

## Sigurnost računalnih sustava

# Izvori prijetnji i prijetnje

doc. dr. sc. Ante Đerek

izv. prof. dr. sc. Stjepan Groš

izv. prof. dr. sc. Miljenko Mikuc

izv. prof. dr. sc. Marin Vuković

# Podsjetimo se...

- Da bi se desio incident (narušila sigurnost) moraju postojati dva preduvjeta: ranjivost i **prijetnja**
- **Prijetnja** (engl. threat) je bilo koja *okolnost* ili *dogadjaj* koji ima potencijal narušiti sigurnost sustava ili informacije
- Prijetnje, kao i ranjivosti, su ključni element sigurnosti i zbog toga im posvećujemo značajnu pažnju na ovom predmetu

# Primjeri prijetnji i pridruže ranjivosti (1)

- Pogađanje kriptografskog ključa
  - Prekratak kriptografski ključ, predvidiv kriptografski ključ, ...
  - Alternativno, **kompromitiranje** kriptografskog ključa
    - U tom slučaju potencijalne ranjivosti su i neodgovarajuća pohrana i razmjena kriptografskog ključa
- Preplavljivanje poslužitelja zahtjevima
  - Poslužitelj malog kapaciteta, složena obrada na poslužitelju, algoritamska ranjivost, ...
- Lažiranje poruka elektroničke pošte
  - Nepostojanje ovjere pošiljatelja, više poslužitelja različitih vlasnika, ...
- DDoS napad na tvrtku
  - Link na Internet malog kapaciteta, usmjernik ograničenih performansi, ...

# Primjeri prijetnji i pridruže ranjivosti (2)

- **Poplava u sistemskoj sali**
  - Klima uređaj direktno iznad ormara s polužiteljima, vododjavni alarm nepostojeći ili nefunkcionalan, vodovodne cijevi prolaze kroz salu (i poslužitelji preblizu podu), ...
- **Napajanje poslužitelja prestane raditi**
  - Loš materijal, preveliko opterećenje, staro napajanje, ...
- **Napad ucjenjivačkim zloćudnim kodom (engl. ransomware)**
  - Nepostojanje antivirusne zaštite, neodgovorno ponašanje ljudi, nepostojanje sigurnosnih kopija, sigurnosne kopije dostupne putem mreže, ...

# Zaključci o prijetnjama (i ranjivostima)

- Ne postoji **formalni** popis prijetnji
  - Naći ćete različite popise, i svi su jednako „ispravni”
- Ne postoji **formalni** popis ranjivosti koje svaka prijetnja iskorištava
  - Također, postoje popisi, ali jesu li dobri ovisi i tko ih koristi
- Prijetnje mogu biti tehničke, taktičke, operativne i strateške
- Posljedica ostvarenja prijetnje je narušavanje sigurnosti – incident, kompromitacija
  - Ništa nismo rekli o **posljedicama** – to nije vezano uz prijetnje i ranjivosti

# Dodatni pojmovi vezani uz prijetnje

- **Agent prijetnje** (engl. threat agent, threat actor) je subjekt koji provodi prijetnju
- **Izvor prijetnje** (engl. threat source) je onaj koji je prijetnju potaknuo
  - Često su izvor prijetnje i agent prijetnje isti, ili ih ne možemo razlikovati, pa ćemo ta dva pojma koristiti jednoznačno
- **Napad** je kombinacija izvora prijetnje, namjere, prijetnje i posljedice

# Podjela izvora prijetnji

- Prirodni izvori
  - Prirodne nepogode – potres, poplava, požar, ...
  - Slučajni po karakteru
  - U nastavku ćemo ignorirati prirodu kao izvor prijetnji
- Ljudski izvori
  - Namjerni ili slučajni
    - Namjerni su napadači, slučajni su posljedica pogrešaka
    - **Bavit ćemo se isključivo namjernim izvorima prijetnje**
  - Vanjski ili unutarnji (u odnosu na sustav koji se štiti)
    - Razlika je u količini znanja i ovlastima koje izvor prijetnje ima
    - Puno opasnije i češće su unutarnji izvori prijetnje (engl. insider threats)

# Namjerni vanjski izvori prijetnji

- Postoji jako puno izvora prijetnji na Internetu
  - Grupiramo ih jer se na taj način lakše nosimo s njima
- Podjelu je moguće napraviti na temelju sljedećih karakteristika
  - *Raspoloživi materijalni resursi* – Koliko materijalnih resursa, uključivo novčanih sredstava, imaju na raspolaganju
  - *Motiv i ciljevi* – Što žele postići, odnosno, do čega žele doći te koga napadaju
  - *Ustrajnost* – Koliko je bitno da do zadanog cilja dođu u nekom specifičnom slučaju
  - *Količina ljudskih resursa i njihove kompetencije* – Koliko ljudi imaju na raspolaganju te kakve su im kompetencije



