Sinkhole Events & Sinkhole HTTP Reports

Malware infection reports for your network/constituency

@shadowserver

contact@shadowserver.org

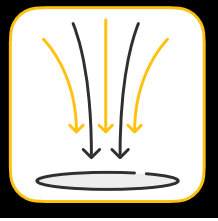
SHADOWSERVER.ORG

Presentation Aims & Objectives

- Introduce Sinkhole Events & Sinkhole HTTP
- Highlight sample Sinkhole Event & HTTP reports
- Describe key features of each report
- Demonstrate how a National CERT can action a Sinkhole report
- Offer guidance on how to protect and remediate from infections taking android.hummer, avalanche.andromeda and Emotet as examples
- Provide a key list of Shadowserver online resources to enable report subscription and use

SHADOWSERVER

What is a malware Sinkhole?



- Sinkholing is a technique whereby a resource used by malicious actors to control malware is taken over and redirected to a benign listener that can (to a varying degree) understand connections coming from infected devices

- Typically, the resources taken over are domain names

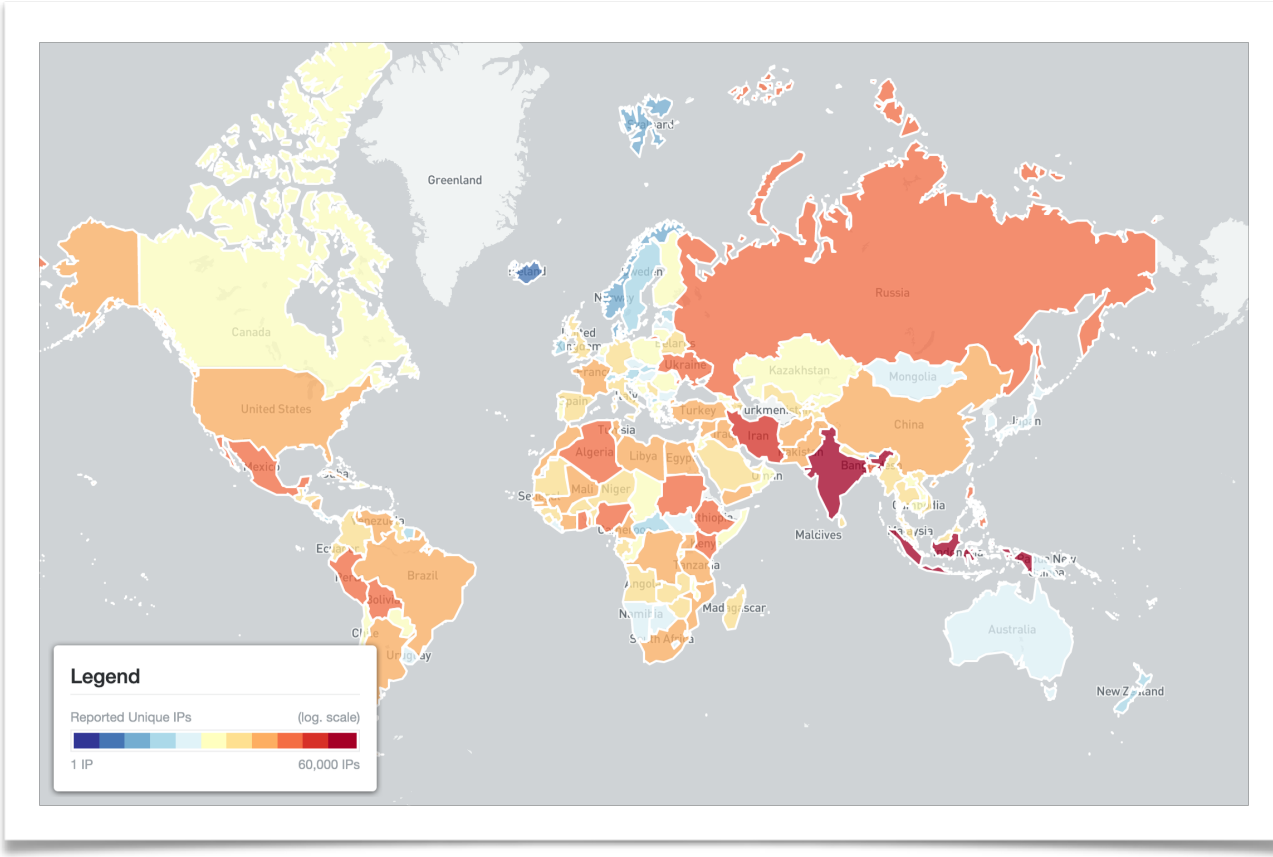
- Other types of sinkholing exist as well, for example P2P botnet poisoning or BGP/routing redirection

