Malware URL Report

A report on possible malware C2 or malware download sites in your network or constituency

@shadowserver

✉ contact@shadowserver.org

SHADOWSERVER.ORG

Presentation Aims & Objectives

- Explain what we mean by Malware URLs
- Introduce Malware URL reports
- Highlight a sample Malware URL report
- Describe key features of the report
- Demonstrate how a National CERT or network owner can action a Malware URL report
- Offer guidance on how to remediate malware callbacks
- Provide a key list of Shadowserver online resources to enable report subscription and use

Exploitation and Malware

- When successful exploitation is carried out, an exploit typically includes malware callbacks to external sites to deliver malware on the successfully exploited host
- Typically this is done by hosting the malicious resource on a URL
- Victims are directed to the malicious URL which can act as a C2 that provides instructions on next actions which can also include malware download. This malware can then engage in subsequent attacks
- One way of observing these URLs is through various kinds of honeypots. Exploitation of these honeypots by attackers is often followed by various malware callbacks
- We run honeypots of various types that observe exploitation attempts and URL callbacks
- We also register any malware downloads and attempt to collect the malware

Malware URL Report

- Malware URL Report: https://www.shadowserver.org/what-we-do/network-reporting/malware-url-report/

- Report is available as a file in CSV format

- The report filename contains `malware_url`

- All timestamps are in UTC

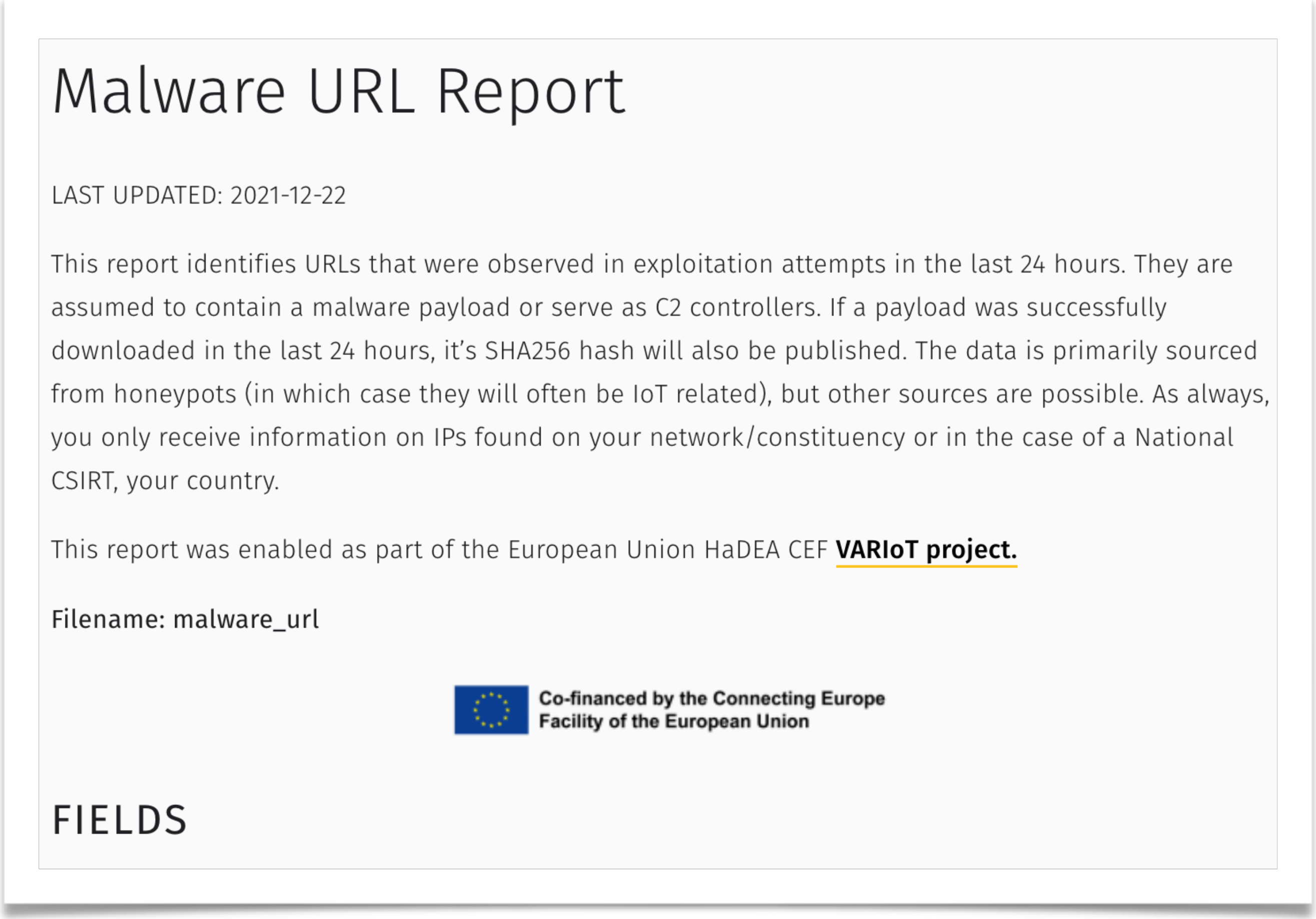
- Reports can be sent as e-mail attachments, downloaded via HTTP or obtained via a RESTful API

