Akademska godina 2025/2026

Ofenzivna sigurnost

Perzistencija

Lucia Crvelin, 27.10.2025.

Pregled predavanja

- Pitanja za ispit
- Motivacija: krhkost inicijalnog pristupa
- Klasifikacija tehnika i primjeri
- Izazovi obrane
- Zaključak

Pitanja

1. Koji je temeljni problem napadača nakon uspješnog inicijalnog pristupa sustavu, a koji perzistencija rješava?
2. Navedite tri kategorije tehnika perzistencije.
3. Zašto se tehnika „DLL Hijacking” smatra naprednijom metodom od korištenja „Registry Run keys” ?
4. Koja kategorija tehnike perzistencije može preživjeti reinstalaciju OS-a i zašto ju je iznimno teško otkriti softverskim alatima unutar OS-a?
5. Kakav je pristup potreban za obranu od modernih tehnika perzistencije?

Problem: krhkost inicijalnog pristupa

- Početni proboj je uspješno izveden – napadač je u sustavu
- Taj pristup je iznimno krhak i privremen
- Napadač može biti izbačen u bilo kojem trenutku:
  - Restart sustava ili gašenje računala
  - Isključenje računala s mreže
  - Reinstalacija OS-a

Problem: krhkost inicijalnog pristupa (2)

- Glavni problemi napadača:
  - Kako preživjeti prekide?
- Cilj: pretvoriti privremeni pristup u trajno i pouzdano uporište
  - Preživjeti restart
  - Održati pristup
  - Automatsko pokretanje zloćudnog koda
  - Osigurati oporavak

Klasifikacija tehnika

- Perzistencija nije jedna tehnika, već širok spektar tehnika
- Klasifikacija prema „ciljanoj imovini” – lokaciji na sustavu gdje napadač postavlja svoj mehanizam
- 3 glavne kategorije:
  - Aplikacija - zloupotreba softvera koji korisnik već koristi
  - OS - modifikacija načina na koji OS radi
  - Firmware/hardware – najdublja i najotpornija razina

Perzistencija unutar aplikacija

- Strategija: sakriti se unutar legitimnih aplikacija
- Zašto? Korisnici vjeruju tim aplikacijama i često ih koriste
- Najlakše za implementaciju, ali i najlakše za spriječiti

Perzistencija unutar aplikacija: primjeri

- **Microsoft Office (Makronaredbe / Add-ins):**
  - Napadač postavi malicioznu makronaredbu (VBA) koja se pokrene svaki put kad se otvori Word ili Excel
- **Web Preglednici (Browser Extensions):**
  - Napadač instalira zlonamjernu ekstenziju (npr. lažni "Ad Blocker") koja se učitava sa svakim pokretanjem preglednika
  - Omogućuje krađu kolačića, lozinki i umetanje sadržaja na stranice

Perzistencija unutar aplikacija: primjeri (2)

- **Web Serveri (Web Shell):**
  - Ako je meta web server, napadač može *uploadati* jednostavnu skriptu (npr. u PHP-u ili ASP.NET-u) na server
  - Ta datoteka mu daje stalnu kontrolu nad serverom sve dok ju netko ne obriše

Perzistencija unutar OS-a

- Strategija: ”Living off the Land” (LOL)
  - Koriste se ugrađeni mehanizmi OS-a dizajnirani za legitimno automatsko pokretanje
- Najčešće korištena strategija

Perzistencija unutar OS-a: primjeri

- Registry Run Keys:
  - Dodaje se putanja do malware-a u HKEY_CURRENT_USER\...\Run
  - OS automatski pokreće sve što je tamo navedeno prilikom prijave korisnika
- Startup Folder:
  - Još jednostavnije: kopira se prečac (.lnk) do malicioznog programa u C:\...\\Start Menu\Programs\Startup

Perzistencija unutar OS-a: primjeri (2)

- Scheduled Tasks:
  - Kreira se novi zadatak (npr. „GoogleUpdateTask”) koji pokreće malware
  - Može se namjestiti da se pokreće svakih sat vremena ili pri prijavi korisnika

Perzistencija unutar OS-a: primjeri (3)

- Korištenje mehanizama koje administratori rjeđe provjeravaju
- Windows servisi
  - Napadač kreira novi Windows servis ili modificira postojeći
  - Omogućuje izvršavanje s visokim SYSTEM privilegijama, često prije prijave korisnika
  - Teže se uočava od Run ključa jer sustav ima puno legitimnih servisa

Perzistencija unutar OS-a: primjeri (4)

- „Fileless” perzistencija
  - Maliciozni kod se nikada ne sprema kao datoteka na disk
  - Perzistencija se postiže zloupotrebom sistemskih alata
  - Kreiranje WMI Event Subscription
    - Napadač registrira WMI event koji se aktivira npr. svakih sat vremena i pokreće malicioznu skriptu izravno iz memorije

Perzistencija unutar OS-a: primjeri (5)

- DLL Hijacking
  - Napadač iskorištava način na koji Windows učitava DLL datoteke
  - Postavlja maliciozni DLL s istim imenom kao i legitimni na lokaciju koja se prva pretražuje
  - Prikrivenija tehnika za razliku od Registry Run Keys

Perzistencija na razini firmware/hardware

- Firmware omogućuje da hardware pravilno funkcionira
- strategija: postati dio samog računala
- Najteže za detektirati - preživljava i reinstalaciju OS-a
- Iznimno kompleksne tehnike i skupe za izvesti

Perzistencija na razini firmware/hardware: primjer

- Bootkit
  - Maliciozni kod se upisuje izravno u firmware sustava
  - Kod se izvršava prije OS-a
  - Gotovo nemoguće otkriti softverskim alatima unutar OS-a
  - Preživljava reinstalaciju OS-a

Zašto je obrana teška?

- „Living off the Land” i ”Fileless” napadi
  - Napadači zloupotrebljavaju legitimne, potpisane alate sustava
  - Tradicionalni antivirus (bazirani na potpisima) ne može blokirati ove alate
- Velika napadna površina
  - izazovno učinkovito nadzirati svaku lokaciju u svakom trenutku
- Problem buke
  - Kako razlikovati legitimnu aktivnost od zlonamjerne
- Perzistencija „ispod OS-a” (Bootkiti)

Zaključak

- Perzistencija = ključna faza napada
  - pretvara privremeni proboj u trajno i pouzdano uporište u sustavu
- **Najučinkovitije tehnike:** pametna **zloupotreba ugrađenih, legitimnih alata** operacijskog sustava
- Antivirusi nisu dovoljni - uspješna obrana zahtijeva dubinski nadzor nad ponašanjem sustava i proaktivni lov na prijetnje

Literatura

- https://attack.mitre.org/tactics/TA0003/
- Gittins, Z., & Soltys, M. (2020). Malware persistence mechanisms. *Procedia Computer Science*, *176*, 88–97. https://doi.org/10.1016/j.procs.2020.08.010
- Villalón-Huerta, A., Marco-Gisbert, H., & Ripoll-Ripoll, I. (2022). A taxonomy for threat actors' persistence techniques. *Computers & Security*, *121*, 102855. https://doi.org/10.1016/j.cose.2022.102855

Dodatna literatura

- https://www.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf
- How hackers persist in Microsoft 365: https://www.youtube.com/watch?v=lh4u2LV1Blc

Hvala!