Honeypot DDoS Target Events & Honeypot DDoS Event Report

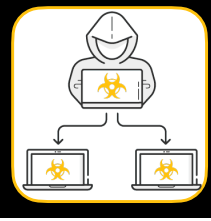
Honeypot drone based reports on DDoS attacks related to your network/constituency

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG

Presentation Aims & Objectives



- Describe how Honeypot Drones can be used to monitor DDoS attacks
- Highlight a sample Honeypot DDoS Target Events Report & Honeypot DDoS Events Report, where DDoS targets and C2's issuing attack commands are reported
- Describe key features of each report of the two Honeypot drone DDoS reports, and explain how the two reports complement each other
- Demonstrate how a National CERT or targeted organization can action an Honeypot DDoS Target Events Report & Honeypot DDoS Events Report
- Provide a key list of Shadowserver online resources to enable report subscription and use

SHADOWSERVER

Honeypot DDoS Target Events & DDoS Events Reports

- Both reports contain information on DDoS attacks observed by honeypot drones

- The drones emulate malware bot infected machines, join DDoS botnets and can listen to commands issued by C2s to those bots

- Information collected can include the C2 issuing the command and target IP information, malware family, protocol being used for C2 and attack destination as well as various attack parameters

- The activity reported is typically related to Mirai like bots and other IoT DDoS botnets. Attacks carried may be varied in nature, and not necessarily be reflective DDoS attacks that are reported in the Honeypot Amplification DDoS Events report. For example, they could include direct SYN flood attacks as well

- The naming convention and description of the reports is consistent with the Mirai source code naming scheme

- Both reports come from the same source (ie honeypot drones), the main difference is that the Honeypot DDoS Target event report is indexed by attack targets, while the Honeypot DDoS Event Report is indexed by C2s

SHADOWSERVER

Honeypot DDoS Target Events Report

Reporting on DDoS attack targets observed by honeypot drones

Honeypot DDoS Target Events Report

Honeypot DDoS Target Events Report

LAST UPDATED: 2022-03-15

This report contains information about DDoS attack targets observed by honeypot drones. These drones emulate malware bot infected machines and can listen to commands given to those bots. These commands include the C2 issuing the command and target information, malware family, protocol being used for C2 and attack destination as well as various attack parameters.

The dst_ip is the IP of the attack victim, the src_ip below is the C2 IP issuing the commands. If you are getting this report, it means an IP (dst_ip) that was targeted was located on your network or constituency (attack destination).

The activity reported is typically related to Mirai like bots. The naming convention and description is consistent with the **Mirai source code** published.

This report has its sister version that contains the same information but filtered by src_ip (address of the C2 issuing commands): the **Honeypot DDoS Event Report.**

This report was enabled as part of the European Union HaDEA CEF **VARIoT project.**

File name: **event4_honeypot_ddos_target**

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

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

SHADOWSERVER

FIELDS

timestamp	Timestamp when the destination IP was seen in UTC+0
protocol	Packet type of the connection traffic (UDP/TCP)
dst_ip	Destination IP (being attacked by a DDoS)
dst_port	Destination port (being attacked by a DDoS)
dst_asn	ASN of the destination IP
dst_geo	Country of the destination IP
dst_region	Region of the destination IP
dst_city	City of the destination IP
dst_hostname	Reverse DNS of the destination IP
dst_naics	North American Industry Classification System Code
dst_sector	Sector to which the destination IP in question belongs; e.g. Communications,

SAMPLE

```
"timestamp","protocol","dst_ip","dst_port","dst_asn","dst_geo","dst_region","dst_city","
"2022-03-14 17:02:28",,"115.238.x.x",80,136190,"CN","HUBEI SHENG","WUHAN",,517311,,,,,"1
"2022-03-14 17:09:46",,"52.184.x.x",43437,8075,"HK","HONG KONG","HONG KONG",,334111,"Inf
"2022-03-14 17:23:17",,"211.99.x.x",80,134763,"CN","SHANDONG SHENG","JINAN",,,,,,,"198.5
"2022-03-14 17:26:59",,"117.172.x.x",80,9808,"CN","SICHUAN SHENG","CHENGDU",,517312,,,,,'
"2022-03-14 17:31:53",,"103.100.x.x",80,136970,"HK","HONG KONG","HONG KONG",,,,,,,"198.5
"2022-03-14 17:35:35",,"45.117.x.x",57991,137697,"CN","BEIJING SHI","BEIJING",,,,,,,"198
```

