Honeypot HTTP Scanner Events Report

A report on HTTP scanning and exploitation activity seen in your network/constituency

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG

Presentation Aims & Objectives

- 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

SHADOWSERVER

HTTP Scanner Events

- 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

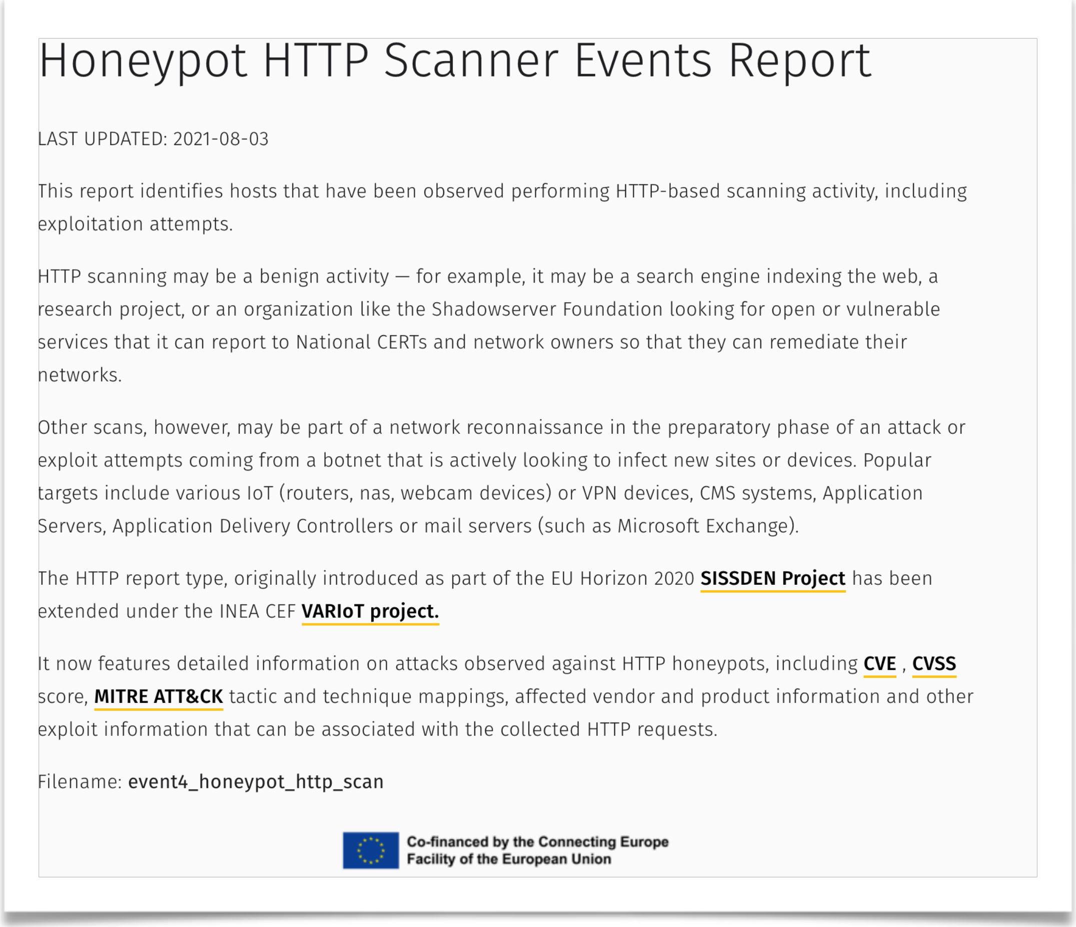
SHADOWSERVER

Honeypot Deployment & Activity

- 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

SHADOWSERVER

Honeypot HTTP Scanner Events Report



Honeypot HTTP Scanner Events Report

LAST UPDATED: 2021-08-03

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).

