts that have the Apple Remote Desktop service on port 3283/udp running and accessible on the Internet. It is a Service Scan and it's updated every 24 hours.
Accessible Cisco Smart Install Report	This report identifies hosts that have the Cisco Smart Install feature running and are accessible to the Internet at large. It's a Service Scan, and it's updated every 24 hours.
Accessible CoAP Report	This report identifies hosts that have the Constrained Application Protocol (CoAP) service enabled on port 5683/UDP and accessible on the Internet. It's a Service Scan, and it's updated every 24 hours.
Accessible FTP Report	This report identifies hosts that have an FTP instance running on port 21/TCP that's accessible on the Internet. It's a Service Scan, and it's updated every 24 hours.
Accessible Hadoop Report	This report identifies hosts that are running Hadoop and have either the NameNode or DataNode web interfaces running and accessible to the world on the Internet. It's a Service Scan, and it's updated every 24 hours.
OPTIONAL: Accessible HTTP Report	This report identifies hosts that have the Hypertext Transfer Protocol (HTTP) running on some port and are accessible on the

SHADOW**SERVER**

Honeypot Brute Force Events Report

This report identifies hosts that have been observed performing brute force attacks, using different networks of honeypots. This includes attacks brute forcing credentials to obtain access using various protocols, such as SSH, telnet, VNC, RDP, FTP etc.

Once access has been obtained, devices may be 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.

Filename: **event4_honeypot_brute_force**

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

Co-financed by the Connecting Europe
Facility of the European Union
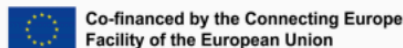
FIELDS

timestamp	Timestamp when the IP was seen in UTC+0
protocol	Packet type of the connection traffic (UDP/TCP)
src_ip	The IP of the device in question
src_port	Source port of the IP connection
src_asn	ASN of the source IP
src_geo	Country of the source IP
src_region	Region of the source IP
src_city	City of the source IP
src_hostname	Reverse DNS of the source IP
src_naics	North American Industry Classification System Code
src_sector	Sector to which the IP in question belongs; e.g. Communications, Commercial

SAMPLE

```
"timestamp","protocol","src_ip","src_port","src_asn","src_geo","src_region","src_city","
"2021-03-27 00:00:00","tcp","141.98.x.x",30123,209588,"NL","NOORD-HOLLAND","AMSTERDAM",,
"2021-03-27 00:00:00","tcp","5.188.x.x",55690,57172,"NL","NOORD-HOLLAND","AMSTERDAM",,51
"2021-03-27 00:00:00","tcp","45.14.x.x",38636,44220,"RO","BIHOR","ORADEA",,,,,,,"82.118.
"2021-03-27 00:00:00","tcp","5.188.x.x",56385,49453,"NL","NOORD-HOLLAND","AMSTERDAM",,51
"2021-03-27 00:00:00","tcp","45.14.x.x",35802,44220,"RO","BIHOR","ORADEA",,,,,,,"82.118.
"2021-03-27 00:00:00","tcp","5.188.x.x",33289,49453,"NL","NOORD-HOLLAND","AMSTERDAM",,51
```

Subscribing to the Daily Network Reports

Subscribe to Reports

Complete the form below to request free, detailed, relevant, daily remediation reports about the state of your networks. We'll evaluate your request and follow up with you. **There is no charge for this service.**

It's really free!

Network Reporting

Investigation Support

Network details

E-mail address where reports or download links will be sent

Your information

Your name

Your organization

Your role within the organization

Your email address

Your phone number

Your PGP key (for an encrypted reply)

Your network

List the ASNs or CIDRs for the network space that you directly control (ASNs are preferred, but only if you control the complete ASN). Do not list the ASNs or CIDRs of your ISP. You can also list domain name space under your control.

If you're a National CSIRT, simply list the country you represent.

Report Recipient(s)

Enter the email(s) where reports should be sent. Use a comma to separate multiple email addresses.

Your references

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 did you hear about us?

— Select one

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 (or at the country level for National CERTs/CSIRTs).