Key Event Report Fields

IP targeted by issuing C2

This IP was seen in your network/constituency

dst_ip	Destination IP (IP being attacked)
dst_port	Destination port of the IP being attacked
dst_asn	ASN of the destination IP
dst_geo	Country of the destination IP
dst_region	Region of the destination IP
dst_city	City of the destination IP
dst_hostname	Reverse DNS of the destination IP
dst_naics	North American Industry Classification System Code
dst_sector	Sector to which the IP in question belongs; e.g. Communications, Commercial
public_source	Source of the event data
infection	Description of the malware/infection
family	Malware family or campaign associated with the event
tag	Event attributes
application	Application name associated with the event
version	Software version associated with the event
event_id	Unique identifier assigned to the source IP or event
dst_network	Network CIDR being attacked
dst_netmask	Mask of the destination network under attack
attack	Attack type (command issued)
duration	Attack duration
attack_src_ip	Spoofed attack source IP (if set)
attack_src_port	Spoofed attack source port (if set)
domain	Domain to attack (in attack command)

Malware associated to the attack

CIDR targeted by the C2

Domain targeted issued by C2

SHADOWSERVER

Honeypot DDoS Target Events Report

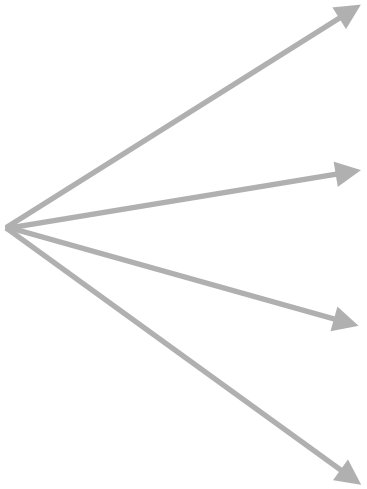
- https://www.shadowserver.org/what-we-do/network-reporting/honeypot-ddos-target-events-report/
- The dst_ip is the IP of the attack victim, the src_ip below is the C2 IP issuing the commands. If you are getting this report, it means an IP (dst_ip) that was targeted was located on your network or constituency (attack destination).
- Report is available as a file in CSV format
- The report filename contains `event4_honeypot_ddos_target`
- All timestamps are in UTC
- Reports can be sent as e-mail attachments, or 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 Report - Honeypot DDoS Target Events

timestamp	protocol	dst_ip	dst_port	dst_asn	dst_geo	dst_region	dst_city	dst_hostname	infection
22/04/2022 00:02	udp	211.99.XX.XX	80	134763	CN	shandong sheng	jinan	XXX	mirai

Key event fields



FIELDS

timestamp	Timestamp when the destination IP was seen in UTC+0
protocol	Packet type of the connection traffic (UDP/TCP)
dst_ip	Destination IP (being attacked by a DDoS)
dst_port	Destination port (being attacked by a DDoS)
dst_asn	ASN of the destination IP
dst_geo	Country of the destination IP
dst_region	Region of the destination IP
dst_city	City of the destination IP
dst_hostname	Reverse DNS of the destination IP
dst_naics	North American Industry Classification System Code
dst_sector	Sector to which the destination IP in question belongs; e.g. Communications,

SHADOWSERVER

Example Report - Honeypot DDoS Target Events - Key Fields

dst_ip	Destination IP (IP being attacked)
dst_port	Destination port of the IP being attacked
dst_asn	ASN of the destination IP
dst_geo	Country of the destination IP
dst_region	Region of the destination IP
dst_city	City of the destination IP
dst_hostname	Reverse DNS of the destination IP
dst_naics	North American Industry Classification System Code
dst_sector	Sector to which the IP in question belongs; e.g. Communications, Commercial
public_source	Source of the event data
infection	Description of the malware/infection
family	Malware family or campaign associated with the event
tag	Event attributes
application	Application name associated with the event
version	Software version associated with the event
event_id	Unique identifier assigned to the source IP or event
dst_network	Network CIDR being attacked
dst_netmask	Mask of the destination network under attack
attack	Attack type (command issued)
duration	Attack duration
attack_src_ip	Spoofed attack source IP (if set)
attack_src_port	Spoofed attack source port (if set)
domain	Domain to attack (in attack command)

IP targeted by issuing C2

Malware associated with the attack

CIDR targeted by the C2

Domain targeted issued by C2

dst_ip 180.97.x.x
dst_port 80
dst_asn 137697
dst_geo CN
dst_region jiangsu
sdst_city nanjing
dst_hostname
dst_naics 517311
domain source caprica.eu
public_source
infection. ddos
family mirai
tag mirai
application
version
event_id 1440
dst_network x.x.x.x
dst_netmask
attack
duration
attack_src_ip x.x.x.x
attack_src_port
domain xxxxxx.xxx

