Darknet Events Report

Observing scanning or backscatter activity from your constituency/network

@shadowserver

contact@shadowserver.org

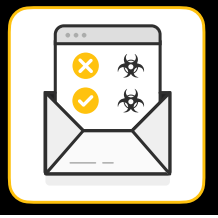
SHADOWSERVER.ORG

Presentation Aims & Objectives

- Introduce the Darknet Report
- Highlight a sample Darknet report
- Describe key features of the report
- Demonstrate how a National CERT or network owner can action a Darknet Report
- Offer general guidance on how to protect against Darknets
- Provide a key list of Shadowserver online resources to enable report subscription and use

SHADOWSERVER

Darknet



- Darknets (also known as network telescopes) are unused sets of IP addresses, which in theory should observe no traffic

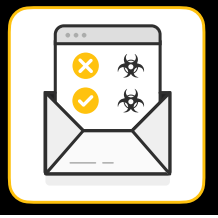
- In practice, however, a lot of traffic reaches such networks through activities such as Internet scanning, malware propagation, or backscatter from spoofed DDoS events – meaning that these network packets can often be immediately classified as suspicious or malicious

- Darknets serve a similar type of function as honeypot listeners, only simpler ie. they do not respond. This means they do not capture full payloads of TCP connections which are never fully established. They can however capture full UDP or ICMP packets with payloads, as these protocols are stateless and do not need a connection to be established first

- Additional packet fingerprinting measures can be employed to attribute tools or malware sending out such packets. For example, Mirai IoT malware sends TCP SYN packets with the sequence number of the initial TCP packet set to the target IP address

SHADOWSERVER

Darknet Events Report



- Darknet Events Report:https://www.shadowserver.org/what-we-do/network-reporting/honeypot-darknet-events-report/
- Report is available as a file in CSV format
- As of 2022-04-26 the report primarily contains data on Mirai related scanning activity. In other words, you are receiving information on Mirai based malware in your network or constituency
- The report filename contains event4_honeypot_darknet
- All timestamps are in UTC
- Reports can be sent as e-mail attachments, downloaded via HTTP or obtained via a RESTful API
- For more documentation on API access, please visit the below URLs and send a request for 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

Example Darknet Events Report

Darknet Events Report

This report records observed traffic to darknet networks.

Darknets (also known as network telescopes) are unused sets of IP addresses, which in theory should observe no traffic. In practice, however, a lot of traffic reaches such networks through activities such as Internet scanning, malware propagation, or backscatter from spoofed DDoS events – meaning that these network packets can often be immediately classified as suspicious or malicious. In this way, darknets serve a similar type of function as honeypot listeners, only simpler. Additional packet fingerprinting measures can be employed to attribute tools or malware sending out such packets.

File name: **event4_honeypot_darknet**

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

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

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

SHADOWSERVER

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

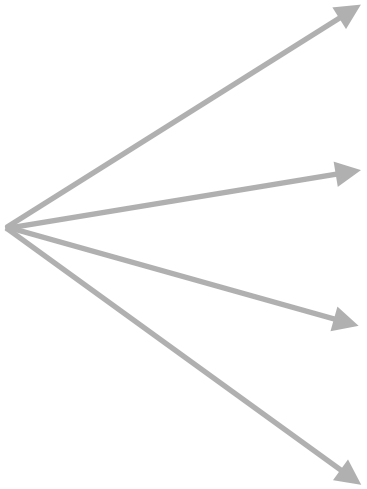
SAMPLE

```
"timestamp","protocol","src_ip","src_port","src_asn","src_geo","src_region","src_city","
"2021-03-07 00:00:00","tcp","61.3.x.x",4717,9829,"IN","KERALA","CHENGANNUR",,518210,,,,,
"2021-03-07 00:00:00","tcp","211.218.x.x",4405,4766,"KR","GANGWON-DO","PYEONGCHANG-EUP",
"2021-03-07 00:00:00","tcp","45.225.x.x",59777,266915,"BR","BAHIA","VITORIA DA CONQUISTA
"2021-03-07 00:00:00","tcp","125.122.x.x",8460,4134,"CN","ZHEJIANG SHENG","HANGZHOU",,51
"2021-03-07 00:00:00","tcp","219.77.x.x",21867,4760,"HK","HONG KONG","HONG KONG","n21907
"2021-03-07 00:00:00","tcp","24.137.x.x",4680,14638,"PR","PUERTO RICO","SAN JUAN","dynam
"2021-03-07 00:00:00","tcp","119.182.x.x",13175,4837,"CN","SHANDONG SHENG","JINING",,517
"2021-03-07 00:00:00","tcp","27.198.x.x",56133,4837,"CN","SHANDONG SHENG","JINAN",,51731
```

