Ofenzivna sigurnost

Izbjegavanje obrane

Leon Tišljarić, 3.11.2025.

Pregled predavanja

- **Motivacija**
- **Pitanja za ispite**
- **O izbjegavanju obrane**
- **Istaknute tehnike**
  - Uklanjanje indikatora
  - Legitimni računi
  - Oslabljivanje obrane
- **Zaključak**

Motivacija

- **Problemi**
  - kompromis između brzine djelovanja i prikrivanja
  - kontinuirana prilagodba telemetrije i politika od obrambene strane
  - svaka interakcija može ostaviti artefakte koji olakšavaju detekciju
  - napadači rade s nepotpunim informacijama o sustavu

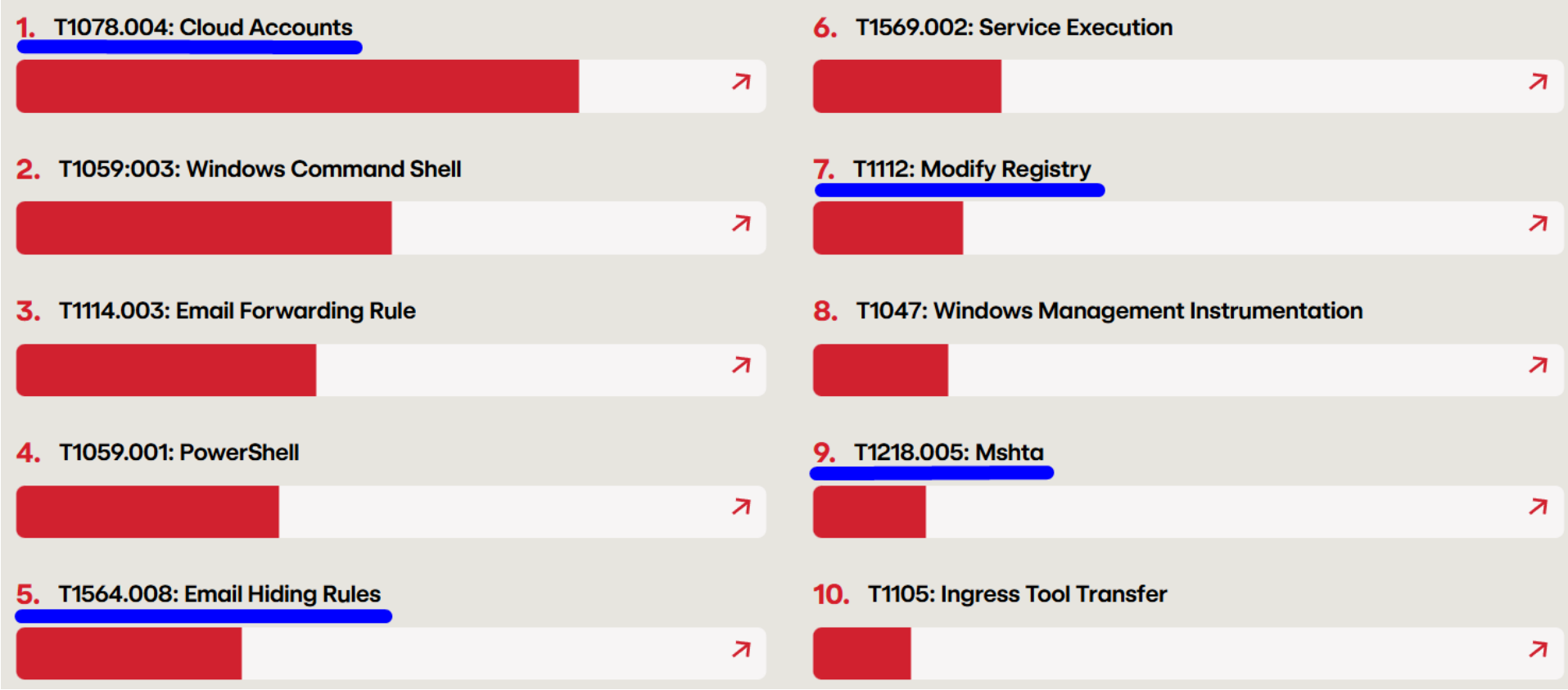
Pitanja za ispite

- Što je taktika izbjegavanja obrane (eng. *Defense Evasion*) te navedite neke od njezinih ciljeva?
- Koji su glavni problemi s kojima se susreću napadači prilikom primjene tehnika izbjegavanja obrane?
- Objasni jednu pod-tehniku tehnike uklanjanja indikatora (eng. *Indicator Removal*).
- Što je tehnika oslabljivanje obrane (eng. *Impair Defenses*) te navedite neke od njezinih ciljeva?
- Koje su prednosti i nedostaci korištenja tehnike legitimnih računa (eng. *Valid Accounts*) za napadače u okruženjima u oblaku?

O izbjegavanju obrane

- izvješća o prijetnjama 2025.[1],[2]
  - **Red Canary**
    1. Cloud Accounts (T1078.004)
    3. Email Hiding Rules (T1564.008)
    7. Modify Registry (T1112)
    9. Mshta (T1218.005)
  - **CrowdStrike**
    - Indicator Removal (T1070)
    - Impair Defenses (T1562)

O izbjegavanju obrane



Slika 1. Deset najčešće uočenih tehnika i pod-tehnika MITRE ATT&CK u 2025. godini, Red Canary

O izbjegavanju obrane

- izbjegavanje obrane nije ograničeno na jedan taktički korak unutar *Kill Chaina*
- taktika koja obuhvaća skup tehnika koje napadači koriste da bi izbjegli otkrivanje tijekom cijele operacije[3]

Najintenzivnije se primjenjuju prilikom:

1. **Instalacije**
2. **Postizanja ciljeva**
3. **Naoružavanja i inicijalnog ulaza**

O izbjegavanju obrane

- **Ciljevi taktike**
  - minimalizira rizik otkrivanja i gubitka pristupa
  - duže prisustvo u sustavu (eng. *dwell time)*
  - smanjuje troškove ponovnog kompromitiranja
  - pruža vremenski prostor za mapiranje sustava i njegovih servisa
  - omogućuje prikupljanje veće količine resursa[4]

Uklanjanje indikatora (eng. *Indicator Removal*)

- **T1070**
- brisanje ili izmjena artefakata stvorenih unutar ciljanog sustava[5]

- **Ciljevi**
  - ometati prikupljanje podataka
  - narušiti integritet obrambene strane (antivirusa, EDR-ova, itd.)
  - otežati forenzičku analizu i odgovor na napad

Uklanjanje indikatora (eng. *Indicator Removal*)

- **brisanje zapisa Windows Event**[6]
  - brisanje i/ili izmjena zapisa na putanji *C:\Windows\System32\winevt\logs*
  - zahtjeva podizanje privilegija, administratorske ovlasti

- **brisanje povijesti naredbi** trenutne (*history -c*) ili više sesija (*ConsoleHost_history.txt)*[7],[8]

- **lažiranje vremenskih oznaka**[9] + **relokacija zlođudnog koda**[10][11]
  - izmjena atributa *$STANDARD_INFORMATION i $FILE_NAME* u datoteci Master File Table

Uklanjanje indikatora (eng. *Indicator Removal*)

- **Mane tehnike**
  - teško skaliranje tehnike u složenijim sustavima
  - neke tehnike zahtijevaju podizanje privilegija
  - prekidi u uzastopnom nizu identifikatora zapisa (npr. *EventRecordID)*[12]
  - EDR agenti mogu slati događaje na centralno mjesto izvan sustava
  - Volume Shadow Copy Service (VSS)[13]
  - praćenje poziva API-ja

Legitimni računi (eng. *Valid Accounts*)

- **T1078**
- zloupotrebljavanje vjerodajnica postojećih, legitimnih korisničkih računa[14],[15]
- omogućuje inicijalni ulaz, perzistenciju, podizanje privilegija te **izbjegavanje obrane**
- tehnika usmjerena najčešće na račune u oblaku
  - međusobna povezanost SaaS, PaaS i IaaS usluga
  - višenamjenska uloga računa (email, pohrana podataka, upravljanje servisima, pristup API-jevima, itd.)

Legitimni računi (eng. *Valid Accounts*)

- **Mane tehnike**
  - vezane uz ponašanje napadača
  - prijave u neobično vrijeme
  - SSH prijave s neočekivanih IP adresa
  - pokretanje neobičnih procesa izvan uobičajenog obrasca korisnika

Oslabljivanje obrane (eng. *Impair Defenses*)

- **T1562**
- napadač mijenja komponente okruženja te otežava i/ili onemogućuje obrambene mehanizme sustava (antivirus, vatrozid, EDR-ove...)[16]

- **Ciljevi**
  - spriječiti automatsko zakrpavanje (eng. *patch*) ranjivosti
  - smanjiti vjerojatnost da će obrambeni alat otkriti aktivnost
  - izoliranje agenata od centralnih servera
  - blokiranje gašenja te odjave korisnika

Oslabljivanje obrane (eng. *Impair Defenses*)

- **onemogućavanje ili izmjena vatrozida u oblaku**[17],[18]
  - okruženja u oblaku koriste raspodjelu korisnika u grupe različitih ovlasti te definirana pravila vatrozida
  - ostavljanje otvorenih, standarnih računa, rad aplikacije na prvom mjestu, podcjenjivanje *cloud* IAM-a (*Identity and Access Management*),
  - **cilj** - dodati nove, pouzdane IP adresa, portove i protokole, otvoriti komunikaciju s poslužiteljem C&C, omogućiti lakše lateralno kretanje do podataka

- **lažiranje sigurnosnih upozorenja**[19],[20]
  - lažno prikazivanje sigurnosnih upozorenja generiranih od strane obrambenih alata

Oslabljivanje obrane (eng. *Impair Defenses*)

- **napad snižavanja verzije**[21]
  - cilj napada je sniziti verzije komponenti sustava na zastarjele i ranjive
  - kompatibilnost sustava unatrag
  - povratak na: slabije verzije šifriranja (TLS/HTTPS), verzija bez bilježenja događaja (PowerShell *Script Block Logging),* itd.
  - pretvara zakrpane ranjivosti u ranjivosti nultog dana

Zaključak

- **olakšava život napadačima**
- taktika koja napadaču omogućuje da nastavi koristiti alate koji bi bez mjera prikrivanja bili brzo uočeni od strane obrambenih mehanizama

- postojeći alati „preživljavaju” u sustavu pa se napadač može fokusirati na druge faze napada umjesto da razvija potpuno nove alate

Literatura

[1] Red Canary, “2025 Threat Detection Report”, Red Canary, https://resource.redcanary.com/rs/003-YRU-314/images/2025ThreatDetectionReport_RedCanary.pdf?version=0 , [mrežno; stranica posjećena: listopad 2025.]

[2] CrowdStrike, “CrowdStrike Global Threat Report 2025”, CrowdStrike, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0, [mrežno; stranica posjećena: listopad 2025.]

[3] MITRE ATT&CK, “Defense Evasion”, MITRE, https://attack.mitre.org/tactics/TA0005/, [mrežno; stranica posjećena: listopad 2025.]

[4] Red Canary, “Defense Evasion - Why is it so prominent & how can you detect it?”, Red Canary, https://redcanary.com/blog/threat-detection/defense-evasion-why-is-it-so-prominent-how-can-you-detect-it, [mrežno; stranica posjećena: listopad 2025.]

[5] MITRE ATT&CK, “Indicator Removal”, MITRE, https://attack.mitre.org/techniques/T1070/001/, [mrežno; stranica posjećena: listopad 2025.]

[6] MITRE ATT&CK, “Indicator Removal: Clear Windows Event Logs”, MITRE, https://attack.mitre.org/techniques/T1070/, [mrežno; stranica posjećena: listopad 2025.]

[7] MITRE ATT&CK, “Indicator Removal: Clear Command History”, MITRE, https://attack.mitre.org/techniques/T1070/003/ , [mrežno; stranica posjećena: listopad 2025.]

[8] Atomic Red Team, “T1070.003 - Indicator Removal on Host: Clear Command History”, Atomic Red Team, https://www.atomicredteam.io/atomic-red-team/atomics/T1070.003 , [mrežno; stranica posjećena: listopad 2025.]

[9] MITRE ATT&CK, “Indicator Removal: Timestomp”, MITRE, https://attack.mitre.org/techniques/T1070/006/, [mrežno; stranica posjećena: listopad 2025.]

[10] MITRE ATT&CK, “Indicator Removal: Relocate Malware”, MITRE, https://attack.mitre.org/techniques/T1070/010/, [mrežno; stranica posjećena: listopad 2025.]

[11] Microsoft, “Configure exclusions for Microsoft Defender Antivirus”, Microsoft, https://learn.microsoft.com/en-us/defender-endpoint/configure-exclusions-microsoft-defender-antivirus, [mrežno; stranica posjećena: listopad 2025.]

Literatura

[12] Microsoft, “SystemPropertiesType Complex Type”, Microsoft, https://learn.microsoft.com/en-us/windows/win32/wes/eventschema-systempropertiestype-complextype , [mrežno; stranica posjećena: listopad 2025.]

[13] Microsoft, “Volume Shadow Copy Service (VSS)”, Microsoft, https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service , [mrežno; stranica posjećena: listopad 2025.]

[14] MITRE ATT&CK, “Valid Accounts”, MITRE, https://attack.mitre.org/techniques/T1078/, [mrežno; stranica posjećena: listopad 2025.]

[15] Red Canary, “Cloud Accounts”, Red Canary, https://redcanary.com/threat-detection-report/techniques/cloud-accounts/, [mrežno; stranica posjećena: listopad 2025.]

[16] MITRE ATT&CK, “Impair Defenses”, MITRE, https://attack.mitre.org/techniques/T1562/, [mrežno; stranica posjećena: listopad 2025.]

[17] MITRE ATT&CK, “Impair Defenses: Disable or Modify Cloud Firewall”, MITRE, https://attack.mitre.org/techniques/T1562/007/, [mrežno; stranica posjećena: listopad 2025.]

[18] Palo Alto Networks Unit 42, “Compromised Cloud Compute Credentials”, https://unit42.paloaltonetworks.com/compromised-cloud-compute-credentials/ , [mrežno; stranica posjećena: listopad 2025.]

[19] MITRE ATT&CK, “Impair Defenses: Disable or Modify Cloud Firewall”, MITRE, https://attack.mitre.org/techniques/T1562/007/, [mrežno; stranica posjećena: listopad 2025.]

[20] SentinelOne, “Black Basta Ransomware Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor”, SentinelOne, https://www.sentinelone.com/labs/black-basta-ransomware-attacks-deploy-custom-edr-evasion-tools-tied-to-fin7-threat-actor/ , [mrežno; stranica posjećena: listopad 2025.]

[21] MITRE ATT&CK, “Impair Defenses: Spoof Security Alerting”, MITRE, https://attack.mitre.org/techniques/T1562/011/, [mrežno; stranica posjećena: listopad 2025.]

Dodatna literatura

Microsoft, “Microsoft Digital Defense Report 2025”, Microsoft, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/security/Microsoft-Digital-Defense-Report-2025.pdf, [mrežno; stranica posjećena: listopad 2025.]

SafeBreach, “Downgrade Attacks Using Windows Updates”, SafeBreach, https://www.safebreach.com/blog/downgrade-attacks-using-windows-updates/, [mrežno; stranica posjećena: listopad 2025.]

Hvala!