2015-08-31

TRAFFIC ANALYSIS EXERCISE

WHAT'S THE EK? – WHAT'S THE PAYLOAD? 분석

20203371

김도연

SCENARIO

-pcap을 검사하여 감염 키드(EK), 페이로드 및 감염된 웹 사이트를 확인합니다.

QUESTIONS

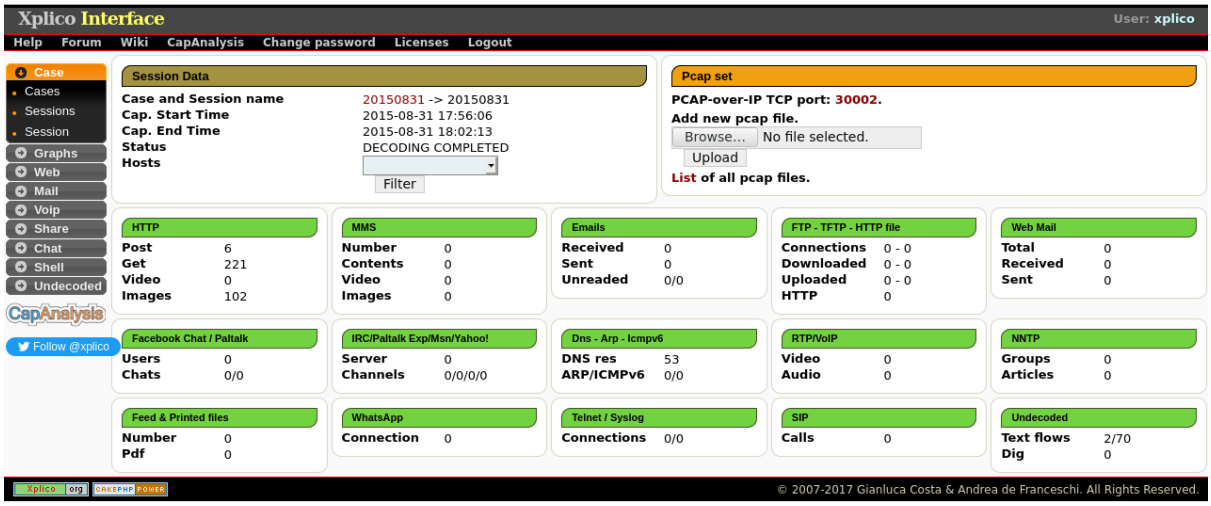
-전체 사건 보고서에는 다음 내용을 포함해야 합니다.

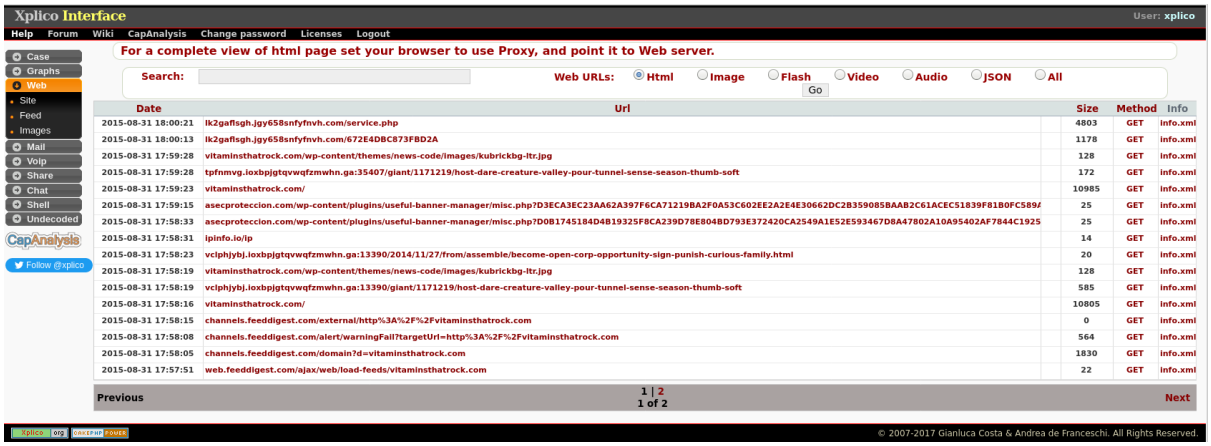
- 감염된 Windows 컴퓨터의 IP 주소
- 감염된 Windows 컴퓨터의 MAC 주소
- 감염된 Windows 컴퓨터의 호스트 이름
- 악용 도구 키트의 이름
- 페이로드 식별 (예 : Bedep, CryptoWall 3.0, Dyre, Rovnix, Vawtrak 등)
- 이 감염 체인을 시작한 감염된 웹 사이트의 식별
- IP 주소 및 도메인 이름을 포함하는 트래픽의 모든 손상 표시기

