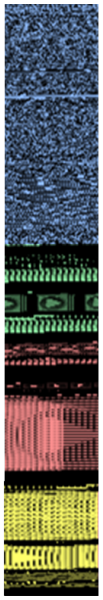
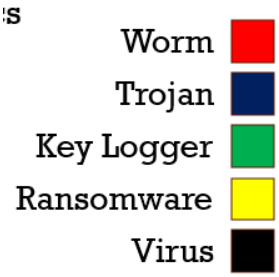
Malware Analysis Report

Code Block Analysis





- Data

- Attributes

Type_description: ZIP

Tlsh:

T102C31238D216B46E875A0F5DC1E5B3420DE900AC078A0CF9F7EDA36E5F66A74EE5200D

Vhash: 477a631d33ec2781cfd5f4da05cb9856

- Type_tags

- compressed

- zip

- Names

- 000.zip

- Unconfirmed 166374.crdownload

- 000 (4).zip

Malware Analysis Report

- 000 (1).zip

- output.183430341.txt

Last_modification_date: 1706416928

Type_tag: zip

Times_submitted: 84

- Total_votes

Harmless: 0

Malicious: 10

Size: 122655

Type_extension: zip

Last_submission_date: 1706410032

- Last_analysis_results

- Bkav

Category: undetected

Engine_name: Bkav

Engine_version: 2.0.0.1

Result: None

Method: blacklist

Engine_update: 20240127

- Lionic

Category: undetected

Engine_name: Lionic

Engine_version: 7.5

Result: None

Method: blacklist

Engine_update: 20240128

- Elastic

Category: type-unsupported

Engine_name: Elastic

Engine_version: 4.0.125

Result: None

Method: blacklist

Engine_update: 20240115

- Microworld-escan

Category: undetected

Engine_name: MicroWorld-eScan

Engine_version: 14.0.409.0

Result: None

Method: blacklist

Engine_update: 20240128

- Cmc

Category: undetected

Engine_name: CMC

Engine_version: 2.4.2022.1

Result: None

Method: blacklist

Engine_update: 20240125

- Cat-quickheal

Category: undetected

Engine_name: CAT-QuickHeal

Engine_version: 22.00

Result: None

Method: blacklist

Engine_update: 20240127

- Skyhigh

Category: undetected

Engine_name: Skyhigh

Engine_version: v2021.2.0+4045

Result: None

Method: blacklist

Engine_update: 20240127

- Alyac

Category: undetected

Engine_name: ALYac

Engine_version: 2.0.0.8

Result: None

Method: blacklist

Engine_update: 20240128

- Malwarebytes

Category: undetected

Engine_name: Malwarebytes

Engine_version: 4.5.5.54

Result: None

Method: blacklist

Engine_update: 20240127

- Vipre

Category: undetected

Engine_name: VIPRE

Engine_version: 6.0.0.35

Result: None

Method: blacklist

Engine_update: 20240127

- Sangfor

Category: undetected

Engine_name: Sangfor

Engine_version: 2.23.0.0

Result: None

Method: blacklist

Engine_update: 20240126

- K7antivirus

Category: undetected

Engine_name: K7AntiVirus

Engine_version: 12.138.50875

Result: None

Method: blacklist

Engine_update: 20240128

- Bitdefender

Category: undetected

Engine_name: BitDefender

Engine_version: 7.2

Result: None

Method: blacklist

Engine_update: 20240128

- K7gw

Category: undetected

Engine_name: K7GW

Engine_version: 12.138.50875

Result: None

Method: blacklist

Engine_update: 20240127

- Trustlook

Category: undetected

Engine_name: Trustlook

Engine_version: 1.0

Result: None

Method: blacklist

Engine_update: 20240128

- Bitdefendertheta

Category: undetected

Engine_name: BitDefenderTheta

Engine_version: 7.2.37796.0

Result: None

Method: blacklist

Engine_update: 20240103

- Virit

Category: failure

Engine_name: VirIT

Engine_version: None

Result: None

Method: blacklist

Engine_update: 20240126

- Symantecmobileinsight

Category: type-unsupported

Engine_name: SymantecMobileInsight

Engine_version: 2.0

Result: None

Method: blacklist

Engine_update: 20240103

- Symantec

Category: undetected

Engine_name: Symantec

Engine_version: 1.21.0.0

Result: None

Method: blacklist

Engine_update: 20240127

- Tehtris

Category: type-unsupported

Engine_name: tehtris

Engine_version: v0.1.4-109-g76614fd

Result: None

Method: blacklist

Engine_update: 20240128

- Eset-nod32

Category: undetected

Engine_name: ESET-NOD32

Engine_version: 28642

Result: None

Method: blacklist

Engine_update: 20240127

- Apex

Category: type-unsupported

Engine_name: APEX

Engine_version: 6.493

Result: None

Method: blacklist

Engine_update: 20240125

- Trendmicro-housecall

Category: undetected

Engine_name: TrendMicro-HouseCall

Engine_version: 10.0.0.1040

Result: None

Method: blacklist

Engine_update: 20240128

- Avast

Category: undetected

Engine_name: Avast

Engine_version: 23.9.8494.0

Result: None

Method: blacklist

Engine_update: 20240128

- Clamav

Category: undetected

Engine_name: ClamAV

