**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)

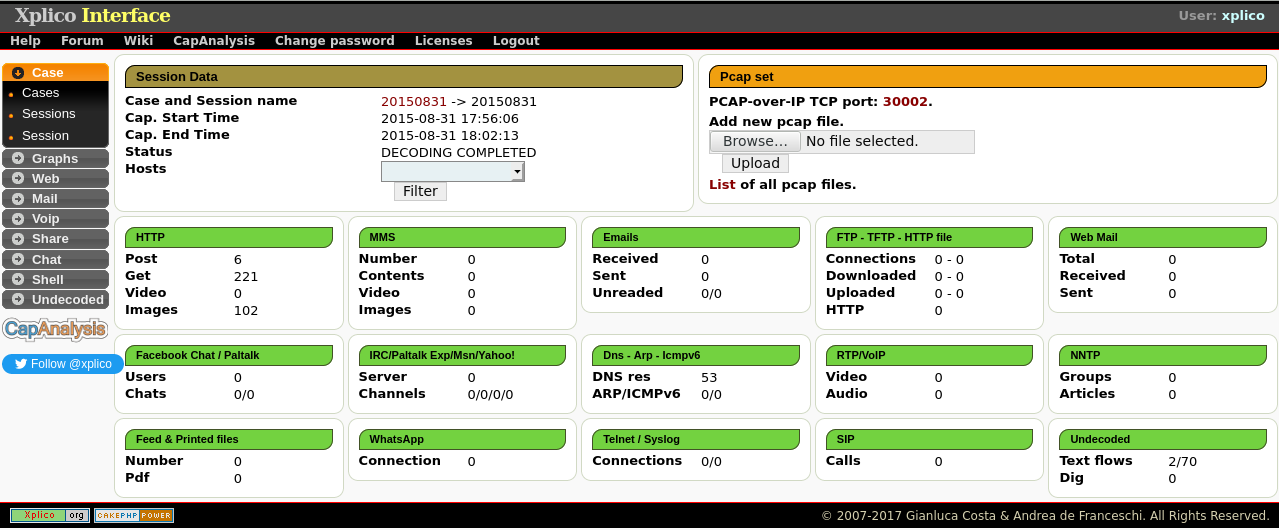
- 이 감염 체인을 시작한 감염된 웹 사이트의 식별

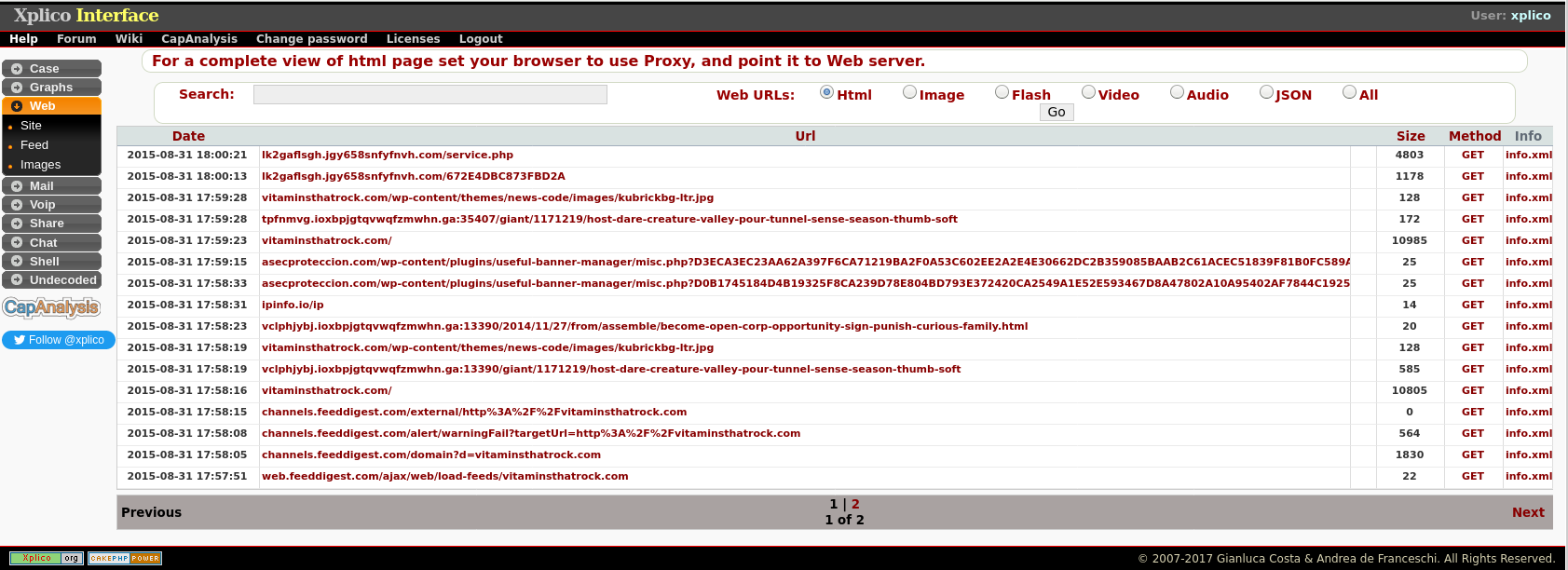
- IP 주소 및 도메인 이름을 포함하는 트래픽의 모든 손상 표시기

**분석 도구**

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

**[Xplico 분석 결과]**

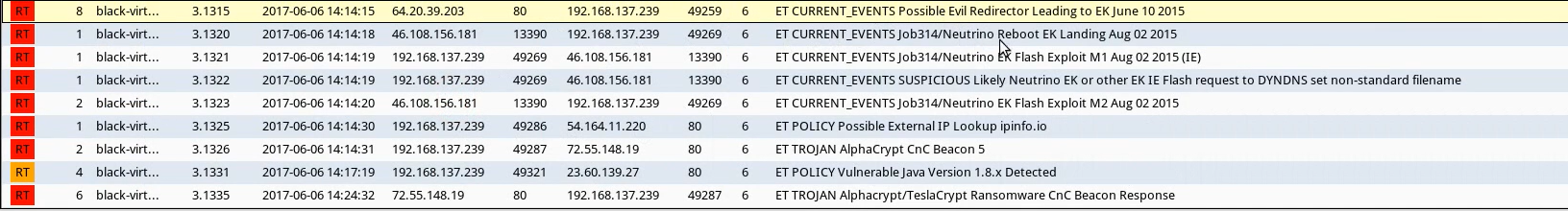




**[sguil로 분석한 결과]**

**terminal**에서 명령어 입력 해주어야 분석 시작할 수 있음.

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



**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]**

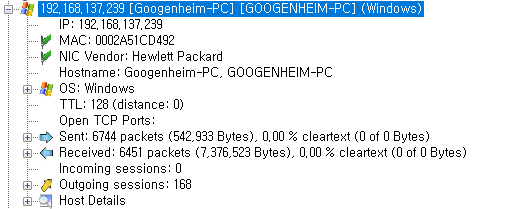
Client IP : 192.168.137.239

Site : 64.20.39.203

Redirection : 46.108.156.181

CnC IP : 72.55.148.19

**[NetworkMiner를 통한 분석 결과]**

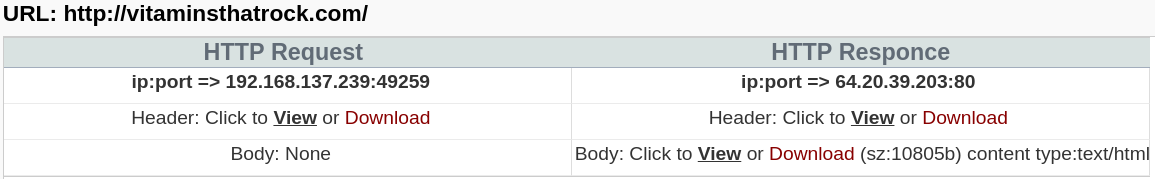


**처음 시작된 IP 주소**인64.20.39.203로 networkminer로 접속해 살펴본 결과, **vitaminsthatrock.com** 에서부터 시작되었다는 것을 알게 됨.

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

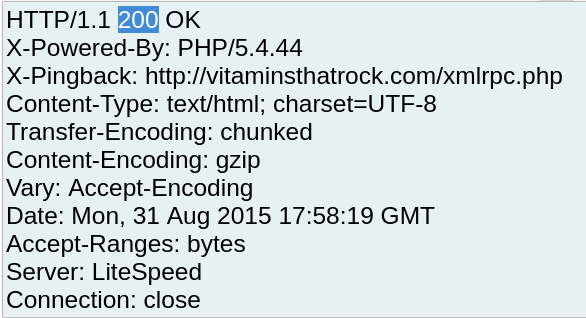


**[실제 페이지]**

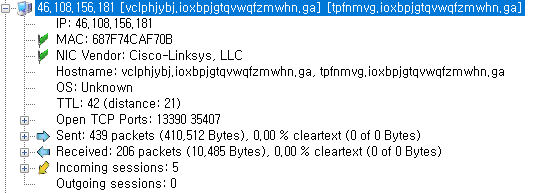


Xplico에서 **vitaminsthatrock.com** 의 **HTTP Response**를 확인해봄.

응답 헤더를 확인



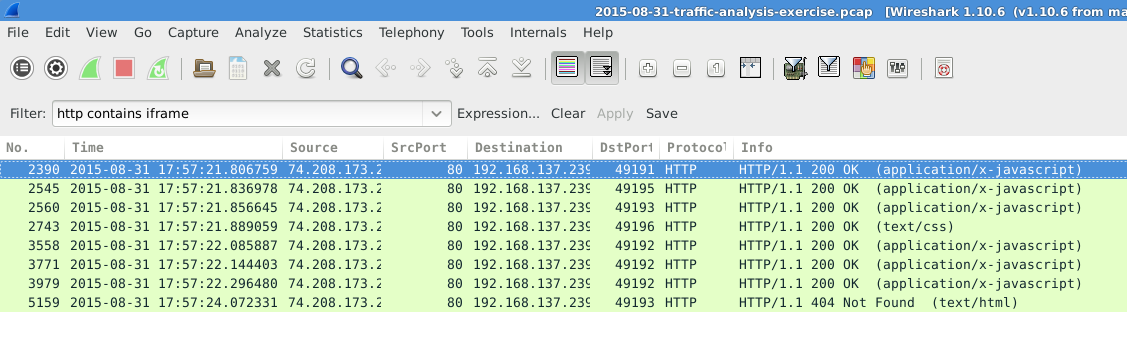
처음 Redirection 이라고 생각했던 IP 주소인 46.108.156.181을 networkminer와 html 소스로 확인 시도



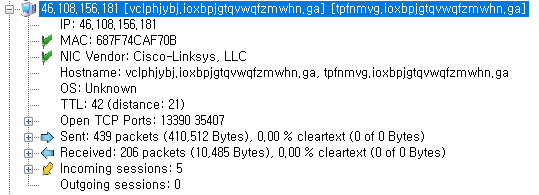


**vclphjybj.ioxbpjgtqvwqfzmwhn.ga:13390/giant/1171219/host-dare-creature-valley-pour-tunnel-sense-season-thumb-soft" width="250" height="250"></iframe></div>**

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



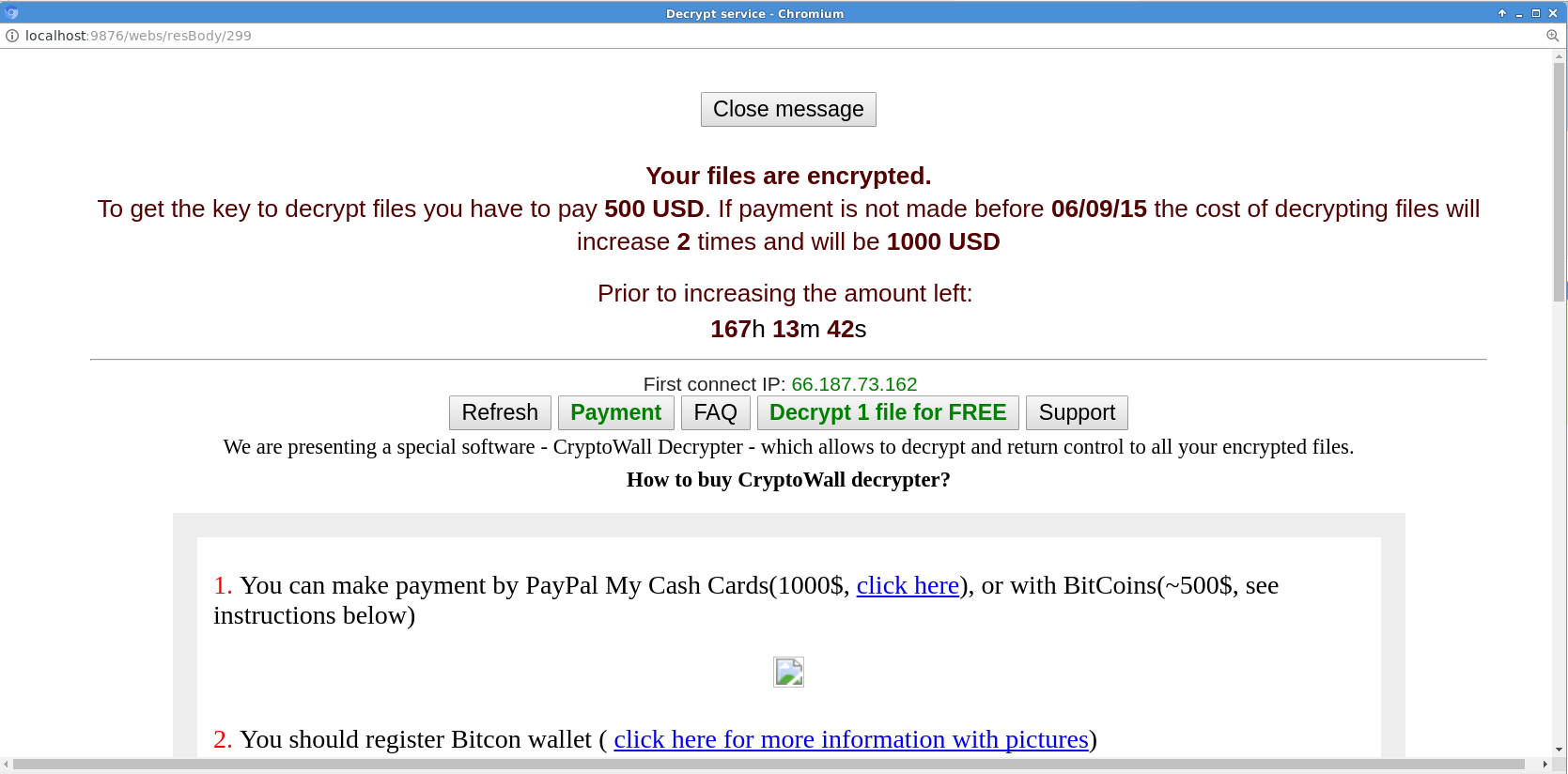
**- IP 주소 및 도메인 이름을 포함하는 트래픽의 모든 손상 표시기**



**[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** |  |