- 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/

Malware URL Report

- This report identifies URLs observed in exploitation attempts in the last 24 hours
- If a payload was successfully downloaded in the last 24 hours, its SHA256 hash will also be published
- Each event is likely to contain an associated malware payload or one that serves as a c2 controller
- The data is primarily honeypot sourced and IoT related (a mix of Web/SSH/telnet/IoT honeypots)
- Other sources may be added in future

Example Malware URL Report



Malware URL Report

LAST UPDATED: 2021-12-22

This report identifies URLs that were observed in exploitation attempts in the last 24 hours. They are assumed to contain a malware payload or serve as C2 controllers. If a payload was successfully downloaded in the last 24 hours, it's SHA256 hash will also be published. The data is primarily sourced from honeypots (in which case they will often be IoT related), but other sources are possible. As always, you only receive information on IPs found on your network/constituency or in the case of a National CSIRT, your country.

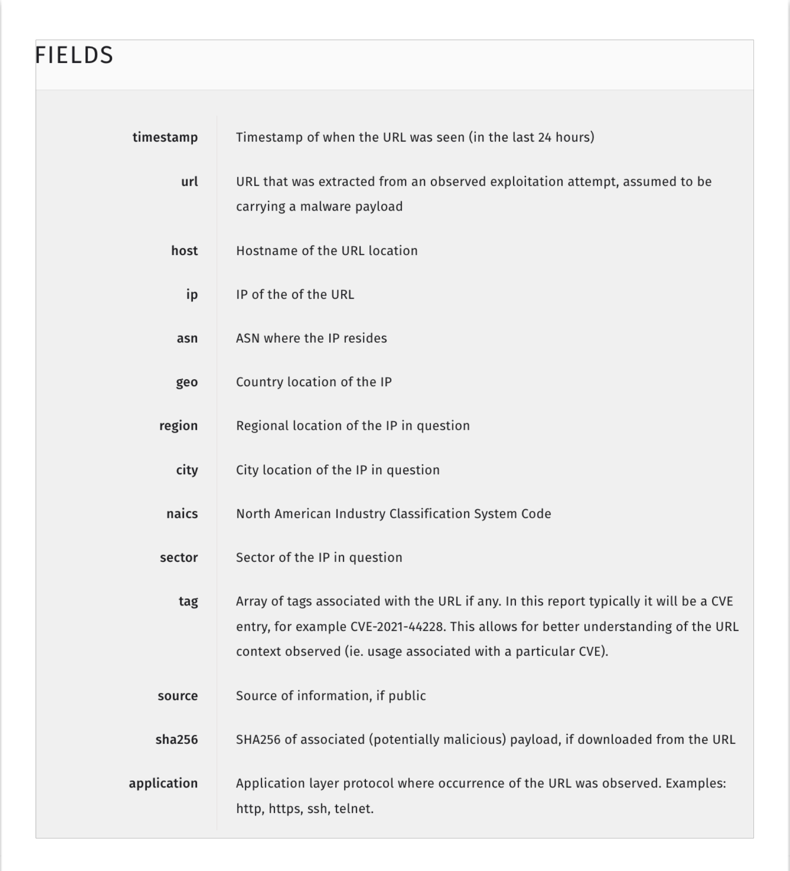
This report was enabled as part of the European Union HaDEA CEF **VARIoT project.**

