區網會議

李墨軒

資安通報

教育機構資安通報平台

- https://info.cert.tanet.edu.tw/prog/index.php
  - 更新聯絡人資訊
  - 定期修改密碼

通報應變

- 通報時間1hr
- 自行通報應變
- 申請DDOS

資安通報排名

連線單位	平均通報處理時間	平均應變處理時間	平均全部處理時間	資安事件數
高中職	05:06:00.5862	00:00:00.0000	05:06:00.5862	116
學院	00:34:52.0000	04:22:07.6667	04:56:59.6667	12
學院	04:54:19.2609	00:00:00.0000	04:54:19.2609	23
高中職	04:08:43.2500	00:00:00.0000	04:08:43.2500	4
大學	02:58:33.0000	00:00:00.0000	02:58:33.0000	28
大學	02:30:53.5455	00:00:07.3273	02:31:00.8728	165
高中職	01:54:52.0000	00:00:00.0000	01:54:52.0000	1
高中職	01:52:05.5000	00:00:00.0000	01:52:05.5000	2
大學	01:49:27.0000	00:00:00.0000	01:49:27.0000	1
專科學校	01:42:04.8333	00:00:00.0000	01:42:04.8333	6
大學	01:37:19.4000	00:00:00.0000	01:37:19.4000	15
高中職	01:28:46.7143	00:00:00.0000	01:28:46.7143	7
高中職	01:24:52.0000	00:00:00.0000	01:24:52.0000	2
大學	01:19:32.7727	00:00:00.0000	01:19:32.7727	22
高中職	01:12:13.0000	00:00:00.0000	01:12:13.0000	2
中心	01:10:55.6667	00:00:00.0000	01:10:55.6667	3
大學	01:06:20.1667	00:00:00.0000	01:06:20.1667	18
大學	01:01:11.2805	00:00:00.0000	01:01:11.2805	82
學院	01:00:39.2857	00:00:00.0000	01:00:39.2857	7

Mo

- 統計時間：2019/01/01 ~ 2019/12/25

資安事件

資安事件分類

- Bot net
  - MALWARE-CNC **Win.**Trojan.Korgapam outbound connection
  - MALWARE-CNC **Unix.**Trojan.Chalubo outbound connection
  - MALWARE-CNC **Andr.**Trojan.Sysch variant outbound connection
  - MALWARE-CNC **Osx.**Trojan.SHLayer variant outbound connection
- 挖礦
  - PUA-OTHER XMRig cryptocurrency mining pool connection attempt
  - PUA-OTHER Cryptocurrency Miner outbound connection attempt
  - PUA-OTHER Bitcoin outbound request attempt

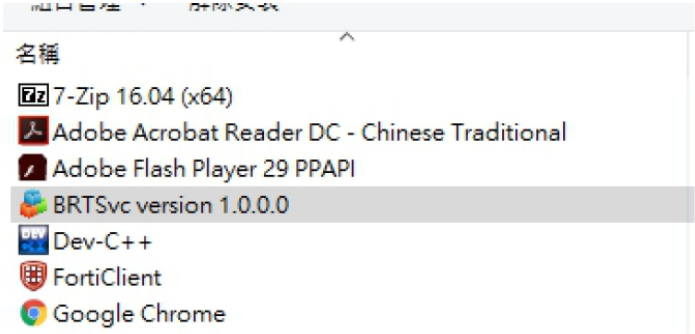
Ohsoft挖礦

- 目標IP
  - 149.28.199.108
- 移除方式

移除挖礦軟體

BRTSvc須單獨移除，此挖礦程式不會隨者主程式移除而移除，使用新增/移除程式也即可順利移除。

移除時建議打開工作管理員關閉相關程式，或是檢查是否被防毒軟體隔離，導致無法移除。



ohsoft 下的軟體(oCam、VirtualDVD、Secret Folder等)在更新或安裝時，也會自動安裝挖礦程式 “BRTSvc ”。請使用者注意。

弱掃平台

https://evs.twisc.ncku.edu.tw/

弱掃平台

- 各校有一組帳密
- 可自行申請掃描

年份	單位	狀態	單位數	網站數	檢測數	總執行時間	平均費時_分鐘	高風險網站數	中風險網站數	低風險網站數
2019	臺北I區域網路中心	執行失敗	11	33	39	10天5小時59分16秒	378	20	17	1
2019	臺北I區域網路中心	執行完成	16	141	227	7天0小時24分35秒	45	62	113	29

END