

黑貓專業沙箱在地部署版

BSA1050

強化內部檔案分析機制，關鍵程式於內部進行模擬分析

- ◀ 內部沙箱整合多面向情資資料，進行特徵碼鑑識與行為分析與鑑識
- ◀ 支援Windows/Linux環境、常見Windows附檔名與Linux ELF檔案
- ◀ 透過API達成自動上傳與自動產出分析報告

分析報告摘要

分數

這個檔案 極度可疑，評分為 10 / 10 !

摘要 - TWCERT-MAL-20190905103555DymRa.exe

檔案資訊

檔名	TWCERT-MAL-20190905103555DymRa.exe
上傳時間	2019-12-08 21:57:06
Mime Type	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
大小	8.9 MB (8916472 bytes)
YARA	N/A
VirusTotal	23 / 72 (2019-12-06 22:19:08)

Event #997 - MISP

172.23.103.45/events/view/997

Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration Audit

FreeText injection queued for background processing. Attributes will be added to the event as they are being processed.

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Populate from...

Enrich Event

Merge attributes from...

Publish Event

Publish (no email)

Contact Reporter

Download as...

List Events

Add Event

釣魚郵件惡意檔案 IOC 資訊

Event ID 997

UUID c1c492e3-33e9-456e-82b2-868866d7c487

Creator org ORGNAME

Owner org ORGNAME

Email misp@ Add a tag

Tags

Date 2021-06-10

Threat Level High

Analysis Initial

Distribution This community

Info

Published No

#Attributes 1 (0 Object)

First recorded change 2021-06-10 15

Last change 2021-06-10 15

malware_classification:malware-category="Botnet"

C2

Cobalt Strike Beacon

Decoy

DLL Dropper

Doc(x)

Download

Flash

Malicious Hatch Script

Download: GroupPG key

This is an

2021-06-10 16:14:32