분석 도구

-Wireshark, Xplico, NetworkMiner, IDS 장비(Sguil)

[Xplico 분석 결과]

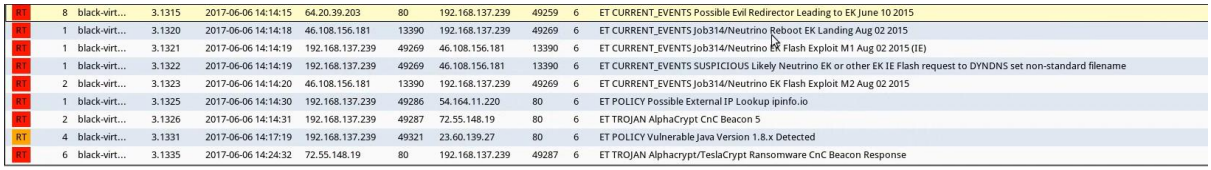




[sguil로 분석한 결과]

terminal에서 명령어 입력 해주어야 분석 시작할 수 있음.

명령어 -> **tcpreplay –인터페이스=인터페이스명 pcap 샘플 이름**



RT	8	black-virt...	3.1315	2017-06-06 14:14:15	64.20.39.203	80	192.168.137.239	49259	6	ET CURRENT_EVENTS Possible Evil Redirector Leading to EK June 10 2015
RT	1	black-virt...	3.1320	2017-06-06 14:14:18	46.108.156.181	13390	192.168.137.239	49269	6	ET CURRENT_EVENTS Job314/Neutrino Reboot EK Landing Aug 02 2015
RT	1	black-virt...	3.1321	2017-06-06 14:14:19	192.168.137.239	49269	46.108.156.181	13390	6	ET CURRENT_EVENTS Job314/Neutrino EK Flash Exploit M1 Aug 02 2015 (IE)
RT	1	black-virt...	3.1322	2017-06-06 14:14:19	192.168.137.239	49269	46.108.156.181	13390	6	ET CURRENT_EVENTS SUSPICIOUS Likely Neutrino EK or other EK IE Flash request to DYNDNS set non-standard filename
RT	2	black-virt...	3.1323	2017-06-06 14:14:20	46.108.156.181	13390	192.168.137.239	49269	6	ET CURRENT_EVENTS Job314/Neutrino EK Flash Exploit M2 Aug 02 2015
RT	1	black-virt...	3.1325	2017-06-06 14:14:30	192.168.137.239	49286	54.164.11.220	80	6	ET POLICY Possible External IP Lookup ipinfo.io
RT	2	black-virt...	3.1326	2017-06-06 14:14:31	192.168.137.239	49287	72.55.148.19	80	6	ET TROJAN AlphaCrypt CnC Beacon 5
RT	4	black-virt...	3.1331	2017-06-06 14:17:19	192.168.137.239	49321	23.60.139.27	80	6	ET POLICY Vulnerable Java Version 1.8.x Detected
RT	6	black-virt...	3.1335	2017-06-06 14:24:32	72.55.148.19	80	192.168.137.239	49287	6	ET TROJAN Alphacrypt/TeslaCrypt Ransomware CnC Beacon Response

ET CURRENT_EVENTS Possible Evil Redirector Leading to EK June 10 2015

> EK로 이끄는 악성 Redirection이 존재한다.

ET TROJAN AlphaCrypt CnC Beacon 5

- AlphaCrypt CnC는 랜섬웨어 CnC 서버로 판명되는 것이 존재한다고 판단.

CnC서버 : command 서버로, 해커가 어떤 서버를 만들어 놓고 자신이 퍼트린 악성코드와 통신하는 서버를 말함

ET TROJAN Alphacrypth/TeslaCrypt Ransomware CnC Beacon Response

- 악성코드가 Response 했다는 것을 의미

[알아낸 결과]