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 you are responsible for (by ASNs, CIDRs, DNS Zones and national authorities).

Any organisation 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).

A

B

C

D

B only gets B's data!
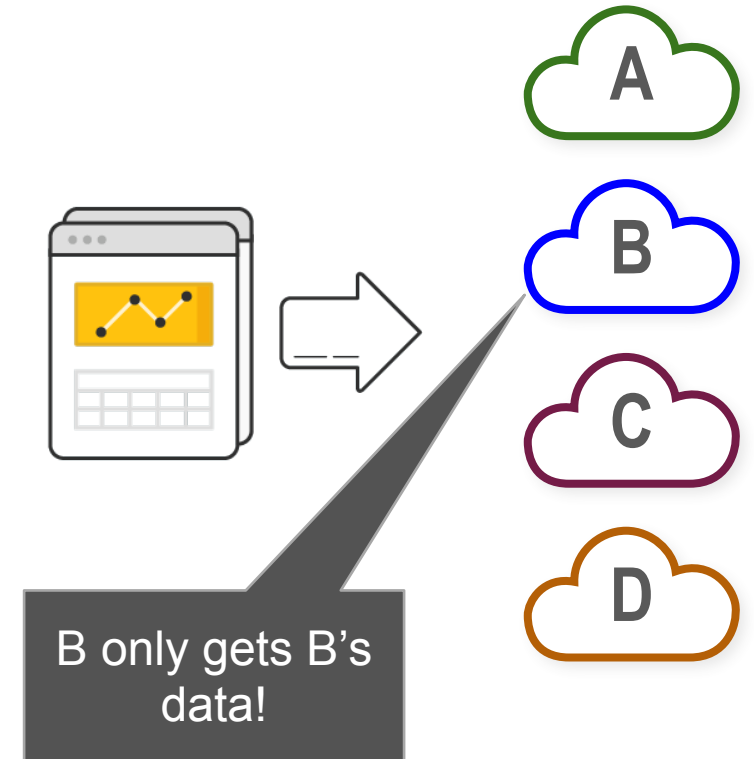
Shadowserver's Data Sharing Principles

Nationals CERTs/CSIRTs 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 though that this would be a good moment to provide an update on our global network remediation coverage.

- E-mail (must always be provided, even if only for notifications)

- Report file download links

- Webspace with report files

- API with report files

Reports are always files in CSV format

https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

API: Reports Query

Last Updated: 2020-10-29

Reports API

An API to query the different reports received as well as to do basic queries of the data itself. This is meant as an optional replacement to the emails received with the report URL's. In all cases the queries and the data that is delivered is only from the reports that you would have normally received. You only get the data on the networks you are responsible for. You will not be able to get data on other networks or systems. Note refer to the **API: Documentation** pages for testing details and examples.

Modules

- reports/subscribed – List of reports that the user is subscribed to

- reports/types – List of all the types of reports that are available for the subscriber

- reports/list – List of actual reports that could be downloaded

- reports/download – Download specific report

- reports/query – Query the stored data

REPORTS METHODS

REPORTS/SUBSCRIBED

Note that most organizations will only have a single list they are subscribed to and can get data on.

Fields:

```
apikey : string : Your API key
```

New Report Developments ...

Changes in Sinkhole and Honeypot Report Types and Formats

APRIL 1, 2021

Over the years, Shadowserver's report list has grown considerably from when we originally started. Our daily reports now number over 80 distinct types and they include data from a large amount of sources, including sinkholes, sandboxes, scans, honeypots and several others. When some of these reports were originally set up, the requirements were different to those needed today.

As a result, various stop gap measures were employed – some of the report types formats had to be modified over time and extended, and sometimes new data types adapted to fit, and in some cases some data sets were more forcibly modified so that the report still worked. This has sometimes led to confusion to our report recipients. What is the exact difference between a drone report and a sinkhole report for example? Additionally, some report types have not been used for a long time.

We have therefore decided to implement changes with some of the existing report types, especially those related to our sinkholes and honeypots, as well as remove some legacy reports.

