ThreatQuotient

MalwareBazaar Operation User Guide

Version 1.0.0

November 01, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported

Introduction

The MalwareBazaar Operation for ThreatQ enables a user to query MalwareBazaar for any threat context for a given file hash.

The operation provides the following action:

- **Query** - queries MalwareBazaar for Threat Context.

The operation is compatible with the following indicator types:

- MD5
- SHA-1
- SHA-256

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the integration file on your local machine

    > ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

Configuration

ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

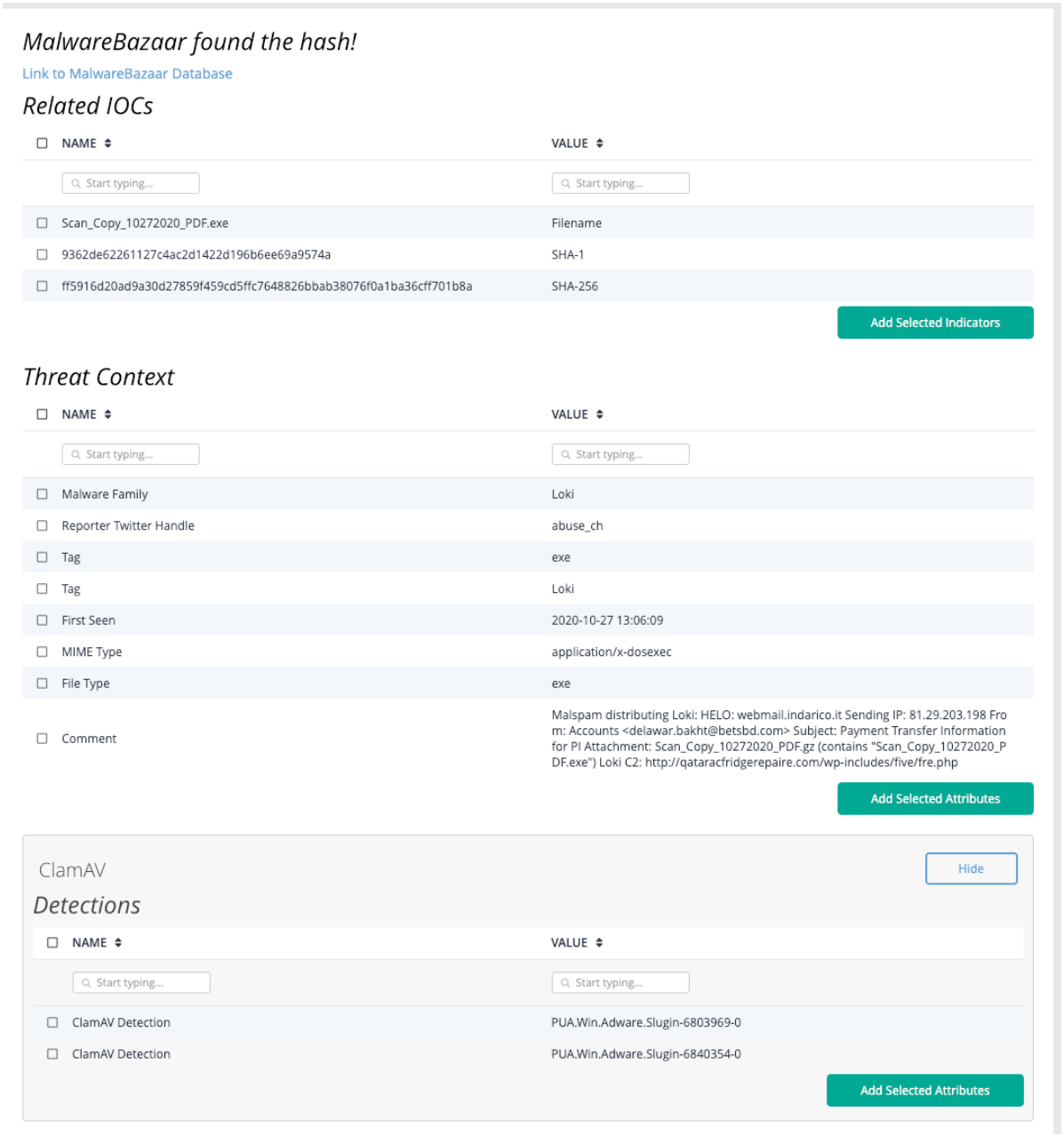
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query	Queries MalwareBazaar for Threat Context.	Indicator	MD5, SHA-1, SHA-256

Example 1 Response



MalwareBazaar found the hash!

