

Free Automated Malware Analysis Service - powered by Falcon Sandbox

Archived: 2026-04-05 23:21:10 UTC

Incident Response

MITRE ATT&CK™ Techniques Detection

This report has 3 indicators that were mapped to 2 attack techniques and 1 tactics. [View all details](#)

Additional Context

Related Sandbox Artifacts

Associated URLs

hxxps://ptpb.pw/~x

Indicators

Not all malicious and suspicious indicators are displayed. Get your own [cloud service](#) or the [full version](#) to view all details.

- External Systems
 - [Sample was identified as malicious by a trusted Antivirus engine](#)
details
No specific details available
source
External System
relevance
5/10
 - [Sample was identified as malicious by at least one Antivirus engine](#)
details
2/58 Antivirus vendors marked sample as malicious (3% detection rate)
source
External System
relevance
8/10
- Environment Awareness
 - [Queries system general information \(syscall\)](#)
details

/bin/bash used: sysinfo

/bin/bash used: uname

source

API Call

relevance

3/10

ATT&CK ID

T1082 ([Show technique in the MITRE ATT&CK™ matrix](#))

- General

- [Executes a shell command](#)

details

/bin/bash executed: bash /tmp/x.sh

source

API Call

relevance

10/10

- Network Related

- [Detected increased number of ARP broadcast requests \(network device lookup\)](#)

details

Attempt to find devices in networks: "192.168.56.1/32, 192.168.56.25/32, ..."

source

Network Traffic

relevance

10/10

ATT&CK ID

T1046 ([Show technique in the MITRE ATT&CK™ matrix](#))

- Environment Awareness

- [Gets user and/or group ID \(syscall\)](#)

details

/bin/bash used: getuid

/bin/bash used: geteuid

source

API Call

ATT&CK ID

T1082 ([Show technique in the MITRE ATT&CK™ matrix](#))

- Network Related

- [Found potential URL in binary/memory](#)

details

Pattern match: "https://ptpb.pw/~u"

Heuristic match: "bash /tmp/x.sh"

source

File/Memory

relevance

10/10

File Details

All Details:

OnOff

x

Filename

x

Size

890B (890 bytes)

Type

script sh

Description

Bourne-Again shell script, ASCII text executable

Architecture

LINUX

SHA256

28553b3a9d2ad4361d33d29ac4bf771d008e0073cec01b5561c6348a608f8dd7 

Resources

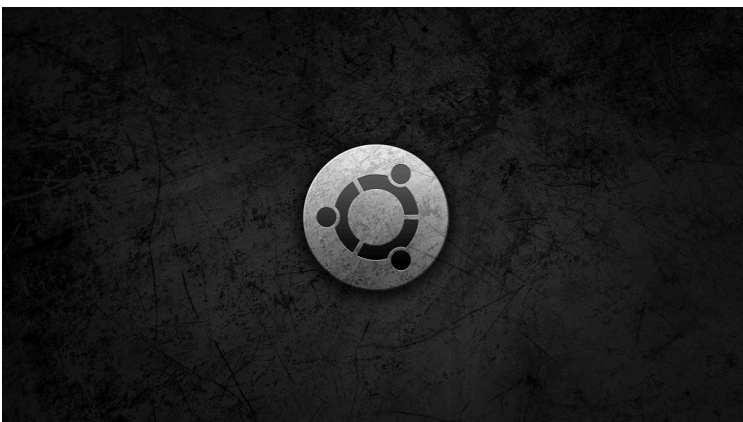
Icon

-

Classification (TrID)

- 100.0% (.SH) Linux/UNIX shell script

Screenshots



Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 1 process in total.

-  [bash](#) bash /tmp/x.sh (PID: 1825)

Network Analysis

DNS Requests

No relevant DNS requests were made.

HTTP Traffic

No relevant HTTP requests were made.

Extracted Files

No significant files were extracted.

Warnings

- Added comment to Virus Total report

Source: <https://www.hybrid-analysis.com/sample/28553b3a9d2ad4361d33d29ac4bf771d008e0073cec01b5561c6348a608f8dd7?environmentId=300>