- Infected machines connect to sinkholes using various C2 protocols for communication, for example HTTP based, DNS and IRC but also many other proprietary protocols

SHADOWSERVER

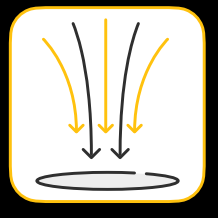
Example Sinkhole Event infection - Android.Hummer

- A common Android threat, widespread across the World
- Virus is installed via malicious applications from Google Play Store and other sources
- Gains admin privileges and then adds unwanted pop-up ads to the phone
- Installs unwanted apps in the background which are reinstalled if a user attempts to uninstall
- At the height of infection, 2bn+ devices alleged to have been infected worldwide



SHADOWSERVER

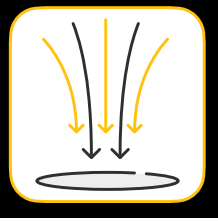
Shadowserver sinkhole reports



- Sinkhole Events Report: https://www.shadowserver.org/what-we-do/network-reporting/sinkhole-events-report/
- Sinkhole HTTP Events Report: https://www.shadowserver.org/what-we-do/network-reporting/sinkhole-http-events-report/
- Microsoft Sinkhole Events Report https://www.shadowserver.org/what-we-do/network-reporting/microsoft-sinkhole-events-report/
- Microsoft Sinkhole HTTP Events Report: https://www.shadowserver.org/what-we-do/network-reporting/microsoft-sinkhole-http-events-report/
- Sinkhole HTTP Referrer Events Report: https://www.shadowserver.org/what-we-do/network-reporting/sinkhole-http-referer-events-report/

SHADOWSERVER

How are sinkhole reports made available?



- Sinkhole Events Report
  - event4_sinkhole
- Sinkhole HTTP Events Report
  - event4_sinkhole_http
  - event6_sinkhole_http
- Microsoft Sinkhole Events Report
  - event4_microsoft_sinkhole
- Microsoft Sinkhole HTTP Events Report
  - event4_microsoft_sinkhole_http
- Sinkhole HTTP Referer Events Report
  - event4_sinkhole_http_referer
  - event6_sinkhole_http_referer

Reports are available as files in CSV format

File names have `sinkhole` in their name

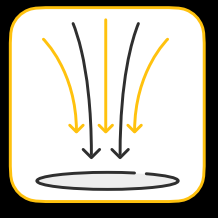
Reports can be sent as e-mail attachments, or downloaded via HTTP or obtained via a RESTful API

All report types have an IPv4 version (`event4_` prefix) and some have an IPv6 version as well (`event6_` prefix)

All events timestamps are in UTC (+0)

SHADOWSERVER

Sinkhole Event Report



Sinkhole Events Report

This report contains events (connections) to non-http sinkholes. Sinkholing is a technique whereby a resource used by malicious actors to control malware is taken over and redirected to a benign listener that can (to a varying degree) understand connections coming from infected devices.

Only infected systems or security researchers should be seen in this list.