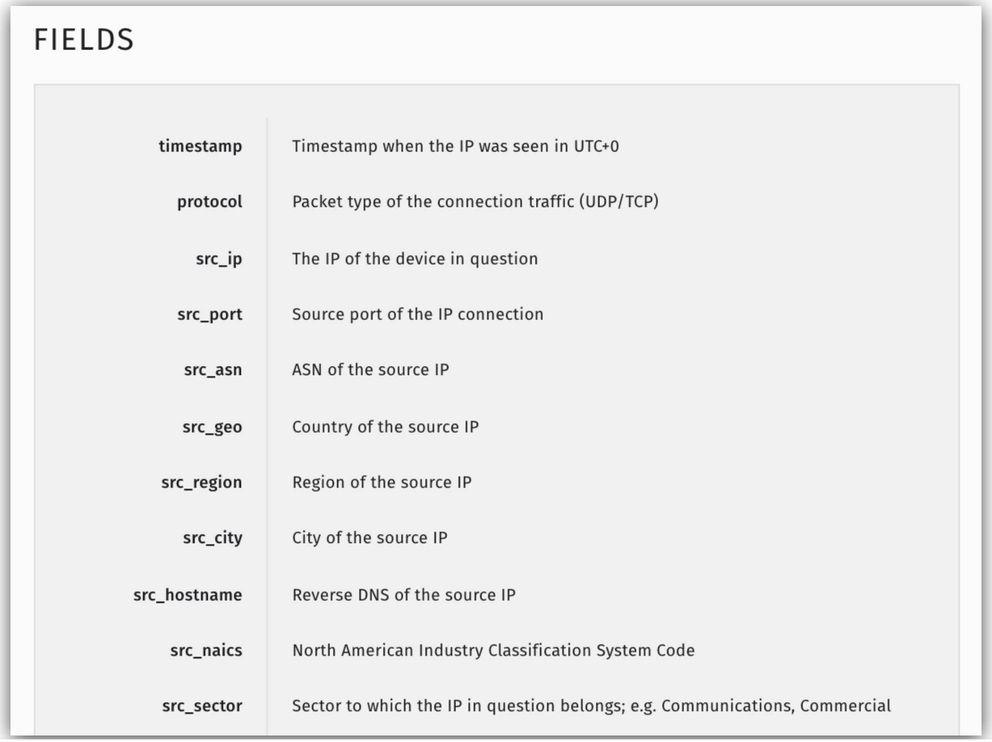
The HTTP report type, originally introduced as part of the EU Horizon 2020 **SISSDEN Project** has been extended under the INEA CEF **VARIoT project.**

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: event4_honeypot_http_scan

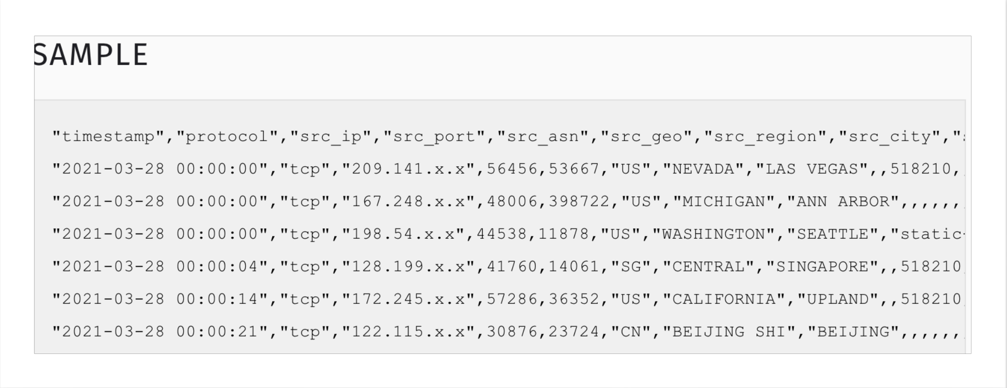
Co-financed by the Connecting Europe Facility of the European Union

