Wykrywanie incydentów - lab 10

Zadanie 1

Korzystając z komend skryptu `ja3`

```
ja3 c2_1.pcap | grep digest | sort | uniq
ja3 c2_2.pcap | grep digest | sort | uniq
```

otrzymano hashe

```
"ja3_digest": "28a2c9bd18a11de089ef85a160da29e4",
"ja3_digest": "37f463bf4616ecd445d4a1937da06e19",
"ja3_digest": "51c64c77e60f3980eea90869b68c58a8",
"ja3_digest": "57f3642b4e37e28f5cbe3020c9331b4c",
"ja3_digest": "6271f898ce5be7dd52b0fc260d0662b3",
"ja3_digest": "7dd50e112cd23734a310b90f6f44a7cd",
"ja3_digest": "9e10692f1b7f78228b2d4e424db3a98c",
"ja3_digest": "a0e9f5d64349fb13191bc781f81f42e1",
"ja3_digest": "df669e7ea913f1ac0c0cce9a201a2ec1",

"ja3_digest": "0ffee3ba8e615ad22535e7f771690a28",
"ja3_digest": "1a5fe5677b0e4fbbc854e8908225637d",
"ja3_digest": "1d095e68489d3c535297cd8dffb06cb9",
"ja3_digest": "66918128f1b9b03303d77c6f2eefd128",
"ja3_digest": "6734f37431670b3ab4292b8f60f29984",
"ja3_digest": "fed8d14fc5a67b40cd470ba239019785",
```

Wyszukiwanie hashy we formularzu wykazało ruch malware z rodziny trojanów bankowych - `Dridex`, `Gozi`, `QakBot` oraz `Trickbot`. Zidentityfikowany został także malware `sdsdsdsd.exe`, który tworzy połączenie P2P i przechwytuje adresy URL dodatkowych plików, które następnie są pobierane.

Zadanie 2

Implant 1

Organizacja: Patron Technology Persia Ltd
C2: HTTPS @ 194[.]147[.]142[.]163:443

C2 Server: 194[.]147[.]142[.]163/pixel[.]gif
POST URI: /submit[.]php
Lokalizacja: Holandia
ASN: SERVERIUS-AS
ISP: Serverius

Implant 2

Organizacja: Guidepoint
C2: HTTPS @ 104[.]37[.]104[.]44:443
C2 Server: 104[.]37[.]104[.]44/ptj
POST URI: /submit[.]php
Lokalizacja: USA
ASN: NSIHOSTING-EQX-VA
ISP: NSI Hosting