Engine_version: 1.2.1.0

Result: None

Method: blacklist

Engine_update: 20240127

- Kaspersky

Category: undetected

Engine_name: Kaspersky

Engine_version: 22.0.1.28

Result: None

Method: blacklist

Engine_update: 20240127

- Alibaba

Category: undetected

Engine_name: Alibaba

Engine_version: 0.3.0.5

Result: None

Method: blacklist

Engine_update: 20190527

- Nano-antivirus

Category: undetected

Engine_name: NANO-Antivirus

Engine_version: 1.0.146.25796

Result: None

Method: blacklist

Engine_update: 20240128

- Virobot

Category: undetected

Engine_name: ViRobot

Engine_version: 2014.3.20.0

Result: None

Method: blacklist

Engine_update: 20240127

- Tencent

Category: failure

Engine_name: Tencent

Engine_version: 1.0.0.1

Result: None

Method: blacklist

Engine_update: 20240128

- Sophos

Category: undetected

Engine_name: Sophos

Engine_version: 2.4.3.0

Result: None

Method: blacklist

Engine_update: 20240128

- Baidu

Category: undetected

Engine_name: Baidu

Engine_version: 1.0.0.2

Result: None

Method: blacklist

Engine_update: 20190318

- F-secure

Category: undetected

Engine_name: F-Secure

Engine_version: 18.10.1547.307

Result: None

Method: blacklist

Engine_update: 20240126

- Drweb

Category: undetected

Engine_name: DrWeb

Engine_version: 7.0.61.8090

Result: None

Method: blacklist

Engine_update: 20240128

- Zillya

Category: undetected

Engine_name: Zillya

Engine_version: 2.0.0.5041

Result: None

Method: blacklist

Engine_update: 20240126

- Trendmicro

Category: undetected

Engine_name: TrendMicro

Engine_version: 11.0.0.1006

Result: None

Method: blacklist

Engine_update: 20240127

- Sentinelone

Category: type-unsupported

Engine_name: SentinelOne

Engine_version: 23.4.2.3

Result: None

Method: blacklist

Engine_update: 20231119

- Fireeye

Category: undetected

Engine_name: FireEye

Engine_version: 35.47.0.0

Result: None

Method: blacklist

Engine_update: 20240128

- Emsisoft

Category: undetected

Engine_name: Emsisoft

Engine_version: 2022.6.0.32461

Result: None

Method: blacklist

Engine_update: 20240127

- Paloalto

Category: type-unsupported

Engine_name: Paloalto

Engine_version: 0.9.0.1003

Result: None

Method: blacklist

Engine_update: 20240128

- Gdata

Category: undetected

Engine_name: GData

Engine_version: A:25.37246B:27.34719

Result: None

Method: blacklist

Engine_update: 20240127

- Jiangmin

Category: undetected

Engine_name: Jiangmin

Engine_version: 16.0.100

Result: None

Method: blacklist

Engine_update: 20240127

- Webroot

Category: type-unsupported

Engine_name: Webroot

Engine_version: 1.0.0.403

Result: None

Method: blacklist

Engine_update: 20240128

- Varist

Category: undetected

Engine_name: Varist

Engine_version: 6.5.1.2

Result: None

Method: blacklist

Engine_update: 20240128

- Avira

Category: undetected

Engine_name: Avira

Engine_version: 8.3.3.16

Result: None

Method: blacklist

Engine_update: 20240127

- Max

Category: undetected

Engine_name: MAX

Engine_version: 2023.1.4.1

Result: None

Method: blacklist

Engine_update: 20240128

- Antiy-avl

Category: undetected

Engine_name: Antiy-AVL

Engine_version: 3.0

Result: None

Method: blacklist

Engine_update: 20240127

- Kingsoft

Category: undetected

Engine_name: Kingsoft

Engine_version: None

Result: None

Method: blacklist

Engine_update: 20230906

- Microsoft

Category: undetected

Engine_name: Microsoft

Engine_version: 1.1.23110.2

Result: None

Method: blacklist

Engine_update: 20240128

- Gridinsoft

Category: undetected

Engine_name: Gridinsoft

Engine_version: 1.0.156.174

Result: None

Method: blacklist

Engine_update: 20240127

- Xcitium

Category: undetected

Engine_name: Xcitium

Engine_version: 36384

Result: None

Method: blacklist

Engine_update: 20240127

- Arcabit

Category: undetected

Engine_name: Arcabit

Engine_version: 2022.0.0.18

Result: None

Method: blacklist

Engine_update: 20240127

- Superantispyware

Category: undetected

Engine_name: SUPERAntiSpyware

Engine_version: 5.6.0.1032

Result: None

Method: blacklist

Engine_update: 20240127

- Zonealarm

Category: undetected

Engine_name: ZoneAlarm

Engine_version: 1.0