Link to MalwareBazaar Database

Related IOCs

NAME	VALUE
Scan_Copy_10272020_PDF.exe	Filename
9362de62261127c4ac2d1422d196b6ee69a9574a	SHA-1
ff5916d20ad9a30d27859f459cd5ffc7648826bbab38076f0a1ba36cff701b8a	SHA-256

Add Selected Indicators

Threat Context

NAME	VALUE
Malware Family	Loki
Reporter Twitter Handle	abuse_ch
Tag	exe
Tag	Loki
First Seen	2020-10-27 13:06:09
MIME Type	application/x-dosexec
File Type	exe
Comment	Malspam distributing Loki: HELO: webmail.indarico.it Sending IP: 81.29.203.198 From: Accounts <delawar.bakht@betsbd.com> Subject: Payment Transfer Information for PI Attachment: Scan_Copy_10272020_PDF.gz (contains "Scan_Copy_10272020_PDF.exe") Loki C2: http://qataracfridgerepaire.com/wp-includes/five/fre.php

Add Selected Attributes

ClamAV

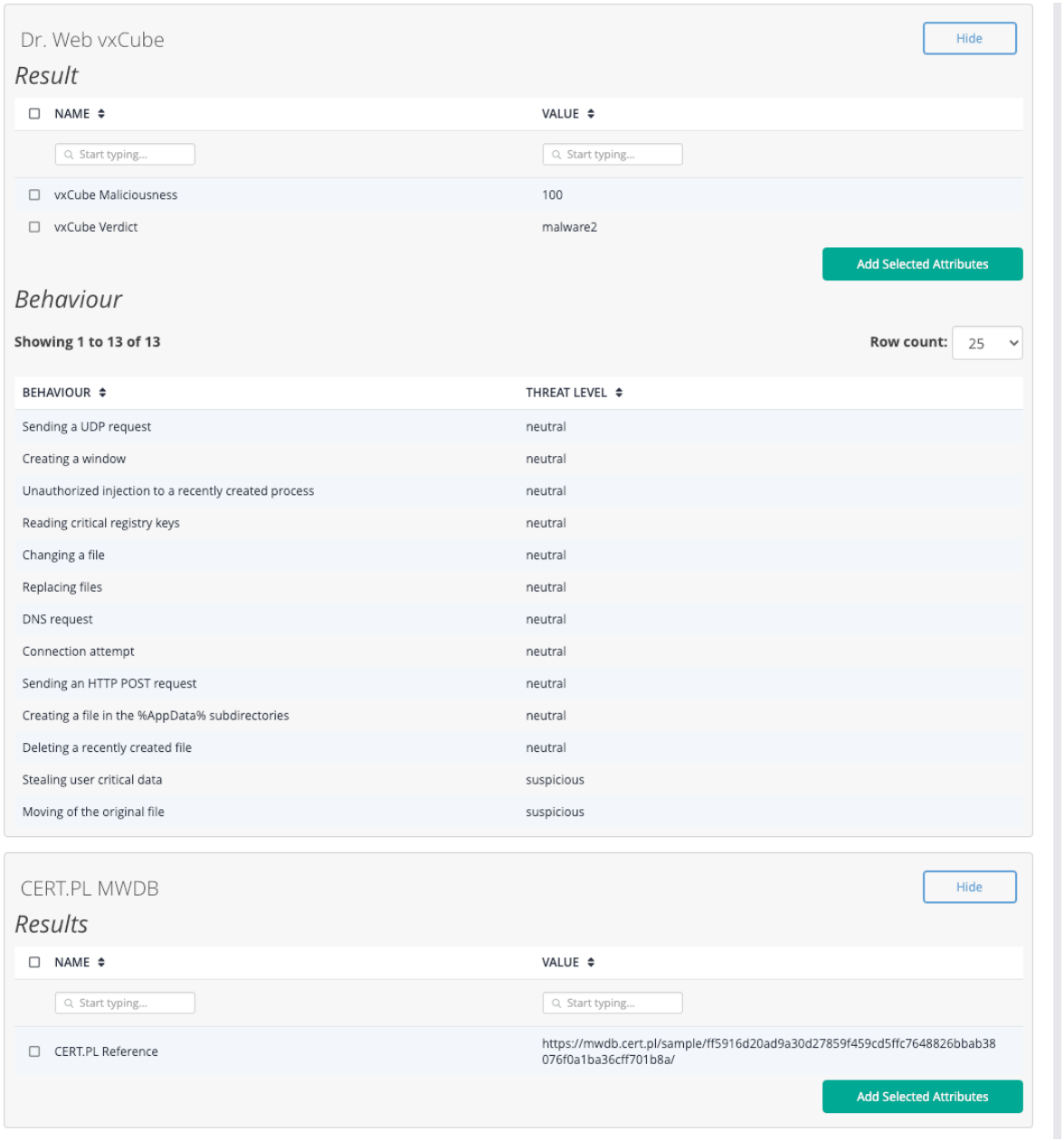
Hide

Detections

NAME	VALUE
ClamAV Detection	PUA.Win.Adware.Slugin-6803969-0
ClamAV Detection	PUA.Win.Adware.Slugin-6840354-0

Add Selected Attributes

Example 2 Response



Dr. Web vxCube

Hide

Result

NAME	VALUE
Start typing...	Start typing...
vxCube Maliciousness	100
vxCube Verdict	malware2

Add Selected Attributes

Behaviour

Showing 1 to 13 of 13 **Row count:** 25

BEHAVIOUR	THREAT LEVEL
Sending a UDP request	neutral
Creating a window	neutral
Unauthorized injection to a recently created process	neutral
Reading critical registry keys	neutral
Changing a file	neutral
Replacing files	neutral
DNS request	neutral
Connection attempt	neutral
Sending an HTTP POST request	neutral
Creating a file in the %AppData% subdirectories	neutral
Deleting a recently created file	neutral
Stealing user critical data	suspicious
Moving of the original file	suspicious