Example Report - Honeypot DDoS Target Events

timestamp	protocol	dst_ip	dst_port	dst_asn	dst_geo	dst_region	dst_city	dst_hostname	infection
22/04/2022 00:02	udp	211.99.XX.XX	80	134763	CN	shandong sheng	jinan	XXX	mirai

IP WHOIS
211.99.XX.XX

```
descr:          ShanDong Sanlian Electronic&Information Cor,ltd.
country:        CN
admin-c:        XX9-AP
tech-c:         XX9-AP
mnt-by:         MAINT-CNNIC-AP
status:         ASSIGNED NON-PORTABLE
last-modified:  2008-09-04T06:50:39Z
source:         APNIC

person:         Xu XiuPing
address:        12 North Baotuquan Street, Jinan, Shandong
country:        CN
phone:          +86-0531-13705409465
fax-no:         +86-0531-6097472
e-mail:         xpxu@sanlian.com.cn
nic-hdl:        XX9-AP
mnt-by:         MAINT-CNNIC-AP
last-modified:  2008-09-04T07:30:02Z
source:         APNIC
```

SHADOWSERVER

Honeypot DDoS Events Report

Reporting on C2 servers issuing DDoS attack commands that were observed by honeypot drones

Honeypot DDoS Events Report

Honeypot DDoS Events Report

LAST UPDATED: 2022-03-15

This report contains information about DDoS attack commands observed by honeypot drones. These drones emulate malware bot infected machines and can listen to commands given to those bots. These commands include the C2 issuing the command and target information, malware family, protocol being used for C2 and attack destination as well as various attack parameters.

The src_ip below is the C2 IP issuing the commands, the dst_ip is the IP of the attack victim. If you are getting this report, it means a C2 (src_ip) issuing the attack command was located on your network or constituency.

The activity reported is typically related to Mirai like bots. The naming convention and description is consistent with the **Mirai source code** published.

This report has its sister version that contains the same information but filtered by dst_ip (address of attack victims): **Honeypot DDoS Target Events Report**.

This report was enabled as part of the European Union HaDEA CEF **VARIoT project.**

File name: **event4_honeypot_ddos**

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

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

SHADOWSERVER

FIELDS

timestamp	Timestamp when the source IP was seen in UTC+0
protocol	Packet type of the connection traffic (UDP/TCP)
src_ip	The source IP of the C2 issuing DDoS attack commands
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","s
"2022-03-14 00:13:30",,"198.50.x.x",61234,16276,"CA","QUEBEC","MONTREAL",,518210,"Commun
"2022-03-14 00:18:31",,"198.50.x.x",61234,16276,"CA","QUEBEC","MONTREAL",,518210,"Commun
"2022-03-14 00:19:03",,"46.101.x.x",6379,14061,"DE","HESSEN","FRANKFURT AM MAIN",,518210
"2022-03-14 00:26:09",,"198.50.x.x",61234,16276,"CA","QUEBEC","MONTREAL",,518210,"Commun
"2022-03-14 00:28:39",,"46.101.x.x",6379,14061,"DE","HESSEN","FRANKFURT AM MAIN",,518210
"2022-03-14 00:29:42",,"198.50.x.x",61234,16276,"CA","QUEBEC","MONTREAL",,518210,"Commun
```

Key Event Report Fields

C2 IP issuing commands

This IP was seen in your network/constituency

src_ip	Source IP (IP acting as C2, ie. issuing commands)
src_port	Source port of attack commands
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 destination IP in question belongs; e.g. Communications, Commercial
public_source	Source of the event data
infection	Description of the malware/infection
family	Malware family or campaign associated with the event
tag	Event attributes
application	Application name associated with the event
version	Software version associated with the event
event_id	Unique identifier assigned to the source IP or event
dst_network	Network CIDR being attacked
dst_netmask	Mask of the destination network under attack
attack	Attack type (command issued)
duration	Attack duration
attack_src_ip	Spoofed attack source IP (if set)
attack_src_port	Spoofed attack source port (if set)
domain	Domain to attack (in attack command)

Malware associated with the attack

CIDR targeted by the C2

Domain targeted issued by C2

SHADOWSERVER

Honeypot DDoS Events Report

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

- The src_ip is the C2 IP issuing the commands, the dst_ip is the IP of the attack victim. If you are getting this report, it means a C2 (src_ip) issuing the attack command was located on your network or constituency.
- Report is available as a file in CSV format

- The report filename contains `event4_honeypot_ddos`

- All timestamps are in UTC

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

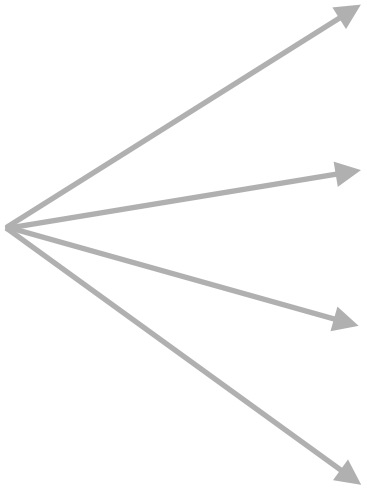
- For more documentation on API access, please visit the below URLs and send a request for access to contact@shadowserver.org
  https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/
  https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

SHADOWSERVER

Example Report - Honeypot DDoS Events

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname	infection
12/04/2022 00:02	udp	198.50.X.X	61234	16276	CA	quebec	montreal	XXX	mirai

Key event fields



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

SHADOWSERVER

Example Report - Honeypot DDoS Events - Key Fields

src_ip	Source IP (IP acting as C2, ie. issuing commands)
src_port	Source port of attack commands
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 destination IP in question belongs; e.g. Communications, Commercial
public_source	Source of the event data
infection	Description of the malware/infection
family	Malware family or campaign associated with the event
tag	Event attributes
application	Application name associated with the event
version	Software version associated with the event
event_id	Unique identifier assigned to the source IP or event
dst_network	Network CIDR being attacked
dst_netmask	Mask of the destination network under attack
attack	Attack type (command issued)
duration	Attack duration
attack_src_ip	Spoofed attack source IP (if set)
attack_src_port	Spoofed attack source port (if set)
domain	Domain to attack (in attack command)

C2 IP issuing commands

Malware associated to the attack

CIDR targeted by the C2

Domain targeted issued by C2

src_ip 198.50.x.x

src_port.

src_asn 61234

src_geo CA

src_region quebec

src_city montreal

src_hostname

src_naics 518210

src_sector communications service provider

domain_source caprica.eu

public_source

infection. ddos

family mirai

tag mirai

application

version

event_id 1440

dst_network x.x.x.x

dst_netmask

attack

duration

attack_src_ip x.x.x.x

attack_src_port

domain xxxxxx.xxx

Example Report - Honeypot DDoS Events

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname	infection
12/04/2022 00:02	udp	198.50.X.X	61234	16276	CA	quebec	montreal	XXX	mirai

IP WHOIS
198.50.XX.XX

