Honeypot HTTP Scanner Events Report
A report on HTTP scanning and exploitation activity seen in your network/constituency

@shadowserver
contact@shadowserver.org
• Introduce Honeypot HTTP Scanner Events & Reports

• Highlight a sample Honeypot HTTP Scanner Events Report

• Describe key features of the report

• Demonstrate how a National CERT or targeted organization can action an Honeypot HTTP Scanner Events Report

• Offer guidance on how to protect and secure your network / device

• Provide a key list of Shadowserver online resources to enable report subscription and use
HTTP scanning may relate to various benign online activities, for example:

- a search engine indexing the web
- a research project
- ...or an organisation like the Shadowserver Foundation looking for open or vulnerable services

Many scans however are malicious in nature:

- may be part of a network reconnaissance in the preparatory phase of an attack (mapping out an external attack surface)
- or exploit attempts coming from a botnet or other threat actor that is actively looking to breach new services or IoT devices or VPN devices or mail servers (such as Microsoft Exchange)
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 certain types of spam campaigns

• Attackers connecting to a honeypot reveal attacker toolsets, techniques and Indicators of Compromise

• Shadowserver investigates Honeypot HTTP scans to provide a window into server-side threat landscapes, especially related to IoT
• Shadowserver runs its own Web/IoT honeypot

• The honeypot listens on all TCP/UDP ports, is able to decode the application protocol of incoming traffic, and has exploit rules in place that allow for CVE tagging of exploitation attempts

• Honeypot may also have personalities, to better mimic a vulnerable device

• The honeypot itself is passive, does not initiate connections

• Any URLs that the honeypot decodes for malware callbacks are visited by a malware downloader system
Honeypot HTTP Scanner Events Report

This report identifies hosts that have been observed performing HTTP-based scanning activity, including exploitation attempts.

HTTP scanning may be a benign activity — for example, it may be a search engine indexing the web, a research project, or an organization like the Shadowserver Foundation looking for open or vulnerable services that it can report to National CERTs and network owners so that they can remediate their networks.

Other scans, however, may be part of a network reconnaissance in the preparatory phase of an attack or exploit attempts coming from a botnet that is actively looking to infect new sites or devices. Popular targets include various IoT (routers, nas, webcam devices) or VPN devices, CMS systems, Application Servers, Application Delivery Controllers or mail servers (such as Microsoft Exchange).

The HTTP report type, originally introduced as part of the EU Horizon 2020 SISSDEN Project, has been extended under the INEA CEF VARIO IoT project.

It now features detailed information on attacks observed against HTTP honeypots, including CVE, CVSS score, MITRE ATT&CK tactic and technique mappings, affected vendor and product information and other exploit information that can be associated with the collected HTTP requests.

Filename: events_honeypot_http_scan

Key Event Report Fields

- Infection
- Family
- Tag
- Application
- Version
- Event ID
- Pattern
- HTTP URL
- HTTP Agent
- HTTP Request Method
- URL Scheme
- Session Tags
- Vulnerability Score
- Vulnerability Class
- Vulnerability CWE
- Threat Framework
- Threat Tactic ID
- Threat Technique ID
- Target Vendor
- Target Product
- Target Class
- File Name
- SHA256
- Request Raw
- Body Raw

Malware associated to the attack
Exploit information associated via collected HTTP requests
CVE, CVSS score
MITRE ATT&CK tactic and technique mappings
Affected vendor and product information
Honeypot HTTP Scanner Events Report


- Report is available as a file in CSV format

- The report filename contains `event4_honeypot_http_scan`

- 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
  
# Example Scan Report - Honeypot HTTP Scanner

<table>
<thead>
<tr>
<th>timestamp</th>
<th>protocol</th>
<th>src_ip</th>
<th>src_port</th>
<th>src_asn</th>
<th>src_geo</th>
<th>src_region</th>
<th>src_city</th>
<th>src_hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2022 00:02</td>
<td>tcp</td>
<td>75.34.213.XX</td>
<td>33289</td>
<td>49453</td>
<td>US</td>
<td>Washington</td>
<td>Redmond</td>
<td>XXX</td>
</tr>
</tbody>
</table>