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



FIELDS

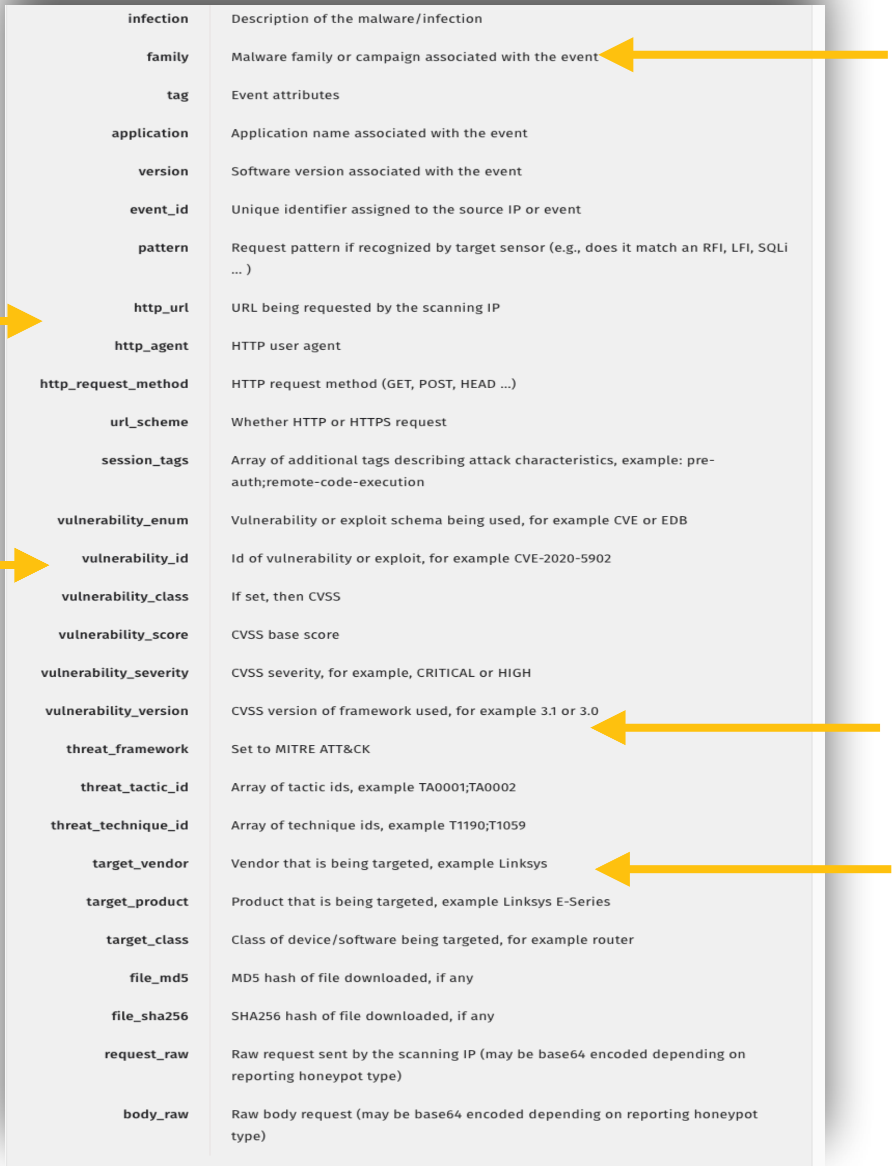
timestamp	Timestamp when the IP was seen in UTC+0
protocol	Packet type of the connection traffic (UDP/TCP)
src_ip	The IP of the device in question
src_port	Source port of the IP connection
src_asn	ASN of the source IP
src_geo	Country of the source IP
src_region	Region of the source IP
src_city	City of 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 00:00:00","tcp","209.141.x.x",56456,53667,"US","NEVADA","LAS VEGAS",,518210,
"2021-03-28 00:00:00","tcp","167.248.x.x",48006,398722,"US","MICHIGAN","ANN ARBOR",,,,,,
"2021-03-28 00:00:00","tcp","198.54.x.x",44538,11878,"US","WASHINGTON","SEATTLE","static
"2021-03-28 00:00:04","tcp","128.199.x.x",41760,14061,"SG","CENTRAL","SINGAPORE",,518210
"2021-03-28 00:00:14","tcp","172.245.x.x",57286,36352,"US","CALIFORNIA","UPLAND",,518210
"2021-03-28 00:00:21","tcp","122.115.x.x",30876,23724,"CN","BEIJING SHI","BEIJING",,,,,,
```

Key Event Report Fields



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
pattern	Request pattern if recognized by target sensor (e.g., does it match an RFI, LFI, SQLi ...)
http_url	URL being requested by the scanning IP
