Honeypot Amplification DDoS Events Report

A honeypot based report on DDoS attacks on your network/constituency

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG

Presentation Aims & Objectives

- Describe DDoS Amplification Attacks
- Describe how Honeypots can be used to detect Amplification DDoS attacks
- Highlight a sample Honeypot Amplification DDoS Events Report
- Describe key features of the report
- Demonstrate how a National CERT or targeted organization can action an Honeypot Amplification DDoS Events Report
- Provide a key list of Shadowserver online resources to enable report subscription and use

SHADOWSERVER

DDoS Amplification

- DDoS Amplification is a prevalent form of denial-of-service attack

- Online services vulnerable to amplification are targeted and then abused as an attack vector

- Amplification occurs via traffic reflection to victims via
  - Unauthenticated IP header information (allowing for spoofed IP attacks)
  - UDP not employing a handshake

- Multiple - primarily UDP - services/protocols are at risk, e.g. NTP, DNS, SSDP, Memcache….and more

- Small spoofed requests may trigger large responses, leading to amplification

- Attacks on such protocols can often exceed more than x100 amplification reflection

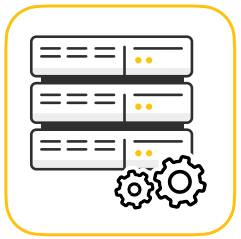
SHADOWSERVER

DDoS Amplification

Attackers

Attacker sends a request with the source IP address of the victim

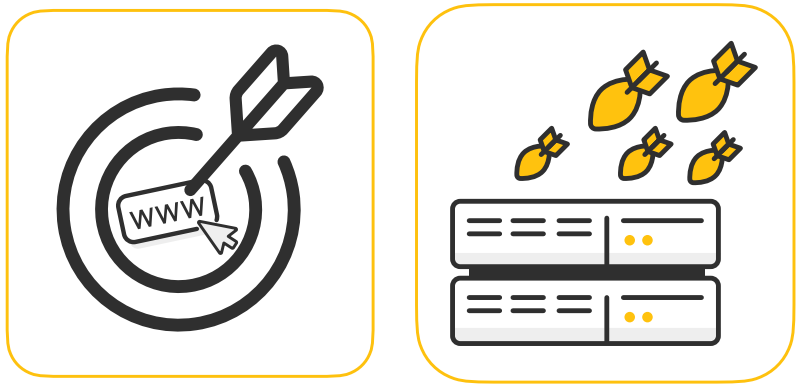
50 byte UDP request



Abused Service

5000 byte UDP response

Service answers with 100x greater response to the victims IP address



Victim

SHADOWSERVER

Reflection & Amplification Attack

Honeypot Sensors

- Honeypots are passive resources that are placed on a network to listen for incoming connections, which typically turn out to be attacks
- Shadowserver runs multiple honeypot sensor types around the World at scale (over 1500 honeypot instances), as do Shadowserver partner organizations
- Honeypots that emulate open, amplifiable UDP services can be used to detect reflective DDoS attacks
- As the source of these attacks is spoofed to the victim address, it is possible only to report on victims being abused, not on on the true source of the DDoS

Honeypot Amplification DDoS Events Report

Honeypot Amplification DDoS Events Report

This report contains information about honeypot observed amplification DDoS events. If you are seeing this report, it means that your IP was DDoSed using other hosts/services as reflectors.

This category of DDoS attacks utilizes UDP-based, open, amplifiable services to reflect packets to a victim, by spoofing the source IP address of the packets sent by the amplifier to the victim's IP address.

Depending on the protocol and type of open services abused, the size of the original packet content sent by the attacker can be amplified in the service response multiple times (even by a factor of hundreds), flooding the victim with packets and enabling DDoS.

Honeypots that emulate open and amplifiable services can be used to detect this kind of abuse. However, as the source of these attacks is spoofed to the victim address, it is possible only to report on victims being abused, not on the true source of the DDoS.

You can read more about our DDoS attack observations **in the SISSDEN blog entry on observations on DDoS attacks in 2018**. For more insight into how amplifiable DDoS attacks work, check out this **writeup and paper by Christian Rossow**, as well as the **US-CERT Alert (TA14-017A)**.

This report contains information about the IP that was attacked (set to src_ip) and the port that was abused on the honeypot to try to make it attack your IP (set to dst_port).

