Hronološki pregled najznačajnijih sajber napada (2000–danas)

Predavač: dr. Dušan Stefanović

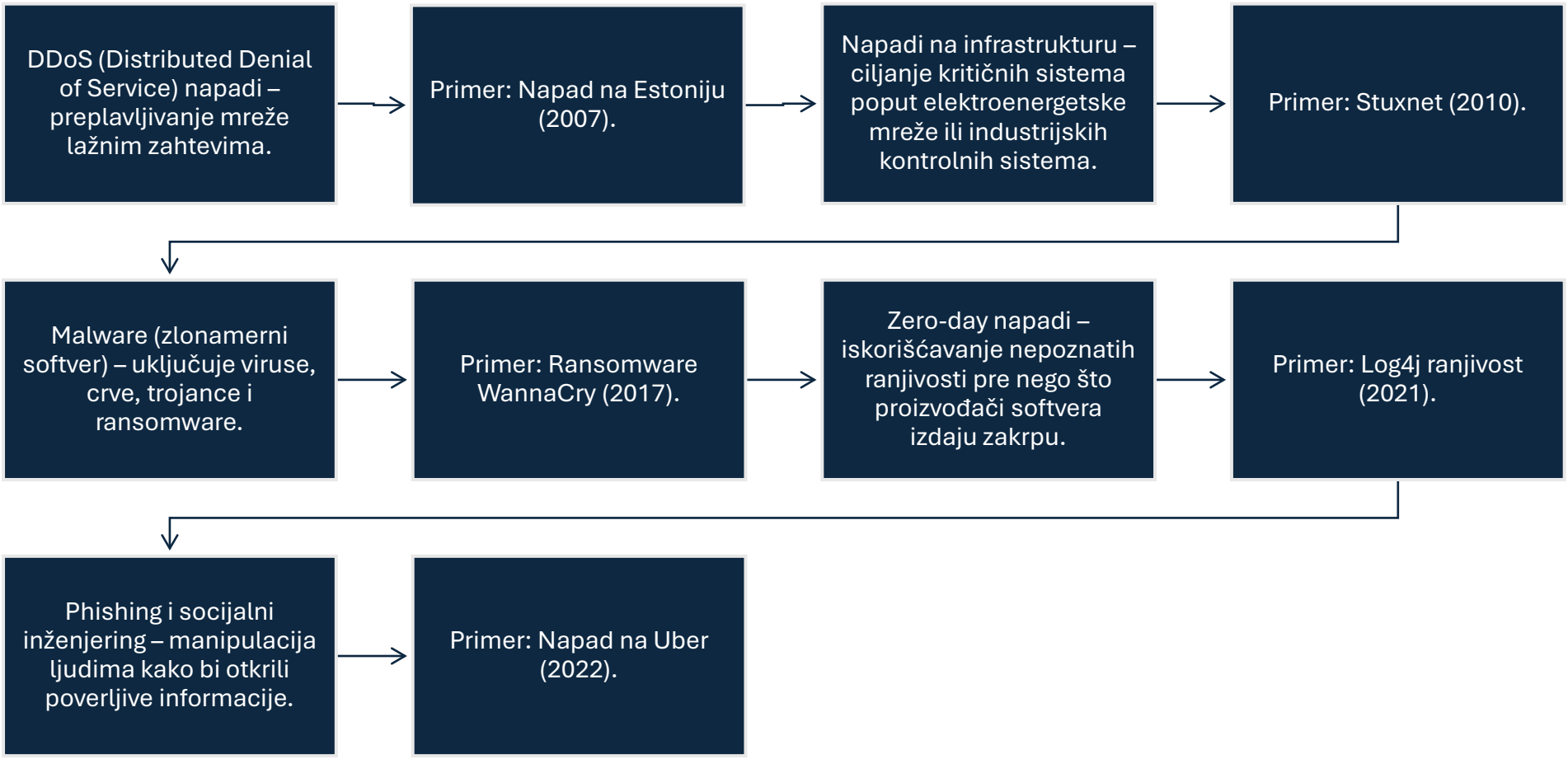
Uvod u temu

Definicija sajber napada: Neovlašćene radnje sa ciljem da se ugrozi, naruši ili kompromituje informacioni sistem.

Razvoj napada kroz istoriju: Od jednostavnih virusa do sofisticiranih APT (Advanced Persistent Threat) napada.

Važnost praćenja sajber pretnji: Razumevanje ranijih napada pomaže u boljoj zaštiti sistema danas.

Vrste sajber napada



Posledice sajber napada

- Finansijski gubici: Kompanije gube milione dolara zbog krađe podataka i prekida rada.
- Krađa podataka: Lične i finansijske informacije korisnika mogu biti zloupotrebljene.
- Geopolitički efekti: Države koriste sajber napade za špijunažu ili sabotažu.
- Poverenje javnosti: Napadi na velike kompanije mogu dugoročno ugroziti reputaciju.

2000–2010: Početak moderne sajber pretnje

Zlonamerni softver (virus i crv)

	Virus	Crv
Način širenja	Zahteva korisničku akciju	Samostalno se širi kroz mrežu
Zavisnost od fajlova	Veže se za izvršne fajlove	Funkcioniše samostalno
Zavisnost od korisnika	Mora biti pokrenut od strane korisnika	Ne zahteva akciju korisnika
Brzina širenja	Sporije širenje	Brzo širenja
Primeri štete	Uništavanje fajlova, usporavanje sistema	Preopterećenje mreže, zauzimanje sistemskih resursa, backdoor pristup

Virus je digitalni parazit – treba mu "domaćin" (fajl ili program)

Crv je "samostalna bakterija" – sam ulazi i sam se širi

"I Love You" Virus (2000)

Opis: Virus koji se širio putem e-maila sa privitkom "LOVE-LETTER-FOR-YOU.txt.vbs".

Efekti: 50 miliona zaraženih računara širom sveta.

Posledice: Gubici procenjeni na 5,5 milijardi dolara.

"I Love You" Virus (2000)

Tip napada: Malware (Crv, socijalni inženjering)

Kako je funkcionisao:

- Virus je bio VBScript (.vbs) fajl prikačen na e-mail sa subjektom **"I Love You"**.
- Kada bi korisnik otvorio fajl, skripta bi pretražila direktorijume i prepisala sve datoteke sa ekstenzijama .jpg, .mp3, .vbs.
- Zatim bi virus slao kopije sebe svim kontaktima u Microsoft Outlook adresaru.
- Izmenio bi Windows Registry kako bi se pokretao pri svakom startovanju sistema.

Zašto je bio uspešan?

- Koristio je psihološki trik (socijalni inženjering).
- Ljudi su otvarali prilog bez provere.
- Iskoristio je široko rasprostranjenu ranjivost u Windows e-mail klijentima.

Crv Code Red (2001)

Opis: Napao Microsoft IIS veb servere, omogućavajući hakerima daljinsku kontrolu.

Efekti: Zaraženo više od 350.000 servera za samo nekoliko sati.

Posledice: Napad na Belu kuću kao ključni cilj.

Code Red (2001)

Tip napada: Crv, Buffer Overflow

Tehnička izvedba:

- Napadao je Microsoft IIS 4.0 i 5.0 servere koristeći **buffer overflow ranjivost** u index.dll.
- Nakon eksploatacije, kreirao bi **backdoor** za dalju kontrolu sistema.
- Zaraženi računari su formirali **DDoS botnet** koji je pokušao da obori www.whitehouse.gov.
- Nije ostavljao tragove na hard disku (radio je u RAM-u).

Zašto je bio uspešan?

- Microsoft IIS je bio popularan web server.
- Administratori nisu redovno ažurirali softver.

Buffer Overflow napad

- **Buffer Overflow** (prekoračenje bafera) je sigurnosna ranjivost koja nastaje kada program upiše više podataka u memorijski bafer (privremeni skladišni prostor) nego što on može da primi.
- Višak podataka se prepisuje preko susednih memorijskih lokacija, što može izazvati **pad sistema, nepredvidivo ponašanje ili omogućiti napadaču izvršenje proizvoljnog koda**.

Buffer over flow napad na steku

Izgled memorije pre napada

```
+----------------------+
| Lokalne promenljive  |  <-- Radni prostor funkcije
+----------------------+
| Buffer (10 bajtova)  |  <-- Ograničen prostor
+----------------------+
| Sačuvan EBP          |  <-- Pokazivač na prethodni stek okvir
+----------------------+
| Povratna adresa      |  <-- Adresa na koju se funkcija vraća
+----------------------+
```

Prelivanje bafera - Prepisivanje memorije

```
+----------------------+
| Lokalne promenljive  |
+----------------------+
| BUFFER OVERFLOW!!!   |  <-- Preliveni podaci
| AAAAAAAAAAAAAAAAAAAA |  <-- Prelazimo granice
+----------------------+
| Sačuvan EBP          |  <-- OŠTEĆENO
+----------------------+
| Povratna adresa      |  <-- PREPISANO!
+----------------------+
```

Buffer over flow napad na steku

Napad sa shellcode-om

```
+---------------------+
| Lokalne promenljive |
+---------------------+
| SHELLCODE IN MEMORY | <-- Ubacivanje malicioznog koda
|      x90 x90 x90 ...| <-- NOP sled za sigurniji skok
+---------------------+
| Sačuvan EBP         | <-- OŠTEĆENO
+---------------------+
| Povratna adresa     | <-- UMERENO NA SHELLCODE!
+---------------------+
```

Napadač može **prepisati povratnu adresu** tako da ona pokazuje na bafer u kojem se nalazi **maliciozni kod (shellcode)**.

Rezultat: Kada funkcija završi, umesto da se vrati na originalnu lokaciju u kodu, skače na **maliciozni kod** koji daje napadaču potpunu kontrolu nad sistemom!

Kod koji dozvoljava Buffer Overflow

```
#include <stdio.h>
#include <string.h>

    void ranjiva_funkcija(char *ulaz) {
    char bafer[10];  // Bafer ograničen na 10 bajtova
    strcpy(bafer, ulaz);  // Kopiranje bez provere dužine
    printf("Uneli ste: %s\n", bafer);
    }

    int main() {
    char unos[100];
     printf("Unesite tekst: ");
     gets(unos); // Opasna funkcija, dozvoljava prelivanje bafera
     ranjiva_funkcija(unos);
     return 0;
     }
```

SQL Slammer (2003)

Opis: Ekstremno brza infekcija korišćenjem ranjivosti u Microsoft SQL Serveru.

Efekti: Značajno usporenje interneta i pad mreža banaka i telekom operatera.

Posledice: Milioni dolara gubitaka i hitne mere zaštite širom sveta.

SQL Slammer (2003)

Tip napada: Crv, SQL Injection

Tehnička izvedba:

- Iskoristio **buffer overflow** ranjivost u Microsoft SQL Server 2000.
- Slanjem specijalno kreiranog UDP paketa na port **1434**, preplavio bi server memorijom i omogućio daljinsko izvršavanje koda.
- Crv se širio tako brzo da je u 10 minuta zarazio 75.000 servera, usporivši globalni internet.

Zašto je bio uspešan?

- Nije koristio fajlove – izvršavao se direktno iz memorije.
- Širio se preko nezaštićenih SQL servera, koji su često imali podrazumevane lozinke.

Napad na Estoniju (2007)

Opis: Veliki DDoS napad na vladu, banke i medije Estonije.

Efekti: Onemogućen pristup ključnim internet uslugama.

Posledice: NATO osniva prvi sajber odbrambeni centar.

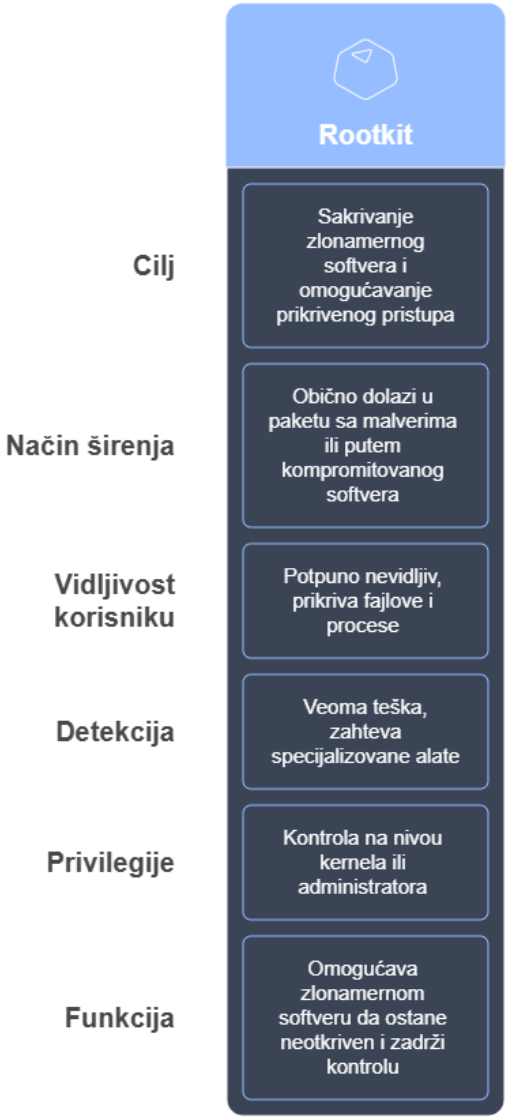
Stuxnet (2010)

Opis: Prvi sajber oružani napad, razvijen da uništi iranske centrifuge za obogaćivanje uranijuma.

Efekti: Oko 1.000 centrifuga uništeno.

Posledice: Pokretanje nove ere sajber ratovanja.

Zlonamerni softver (rootkit)



Rootkit je softverski alat dizajniran da sakrije prisustvo određenih procesa, fajlova ili aktivnosti na računaru.

Cilj dugoročna kontrola i nadzora nad sistemom bez znanja korisnika ili antivirusnog softvera.

Stuxnet (2010)

Tip napada: Zero-Day Malware, ICS (SCADA) Napad

Tehnička izvedba:

- Koristio je **zero-day ranjivost** u Windows OS.
- Širio se preko USB uređaja i mreža bez interneta (**air-gapped systems**).
- Ciljao je **Siemens Step7 SCADA kontrolere** povezane na centrifuge u iranskim nuklearnim postrojenjima.
- Manipulisao je **PLC (Programmable Logic Controller)** kod, lažno prikazujući da centrifuge rade normalno dok ih je ubrzavao do tačke loma.
- **Rootkit** koji je skrivao prisustvo virusa.

Zašto je bio uspešan?

- Prvi napad koji je fizički uništio industrijske sisteme.
- Bio je specijalizovan i veoma ciljan (pretpostavlja se da su ga razvile obaveštajne agencije SAD-a i Izraela).

2011–2020: Razvoj sofisticiranih sajber napada

Sony PlayStation Hack (2011)

Opis: Napad na PlayStation Network, krađa podataka 77 miliona korisnika.

Shamoon Malware (2012)

Opis: Napad na naftnu industriju Saudijske Arabije.

Efekti: 30.000 računara u Aramco kompaniji obrisano.

Posledice: Osveta protiv zapadnih interesa u IT sektoru.

Target Breach (2013)

Opis: Hakovanje sistema za plaćanje Target supermarketa.

Efekti: Ukradeni podaci 40 miliona kreditnih kartica.

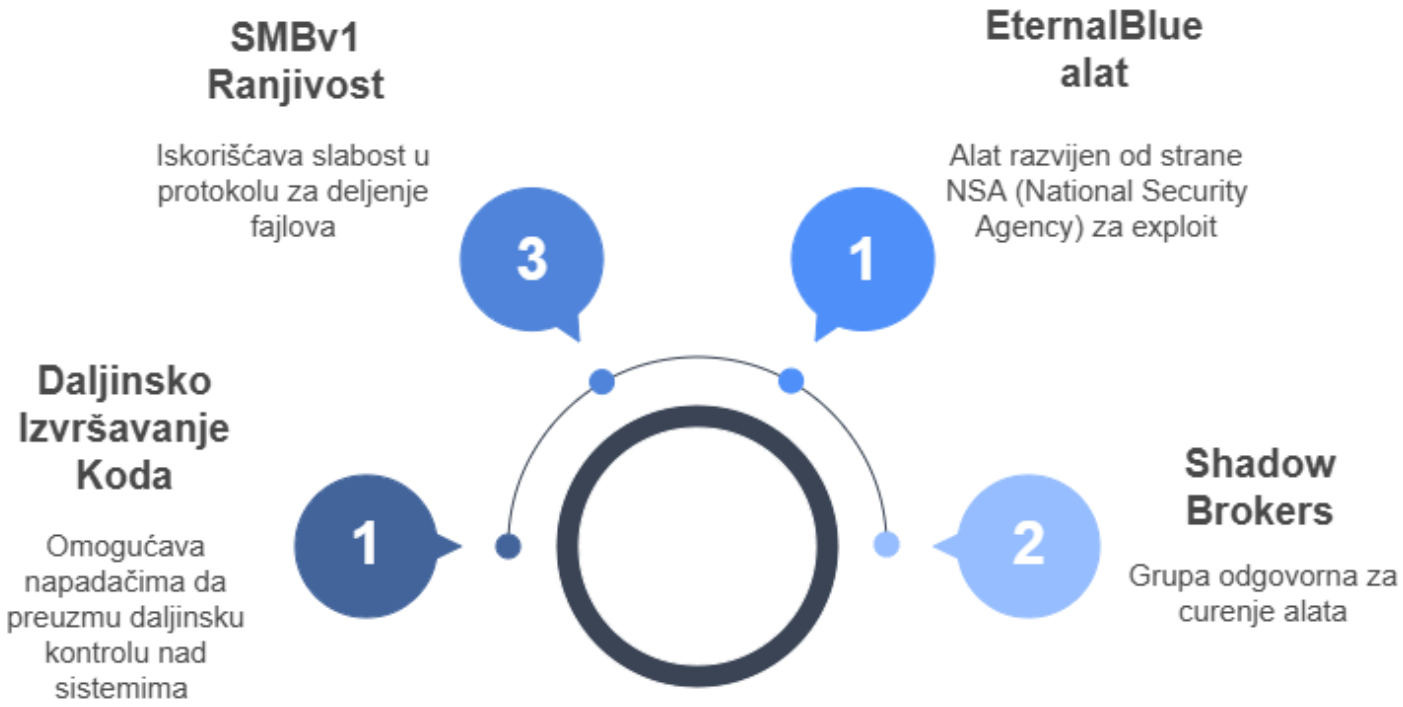
WannaCry Ransomware (2017)

Opis: Korišćenje exploit-a EternalBlue za širenje kroz mreže.

Efekti: Bolnice, vlade i kompanije širom sveta blokirane.

Posledice: Microsoft objavio zakrpu i osnažio sajber bezbednost.

Zlonamerni softver (EternalBlue Exploit)



WannaCry (2017)

Tip napada: Ransomware, Zero-Day Exploit

Tehnička izvedba:

- Koristio NSA (National Security Agency) **EternalBlue exploit**, koji je iskoristio propust **SMBv1 protokola** na Windows sistemima.
- Jednom kada bi ušao u mrežu, automatski bi se širio bez interakcije korisnika (**worm-like behavior**).
- Zaključavao je fajlove korisnika i tražio otkupninu u Bitcoin-u.

Zašto je bio uspešan?

- Koristio ranjivost koju je NSA znala, ali nije prijavila Microsoftu.
- Mnoge bolnice i kompanije nisu imale zakrpe jer su koristile zastarele sisteme.

NotPetya (2017)

Opis: Malver dizajniran da izgleda kao ransomware, ali je uništavao podatke.

Efekti: Globalna šteta od 10 milijardi dolara.

NotPetya (2017)

Tip napada: Ransomware, destruktivni malware

Tehnička izvedba:

- Iskoristio **EternalBlue** i **Mimikatz** za širenje unutar Windows mreža.
- Nije zapravo bio ransomware – nije imao funkcionalan sistem za dešifrovanje.
- Ciljao je ukrajinske kompanije, ali se proširio širom sveta.

Zašto je bio uspešan?

- Automatsko širenje preko Windows mreža.
- Ciljao firme sa zastarelim bezbednosnim praksama.

SolarWinds Hack (2020)

Opis: Napad na američke vladine agencije.

Metod: Hakeri kompromitovali ažuriranja SolarWinds softvera.

SolarWinds Hack (2020)

Tip napada: Supply Chain Attack, APT (Advanced Persistent Threat)

Tehnička izvedba:

- Napadači su kompromitovali **SolarWinds Orion** softver i ubacili **maliciozni update** (SUNBURST backdoor).
- Kada bi kompanije preuzele update, napadači bi dobili daljinski pristup mreži.
- Ciljali su američke vladine agencije i korporacije (Microsoft, FireEye).

Zašto je bio uspešan?

- Napao je **supply chain** – kompanije su same instalirale maliciozni softver.
- Napad je bio neprimetan mesecima.

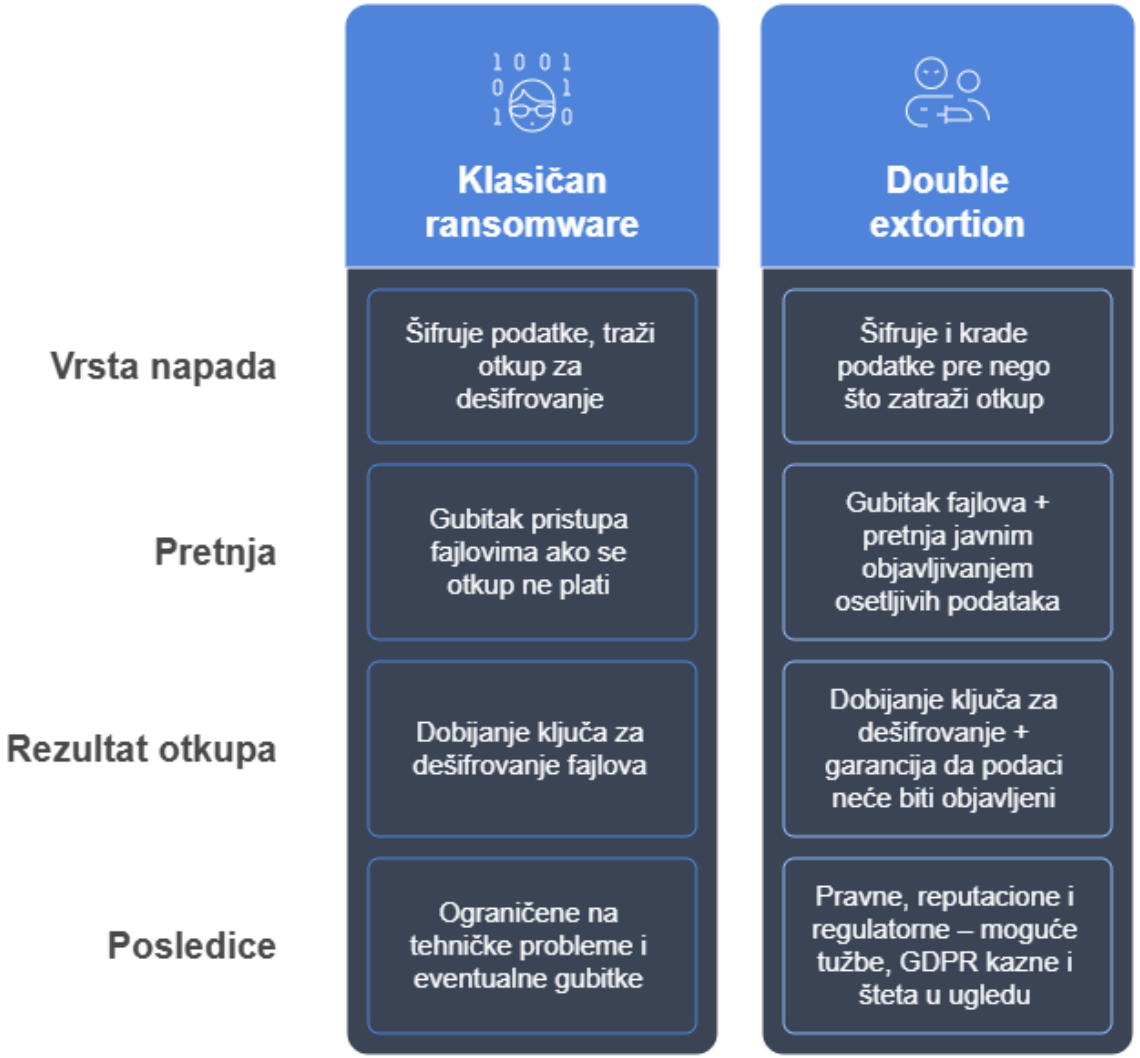
2021–danas: Savremeni sajber izazovi

Colonial Pipeline Ransomware (2021)

Opis: Napad na ključnu američku energetsku infrastrukturu.

Efekti: Prekid snabdevanja gorivom na istočnoj obali SAD-a.

Zlonamerni softver (Ransomware)



Colonial Pipeline Ransomware (2021)

- **Tip napada**: Ransomware (DarkSide grupacija)
- **Tehnička izvedba**:
  - Napadači su koristili **ukradene VPN kredencijale** (bez 2FA zaštite) da uđu u mrežu.
  - Nakon što su ušli, koristili su **ransomware enkripciju** da zaključaju interne sisteme.
  - Primenili su **double extortion** – pored šifrovanja podataka, pretili su objavljivanjem ukradenih fajlova.
- **Zašto je bio uspešan?**
  - Napao je ključnu infrastrukturu.
  - Kompanija je platila otkupninu ($4,4 miliona) jer nije imala odgovarajući **incident response plan**.

Log4j Ranjivost (2021)

Opis: Kritična ranjivost u popularnoj Java biblioteci.

Posledice: Milioni uređaja širom sveta u opasnosti.

Uber i Rockstar Games Hack (2022)

Opis: Napadi koristeći socijalni inženjering i phishing.

Lekcije naučene iz sajber napada

Zaštita mreže i ažuriranje softvera.

Multi-faktorska autentifikacija i enkripcija.

Budućnost sajber bezbednosti

AI i sajber bezbednost

Kvanta pretnja