http_agent	HTTP user agent
http_request_method	HTTP request method (GET, POST, HEAD ...)
url_scheme	Whether HTTP or HTTPS request
session_tags	Array of additional tags describing attack characteristics, example: pre-auth;remote-code-execution
vulnerability_enum	Vulnerability or exploit schema being used, for example CVE or EDB
vulnerability_id	Id of vulnerability or exploit, for example CVE-2020-5902
vulnerability_class	If set, then CVSS
vulnerability_score	CVSS base score
vulnerability_severity	CVSS severity, for example, CRITICAL or HIGH
vulnerability_version	CVSS version of framework used, for example 3.1 or 3.0
threat_framework	Set to MITRE ATT&CK
threat_tactic_id	Array of tactic ids, example TA0001;TA0002
threat_technique_id	Array of technique ids, example T1190;T1059
target_vendor	Vendor that is being targeted, example Linksys
target_product	Product that is being targeted, example Linksys E-Series
target_class	Class of device/software being targeted, for example router
file_md5	MD5 hash of file downloaded, if any
file_sha256	SHA256 hash of file downloaded, if any
request_raw	Raw request sent by the scanning IP (may be base64 encoded depending on reporting honeypot type)
body_raw	Raw body request (may be base64 encoded depending on reporting honeypot type)

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

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

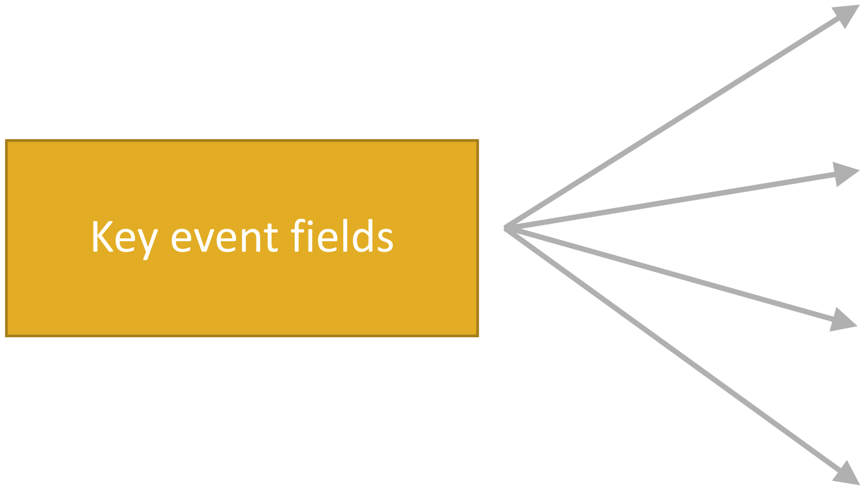
  https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/

  https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

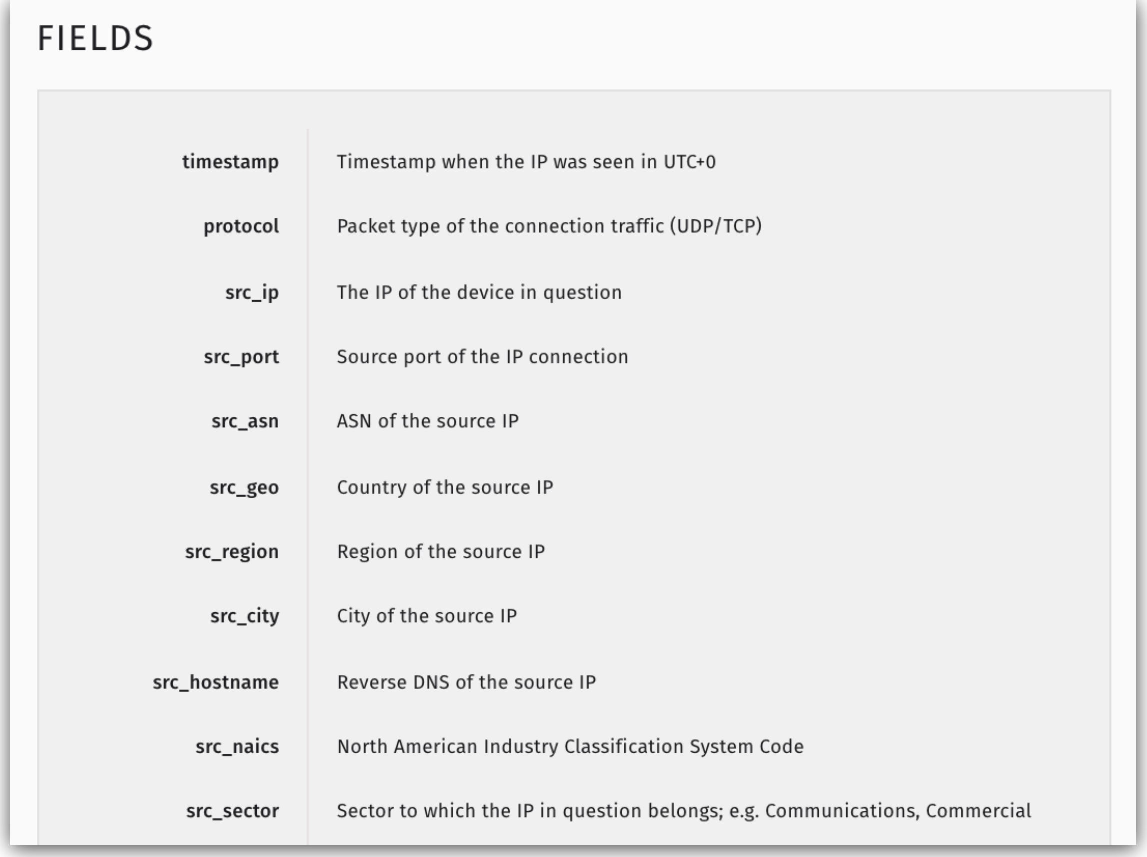
SHADOWSERVER

Example Scan Report - Honeypot HTTP Scanner

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname
05/0/2022 00:02	tcp	75.34.213.XX	33289	49453	US	Washington	Redmond	XXX



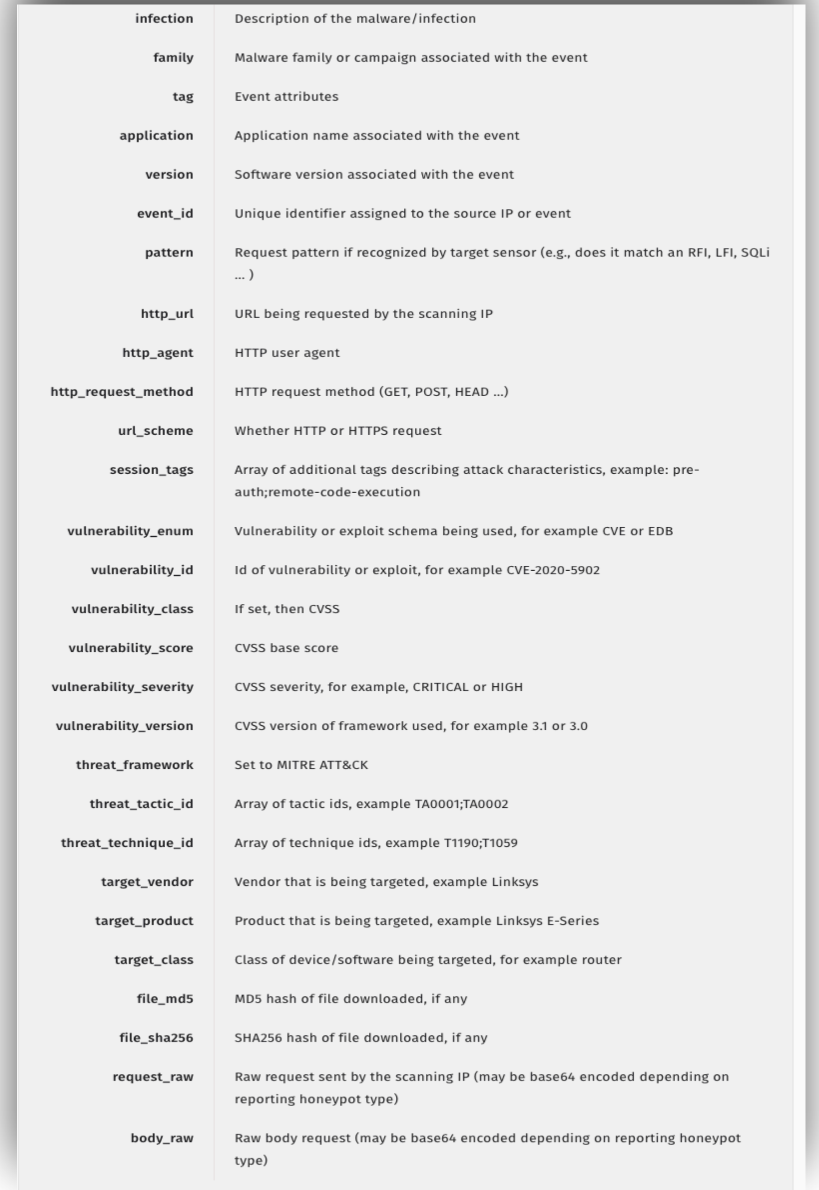
Key event fields



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

Key Report Fields



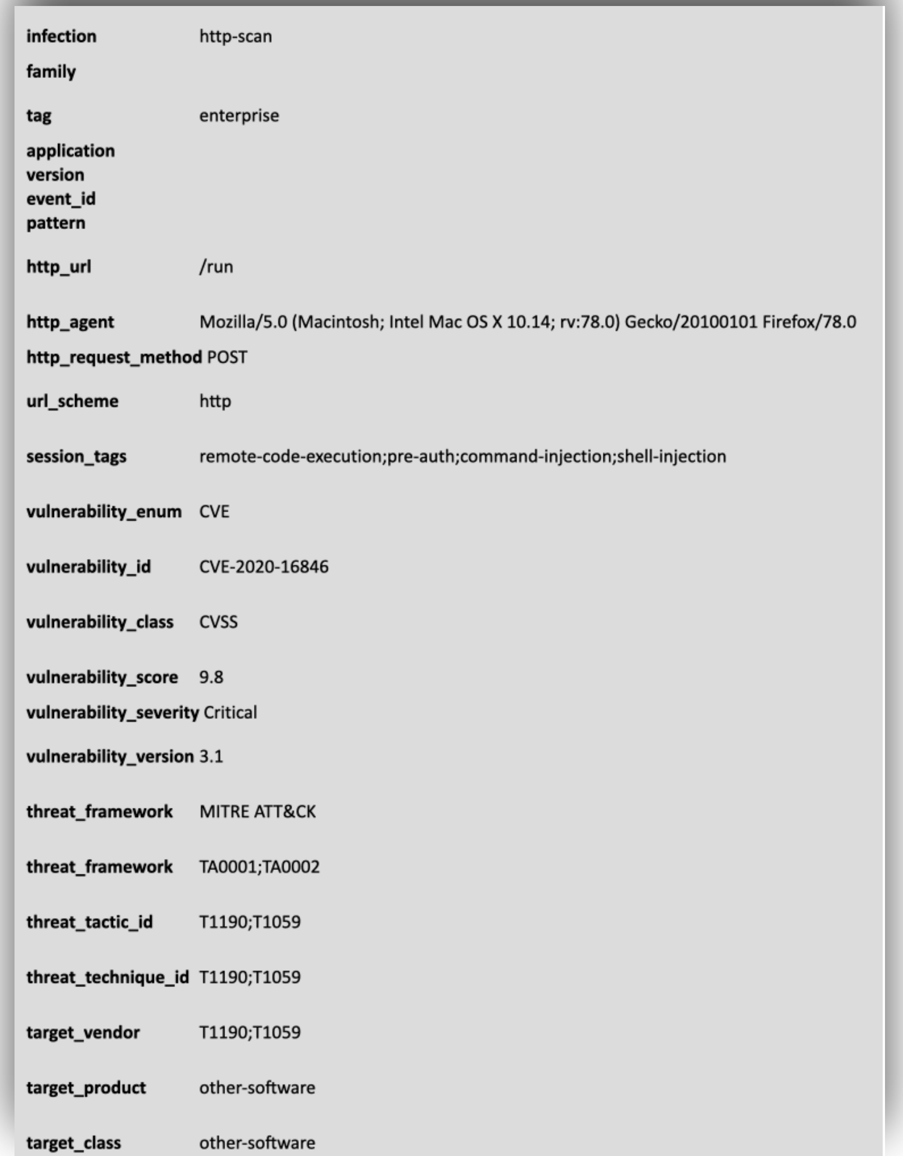
infection	Description of the malware/infection
family	Malware family or campaign associated with the event
tag	Event attributes
application	Application name associated with the event
version	Software version associated with the event
event_id	Unique identifier assigned to the source IP or event
pattern	Request pattern if recognized by target sensor (e.g., does it match an RFI, LFI, SQLi …)
http_url	URL being requested by the scanning IP
