Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

Zaštita računarskih sistema i mreža

- Nulta laboratorijska vežba -

0. Izviđanje

0.1 DNS izviđanje

Korišćenjem google dig alata (https://toolbox.googleapps.com/apps/dig/) prikupiti sledeće informacije o firmi Cisco (domen cisco.com):

1) simbolička imena i IP adrese web servera: _____
2) simboličke i IP adrese mejl servera: _____
3) simboličke i IP adrese DNS servera: _____

Na osnovu IP adrese web servera, da li Cisco sam hostuje svoj web server?_____
Na osnovu IP adresa mejl servera, da li Cisco sam hostuje svoj mejl server?_____

Za proveru IP adresa, koristiti whois alate regionalnih internet registara:

- ARIN: https://search.arin.net/
- RIPE: https://www.ripe.net/
- APNIC: https://wq.apnic.net/static/search.html
- LACNIC: https://query.milacnic.lacnic.net/home

0.2 Izviđanje autonomnih sistema

Otići na sajt RIPE: www.ripe.net i u gornjem desnom uglu videti svoju IP adresu. Ukucati tu IP adresu u polje iznad i videti kod kog provajdera je registrovana. Zabeležiti broj autonomnog sistema provajdera.

Otići na sajt za RIPE statistiku (https://stat.ripe.net/about/) i onda kliknuti na “Go to the old UI”. Kada se otvori strana, uneti broj autonomnog sistema provajdera i pogledati ispis.

Kliknuti na karticu “Routing” i pogledati prozor Announced prefixes. Koje adrese pripadaju ovom provajderu?

Kliknuti na karticu “Database” i pogledati prozor “Historical Whois”. Da li ima nekih objekata kojima su definisana imena administratora provajdera? Kliknuti na te objekte i videti koje informacije su raspoložive.

0.3 Izviđanje email zaglavlja

Uz ovaj deo vežbe su data tri primera spam/phishing mejla od kojih su prva dva uverljiviji od preostalih, iako su sva četiri mejla prošla spam proveru na mejl serveru. Dat je kompletan izvorni oblik mejla koji sadrži zaglavlje, tekst mejla i atačmente (slike i zip fajlove):

1) Lažni mejl od Kancelarije za IT Republike Srbije
2) Lažni mejl od Banke Intesa
3) Lažna dostava pošiljke
4) Lažni mejl od "direktora policije"

Napomena: Iz ovih fajlova je moguće izvući kompletne atačmente u izvornom obliku (poglavlje 0.4). zip atačmenti u primerima 1) i 2) sadrže malver koji je žrtva trebalo da instalira na svoj računar otvaranjem atačmenta. Ko želi, može da ih izvuče iz mejla, ali pažljivo, da ih slučajno ne otvori na svom računaru i tako ga zarazi. Atačment kada se izvuče može da se proveri na nekom od dobro poznatih sajtova za proveru malvera kao što je Virustotal: https://www.virustotal.com

1) Sajt: https://www.ip2location.com/free/email-tracer
   U polje Email header kopirati i nalepiti heder i kliknuti na Lookup.
   - Odrediti preko kojih računara/servera su stigli mejlovi.
   - Da li adrese računara sa kojih je poslat mejl odgovaraju onom pošiljaocu mejla za koji se pretpostavlja da je poslao na osnovu adrese pošiljaoca u mejlu?
2) Sajt: https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx
   U polje kopirati i nalepiti heder i kliknuti na Analyze header.
   - Da li je zaglavlje regularno ili ima greške?
   - Koje se greške prijavljuju?

0.4 Dodatak - preuzimanje atačmenta

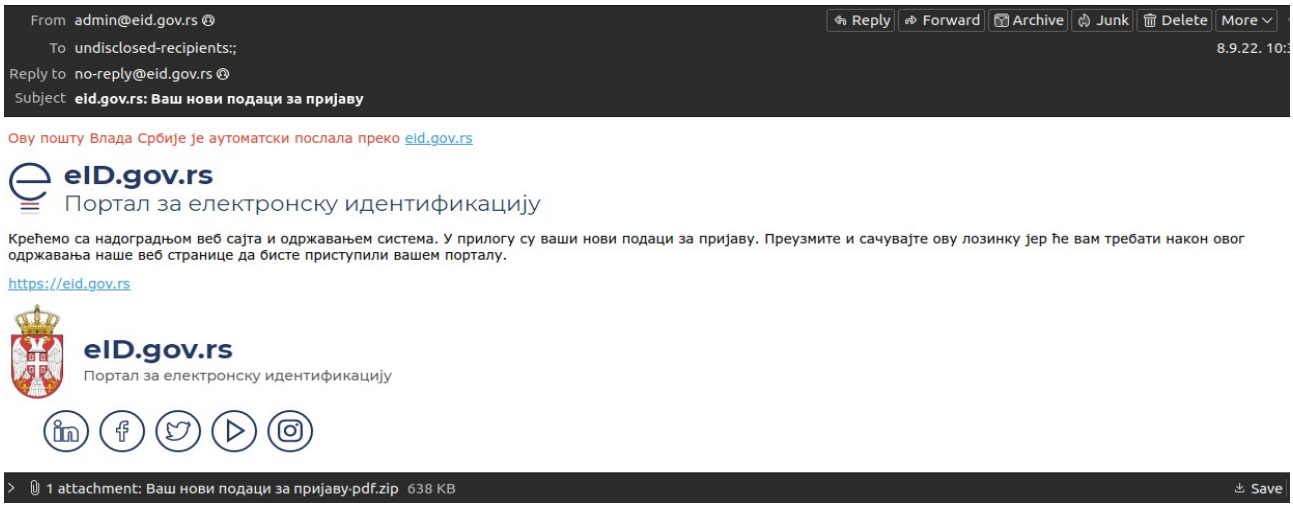
Prvi atačmentu u mejlu 1) je opisan u delu mejla koji počinje sa:
--=_da9b059f32e50aee25f35b0a124186b0

U opisu atačmenta se vidi da je atačment enkodovan pomoću Base64 i da je tipa PNG (slika), a vidi se ime fajla i njegova veličina. Selektovati atačment koji počinje sa: "iVBORw0K…" i završava se sa: "...DohVEAAAAAElFTkSuQmCC". Kraj atačmenta je označen istom oznakom kao i početak:
--=_da9b059f32e50aee25f35b0a124186b0

Selektovani atačment kopirati na sajt CyberChef u polje Input:
https://gchq.github.io/CyberChef/
Iz dela Operations prevući "From Base64" u polje Recipe. U polju Output će se pojaviti dekodovani atačment. U desnom gornjem uglu kliknuti na ikonu diskete i snimiti fajl sa ekstenzijom .png. Otvoriti fajl.

Izgled fišing mejlova u klijentskoj aplikaciji:

1)



2)