### 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
- **src_naics**: North American Industry Classification System Code
- **src_sector**: Sector to which the IP in question belongs; e.g. Communications, Commercial
CVE-2020-16846
Critical shell injection in the netapi SaltStack SSH client

Critical Vulnerability / Severity Score

https://attack.mitre.org/techniques/T1190/
### Example Scan Report - Honeypot HTTP Scanner

<table>
<thead>
<tr>
<th>timestamp</th>
<th>protocol</th>
<th>src_ip</th>
<th>src_port</th>
<th>src_asn</th>
<th>src_geo</th>
<th>src_region</th>
<th>src_city</th>
<th>src_hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/0/2022 00:02</td>
<td>tcp</td>
<td>75.34.213.XX</td>
<td>33289</td>
<td>49453</td>
<td>US</td>
<td>Washington</td>
<td>Redmond</td>
<td>XXX</td>
</tr>
</tbody>
</table>

### IP WHOIS
75.34.213.XX

[OrgName: AT&T Corp.]
[OrgId: AC-3280]
[Address: 7277 164th Ave NE]
[City: Redmond]
[StateProv: WA]
[PostalCode: 98052]
[Country: US]

RegDate: 2018-03-05
Updated: 2021-04-26

Comment: For policy abuse issues contact abuse@att.net
Comment: For all subpoenas, Internet, court order related matters and emergency requests contact
Comment: 11760 US Highway 1
Comment: North Palm Beach, FL 33408
Comment: Main Number: 800-635-6840
Comment: Fax: 888-938-4715
Ref: https://rdap.arin.net/registry/entity/AC-3280

[OrgTechHandle: Z544-ARIN]
[OrgTechName: IPAdmin-ATT Internet Services]
[OrgTechPhone: +1-888-510-5545]
[OrgTechEmail: ipadmin@email.att.com]
[OrgTechRef: https://rdap.arin.net/registry/entity/Z544-ARIN]

[OrgAbuseHandle: ABUSE7-ARIN]
[OrgAbuseName: abuse]
[OrgAbusePhone: +1-919-319-8167]
[OrgAbuseEmail: abuse@att.net]
[OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE7-ARIN]
• Some of the scans picked up in this report may be benign. To determine if a scan is benign, make sure to verify the actual query being registered and any meta-data. Simple GET / or similar queries may be just benign spiders.

• Many of the events reported will have vulnerability or exploit related meta-data attached, such as vulnerability_id numbers, from CVE, EDB, CNVD or other vulnerability/exploit databases, offering exact information on the nature of the scan or attack. Note that a CVE presence may not mean an actual exploit was executed.

• For most of the entries that do have exact vulnerability_ids assigned and do involve exploitation, contact with the device owner is necessary to determine the exact nature of the problem (ie. to determine what kind of infection we are dealing with or perhaps whether a hosting facility is being abused for wide-scale exploitation).

• Remember the results we share are for the previous day (up to 24 hour delay)
• Reduce your external Web service exposure only to services that really need to be exposed

• Maintain an inventory of public facing assets

• Ensure best security practices are in place for any Web services that you need to expose

• Patch regularly

• If you have a constituency of users with IoT devices (including home routers etc) consider filtering traffic that initiates connections to their devices to limit exposure

• If you have direct control of such devices, make sure they do not expose unnecessary services and patch regularly when new firmware updates appear.
Honeypot HTTP Scanner - REMEDIATION

• There is a wide variety of potentially infected services/hosts being reported as part of the report

• You should follow general security best practices for your organization, particular service/operating system as well as best practice incident response procedures

• If you are an individual user and your IoT device is reported here:
  • 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
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/

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