```
OrgName:        iWeb Technologies Inc.
OrgId:          GIT-20
Address:        20, place du Commerce
City:           Montreal
StateProv:      QC
PostalCode:     H3E-1Z6
Country:        CA
RegDate:        2003-11-06
Updated:        2019-09-25
Comment:        http://www.iweb.com
Ref:            https://rdap.arin.net/registry/entity/GIT-20


OrgAbuseHandle: ABUSE1906-ARIN
OrgAbuseName:   Abuse Coordinator
OrgAbusePhone:  +1-514-286-4242
OrgAbuseEmail:  abuse@iweb.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE1906-ARIN

OrgNOCHandle: NETWO2356-ARIN
OrgNOCName:   Network Administrator
OrgNOCPhone:  +1-514-286-4242
OrgNOCEmail:  netops@ca.leaseweb.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/NETWO2356-ARIN
```

SHADOWSERVER

Verifying our results

- Honeypots can pick up traces of smaller attacks or ones that had little impact as well, so might have been missed by your organization. You can use this report to gain awareness you (or your constituency) may be a target
- If the attack was large it is likely that you are well aware of the DDoS as it has impacted your operations, but the report can still provide extra insight into the techniques used
- If you do log network traffic in any way you can verify our findings and possibly identify other vectors
- If you are a National CSIRT, the report will give you an overview of typically IoT based DDoS attacks against your country's infrastructure. However, as you are unlikely to have direct insight into network traffic, to verify the impact of the DDoS you would have to contact the targeted organization
- If you are getting a DDoS Target Event report, it means an IP (dst_ip) that was targeted was located on your network or constituency (attack destination)
- If you are getting a DDoS Event report, it means a C2 (src_ip) issuing the attack command was located on your network or constituency.
- Remember the results we share are for the previous day (up to 24 hour delay)

SHADOWSERVER

DDoS - PROTECT

- Follow network security best practices in:
  - Firewalls / IDS
  - Port blocking
  - Rate limiting
  - Blocking of known, malicious IPs
  - Restrict network broadcasting

- Monitor continuously for poor connectivity, traffic spikes / high demand, abnormal / spoofed traffic

- Enhance network redundancy and protection by using a cloud based protection / DDoS mitigation providers, that allow for traffic scrubbing etc

- If you have externally facing UDP based services, such as NTP, DNS etc, you may be contributing to the DDoS problem by also being abused as a reflector. Take steps to restrict external access to such services if possible. See our scan based reports on accessible or open services on your network/constituency and act accordingly to fix issues reported there.

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

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