http_agent	HTTP user agent
http_request_method	HTTP request method (GET, POST, HEAD …)
url_scheme	Whether HTTP or HTTPS request
session_tags	Array of additional tags describing attack characteristics, example: pre-auth;remote-code-execution
vulnerability_enum	Vulnerability or exploit schema being used, for example CVE or EDB
vulnerability_id	Id of vulnerability or exploit, for example CVE-2020-5902
vulnerability_class	If set, then CVSS
vulnerability_score	CVSS base score
vulnerability_severity	CVSS severity, for example, CRITICAL or HIGH
vulnerability_version	CVSS version of framework used, for example 3.1 or 3.0
threat_framework	Set to MITRE ATT&CK
threat_tactic_id	Array of tactic ids, example TA0001;TA0002
threat_technique_id	Array of technique ids, example T1190;T1059
target_vendor	Vendor that is being targeted, example Linksys
target_product	Product that is being targeted, example Linksys E-Series
target_class	Class of device/software being targeted, for example router
file_md5	MD5 hash of file downloaded, if any
file_sha256	SHA256 hash of file downloaded, if any
request_raw	Raw request sent by the scanning IP (may be base64 encoded depending on reporting honeypot type)
body_raw	Raw body request (may be base64 encoded depending on reporting honeypot type)

Exploit information associated via collected HTTP requests

CVE-2020-16846
Critical shell injection in the netapi SaltStack SSH client

Critical Vulnerability / Severity Score

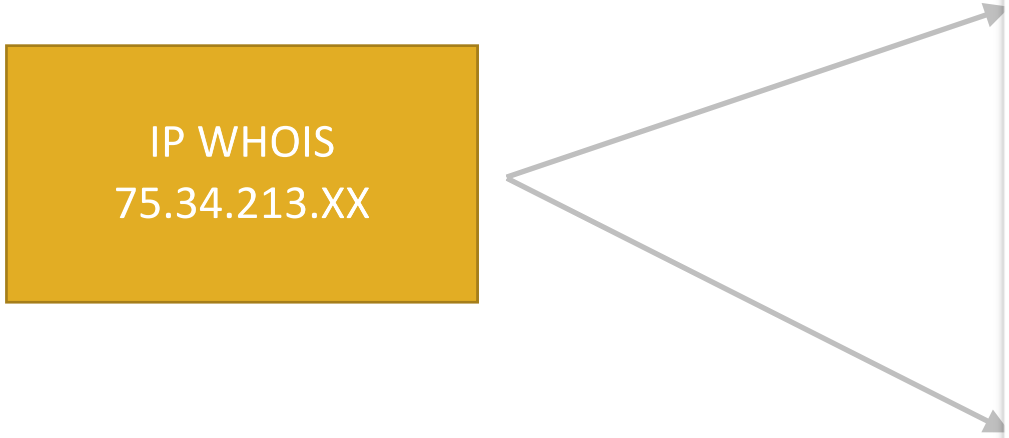
https://attack.mitre.org/techniques/T1190/

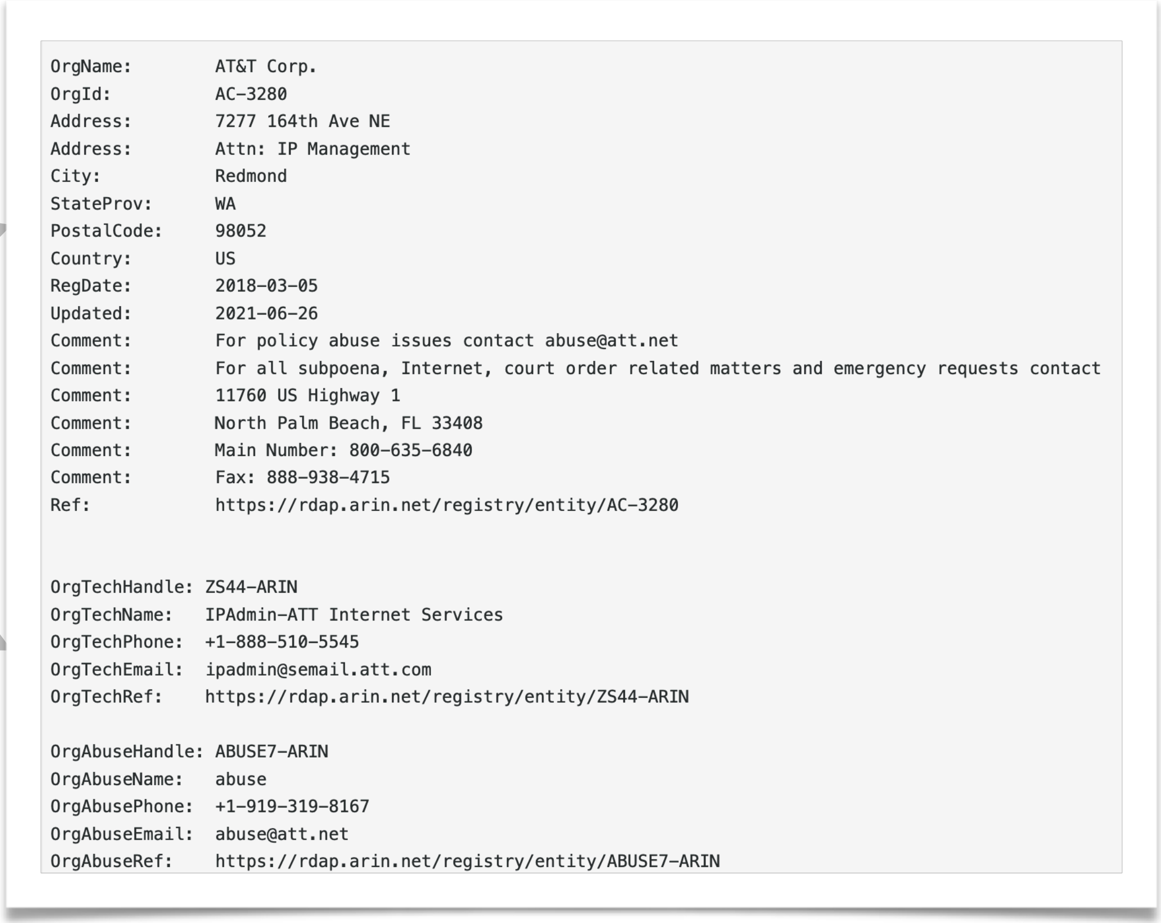


infection	http-scan
family	
tag	enterprise
application	
version	
event_id	
pattern	
http_url	/run
http_agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:78.0) Gecko/20100101 Firefox/78.0
http_request_method	POST
url_scheme	http
session_tags	remote-code-execution;pre-auth;command-injection;shell-injection
vulnerability_enum	CVE
vulnerability_id	CVE-2020-16846
vulnerability_class	CVSS
vulnerability_score	9.8
vulnerability_severity	Critical
vulnerability_version	3.1
threat_framework	MITRE ATT&CK
threat_framework	TA0001;TA0002
threat_tactic_id	T1190;T1059
threat_technique_id	T1190;T1059
target_vendor	T1190;T1059
target_product	other-software
target_class	other-software

Example Scan Report - Honeypot HTTP Scanner

timestamp	protocol	src_ip	src_port	src_asn	src_geo	src_region	src_city	src_hostname
05/0/2022 00:02	tcp	75.34.213.XX	33289	49453	US	Washington	Redmond	XXX





```
OrgName:        AT&T Corp.
OrgId:          AC-3280
Address:        7277 164th Ave NE
Address:        Attn: IP Management
City:           Redmond
StateProv:      WA
PostalCode:     98052
Country:        US
RegDate:        2018-03-05
Updated:        2021-06-26
Comment:        For policy abuse issues contact abuse@att.net
Comment:        For all subpoena, 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: ZS44-ARIN
OrgTechName:   IPAdmin-ATT Internet Services
OrgTechPhone:  +1-888-510-5545
OrgTechEmail:  ipadmin@semail.att.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZS44-ARIN

OrgAbuseHandle: ABUSE7-ARIN
OrgAbuseName:   abuse
OrgAbusePhone:  +1-919-319-8167
OrgAbuseEmail:  abuse@att.net
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE7-ARIN
```

Verifying our results

- 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)

Honeypot HTTP Scanner - PROTECT

- 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/
- https://www.shadowserver.org/what-we-do/network-reporting/honeypot-http-scanner-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

Lighting the way to a more secure Internet

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG