Honeypot Brute Force Events Report

A honeypot based report on infected machines and IoT devices in your network/constituency

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG

Presentation Aims & Objectives

- Introduce Honeypot sensors and Brute Force Events
- Highlight a sample Honeypot Brute Force Events report
- Describe key features of the report
- Demonstrate how a National CERT can action a Honeypot Brute Force Events report
- Offer guidance on how to protect and remediate attacks taking IoT devices as examples
- Provide a key list of Shadowserver online resources to enable report subscription and use

SHADOWSERVER

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)
- These observe server-side attack activity, from brute force attack attempts, vulnerability exploitation (including remote code execution) and scans/reconnaissance attempts
- Server-side honeypots are effective at observing IoT related threats, botnets, scanning activity, exploitation of known server side vulnerabilities, amplification DDoS and spam

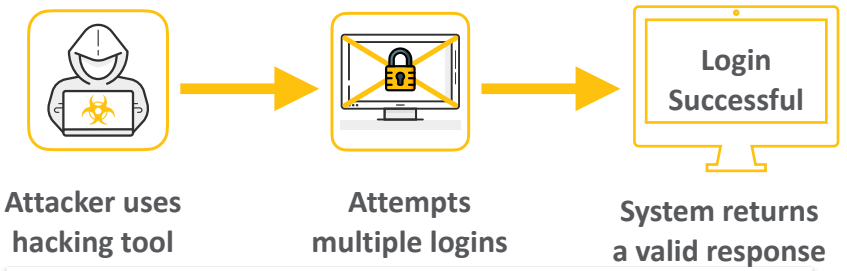
SHADOWSERVER

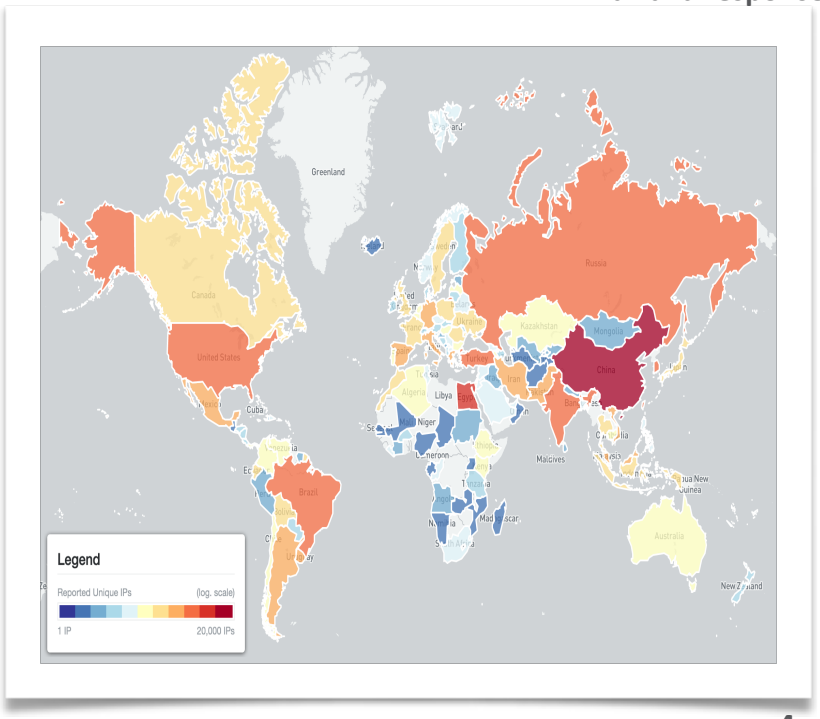
Honeypot Brute Force

- Shadowserver investigates credential brute-force attacks to provide a window into current threat landscapes
- Attackers connecting to a honeypot reveal attacker toolsets, techniques and Indicators of Compromise
- Secure Shell (SSH), Remote Desk Protocol (RDP) are some of the most popular targets, acting as front door gateways to network intrusion
- According to Microsoft, in 2021 attacks on RDP servers have seen a rise of 325% against their honeypots
- IoT device attacks also start with exploiting a vulnerability in the target device or brute-forcing device credentials
- In 2016, the success of the Mirai botnet was due to only 61 hard-coded username-password pairs

SHADOWSERVER

Brute Force Attack Explained





Honeypot sensors - Brute Force

- Primary source of the Honeypot Brute Force Report are Telnet/SSH honeypots
- These honeypots emulate devices that have easily guessable passwords
- After successful log in by the attacker, honeypots collect session information which may include downloaded malware
- Other honeypots also emulate FTP/VNC/SMTP services and can observe brute force attacks
- IoT malware is typically behind most of these types of attacks

Honeypot Brute Force Events Report

- Report is available as a file in CSV format
- The report filename contains `honeypot_brute_force`
- 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

Honeypot Brute Force Events Report

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
```

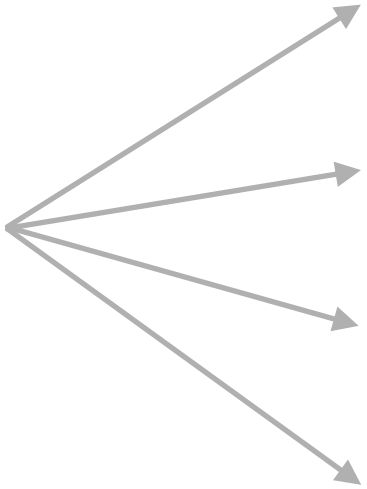
https://www.shadowserver.org/what-we-do/network-reporting/honeypot-brute-force-events-report/

SHADOWSERVER

Action a Brute Force Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname
06/03/2022 00:02	tcp	185.23.214.XX	33289	49453	NL	NOORD-HOLLAND	AMSTERDAM	XXX

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

SHADOWSERVER

Action a Brute Force Report

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname
06/03/2022 00:02	tcp	185.23.214.XX	33289	49453	NL	NOORD-HOLLAND	AMSTERDAM	XXX

IP WHOIS
185.23.214.XX

```
inetnum:        185.23.214.0 - 185.23.214.255
netname:        GLOBALLAYER
descr:          Global Layer B.V.
country:        NL
descr:          ************************************************
descr:          The Netherlands
descr:          IP space for Global Layer customers
descr:          For abuse, please e-mail only: abuse@global-layer.com
descr:          Abuse messages will be handled within 24 hours time
descr:          ************************************************
admin-c:        GL6540-RIPE
tech-c:         GL6540-RIPE
status:         ASSIGNED PA
remarks:        INFRA-AW
mnt-by:         GLOBALLAYER
created:        2015-04-09T20:07:21Z
last-modified:  2016-05-31T11:18:32Z
source:         RIPE # Filtered
```

SHADOWSERVER

Verifying our results

- False positives may be possible if a researcher attempts to connect to our honeypot
- A user may also mistype an IP addresses and connect. A successful SSH/telnet connection will be enough to generate a report
- A report will summarize an SSH/telnet session, which will typically include multiple passwords being brute-forced, commands executed and sometimes a hash of any binaries downloaded

SHADOWSERVER

Honeypot Brute Force Events - PROTECT

- Restrict access to those that need it
- Enhance security of the port and the protocol
- Implement strong password policies
- Enable 2FA
- Use CAPTCHAs
- Limit the number of open ports
- Limit login attempts
- Block malicious IP addresses

SHADOWSERVER

Honeypot Brute Force Events -REMEDIATION

- Install the latest AV / Malware Remover tools to scan and quarantine the infection if applicable
- Update the firmware of a device if applicable by going to the manufacturer website to download and install the latest version
- Reboot the device
- If all else fails perform a factory reset

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-brute-force-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