Filename: malware_url

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

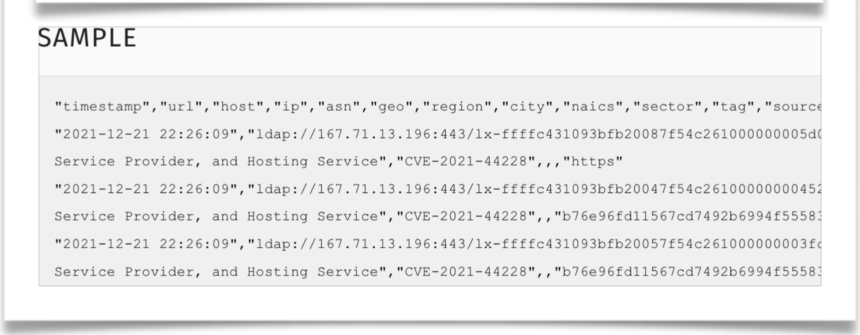
FIELDS

https://www.shadowserver.org/what-we-do/network-reporting/malware-url-report/



FIELDS

timestamp	Timestamp of when the URL was seen (in the last 24 hours)
url	URL that was extracted from an observed exploitation attempt, assumed to be carrying a malware payload
host	Hostname of the URL location
ip	IP of the of the URL
asn	ASN where the IP resides
geo	Country location of the IP
region	Regional location of the IP in question
city	City location of the IP in question
naics	North American Industry Classification System Code
sector	Sector of the IP in question
tag	Array of tags associated with the URL if any. In this report typically it will be a CVE entry, for example CVE-2021-44228. This allows for better understanding of the URL context observed (ie. usage associated with a particular CVE).
source	Source of information, if public
sha256	SHA256 of associated (potentially malicious) payload, if downloaded from the URL
application	Application layer protocol where occurrence of the URL was observed. Examples: http, https, ssh, telnet.