The following reports will be reorganized (old reports will be marked as *LEGACY* on **2021-06-01**, and after **2021-06-01** only the new reports will be available in their place):

- Amplification DDoS Victim Report –> Honeypot Amplification DDoS Events [event-honeypot-ddos-amp]
- Brute Force Attack Report –> Honeypot Brute Force Events [event-honeypot-brute-force]
- CAIDA IP Spoofer report –> IP Spoofer Events Report [event-ip-spoofer]
- Darknet Report –> Darknet Events [event-honeypot-darknet]
- Drone/Botnet-Drone Report –> Sinkhole Events Report [event-sinkhole], Darknet Events [event-honeypot-darknet], Sinkhole HTTP Events Report [event-sinkhole-http]
- HTTP Scanners Report –> Honeypot HTTP Scanner Events [event-honeypot-http-scan]
- ICS Scanners Report –> Honeypot ICS Scanner Events [event-honeypot-ics-scan]
- Microsoft Sinkhole Report –> Sinkhole HTTP Events Report [event-sinkhole-http]
- Sinkhole DNS Report –> Sinkhole DNS Events Report [event-sinkhole-dns]
- Sinkhole HTTP Drone Report –> Sinkhole HTTP Events Report [event-sinkhole-http]
- Sinkhole HTTP Referrer Report –> Sinkhole HTTP Referer Events Report [event-sinkhole-http-referer]

Announcing the New Report Delta Mode Option

APRIL 29, 2021

Standard **Shadowserver reports** cover a 24 hour period (the previous day) of events. Every single day we send out a full day of observed events from the previous day to report subscribers. This means that whenever we detect an event within a network and this event persists, we will continue to report that same event every single day. For some networks, that means a lot of events get sent daily. Additional effort is required by the recipient to be able to detect any daily changes in the reported events, which is often of interest to many report consumers.

A **new opt-in** feature in our reporting mechanism will allow for reporting only the changes of the data from day to day: the **report delta mode option**. In this mode, every Sunday we will continue to deliver a full set of reports on all events observed on a report recipient's network. For the rest of the week, for every distinct report type we will report only the difference between events seen on that day relative to the Sunday report. This will continue throughout the week until the following Sunday, when everything is reset and a full report is delivered again.

Deltas are calculated based on a row hash excluding the timestamp and source port columns. Not all report types support the delta option. For report types that do not support the delta option, a full report will be created.

The new report delta feature is **opt-in only**. If you would like to enable this mode **please request it explicitly**. You can do so by using the **contact us** form. Of course, if you are not interested in using this mode you will continue to receive the full data set every day as always.

If you have not subscribed yet but are about to do so and would like to have access to our reports using the report delta mode, method please mention this when **subscribing to our reports**.

When using our **new Report API** and downloading the daily reports, the reports will be the delta version if this option is enabled. Note that the report statistics from the API will also be affected and reflect the data in the daily reports. All the changes are reflected on the actual data being shared daily.

This will also impact the statistics that are sent in the quarterly review report from Shadowserver. The total number of reported events will be less for any period since only unique events are being reported over a week period.

Case Studies

Using the Shadowserver Reports to improve the cybersecurity of your networks/constituency