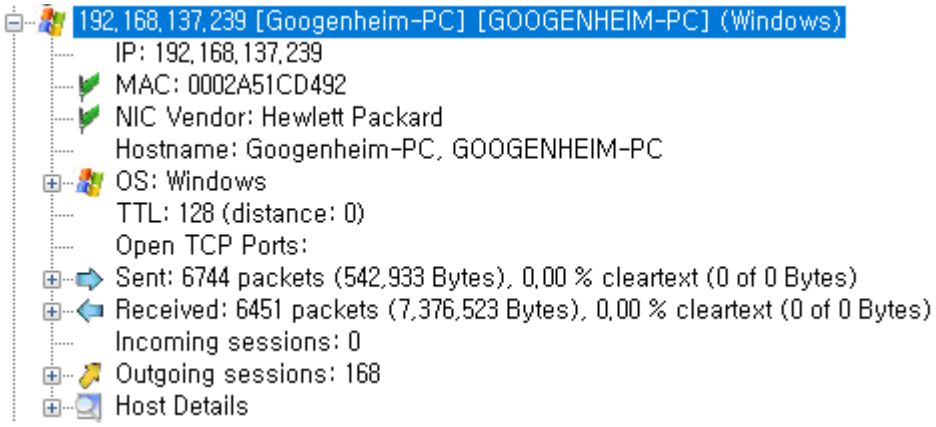
Client IP : 192.168.137.239

Site : 64.20.39.203

Redirection : 46.108.156.181

CnC IP : 72.55.148.19

[NetworkMiner를 통한 분석 결과]



처음 시작된 IP 주소인 64.20.39.203로 networkminer로 접속해 살펴본 결과, **vitaminsthatrock.com** 에서부터 시작되었다는 것을 알게 됨.

- **Xplico**에서 **vitaminsthatrock.com** 사이트를 접속해봄.

[실제 페이지]

URL: http://vitaminsthatrock.com/

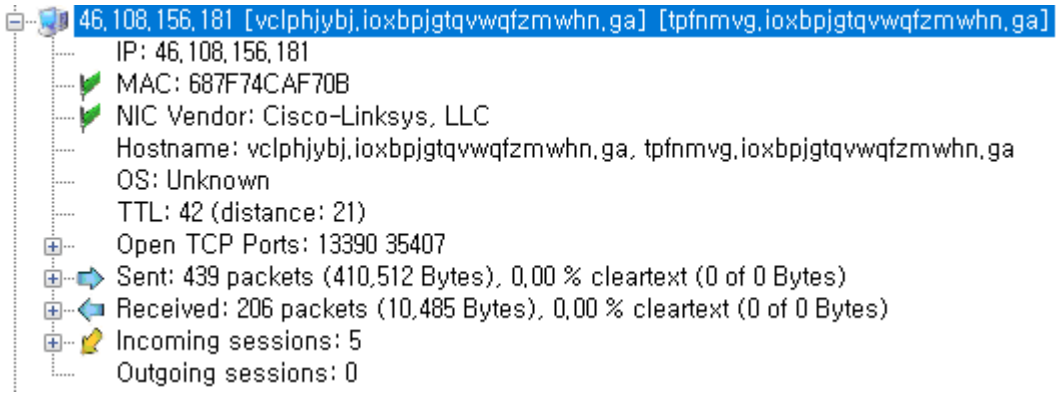
HTTP Request	HTTP Responce
ip:port => 192.168.137.239:49259	**ip:port => 64.20.39.203:80**
Header: Click to **View** or Download	Header: Click to **View** or Download
Body: None	Body: Click to **View** or Download (sz:10805b) content type:text/html

Xplico에서 **vitaminsthatrock.com** 의 **HTTP Response**를 확인해봄.

응답 헤더를 확인

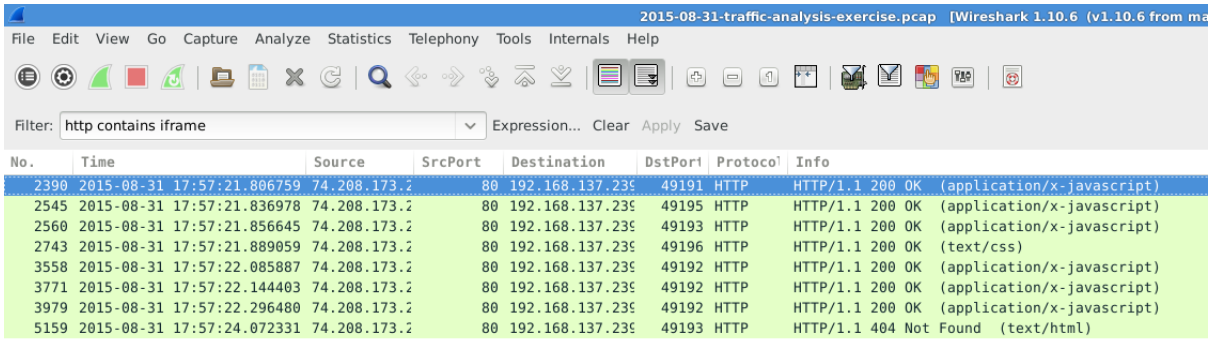
```
HTTP/1.1 200 OK
X-Powered-By: PHP/5.4.44
X-Pingback: http://vitaminsthatrock.com/xmlrpc.php
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding: gzip
Vary: Accept-Encoding
Date: Mon, 31 Aug 2015 17:58:19 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Connection: close
```

처음 Redirection 이라고 생각했던 IP 주소인 46.108.156.181을 networkminer와 html 소스로 확인 시도

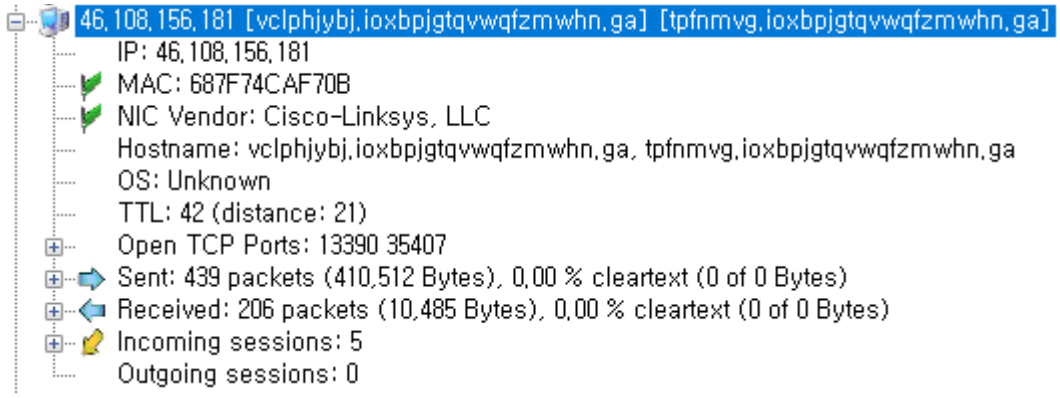


**vclphjybj.ioxbpjgtqvwqfzmwhn.ga:13390/giant/1171219/host-dare-creature-valley-pour-tunnel-sense-season-thumb-soft" width="250" height="250"></iframe> **

위와 같은 코드를 찾아냈음 -> iframe / wireshark의 display 기능을 통해 살펴보았음



- IP 주소 및 도메인 이름을 포함하는 트래픽의 모든 손상 표시기



[분석을 위한 전체적인 흐름]

- Wireshark, Xplico, Sguil 로 먼저 분석을 실시한 후 특이점이 있는 IP 주소 확인
- NetworkMiner에서 해당 IP 주소를 따라 정보를 확인
- Xplico와 WrieShark의 display 기능을 이용해 자료를 검토

가장 마지막으로 접속한 페이지를 들어갔을 때를 확인해보면 나오는 **협박성 글**

[최종 결과]

감염된 Windows 컴퓨터의 IP 주소	192.168.137.239
감염된 Windows 컴퓨터의 MAC 주소	00:02:A5:1C:D4:92
감염된 Windows 컴퓨터의 호스트 이름	Googenheim-PC
악용 도구 키트의 이름	Neutrino
페이로드 식별 (예 : Bedep, CryptoWall 3.0, Dyre, Rovnix, Vawtrak 등)	Alphacrypt
이 감염 체인을 시작한 감염된 웹 사이트의 식별	vitaminsthatrock.com
IP 주소 및 도메인 이름을 포함하는 트래픽의 모든 손상 표시기	46.108.156.181 [vclphjybj.ioxbpjgtqvwqfzmwhn.ga] [tpfnmvg.ioxbpjgtqvwqfzmwhn.ga] IP: 46.108.156.181 MAC: 687F74CAF70B NIC Vendor: Cisco-Linksys, LLC Hostname: vclphjybj.ioxbpjgtqvwqfzmwhn.ga, tpfnmvg.ioxbpjgtqvwqfzmwhn.ga OS: Unknown TTL: 42 (distance: 21) Open TCP Ports: 13390 35407 Sent: 439 packets (410,512 Bytes), 0,00 % cleartext (0 of 0 Bytes) Received: 206 packets (10,485 Bytes), 0,00 % cleartext (0 of 0 Bytes) Incoming sessions: 5 Outgoing sessions: 0