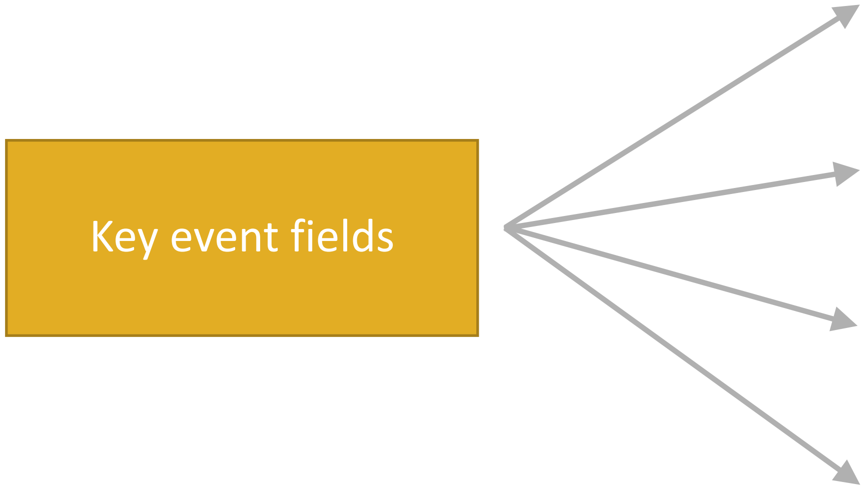


SAMPLE

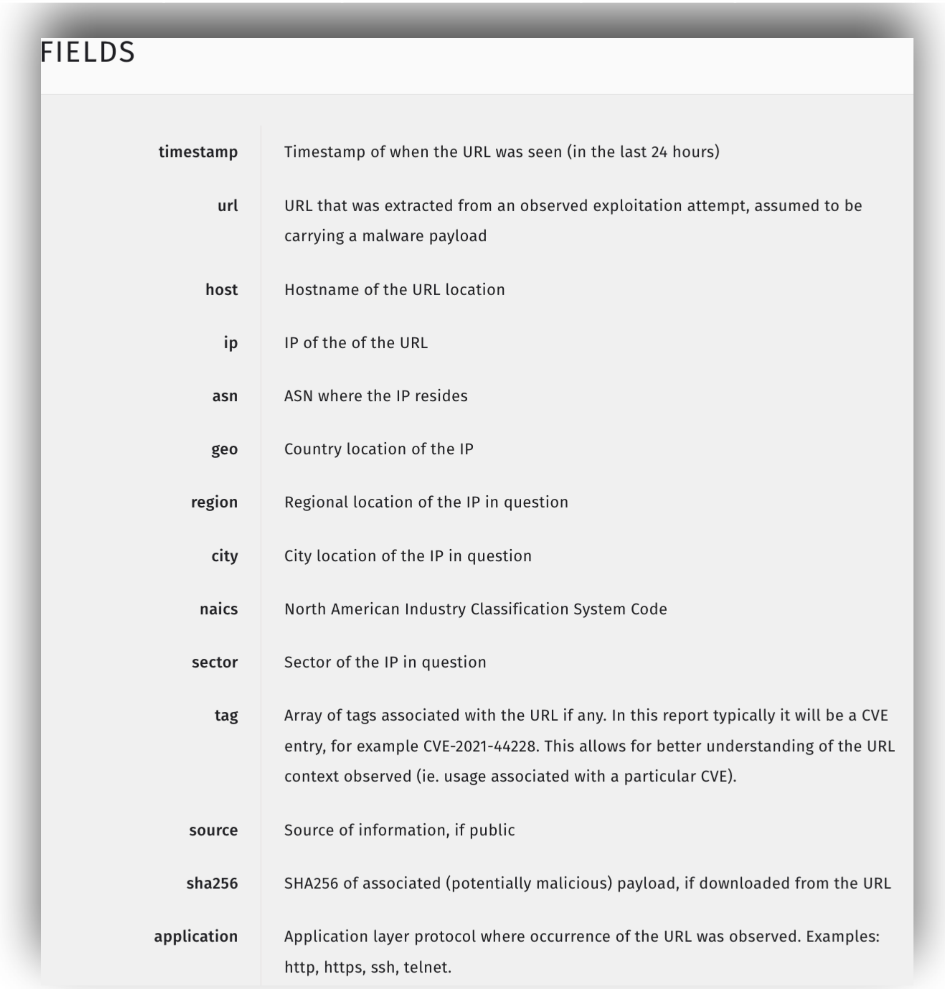
```
"timestamp","url","host","ip","asn","geo","region","city","naics","sector","tag","source
"2021-12-21 22:26:09","ldap://167.71.13.196:443/lx-ffffc431093bfb20087f54c261000000005d
Service Provider, and Hosting Service","CVE-2021-44228",,,"https"
"2021-12-21 22:26:09","ldap://167.71.13.196:443/lx-ffffc431093bfb20047f54c26100000000452
Service Provider, and Hosting Service","CVE-2021-44228",,"b76e96fd11567cd7492b6994f5558
"2021-12-21 22:26:09","ldap://167.71.13.196:443/lx-ffffc431093bfb20057f54c261000000003f
Service Provider, and Hosting Service","CVE-2021-44228",,"b76e96fd11567cd7492b6994f5558
```