Case #1 - Situational Awareness at Country Level
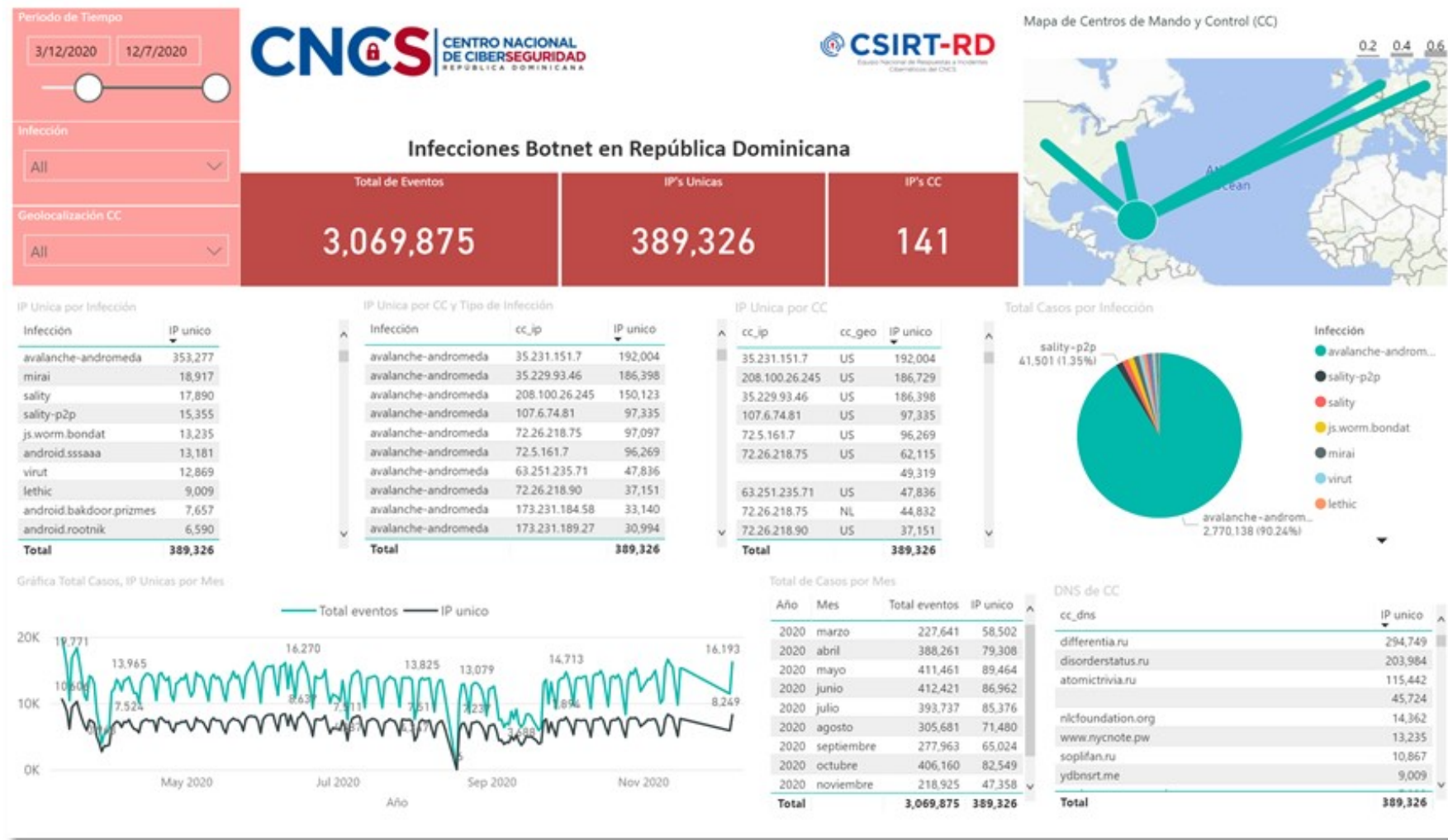
Obtaining the situational awareness picture

How can a National CSIRT obtain the big picture of what is happening in its country's networks?