File names: **event4_sinkhole**

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

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
device_vendor	Source device vendor
device_type	Source device type

SAMPLE

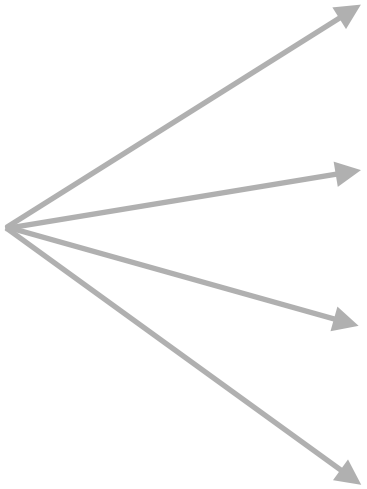
```
"timestamp","protocol","src_ip","src_port","src_asn","src_geo","src_region","src_city","
"2021-03-04 00:00:00","tcp","190.113.x.x",17409,12252,"PE","METROPOLITANA DE LIMA","LIMA
"2021-03-04 00:00:00","tcp","217.173.x.x",28940,8220,"IE","DUBLIN","DUBLIN",,541611,"Com
"2021-03-04 00:00:00","tcp","37.212.x.x",36735,6697,"BY","VITEBSKAJA OBLAST'","VITEBSK",
"2021-03-04 00:00:00","tcp","86.130.x.x",50395,2856,"UK","MID ULSTER","DUNGANNON",,51731
"2021-03-04 00:00:00","tcp","35.205.x.x",44696,15169,"BE","BRUXELLES-CAPITALE","BRUSSELS
"2021-03-04 00:00:00","tcp","35.197.x.x",36968,15169,"US","OREGON","THE DALLES","x.x.197
```

SHADOWSERVER

Action a Sinkhole Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	infection
01/03/2022 00:02	tcp	102.70.62.XX	5767	37294	MW	SOUTHERN REGION	BLANTYRE	android.hummer

Key event 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

SHADOWSERVER

Action a Sinkhole Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	infection
01/03/2022 00:02	tcp	102.70.62.XX	5767	37294	MW	SOUTHERN REGION	BLANTYRE	android.hummer

IP WHOIS
102.70.62.XX

```
aut-num:        AS37294
as-name:        TNM
descr:          Telecom Networks Malawi Ltd
admin-c:        VC14-AFRINIC
admin-c:        PS33-AFRINIC
admin-c:        EP15-AFRINIC
tech-c:         LP16-AFRINIC
tech-c:         MN55-AFRINIC
tech-c:         PS33-AFRINIC
tech-c:         EP15-AFRINIC
tech-c:         JK47-AFRINIC
org:            ORG-TNML1-AFRINIC
mnt-by:         AFRINIC-HM-MNT
mnt-lower:      TNM-MNT
mnt-routes:     TNM-MNT
source:         AFRINIC # Filtered
status:         ASSIGNED
```

```
address:        Telekom Networks Malawi, Livingstone Towers, GYn Jones Rd, Blantyre, Malawi
phone:          tel:+265-88209252
nic-hdl:        EP15-AFRINIC
mnt-by:         GENERATED-M7VKZ7WXHBYWMU2MF4FXEBYIXI1UODJX-MNT
source:         AFRINIC # Filtered
```

SHADOWSERVER

Android.Hummer - PROTECT

- Ensure Android OS are up to date
  - e.g. Android OS updates can patch vulnerabilities and remove access to malicious software
- Install Android AV products
- Keep apps and permissions up to date
  - e.g. review if an app have the ability to send SMS messages
- Consider downloading apps from official stores and not third parties

SHADOWSERVER

Android.Hummer - REMEDIATE

- Use an Anti Virus product as best practice removal of Android malware
- For manual removal :
  - Prevent pop up's and redirects by clearing the device cache either via browser settings or by going to Apps & Notifications
  - Access Safe mode in your device power options menu or try holding volume-down as you reboot the phone. Alternatively, search for your device make and model to obtain safe mode instructions
  - Manually remove malicious apps in safe mode whilst preventing third party apps from executing
  - Attempting to remove in normal mode will likely result in permissions to remove denied
  - In safe mode, open Settings and select the Apps & Notifications menu to remove non familiar apps / apps you have not installed
  - If this is not a preinstalled app you should see an uninstall button to remove
  - If uninstall is 'greyed out' it is possible the app has given itself administrator rights which can be disabled in Settings > Security & Location > Device Admin Apps in order to uninstall
  - Restart the device to take it out of safe mode
  - If all else fails, perform a system reset Settings > System > Reset Options > Erase All Data

SHADOWSERVER

Source - https://www.techadvisor.com/how-to/google-android/remove-android-virus-3633110/

Sinkhole HTTP Event Report

Sinkhole HTTP Events Report

This report contains events (connections) to HTTP Sinkholes. Sinkholing is a technique whereby a resource used by malicious actors to control malware is taken over and redirected to a benign listener that can (to a varying degree) understand connections coming from infected devices.

This report identifies the IP addresses from all the devices that joined a sinkhole server that did not arrive through an HTTP referrer.

Since a sinkhole server is only accessed through previously malicious domain names, only infected systems or security researchers should be seen in this list. However, the sinkholes may also pick up web crawlers requesting malicious domains.

This report can come in 2 versions, one for IPv4 only connections, the other for IPv6 only connections.

File names: **event4_sinkhole_http** and **event6_sinkhole_http.**

https://www.shadowserver.org/what-we-do/network-reporting/sinkhole-http-events-report/

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

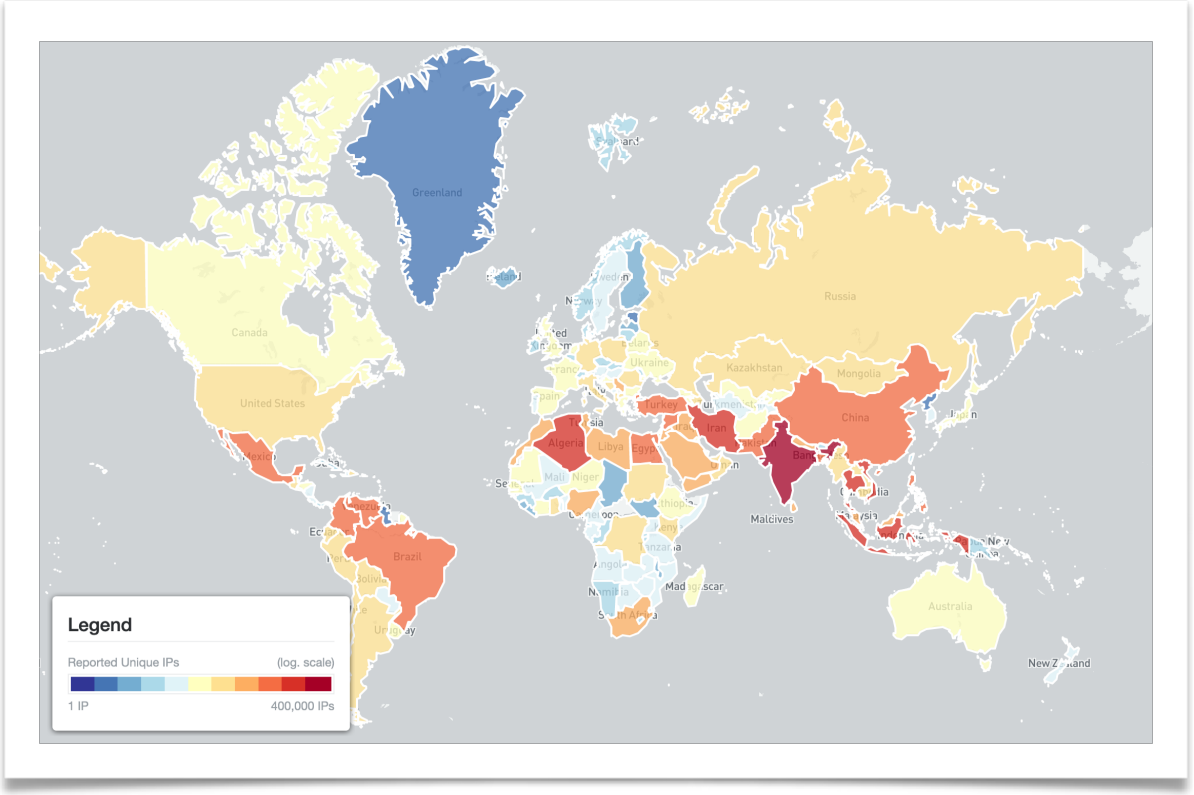
SAMPLE

```
"timestamp","protocol","src_ip","src_port","src_asn","src_geo","src_region","src_city","
"2021-03-04 00:00:00","tcp","103.196.x.x",60902,134707,"PH","NUEVA ECIJA","DEL PILAR",,,
"2021-03-04 00:00:00","tcp","5.14.x.x",55002,8708,"RO","CONSTANTA","CONSTANTA",,517311,"
"2021-03-04 00:00:00","tcp","49.145.x.x",31350,9299,"PH","CEBU","CEBU",,517311,,,,,"184.
"2021-03-04 00:00:00","tcp","200.44.x.x",28063,8048,"VE","CARABOBO","VALENCIA",,517311,,
"2021-03-04 00:00:00","tcp","187.189.x.x",45335,17072,"MX","CHIHUAHUA","JUAREZ",,,,,,,"1
```

SHADOWSERVER

Example Sinkhole HTTP Infection : avalanche-andromeda

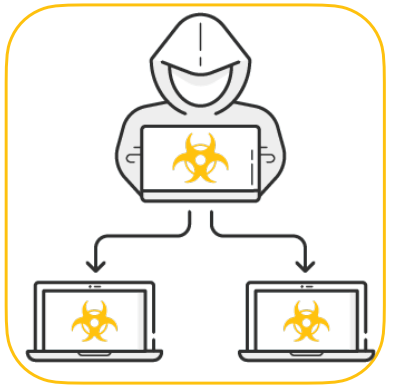
- Malware family refers to variants tied to the ANDROMEDA botnet
- Also known as Gamarue, Wauchos
- Stealth encrypted virus resident in memory which infects all executed COM and EXE files and deletes AV products when executed
- One of the longest malware families to have existed since its 2011 creation
- Linked to phishing, SPAM campaigns, illegal software downloads and various exploit kits as a means of distribution by the Avalanche platform



SHADOWSERVER

Avalanche MaaS Platfrom

- The Avalanche platform served as a criminal MaaS network
- Launched and managed mass global malware attacks and money mule recruiting campaigns
- Responsible for delivering resilient botnet command and control (C2) services for 20 different malware strains, all of which utilized Domain Generation Algorithms (DGAs)
- Monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of euros worldwide
- Disrupted in 2016 but legacy ‘Avalanche’ named malware still being sinkholed today

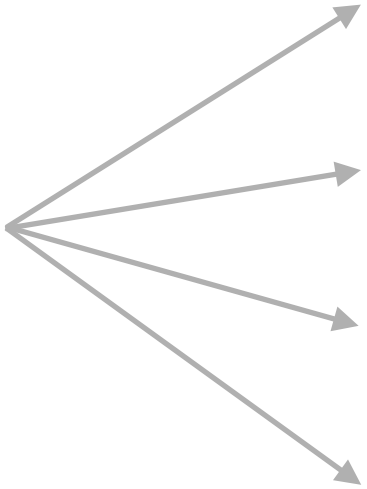


SHADOWSERVER

Action a Sinkhole Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	infection
01/03/2022 00:02	tcp	197.218.92.XX	5767	37294	MW	SOUTHERN REGION	BLANTYRE	android.hummer