Action a Darknet Events Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname	infection	family	tag
06/04/2022 00:00	tcp	219.77.X.X	21867	4760	HK	hong kong	hong kong	XXX	mirai	XXX	mirai

Key event fields



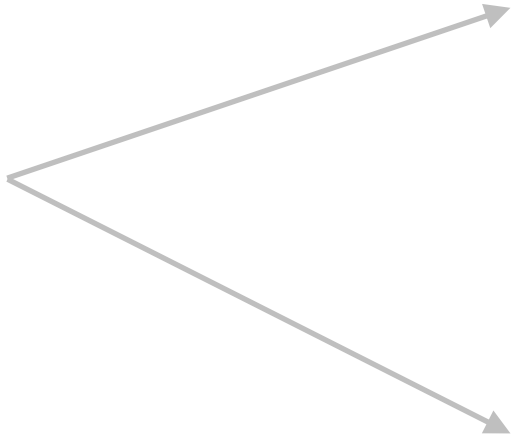
timestamp	Timestamp when the IP was seen in UTC+0
protocol	Packet type of the connection traffic (UDP/TCP)
src_ip	The IP of the device in question
src_port	Source port of the IP connection
src_asn	ASN of the source IP
src_geo	Country of the source IP
src_region	Region of the source IP
src_city	City of the source IP
src_hostname	Reverse DNS of the source IP
infection	Description of the malware/infection
family	Malware family or campaign associated with the event
tag	Event attributes

SHADOWSERVER

Action a Darknet Events Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname	infection	family	tag
06/04/2022 00:00	tcp	219.77.X.X	21867	4760	HK	hong kong	hong kong	XXX	mirai	XXX	mirai

IP WHOIS
219.77.X.X

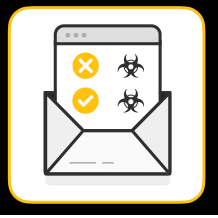


```
inetnum:        219.77.0.0 - 219.77.255.255
netname:        NETVIGATOR
descr:          Hong Kong Telecommunications (HKT) Limited Mass Internet
country:        HK
admin-c:        NA45-AP
tech-c:         NA45-AP
abuse-c:        AH981-AP
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-HK-IMS-CS
mnt-lower:      MAINT-HK-IMS-CS
mnt-routes:     MAINT-HK-IMS-WILSON
mnt-irt:        IRT-HKTIMS-HK
last-modified:  2021-01-27T13:20:40Z
source:         APNIC

irt:            IRT-HKTIMS-HK
address:        PO Box 9896 GPO
e-mail:         noc@imsbiz.com
abuse-mailbox:  noc@imsbiz.com
admin-c:        WC109-AP
tech-c:         WC109-AP
auth:           # Filtered
remarks:        noc@imsbiz.com
remarks:        noc@imsbiz.com was validated on 2021-11-11
mnt-by:         MAINT-HK-IMS
last-modified:  2021-11-11T02:01:21Z
source:         APNIC
```

SHADOWSERVER

Verifying results



- False positives may be possible with observed spoofed Darknet events which applies to both TCP and UDP packets

- In practice, for Mirai SYN based detections we do not receive feedback on false positives. If you receive a report with a Mirai infection, the confidence that the device is infected is high. It may also mean that in practice a device behind that IP may also be infected, rather than the actual IP itself (due to NAT)

- DDoS backscatter is more likely to include false positives. However, as of 2022-04-26, we do not include such data in the report (may change in the future)

SHADOWSERVER

Darknet Events Report - PROTECT

- In order to reduce the amount of Darknet Events reported on Mirai you should :
  - Implement best practices for securing IoT devices in your constituency
  - Consider filtering traffic to certain ports to your constituency, such as TELNET or web services
  - Ensure that devices with SSH services enabled (under your direct control) have implemented best practices related to password management or use key based authentication mechanisms instead

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/honeypot-darknet-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