CERT.PL MWDB

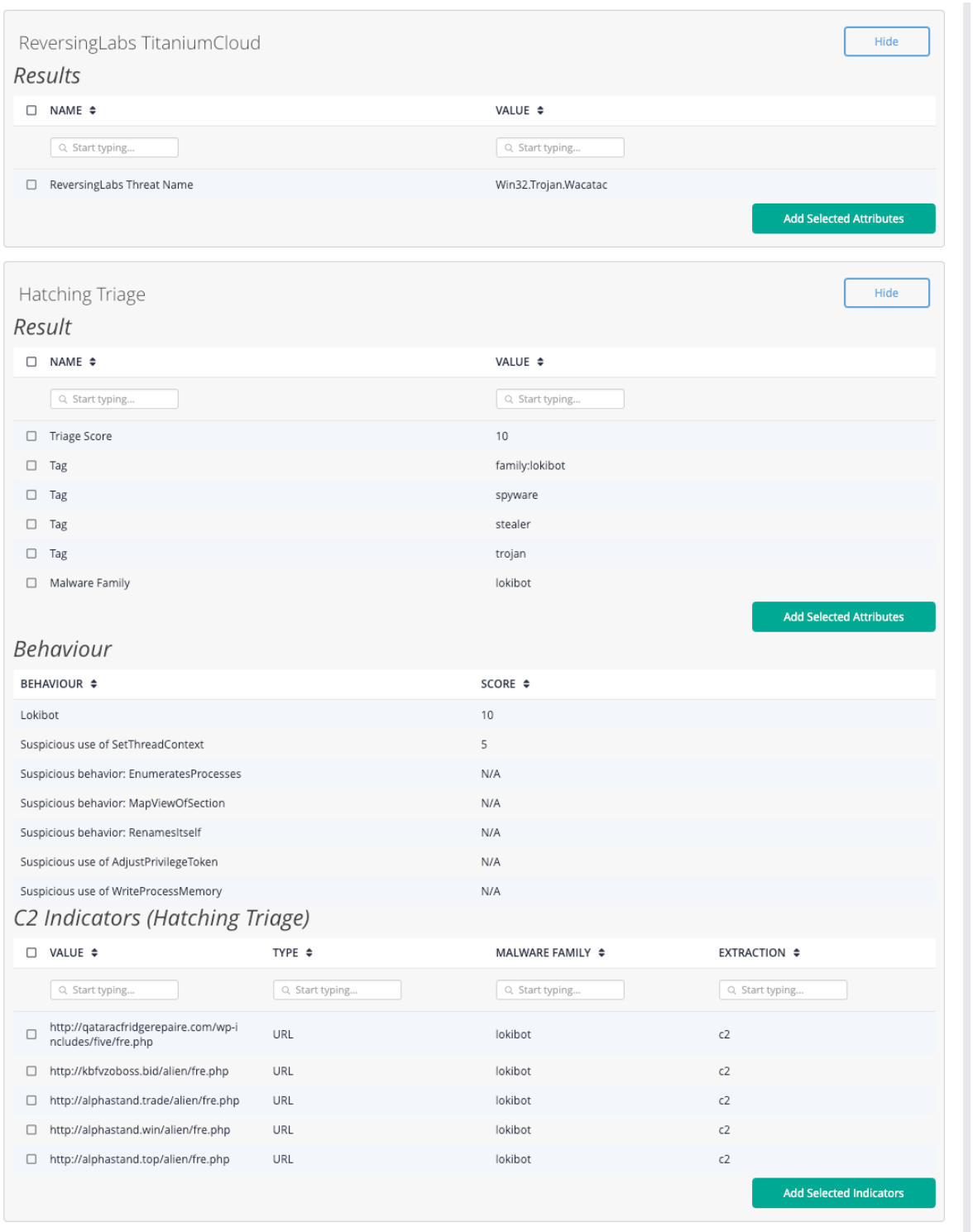
Hide

Results

NAME	VALUE
Start typing...	Start typing...
CERT.PL Reference	https://mwdb.cert.pl/sample/ff5916d20ad9a30d27859f459cd5ffc7648826bbab38076f0a1ba36cff701b8a/

Add Selected Attributes

Example 3 Response



ReversingLabs TitaniumCloud

Hide

Results

NAME	VALUE
Start typing...	Start typing...
ReversingLabs Threat Name	Win32.Trojan.Wacatac

Add Selected Attributes

Hatching Triage

Hide

Result

NAME	VALUE
Start typing...	Start typing...
Triage Score	10
Tag	family:lokibot
Tag	spyware
Tag	stealer
Tag	trojan
Malware Family	lokibot