Key event 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

SHADOWSERVER

Action a Sinkhole Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	infection
01/03/2022 00:02	tcp	197.218.92.XX	5767	37294	MW	SOUTHERN REGION	BLANTYRE	android.hummer

IP WHOIS
197.218.92.XX

```
inetnum:        197.218.64.0 - 197.218.127.255
netname:        GPRS-3G-01
descr:          For 3G Customer
country:        MZ
admin-c:        NTH1-AFRINIC
tech-c:         NTH1-AFRINIC
status:         ASSIGNED PA
remarks:        Admin
mnt-by:         Movitel-MNT
source:         AFRINIC # Filtered
parent:         197.218.0.0 - 197.219.255.255

person:         NGUYEN TRUNG HAU
address:        Av Mohamed Siad Barre, No 225.
address:        Maputo
address:        Mozambique
phone:          tel:+258-86-010-0047
nic-hdl:        NTH1-AFRINIC
mnt-by:         GENERATED-TEEWXI57WSC9KB23TSOR0JL9MM2HVCGM-MNT
source:         AFRINIC # Filtered

% Information related to '197.218.92.0/24AS37342'

route:          197.218.92.0/24
descr:          Movitel's IP
origin:         AS37342
mnt-by:         Movitel-MNT
source:         AFRINIC # Filtered
```

SHADOWSERVER

avalanche.andromeda - PROTECT

- Perform efficient antivirus scans
  - Perform in depth scans to look for associated threat installing Avalanche exploits and related registry entries, file-lockers, Remote Access Tools (RATs) and associated backdoor Trojans that connect to the Avalanche platform
- Keep your antivirus updated
  - If automatic updates are available, configure your antivirus to use them
- Keep your permanent antivirus protection enabled at all times

SHADOWSERVER

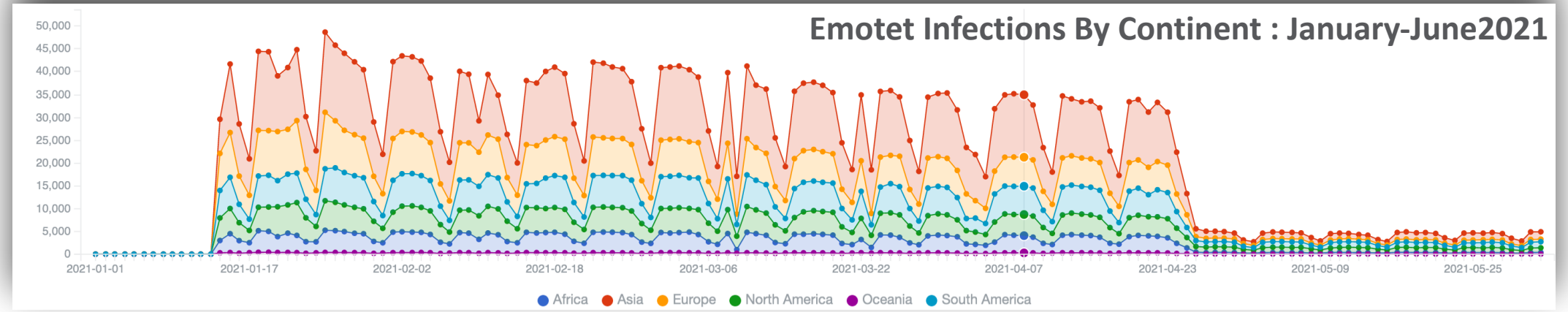
avalanche.andromeda - REMEDIATE

- Use an Anti Virus removal tool
- Perform an in depth scan to look for associated threat installing Avalanche exploits and related registry entries, file-lockers, Remote Access Tools (RATs) and associated backdoor Trojans that connect to the Avalanche platform
- Uninstall recently added apps
- Delete unwanted browser extensions via browser settings
- If all else fails, perform a full factory reset of the device, document any required Registry keys and back up important files