Action a Malware URL Report

timestamp	url	host	ip	geo	region	city	naics	sector	tag	source	sha256	application
12/04/2022 00:00	223.130.X.X:51032/Mozi.m	223.130.X.X	223.130.X.X	IN	punjab	ludhiana	XXX	XXX	CVE-2014-8361	XXX	XXX	http



Key event fields



FIELDS

timestamp Timestamp of when the URL was seen (in the last 24 hours)

url URL that was extracted from an observed exploitation attempt, assumed to be carrying a malware payload

host Hostname of the URL location

ip IP of the of the URL

asn ASN where the IP resides

geo Country location of the IP

region Regional location of the IP in question

city City location of the IP in question

naics North American Industry Classification System Code

sector Sector of the IP in question

tag Array of tags associated with the URL if any. In this report typically it will be a CVE entry, for example CVE-2021-44228. This allows for better understanding of the URL context observed (ie. usage associated with a particular CVE).

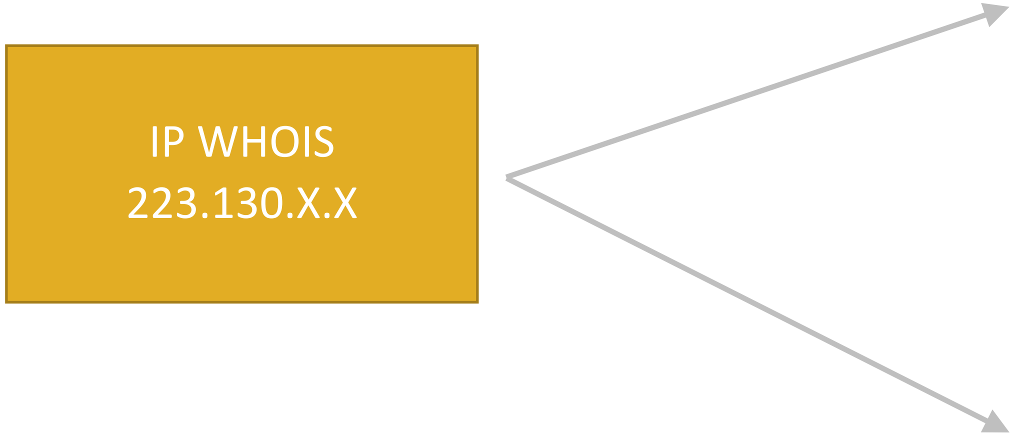
source Source of information, if public

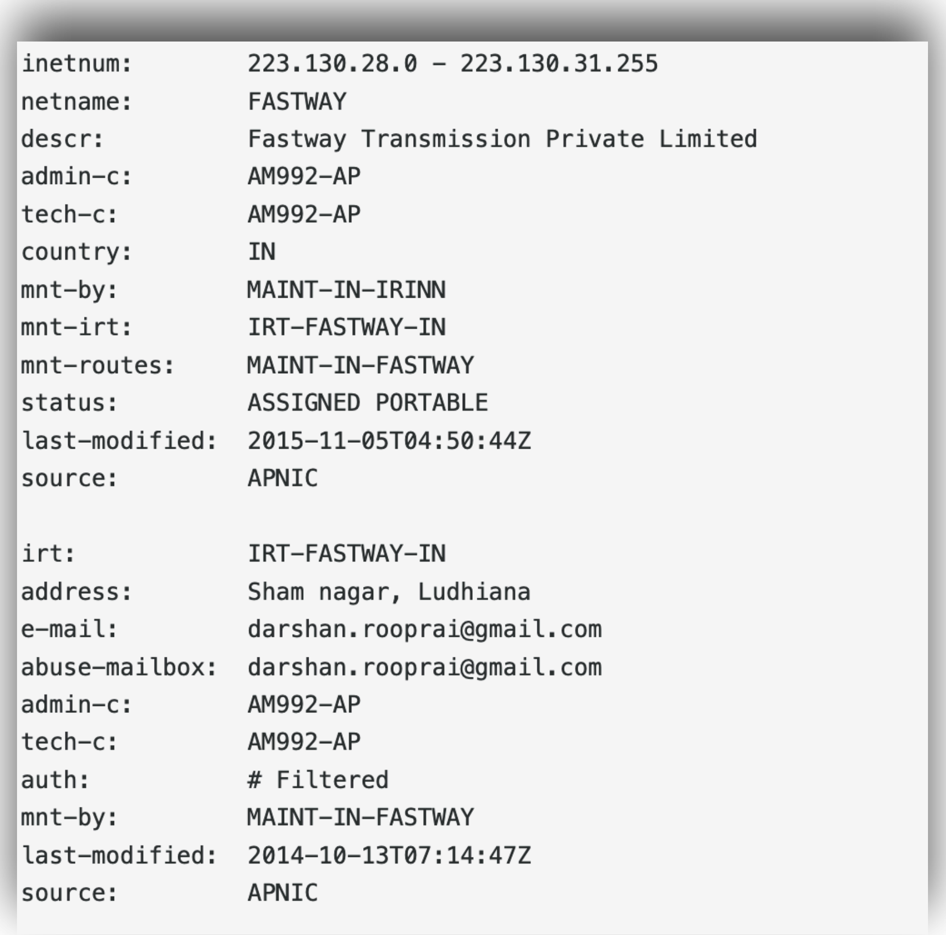
sha256 SHA256 of associated (potentially malicious) payload, if downloaded from the URL

application Application layer protocol where occurrence of the URL was observed. Examples: http, https, ssh, telnet.

Action a Malware URL Report

timestamp	url	host	ip	geo	region	city	naics	sector	tag	source	sha256	application
12/04/2022 00:00	223.130.X.X:51032/Mozi.m	223.130.X.X	223.130.X.X	IN	punjab	ludhiana	XXX	XXX	CVE-2014-8361	XXX	XXX	http


IP WHOIS
223.130.X.X


```
inetnum:        223.130.28.0 - 223.130.31.255
netname:        FASTWAY
descr:          Fastway Transmission Private Limited
admin-c:        AM992-AP
tech-c:         AM992-AP
country:        IN
mnt-by:         MAINT-IN-IRINN
mnt-irt:        IRT-FASTWAY-IN
mnt-routes:     MAINT-IN-FASTWAY