File name: event4_honeypot_ddos_amp

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

SAMPLE

```
"timestamp","protocol","src_ip","src_port","src_asn","src_geo","src_region","src_city","
"2021-03-28 00:00:02",,"107.141.x.x",,7018,"US","CALIFORNIA","VISALIA","107-141-x-x.ligh
"2021-03-28 00:00:02",,"74.59.x.x",,5769,"CA","QUEBEC","CHICOUTIMI","modemcablex-x-59-74
"2021-03-28 00:00:02",,"65.131.x.x",,209,"US","WYOMING","CASPER","65-131-x-x.chyn.qwest.
"2021-03-28 00:00:02",,"104.162.x.x",,12271,"US","NEW YORK","KINGSTON","cpe-104-162-x-x.
"2021-03-28 00:00:02",,"37.120.178.x.x",,197540,"DE","NIEDERSACHSEN","GIFHORN","v2202011
```

SHADOWSERVER

Honeypot Amplification DDoS Events Report

- If you are seeing this report, it means that at least 1 IP on your network or constituency was DDoSed by spoofed packets reflected from another host

- IP provided identifies the device being attacked (src_ip) and not that of the attacker, as the attacker has set his attack source to your IP by a process called spoofing (trivial for UDP based protocols)

- The dst_port field identifies the port that was abused on the honeypot. This can give you an understanding of the type of DDoS reflection attack

SHADOWSERVER

Honeypot Amplification DDoS Events Report

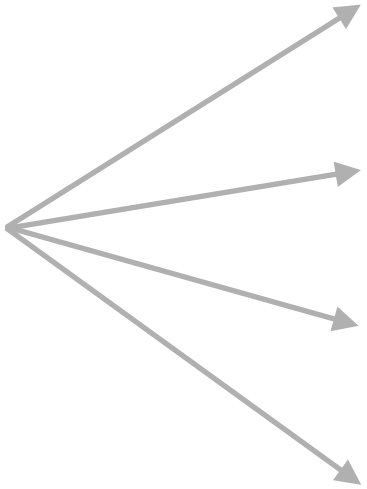
- https://www.shadowserver.org/what-we-do/network-reporting/honeypot-amplification-ddos-events-report/
- Report is available as a file in CSV format
- The report filename contains `event4_honeypot_ddos_amp`
- All timestamps are in UTC
- Reports can be sent as e-mail attachments, or downloaded via HTTP 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

Action a Honeypot Amplification DDoS Event report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname	infection	dst_port
22/04/2022 00:02	udp	63.131.220.83	51731	26133	US	Kentucky	Frankfort	XXX	ddos-amplification	389

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

Key Event Report Fields

Device being attacked

This IP was seen in your network/constituency

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
device_model	Source device model
dst_ip	Destination IP
dst_port	Destination port of the IP connection
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

dst_port that was abused on the honeypot

Providing information on the type of DDoS attack used

Malware associated with the attack

SHADOWSERVER

Action a Honeypot Amplification DDoS Event report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname	infection	dst_port
22/04/2022 00:02	udp	63.131.220.83	51731	26133	US	Kentucky	Frankfort	XXX	ddos-amplification	389

IP WHOIS
63.131.220.XX

```
OrgName:        Frankfort Plant Board
OrgId:          FEWPB
Address:        PO Box 308
Address:        151 Flynn Ave
City:           Frankfort
StateProv:      KY
PostalCode:     40602-0308
Country:        US
RegDate:        2002-07-11
Updated:        2019-12-19
Comment:        https://fpb.cc
Ref:            https://rdap.arin.net/registry/entity/FEWPB


OrgTechHandle: HENRY202-ARIN
OrgTechName:   Henry, Ryan
OrgTechPhone:  +1-502-352-4319
OrgTechEmail:  rhenry@fewpb.com
OrgTechRef:    https://rdap.arin.net/registry/entity/HENRY202-ARIN

OrgAbuseHandle: HENRY202-ARIN
OrgAbuseName:   Henry, Ryan
OrgAbusePhone:  +1-502-352-4319
OrgAbuseEmail:  rhenry@fewpb.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/HENRY202-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 (ie. that is was in fact a reflected attack using a specific set of protocols).
- 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 reflective 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.
- In some cases it may be possible to derive information on the source of the attacks - despite the spoofing. Contact us and we may be able to provide additional information in some cases.
- Remember the results we share are for the previous day (up to 24 hour delay).

SHADOWSERVER

DDoS Amplification - 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-amplification-ddos-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