SHADOWSERVER

Example Sinkhole HTTP Infection : Emotet

- Malware that targets multiple devices and OS, spread via email, using malicious links or attachments, e.g. COVID-19
- Evolved from a ‘loader’ allowing access to hijack systems into a banking trojan in 2014
- Uses worm like capabilities to help spread to other connected computers and distribute malware
- Later versions saw the addition of MaaS access given to cybercrime groups enabled payloads to be sent to victims, e.g. Ryuk Ransomware
- First quarter 2021 saw the Emotet group crippled by International authorities with victims sinkholed by law enforcement
- Last quarter 2021 saw the re-emergence of Emotet malware and an increase in associated Trickbot infections downloading new Emotet binaries

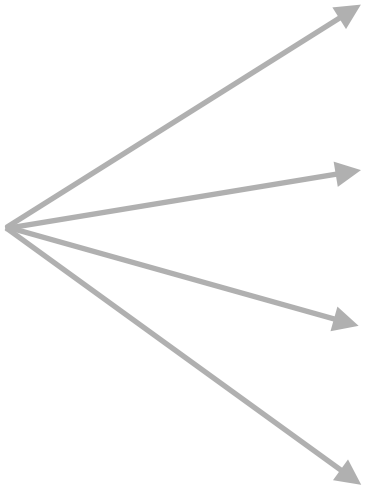


SHADOWSERVER

Action a Sinkhole Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	infection
03/03/2022 00:02	tcp	104.131.11.150	443	14061	US	SANTA CLARA	CALIFORNIA	EMOTET

Key event 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

SHADOWSERVER

Action a Sinkhole Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	infection
03/03/2022 00:02	tcp	104.131.11.150	443	14061	US	SANTA CLARA	CALIFORNIA	EMOTET

IP WHOIS
104.131.11.XX

```
OrgName:        DigitalOcean, LLC
OrgId:          DO-13
Address:        101 Ave of the Americas
Address:        10th Floor
City:           New York
StateProv:      NY
PostalCode:     10013
Country:        US
RegDate:        2012-05-14
Updated:        2021-05-03
Comment:        http://www.digitalocean.com
Comment:        Simple Cloud Hosting
Ref:            https://rdap.arin.net/registry/entity/DO-13


OrgAbuseHandle: ABUSE5232-ARIN
OrgAbuseName:   Abuse, DigitalOcean
OrgAbusePhone:  +1-347-875-6044
OrgAbuseEmail:  abuse@digitalocean.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5232-ARIN
```

SHADOWSERVER

Emotet - PROTECT

- Ensure AV, associated OS, browsers, email clients, Office, and PDF programs are all have the lates security updates installed
- Do not download dubious attachments from emails or click on suspicious links
- Back up your data regularly to an external storage device. In the event of an infection, you will always have a backup to fall back on
- Use strong passwords for all logins and 2FA
- Display file extensions by default to detect malicious files
- Infected systems need to be remediated quickly, since they may still have other active, ongoing infections inside their networks too

SHADOWSERVER

Emotet - REMEDIATE

- Immediately isolate infected computers from a network
- Use an Anti Virus product for best practice removal
- As Emotet has worm like capabilities, patch and clean infected systems one by one to prevent re-infection when plugged back into a network

- To manually remove :
  - identify the named malware using an appropriate programme manager, for example the ‘Autoruns’ application and ensure hidden files and folders are searchable
  - restart your computer in safe mode / safe mode with networking (dependent upon OS version)
  - search and extract the malware and associated files / processes to ensure deletion
- Reboot to normal mode and confirm removal

SHADOWSERVER

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/sinkhole-events-report/
- https://www.shadowserver.org/what-we-do/network-reporting/sinkhole-http-events-report/

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

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG