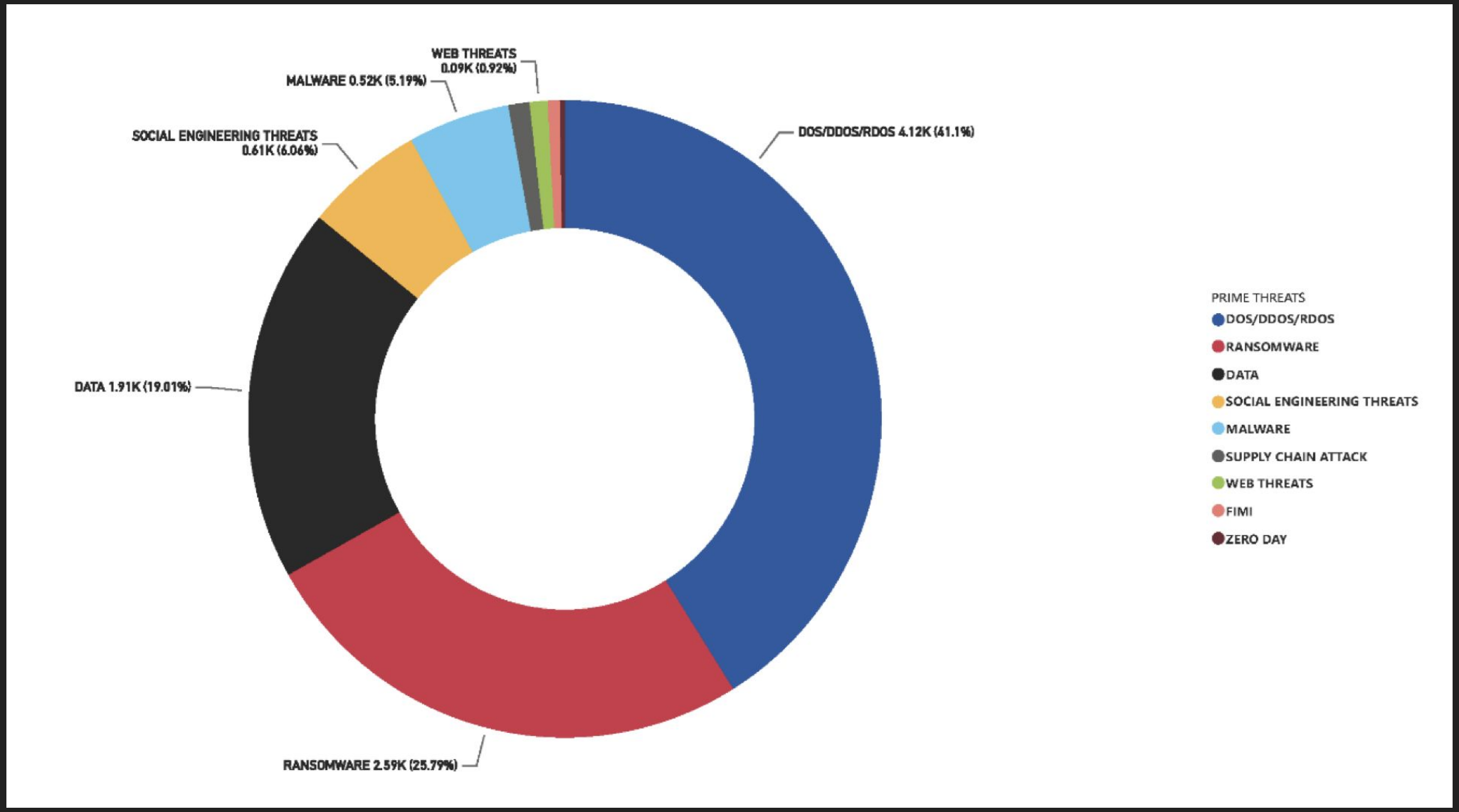
Social Engineering

Ljudska strana bezbednosti :)

Najčešći tipovi *identifikovanih* napada



Šta bi bio socijalni inženjering?

- Cilj: Dobiti pristup informacijama ili servisima
- Kako: Iskorištavajući ljudske greške ili ljudsko ponašanje

Obuhvata širok spektar aktivnosti koje pokušavaju da iskoriste ljudski faktor kako bi se ispunio cilj.

Različite vrste manipulacije se koriste radi prevare, kako bi žrtva pogrešila, otkrila osetljive ili poverljive podatke.

Šta bi bio socijalni inženjering?

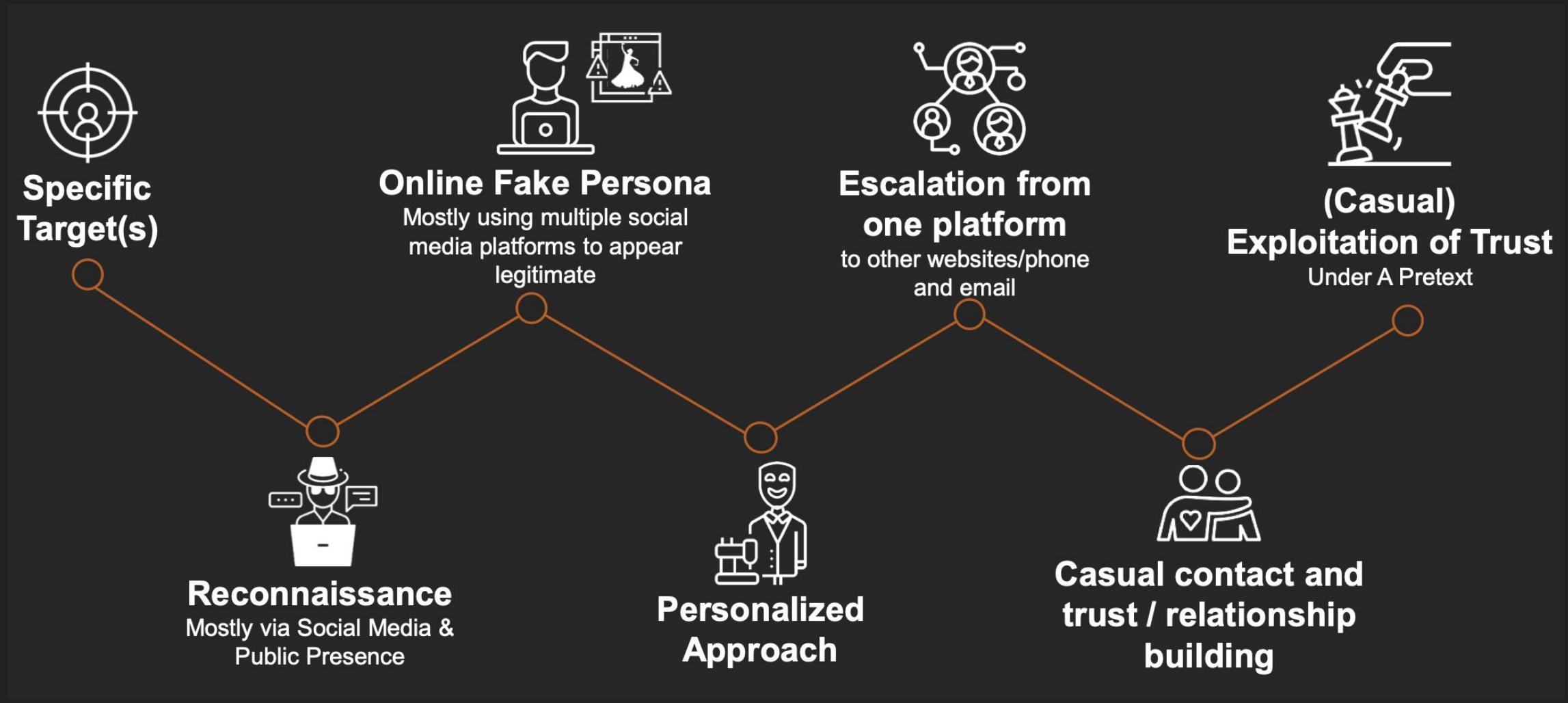
- Čini da bezbednost informacionih sistema ne bude samo tehnički izazov, već i sociološki!
- Dok god menadžeri I ostali zaposleni mogu obezbediti pristup sistemima I informacijama visoke vrednosti, oni postaju mete (target)
- Kratak primer socijalnog inženjeringa :)

Primeri zabeleženih napada

- Marcella (Marcy) Flores - persona osmišljena s ciljem "upada" u informacioni sistem kompanije koja sudeluje u bezbednosnom sektoru
- Mia Ash - persona osmišljena radi napada na kompanije Saudijske Arabije

- Drugi primeri, poput napada na Tojotu, RSA kompaniju

Cyberattack chain (kill chain) – lanac napada



OSINT

- Open Source INTelligence (OSINT): proces prikupljanja i analize javno dostupnih informacija kako bi se procenila pretnja, odgovorilo na specifična pitanja, te donele informisane odluke.
- Ključan za *reconnaissance (osmatranje)* kariku u lancu napada
- Cilj – prikupiti što više informacija o meti, žrtvi

OSINT – podaci od interesa

Kako se zaštititi?

- Raditi na razumevanju problema, automatizaciji odgovora

- Potrebno je:
  - **Znati** koje informacije su **osetljive**, pa se **ne smeju deliti**
  - **Biti sumnjičav** prema onima koji se interesuju za takve informacije
  - **Biti sumnjičav** ka elektronskim artefaktima
  - **Ne deliti informacije** sa onima koji nisu autorizovani da ih imaju

- U okviru organizacije:
  - Održati treninge i simulacije napada
  - Periodično izvršiti *procene ranjivosti* zaposlenih kroz OSINT

Procena ranjivosti mete

1) **Kritičnost**
Shvatiti koliko je meta bitna, koliko ima privilegija, koliki pristup informacijama i imovini.

2) **Prepoznatljivost**
Koliko je lako napadaču da identifikuje metu i sakupi informacije o njoj

3) **Pristupačnost**
Koliko je lako napadaču da priđe meti

4) **Ranjivost**
Meta: izloženost, predvidivost, tačnost profilisanja
Napadač: mogućnost, istrajnost, resursi koje ima

5) **Detekcija i mogućnost odgovora**
Koliko meta ima znanja i mogućnosti da prepozna napad, koliko ima mogućnost da ga spreči?

Zadatak za vas

- OWASP organizacija je razvila “ranjivu” aplikaciju koja je korisna za proučavanje bezbednosnih rizika u *web* aplikacijama
- Kao vežbu za socijalni inženjering, možete probati da rešite zadatak Bjoern's Favorite Pet
  - cilj je promeniti lozinku na Bjornovom nalogu tako što ćete saznati odgovor na njegovo sigurnosno pitanje :)
- Ostale izazove u aplikaciji možete pronaći ovde

Dodatni materijali

- Najbolji način da se edukujete na ovu temu je da slušate i čitate :)

- Preporučujemo vam:
  - Video materijale sa najveće bezbednosne konferencije Def Con. Konkretno, na datoj stranici pretražite temu *social engineering*
  - Knjiga o temi: Social Engineering: The Science of Human Hacking

Resursi

- https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
- https://www.ibm.com/think/topics/osint
- https://www.dcsa.mil/Portals/91/Documents/CI/DCSA-CI_Elicitation_2021.pdf
- https://god.owasp.de/2023/schedule/slides/Christina%20Lekati%20--%20What%20if%20the%20User%20Opens%20Back%20Door%20to%20Strangers.pdf