微步云沙箱

一站式文件分析平台，场景化专业云沙箱

S-230528-543586

样本分析报告

文件名称：main-kill

SHA256：54358628ab92fdb2a1ec8771de7a1774becc7a524b9791c41265aba514749d4b

文件大小：1019 B

文件类型：Bourne-Again shell script, Unicode text, UTF-8 text executable

分析环境：Linux(Ubuntu 17.04 64bit)

微步判定：安全

目录

main-kill

安全

首次提交: 2023/05/28　末次提交: 2023/05/28　末次分析: 2023/05/28 03:37:37

文件大小： 1019 B　文件类型： Bourne-Again shell script, Unicode text, UTF-8 text executable

引擎检出： 0 / 24　分析环境： Linux(Ubuntu 17.04 64bit)

HASH

SHA256: 54358628ab92fdb2a1ec8771de7a1774becc7a524b9791c41265aba514749d4b

MD5: 349cfd13dde22be2548e791891053eab

SHA1: 1c7cc9f0286932c226e2a06e572ef0100798b6d1

行为检测

MITRE ATT&CK™ 矩阵（技术）检测到 **1** 条技术指标。 查看完整结果　Linux(Ubuntu 17.04 64bit)

通用行为（2）　全部展开

系统环境探测	获得用户或组的ID	Linux(Ubuntu 17.04 64bit)
一般行为	访问/etc/ld.so.preload文件	Linux(Ubuntu 17.04 64bit)

多引擎检测

检出率：0 / 24　最近检测时间：2023-05-28 03:37:37

引擎	检出	引擎	检出
微软（MSE）	无检出	ESET	无检出
卡巴斯基（Kaspersky）	无检出	小红伞（Avira）	无检出
IKARUS	无检出	大蜘蛛（Dr.Web）	无检出
Avast	无检出	AVG	无检出
GDATA	无检出	K7	无检出
安天（Antiy）	无检出	江民（JiangMin）	无检出
360（Qihoo 360）	无检出	Baidu	无检出
NANO	无检出	Trustlook	无检出
瑞星（Rising）	无检出	熊猫（Panda）	无检出
Sophos	无检出	ClamAV	无检出
WebShell专杀	无检出	Baidu-China	无检出
MicroAPT	无检出	OneAV	无检出

收起全部

静态分析

基础信息

文件名称	54358628ab92fdb2a1ec8771de7a1774becc7a524b9791c41265aba514749d4b
文件格式	SH
文件类型(Magic)	Bourne-Again shell script, UTF-8 Unicode text executable
文件大小	1019.0B
SHA256	54358628ab92fdb2a1ec8771de7a1774becc7a524b9791c41265aba514749d4b
SHA1	1c7cc9f0286932c226e2a06e572ef0100798b6d1
MD5	349cfd13dde22be2548e791891053eab
CRC32	C308B1EE
SSDEEP	24:YIkDX0GJzxQ5h/m6UvDpkAT5M/OEX6bGNKBQn4E0KyugSoDW65pYXX0udHWY5Nv:FkDX0GFxQ5h/gM/lNKBcWugSeWaQXpBV
TLSH	T11B11EF99B95C4EF2011A852F26877989B6E6110B25228E04F503D1EC093ACB236ABB84
Tags	sh

元数据

ExifTool

FileType	bash script
FileTypeExtension	sh
MIMEType	text/x-bash

TrID

100.0% (.SH)	Linux/UNIX shell script (7000/1)

沙箱动态检测

Linux(Ubuntu 17.04 64bit)

执行流程

进程详情

共分析了1个进程

sh（PID：1529）

sh /tmp2jhwlr/54358628ab92fdb2a1ec8771de7a1774becc7a524b9791c41265aba514749d4b

运行截图

无运行截图

网络行为

指纹	域名	DNS	HTTP	HTTPS	TCP	UDP	SMTP	ICMP	IRC	Hosts	Dead-Hosts
0	0	0	0	0	0	0	0	0	0	0	0

释放文件

无释放文件