Result: None

Method: blacklist

Engine_update: 20240128

- Avast-mobile

Category: undetected

Engine_name: Avast-Mobile

Engine_version: 240127-00

Result: None

Method: blacklist

Engine_update: 20240127

- Cynet

Category: undetected

Engine_name: Cynet

Engine_version: 4.0.0.29

Result: None

Method: blacklist

Engine_update: 20240127

- Bitdefenderfalx

Category: type-unsupported

Engine_name: BitDefenderFalx

Engine_version: 2.0.936

Result: None

Method: blacklist

Engine_update: 20240108

- Ahnlab-v3

Category: undetected

Engine_name: AhnLab-V3

Engine_version: 3.25.0.10459

Result: None

Method: blacklist

Engine_update: 20240128

- Acronis

Category: undetected

Engine_name: Acronis

Engine_version: 1.2.0.121

Result: None

Method: blacklist

Engine_update: 20230828

- Mcafee

Category: undetected

Engine_name: McAfee

Engine_version: 6.0.6.653

Result: None

Method: blacklist

Engine_update: 20240127

- Google

Category: undetected

Engine_name: Google

Engine_version: 1706405425

Result: None

Method: blacklist

Engine_update: 20240128

- Tachyon

Category: undetected

Engine_name: TACHYON

Engine_version: 2024-01-28.01

Result: None

Method: blacklist

Engine_update: 20240128

- Deepinstinct

Category: type-unsupported

Engine_name: DeepInstinct

Engine_version: 5.0.0.8

Result: None

Method: blacklist

Engine_update: 20240122

- Vba32

Category: undetected

Engine_name: VBA32

Engine_version: 5.0.0

Result: None

Method: blacklist

Engine_update: 20240126

- Cylance

Category: type-unsupported

Engine_name: Cylance

Engine_version: 2.0.0.0

Result: None

Method: blacklist

Engine_update: 20240103

- Zoner

Category: undetected

Engine_name: Zoner

Engine_version: 2.2.2.0

Result: None

Method: blacklist

Engine_update: 20240128

- Rising

Category: undetected

Engine_name: Rising

Engine_version: 25.0.0.27

Result: None

Method: blacklist

Engine_update: 20240127

- Yandex

Category: undetected

Engine_name: Yandex

Engine_version: 5.5.2.24

Result: None

Method: blacklist

Engine_update: 20240127

- Ikarus

Category: undetected

Engine_name: Ikarus

Engine_version: 6.2.4.0

Result: None

Method: blacklist

Engine_update: 20240127

- Maxsecure

Category: undetected

Engine_name: MaxSecure

Engine_version: 1.0.0.1

Result: None

Method: blacklist

Engine_update: 20240125

- Fortinet

Category: undetected

Engine_name: Fortinet

Engine_version: None

Result: None

Method: blacklist

Engine_update: 20240127

- Avg

Category: undetected

Engine_name: AVG

Engine_version: 23.9.8494.0

Result: None

Method: blacklist

Engine_update: 20240128

- Cybereason

Category: type-unsupported

Engine_name: Cybereason

Engine_version: 1.2.449

Result: None

Method: blacklist

Engine_update: 20231102

- Panda

Category: undetected

Engine_name: Panda

Engine_version: 4.6.4.2

Result: None

Method: blacklist

Engine_update: 20240127

- Crowdstrike

Category: type-unsupported

Engine_name: CrowdStrike

Engine_version: 1.0

Result: None

Method: blacklist

Engine_update: 20231026

- Trid

File_type: ZIP compressed archive

Probability: 80.0

File_type: PrintFox/Pagefox bitmap (640x800)

Probability: 20.0

Sha256: 9d3fe04d88c401178165f7fbdf307ac0fb690cc5fef8b70ee7f380307d4748f8

- Tags

- encrypted

- zip

Last_analysis_date: 1706409518

Unique_sources: 76

First_submission_date: 1558836942

Ssdeep: 3072:QxpL6ECUOVjuZ6HwZ3KMh8N73lLrKG+PE9g4CN33:2961UwjuDZn65nxIE9y33

Malware Analysis Report

- Bundle_info

Highest_datetime: 2016-09-22 06:02:12

Lowest_datetime: 2016-09-22 06:02:12

Num_children: 1

- Extensions

Exe: 1

Type: ZIP

Uncompressed_size: 6983680

Md5: d113bd83e59586dd8f1843bdb9b98ee0

Sha1: 6c203d91d5184dade63dbab8aecbdfaa8a5402ab

Magic: Zip archive data, at least v2.0 to extract, compression method=deflate

- Last_analysis_stats

Harmless: 0

Type-unsupported: 12

Suspicious: 0

Confirmed-timeout: 0

Timeout: 0

Failure: 2

Malicious: 0

Undetected: 61

Meaningful_name: 000.zip

Reputation: -38

Type: file

Id: 9d3fe04d88c401178165f7fbdf307ac0fb690cc5fef8b70ee7f380307d4748f8

- Links

Self:

https://www.virustotal.com/api/v3/files/9d3fe04d88c401178165f7fbdf307ac0fb690cc5fef8b70ee7f380307d4748f8