# Izvori prijetnji

- Napredne ustrajne prijetnje (engl. advanced persistent threats, APT)
- Kibernetički kriminalci (engl. cyber criminals)
- Haktivisti (engl. hactivists)
- Pojedinačni napadači
- Automatizirane probe

# Napredne ustrajne prijetnje

- **Napredne ustrajne prijetnje** su dijelovi obavještajnih službi ili dio vojne organizacije
  - Na raspolaganju imaju skoro neograničene količine resursa
    - Novčani resursi, ljudski resursi
  - Raspoloživi ljudi imaju vrlo visoke kompetencije
  - Ciljevi su određeni državnim interesima
    - Industrijska špijunaža, špijunaža, nanošenje fizičke štete
  - Vrlo su ustrajni i ciljani u svom djelovanju
  - Prikrivaju svoju prisutnost – protekne po više mjeseci dok se ne otkrije incident

# Primjeri napada APT-ova

- APT-ovi su odgovorni za neke od najsofisticiranijih napada
  - Planiranje i provođenje napada je dugotrajno
- Neki primjeri
  - Stuxnet (2010) – napad na Iransku nuklearnu elektranu i proces obogaćivanja urana
  - SolarWinds (2020) – napad na tvrtku SolarWinds te preko njih niz drugih tvrtki, agencija i institucija
  - Napad na elektroenergetski sustav u Ukrajini (2020)

# Zanimljivost u vezi APT-ova

- Pitanje je koliko doista APT-ovim imaju resursa jer malo se zna o njima



<https://twitter.com/SwiftOnSecurity/status/1188642971438202880?s=19>

- Ali baš zbog toga što se malo zna ne možemo znati i je li ovo istina...

# Primjeri APT-ova

- Kina, APT1 – bazirani u Šangaju u prostorijama PLA
- Rusija, APT28 – Cozzy Bear (i niz drugih imena)
- Ujedinjeno Kraljevstvo/Velika Britanija, GCHQ
- Sjedinjene Američke Države, NSA
- **Izrael**, Iran, ...
- Više primjera na <https://apt.threattracking.com>

# Pojam APT u praksi

- Pojmovi napredno i ustrajno su relativni
- Upotrebljavati pojam APT-a je vrlo popularno jer daje dodatnu dozu ozbiljnosti situacije
- Rezultat je da pojedini autori koriste pojam APT i za kibernetičke kriminalce, odnosno, općenito za bilo koga „naprednog” ili „ustrajnog”

# Kibernetički kriminalci

- Motiv je zarada, a ustrajnost srednja
  - Napast će sve za što smatraju da im može donijeti nekakvu zaradu
  - Gledaju potrošiti što manje resursa kako bi maksimizirali profit – zato nisu ustrajni kao APT-ovi
- Dvije vrste kriminalnih aktivnosti
  - Tradicionalne kriminalne aktivnosti koje se obavljaju putem kibernetičkog prostora
    - Prosjaci i sinovi...
  - Kriminalne aktivnosti koje je omogućio kibernetički prostor
    - Ransomware, ...

# Načini zaradivanja

- **Krađa podataka koji se mogu monetizirati**
  - Kreditne kartice, privatni podaci pojedinaca, medicinski podaci
- **Prodaja ilegalne robe i usluga**
  - Falsificirani proizvodi
  - Prodaja zloćudnog koda, iznajmljivanje infrastrukture za napade
- **Ucjenjivanje i iznuđivanje**
  - Ransomware
  - Prijetnje objavljivanja tajnih podataka
- **Prijevare**



# Kibernetički kriminal

- Radi se o cijelom nabavnom lancu
  - Specijalizacija za izradu zloćudnog koda, širenje zloćudnog koda, monetizacija podataka, izvlačenje novaca, ...
- Kriminalcima ponekad svjesno ili nesvjesno pomažu ljudi koje regrutiraju putem Interneta
  - Mule – pomažu kriminalcima da izvuku novce
- Komunikacija putem foruma na “dark web-u”
  - “Tržnice” na kojima se prodaju razne ilegalne robe

# Više o kibernetičkom kriminalu

- Ochko123 – prezentacija FBI-ja o hvatanju jednog ruskog “cardera”  
<https://www.youtube.com/watch?v=6Chp12sEnWk>
- Koobface Gang – tekst o otkrivanju jedne kriminalne skupine  
<https://nakedsecurity.sophos.com/koobface/>

# Haktivisti

- Slabo povezana grupa anonimaca
  - Ne pretjerano velikih kompetencija i resursa
  - S iznimkom mogućnosti provođenja napada uskraćivanja usluga
- Promoviraju nekakve političke, svjetonazorske i slične stavove
- Trude se biti što vidljiviji
  - Ako uspiju negdje narušiti sigurnost to odmah oglašavaju javno
- Nisu pretjerano uporni prema specifičnim ciljevima
  - Uporni su prema grupi ciljeva
  - Grupa na nekakav način simbolizira ono protiv čega se bore

# Pojedinačni napadači

- **Gray Hats, Black Hats, White Hats**
  - Napadači potencijalno vrlo velikih vještina i kompetencija
  - Razlikuju se po tome djeluju li etično (white hats) ili ne (black hats)
  - Vrsta Gray Hats su na granici
- **Script Kiddies**
  - Ime koje se daje svima koji ne znaju ništa o računarstvu osim pokretati tuđe alate
  - Radi se o napadačima najmanje razine vještine
  - Uglavnom to rade zbog znatiželje ili stjecanja nekakve slave
- **Pojam hakera i zloupotreba tog pojma**

# Automatizirane probe

- Dvije vrste automatiziranih proba
  - Skeneri koji stalno pretražuju Internet za ranjivim servisima
    - Često specijalizirani za pojedini servis i ranjivosti – primjerice WordPress
  - Crvi koji se pokušavaju zaraziti druga računala na mreži
- Karakteristike automatiziranih probi
  - Na internetu je aktivno jako puno različitih proba
  - Više spadaju pod smetnju/dosadu nego nešto ozbiljno
  - Vrlo lako se štititi od ovih izvora prijetnji – ne koristiti ranjive servise
  - Često se u marketinške svrhe ovi napadi računaju

# Kako izgleda napad?

- Što je napadač sposobniji napad je bolje organiziran
  - Što je napadač nesposobniji – napad je kaotičniji
- Napad (ponašanje napadača) pokušavamo opisati modelom
  - Modeliranje napada
  - Model napada opisuje generički niz koraka koje svaki napad mora imati
  - Postoji niz pokušaja modeliranja napada
    - Svi imaju svoje prednosti i mane
- Razlozi za modeliranje napada
  - Poznavanjem napadača lakše je spriječiti, prepoznati, zaustaviti napad
  - Modeli napada **sastoje se od prijetnji** – s nekim iznimkama

# Cyber Kill Chain

- Najpoznatiji model napada je *Cyber Kill Chain*
- Postoje razne varijacije na temu, ali u osnovi sastoji se od sljedećeg generičkog niza koraka
  - Istraživanje (engl. reconnaissance)
  - Naoružavanje (engl. weaponization)
  - Isporuka (engl. delivery)
  - Iskorištavanje (engl. exploitation)
  - Instalacija (engl. installation)
  - Uspostava upravljačkog kanala (engl. command&control, C2)
  - Djelovanje (engl. action on objectives)

# MITRE ATT&CK

- Organizacija MITRE slaže bazu taktika, tehnika i procedura uočenih u napadima
  - TAKTIKA – zašto se nešto radi, taktički cilj
  - TEHNIKA – kako nešto napraviti
  - PROCEDURA – točan (tehnički) način provođenja
- Navedena baza bi trebala omogućiti razvoj modela prijetnji i metodologija zaštite.



# MITRE ATT&CK

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Access Token Manipulation (5)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Execution Guardrails (1)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Domain Policy Modification (2)	Exploitation for Defense Evasion	Man-in-the-Middle (2)	Domain Trust Discovery	Software Deployment Tools
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	File and Directory Discovery	Taint Shared Content
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Hide Artifacts (7)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (4)
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	OS Credential Dumping (8)	Network Share Discovery	
				Hijack Execution	Process Injection (4)	Indicator Removal on Host (6)	Steal Application Access Token	Network Sniffing	
								Password Policy Discovery	
								Peripheral Device Discovery	

<https://attack.mitre.org/>

# Česte tehnike: Društveni inženjering

- Čovjek je najslabija karika
  - Napadači često iskorištavaju ljudske slabosti jer im je to najjednostavnije
- Ciljevi napadača
  - Instalirati zloćudni kod na korisničko računalo
  - Doći do nekakvih tajnih podataka – korisničkih imena i lozinki, osobnih podataka, financijskih podataka
- Neke metode napada
  - Phishing – slanje poruke elektroničke pošte svim korisnicima
  - Spear Phishing

# Problem atribucije

- Atribucija: Odgovor na pitanje tko stoji iza napada?
- Zbog načina kako Internet radi teško je dati odgovor na to pitanje
  - Sposobniji napadači prikrivaju svoj pravi identitet
- Načini prikrivanja identiteta
  - Korištenje računala na koja je napadač provalio
  - Korištenje VPN usluge
  - Korištenje anonimizacijskih mreža (Tor)

# Model prijetnje

- **Koga** želimo spriječiti da učini **što**
- Model prijetnje ne opisuje naš sustav već okolinu u kojoj naš sustav djeluje
- Model prijetnje daje se opisno
  - Primjer modela prijetnje za protokol TLS
    - Krajnje točke komunikacije su sigurne
    - Komunikacijski kanal je pod potpunom kontrolom napadača
    - Protokol ne rješava problem dostupnosti

# Hvala!