A National CSIRT is set up by the Government of a country. It is seeking situational awareness into what is happening on the Internet in its country and obtaining the big picture of threats and vulnerabilities identified. It signs up to Shadowserver's free daily network reports that quickly provide the big national picture. Daily actionable information is delivered to the CSIRT which helps identify the "hot spots" of malicious activity.
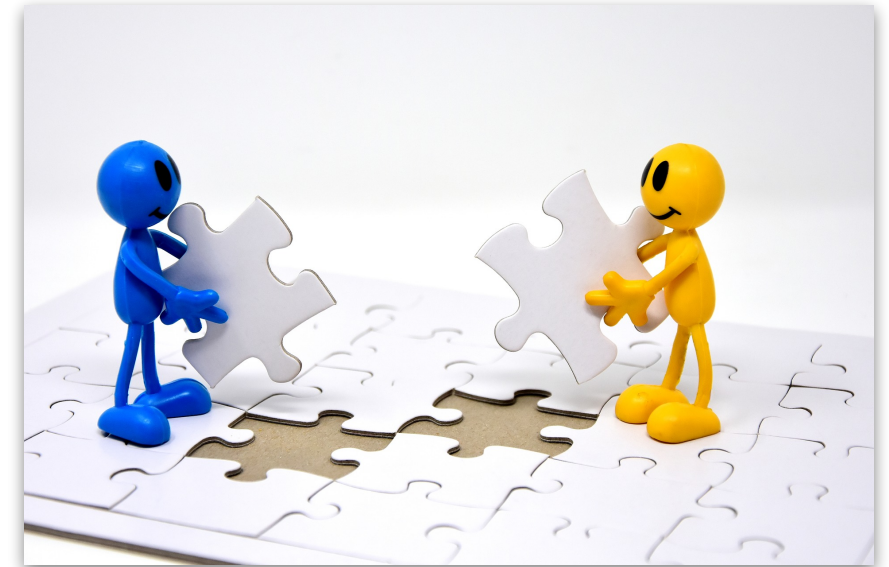
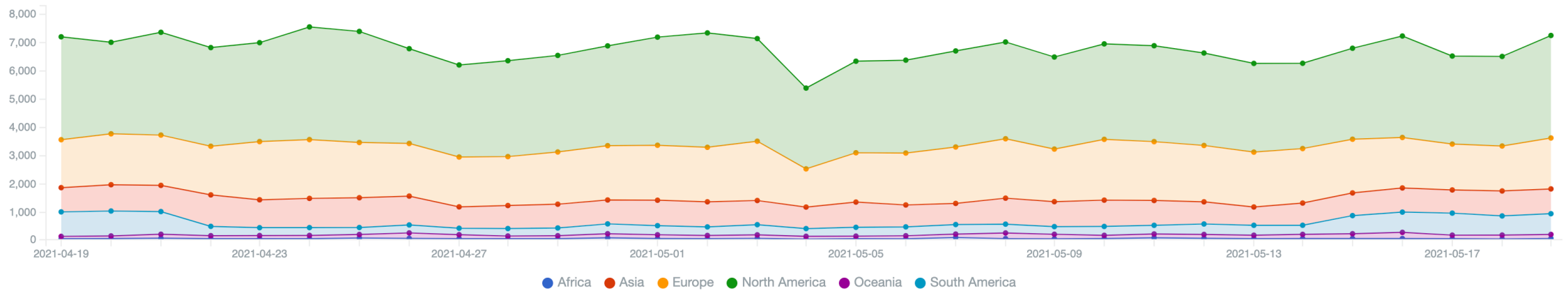The CSIRT quickly gains relevance in its country by sharing the information with affected parties and jointly remediating victims and closing vulnerabilities.

SHADOWSERVER

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

Improving Situational Awareness at a National Level

https://cncs.gob.do/ciber-observatorio/

Case #2 - Assisting Your Top ISP

How to help a major ISP be more proactive in handling incidents?

Once your National CSIRT subscribes to Shadowserver daily reports, it quickly identifies hot-spots of malicious activity in the country. One of them is a major ISP, that is struggling to contain malware infections and compromises.

Your CSIRT works to establish connections with the ISP and demonstrates the problems it sees thanks to the Shadowserver report. You encourage the ISP to subscribe to the Shadowserver data, either via your hub or directly with Shadowserver. That provides +70 reports of an "outside scan," malware, botnets, and other vulnerabilities.