Add Selected Attributes

Behaviour

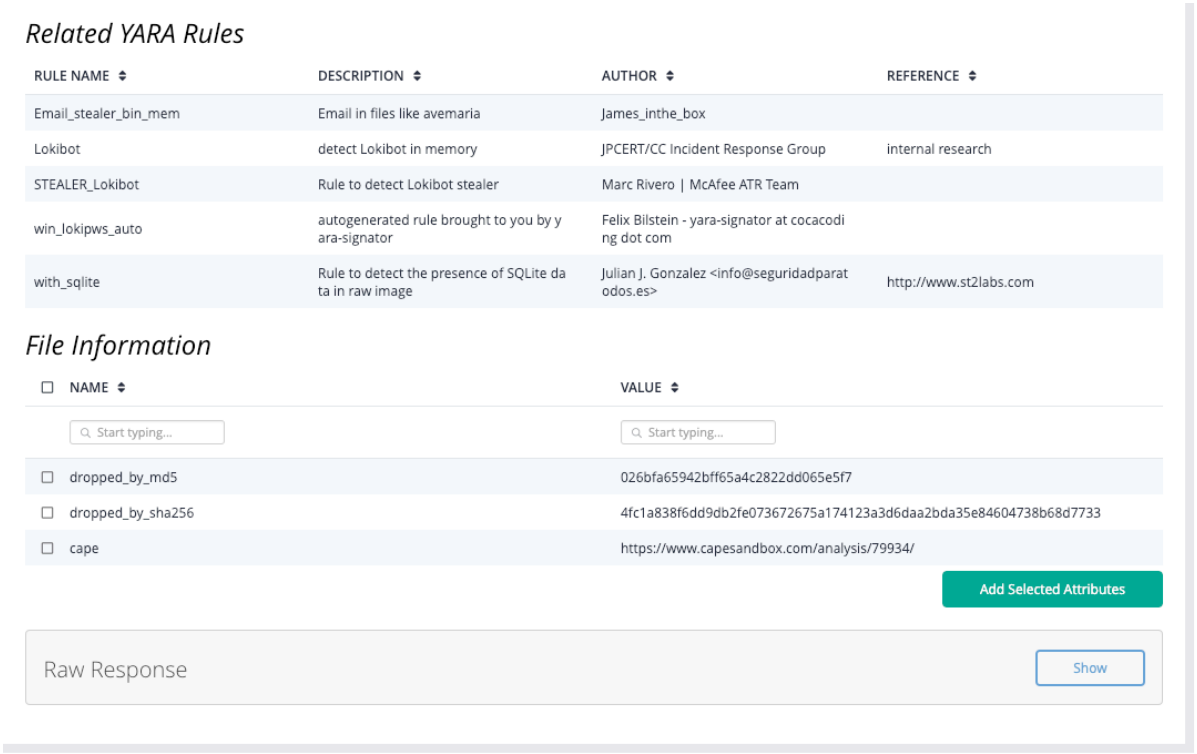
BEHAVIOUR	SCORE
Lokibot	10
Suspicious use of SetThreadContext	5
Suspicious behavior: EnumeratesProcesses	N/A
Suspicious behavior: MapViewOfSection	N/A
Suspicious behavior: RenamesItself	N/A
Suspicious use of AdjustPrivilegeToken	N/A
Suspicious use of WriteProcessMemory	N/A

C2 Indicators (Hatching Triage)

VALUE	TYPE	MALWARE FAMILY	EXTRACTION
Start typing...	Start typing...	Start typing...	Start typing...
http://qataracfridgerepaire.com/wp-includes/five/fre.php	URL	lokibot	c2
http://kbfvzoboss.bid/alien/fre.php	URL	lokibot	c2
http://alphastand.trade/alien/fre.php	URL	lokibot	c2
http://alphastand.win/alien/fre.php	URL	lokibot	c2
http://alphastand.top/alien/fre.php	URL	lokibot	c2

Add Selected Indicators

Example 4 Response



Related YARA Rules

RULE NAME	DESCRIPTION	AUTHOR	REFERENCE
Email_stealer_bin_mem	Email in files like avemaria	James_inthe_box	
Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	internal research
STEALER_Lokibot	Rule to detect Lokibot stealer	Marc Rivero | McAfee ATR Team	
win_lokipws_auto	autogenerated rule brought to you by y ara-signator	Felix Bilstein - yara-signator at cocacodi ng dot com	
with_sqlite	Rule to detect the presence of SQLite da ta in raw image	Julian J. Gonzalez <info@seguridadparat odos.es>	http://www.st2labs.com

File Information

NAME	VALUE
Start typing...	Start typing...
dropped_by_md5	026bfa65942bff65a4c2822dd065e5f7
dropped_by_sha256	4fc1a838f6dd9db2fe073672675a174123a3d6daa2bda35e84604738b68d7733
cape	https://www.capesandbox.com/analysis/79934/

Add Selected Attributes

Raw Response Show

Change Log

- **Version 1.0.0**
  - Initial release