status:         ASSIGNED PORTABLE
last-modified:  2015-11-05T04:50:44Z
source:         APNIC

irt:            IRT-FASTWAY-IN
address:        Sham nagar, Ludhiana
e-mail:         darshan.rooprai@gmail.com
abuse-mailbox:  darshan.rooprai@gmail.com
admin-c:        AM992-AP
tech-c:         AM992-AP
auth:           # Filtered
mnt-by:         MAINT-IN-FASTWAY
last-modified:  2014-10-13T07:14:47Z
source:         APNIC
```

Verifying results

- Extracting malware URLs from exploitation attempts is a non-trivial task. We extract those URLs then visit them via a malware download system to trigger potential malware downloads

- It is possible that the spider we have developed attempts to follow benign links as well, leading to false positives

- If you suspect a false positive, please contact us. We can add certain URLs to allow lists and not report them out

- Sites that host malware tend to be taken down relatively quickly, so you may have received a report for a resource already actioned on

- In some cases, a URL may not service you malware based on your location/source

- In some cases, a URL may be long dead, but the malware is still actively trying to exploit hosts and spread - not much can be done here from the perspective of this report other than fixing all the hosts that are actively involved in exploitation

Malware Callbacks - PROTECT/REMEDIATE

- Ensure best security practices are in place at your organization so you do not become a host for malware C2

- If you are a hosting provider, make sure you have procedures in place to quickly investigate and take down reported cases

- If you are an owner of an IoT device that has been reported, follow guidance from your manufacturer to secure/update/reset it

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/malware-url-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