You help establish a small team at the ISP that 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 that are ultimately resolved.
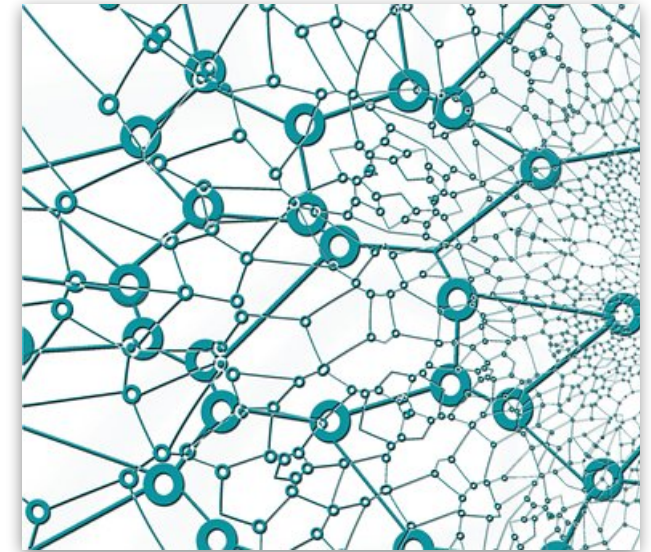
Your CSIRT and the Shadowserver Daily Network Reports cost effectively kick started the ISP Security Team - translating vast amounts of high-quality security data into actionable insights. These reports cleaned up the network and prevented major loss to the carrier's business.

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

Case #3 - Handling Emotet infections in an Enterprise

Why are there 3 Computers infected with Emotet in Enterprise X?

Emotet data is now part of the Shadowserver "victim notification" process through a malware takedown operation conducted by Europol and other law enforcement agencies. The Sinkhole Infection report arrives with information about Emotet botnet victims. Three hosts in the network of Enterprise X are infected and have been observed contacting the Emotet command and control (C2) infrastructure

Your CSIRT quickly shares the information with the affected Enterprise.


EUROPOL

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

27 January 2021
Press Release

Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

This operation is the result of a collaborative effort between authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine, with international activity coordinated by Europol and Eurojust. This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

EMOTET has been one of the most professional and long lasting cybercrime services out there. First discovered as a banking Trojan in 2014, the malware evolved into the go-to solution for cybercriminals over the years. The EMOTET infrastructure essentially acted as a primary door opener for computer systems on a global scale. Once this unauthorised access was established, these were sold to other top-level criminal groups to deploy further illicit activities such data theft and extortion through ransomware.

Spread via Word documents

The EMOTET group managed to take email as an attack vector to a next level. Through a fully automated process, EMOTET malware was delivered to the victims' computers via infected e-mail attachments. A variety of different lures were used to trick unsuspecting users into opening these malicious attachments. In the past, EMOTET email campaigns

https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

The potential damage to the organisation (for example Ryuk ransomware deployment) was prevented by Shadowserver's Network Report. The infection vector was identified and extra network protections were put in place to protect the organisation. All from a free public benefit report!

SHADOWSERVER

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

Emotet infections over time
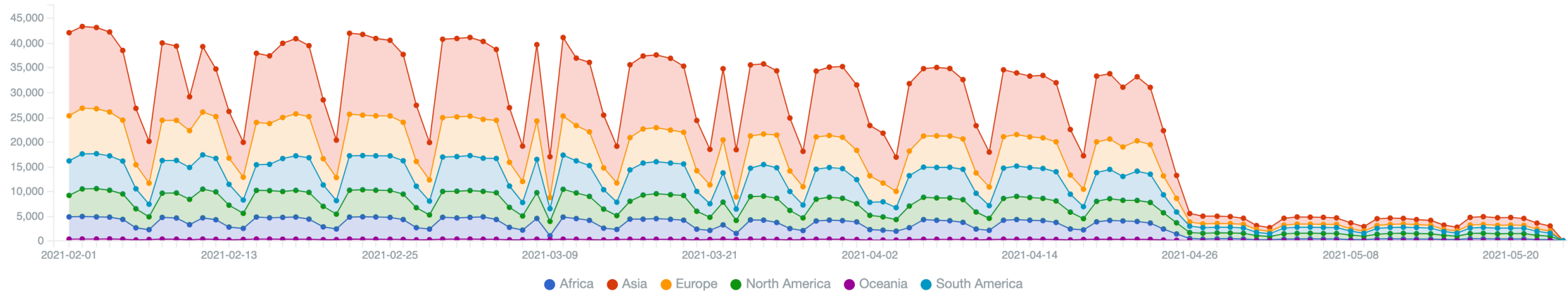
Case #4 - Discovering HAFNIUM/Exchange webshells

Have we been compromised by HAFNIUM or other actors targeting Exchange?

Shadowserver's Daily Network Report arrives with a new report on HAFNIUM victims.
Multiple Government networks running Exchange appear to have been compromised.

A Shadowserver report arrives with information about webshells detected through Shadowserver scanning that have been planted by HAFNIUM and other actors, after the HAFNIUM and other actors successfully compromised the organisation's Exchange servers.

Your CSIRT alerts the appropriate Government department.

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE   Product ID: AA21-069A

March 10, 2021

Compromise of Microsoft Exchange Server

This Joint Cybersecurity Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 8. See the ATT&CK for Enterprise framework for referenced threat actor techniques and for mitigations.

SUMMARY

This Advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to highlight the cyber threat associated with active exploitation of vulnerabilities in Microsoft Exchange on-premises products. The FBI and CISA assess that nation-state actors and cyber criminals are likely among those exploiting these vulnerabilities. The exploitation of Microsoft Exchange on-premises products poses a serious risk to Federal Civilian Executive Branch agencies and private companies. Successful exploitation of these vulnerabilities allows an attacker to access victims' Exchange Servers, enabling them to gain persistent system access and control of an enterprise network. It has the potential to affect tens of thousands of systems in the United States and provides adversaries with access to networks containing valuable research, technology, personally identifiable information (PII), and other sensitive information from entities in multiple U.S. sectors. FBI and CISA assess that adversaries will continue to exploit this vulnerability to compromise networks and steal information, encrypt data for ransom, or even execute a destructive attack. Adversaries may also sell access to compromised networks on the dark web.

On March 2, 2021, Microsoft and Volexity announced the detection of multiple zero-day exploits used to target vulnerabilities in on-premises versions of Microsoft Exchange Servers. In light of this public announcement, FBI and CISA assess that other capable cyber actors are attempting to exploit these vulnerabilities before victims implement the Microsoft updates.

https://www.ic3.gov/Media/News/2021/210310.pdf

An intrusion to a Government organisation was discovered thanks to Shadowserver's Network Report. The host calling out was identified and an investigation was launched into understanding the extent of the breach and what data was exfiltrated. All from a free public benefit report!

Case #5 - A Bank and an accessible RDP service

A Bank with an accidentally open RDP service

One of the top banks in your country in general takes great care of its network. One day however, there is a firewall upgrade and the access rules fail, exposing an RDP service that should not be accessible from the outside.

Shadowserver daily full internet IPv4 scanning quickly picks up the exposed service and alerts you.

Your CSIRT quickly alerts the bank's security team.

Big jump in RDP attacks as hackers target staff working from home

Researchers at ESET detected billions of cyberattacks attempting to take advantage of people working remotely - and cyber criminals aren't letting up yet.

By Danny Palmer | February 8, 2021 -- 11:56 GMT (11:56 GMT) | Topic: Security

MORE FROM DANNY PALMER

Security
Smishing: Police make arrests in crackdown on scam text messages

Security
This massive phishing campaign delivers password-stealing malware disguised as ransomware

Security
Mobile spyware: How it works and how to avoid becoming a victim

Security
Cybersecurity: How talking about mistakes can make everyone safer

How remote working is making life easier for hackers

There's been a huge increase in cyber criminals attempting to perform attacks by exploiting remote login credentials over the last year, as many employees continue to work from home.

https://www.zdnet.com/article/big-jump-in-rdp-attacks-as-hackers-target-staff-working-from-home/

Thanks to the report and your CSIRT's actions, the bank was able to identify the firewall failure and fix the access rules, avoiding a possible breach. All from a free public benefit report!

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

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/

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG