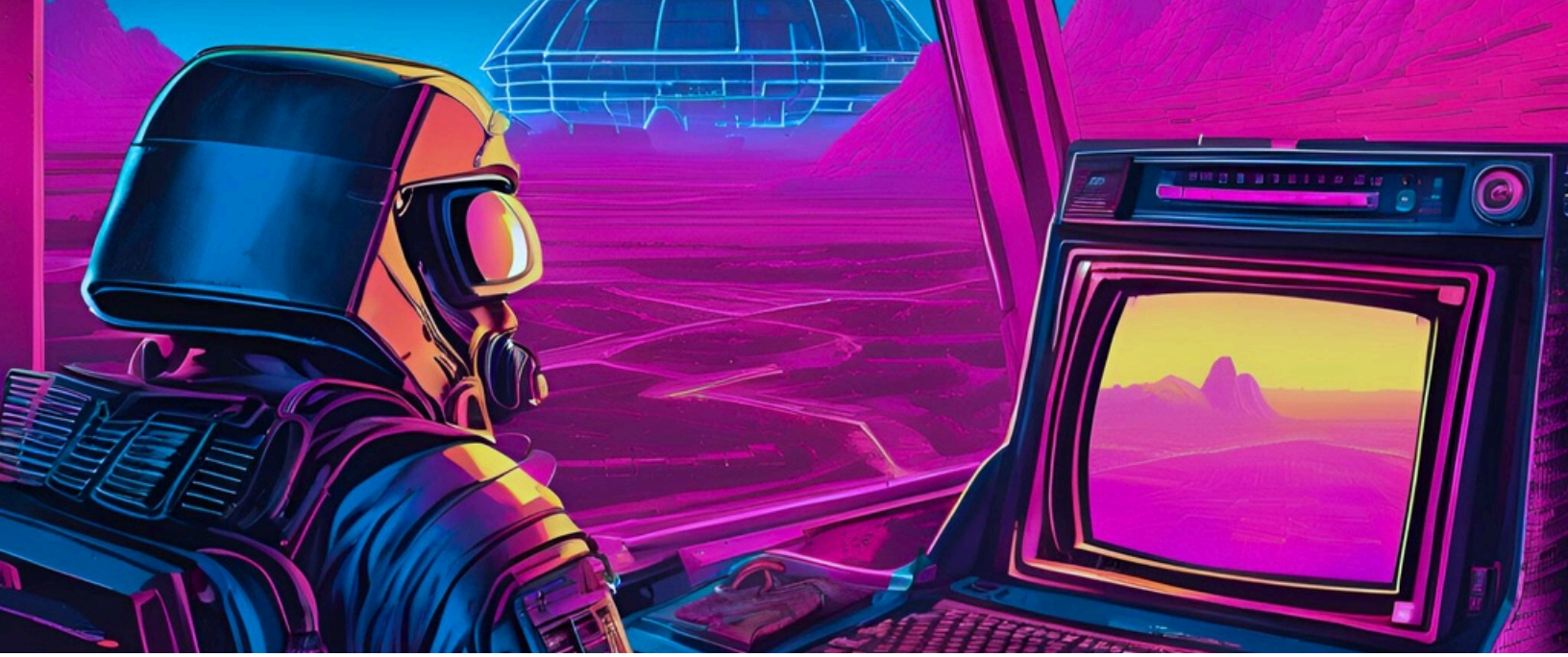
IT KLINIKA

Vodič za Detekciju Living off the Land (LotL) napada

www.it-klinika.rs



Šta su Living off the Land (LotL) napadi?

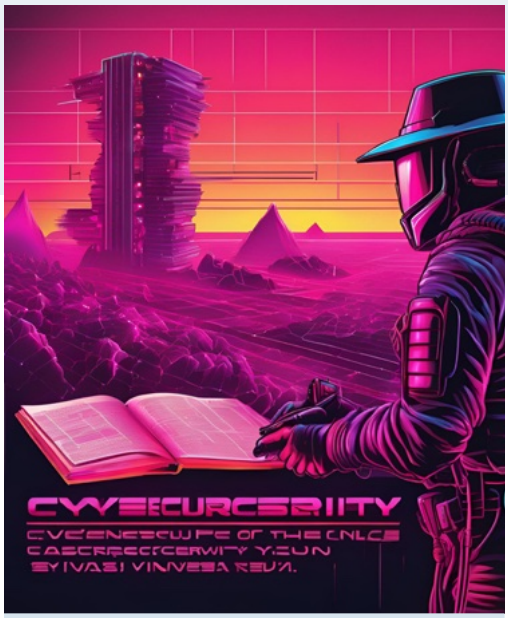
Living off the Land (LotL) napadi predstavljaju jedan od najvećih izazova u modernoj sajber bezbednosti. Ovi napadi su posebno opasni jer koriste legitimne sistemske alate i procese - upravo one alate koje vaši administratori koriste svakodnevno. Zamislite lopova koji koristi vaše vlastite ključeve da uđe u kuću - to je suština LotL napada.

Zašto je ovo važno?

Tradicionalni bezbednosni alati često ne mogu detektovati LotL napade jer:

- Aktivnosti izgledaju legitimno na prvi pogled
- Koriste se standardni sistemski alati (PowerShell, WMI, PsExec)
- Napadači "se stapaju" sa normalnim administrativnim aktivnostima

O vodiču



Šta ćete naučiti?

Ovaj vodič će vam pomoći da:

- Prepoznate suptilne znakove LotL napada
- Implementirate efikasne mere detekcije
- Razvijete proaktivni pristup odbrani
- Zaštitite kritične sistemske alate od zloupotrebe

Kome je namenjen vodič?

Vodič je kreiran za:

- IT administratore
- Security analitičare
- SOC timove
- Security inženjere

Spremni?
Hajde da krenemo sa prvim korakom - razumevanjem PowerShell aktivnosti i kako ih možemo efikasno pratiti.

Praćenje PowerShell aktivnosti

PowerShell je jedan od najčešće korišćenih alata u LotL napadima zbog svoje fleksibilnosti i mogućnosti izvršavanja skripti. Da biste identifikovali sumnjivu upotrebu PowerShell-a, pratite sledeće:

KLJUČNI INDIKATORI

✓ Izvršavanje bez logovanja

- Implementirajte obavezno logovanje svih PowerShell sesija
- Koristite Group Policy za forsiranje modula ScriptBlock Logging
- Postavite alerting za pokušaje isključivanja logovanja

✓ Neuobičajeno trajanje sesija

- Definišite baseline za prosečno trajanje PowerShell sesija
- Postavite automatske alerte za sesije koje prelaze definisane pragove
- Implementirajte automatsko prekidanje dugih sesija nakon revizije

✓ Obfuskacija komandi

- Implementirajte dekodiranje i logging base64 stringova
- Koristite AMSI (Anti-Malware Scan Interface) za analizu deobfuskovanih komandi
- Postavite pravila za blokiranje poznatih obrazaca obfuskacije

Monitoring WMI aktivnosti

WMI je često korišćen za prikupljanje informacija u mreži bez otkrivanja prisustva napadača. Da biste identifikovali anomalije:

PREVENTIVNE MERE

- **Kontrola WMI pristupa**
  - Ograničite WMI pristup samo na neophodne korisnike
  - Implementirajte whitelisting za WMI upite
  - Uspostavite baseline za normalne WMI operacije
- **Detekcija anomalija**
  - Koristite machine learning za prepoznavanje neuobičajenih obrazaca
  - Pratite povezanost WMI aktivnosti sa drugim sumnjivim događajima
  - Implementirajte real-time monitoring kritičnih WMI događaja

Ako sistem iznenada počne da šalje WMI zahteve na načine koji nisu deo standardnih operacija, to može biti znak napada.

Neobičan broj WMI poziva može ukazivati na pokušaje prikupljanja podataka ili daljinsko izvršavanje komandi.

Kontrola PsExec Aktivnosti

PsExec je alat za daljinsko upravljanje i izvršavanje komandi. Kako bi se detektovale maliciozne aktivnosti preporučuje se:

Ako PsExec dolazi sa mašina ili korisničkih naloga koji nisu admin, to može biti pokušaj lateralnog kretanja napadača.

Redovno pregledajte sve izvršne procese pokrenute putem PsExec-a, jer napadači mogu koristiti PsExec za preuzimanje kontrole nad uređajima.

BEZBEDNOSNE MERE

- **Striktna kontrola pristupa**
  - Ograničite PsExec na specifične admin naloge
  - Implementirajte whitelisting izvršnih lokacija
  - Uspostavite monitoring za lateralno kretanje
- **Procesna kontrola**
  - Pratite lanac procesa (process chain)
  - Implementirajte alerting za neuobičajene parent-child relacije
  - Koristite EDR rešenja za detaljnu analizu procesa

Monitoring korisničkog ponašanja

Jedan od ključnih aspekata odbrane protiv LotL napada je prepoznavanje promene u standardnim aktivnostima:

Ako admin nalozi pokreću operacije u neobično vreme ili pristupaju neuobičajenim resursima, to može biti signal kompromitacije.

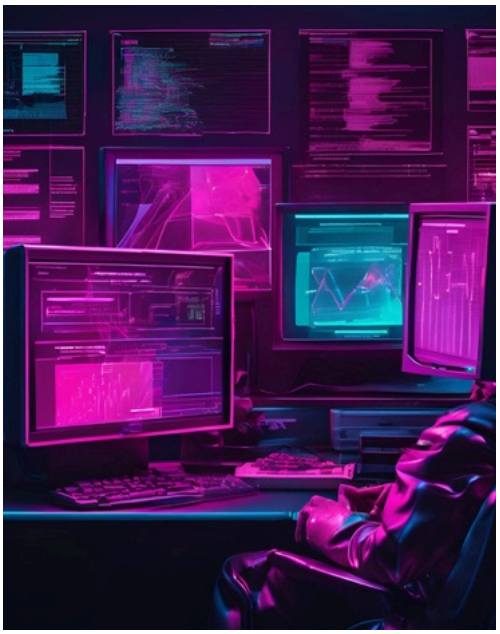
Pratite promene u privilegijama korisnika, jer napadači često eskaliraju svoje ovlašćenja pomoću legitimnih alata.

KLJUČNE OBLASTI PRAĆENJA

- **Analiza admin aktivnosti**
  - Uspostavite baseline normalnog ponašanja
  - Implementirajte vremensko ograničenje admin sesija
  - Koristite UEBA (User and Entity Behavior Analytics)
- **Upravljanje privilegijama**
  - Implementirajte Just-In-Time (JIT) privilegije
  - Pratite svaku promenu u privilegijama
  - Uspostavite workflow za odobravanje privilegija

Napredna analitika

Zbog prirode LotL napada, antivirusni i klasični sigurnosni sistemi često nisu dovoljni. Zbog toga je potrebno implementirati:



IMPLEMENTACIJA

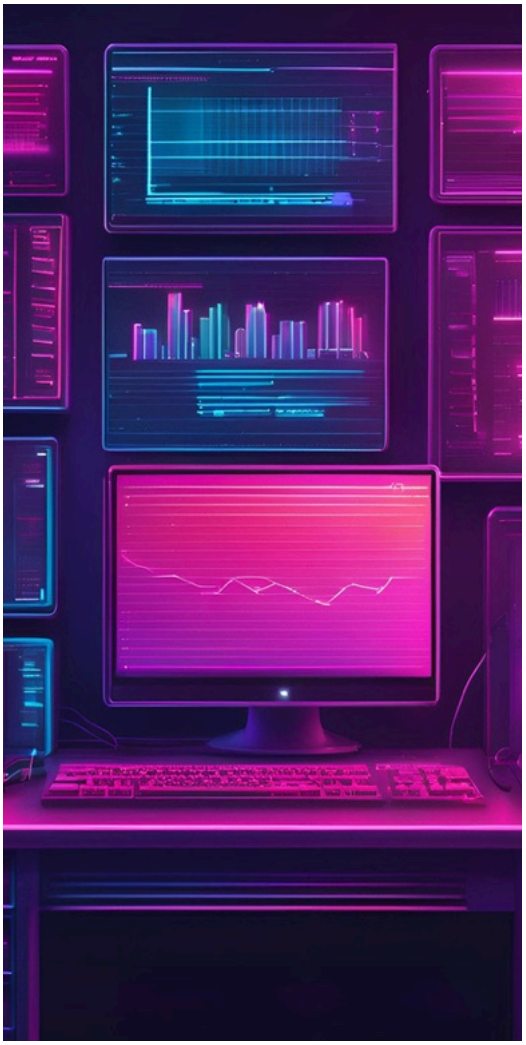
- ✓ **SIEM**
  - Centralizujte logove iz svih kritičnih sistema
  - Implementirajte korelaciona pravila
  - Uspostavite automatizovane response procedure
- ✓ **Bihejvioralna analiza**
  - Koristite machine learning za detekciju anomalija
  - Implementirajte threat hunting procedure
  - Uspostavite kontinuirano unapređenje detekcijskih pravila

Alati poput SIEM-a (Security Information and Event Management) mogu detektovati anomalije u uobičajenim procesima i radnim tokovima.

Ako neki alat počne da se koristi van svojih uobičajenih operativnih okvira, sistemi za detekciju anomalija mogu označiti ovu aktivnost kao potencijalno malicioznu.

Upravljanje logovima

Redovno analizirajte logove sistema kako biste prepoznali promene u pristupu resursima ili korišćenje alata u nepre-dviđenim kontekstima.



BEST PRACTICE

Centralizovano logovanje

- Implementirajte secure log forwarding
- Uspostavite retencione politike Osigurajte integritet logova
-

Automatizovana analiza

- Implementirajte automatsko parsiranje logova
- Koristite AI za prepoznavanje patterns of attack
- Uspostavite automatske response procedure

Bilo kakva iznenadna promena u šemama pristupa može ukazivati na malicioznu aktivnost.

Korišćenje legitimnih alata u neoče-kivanim kontekstima ili na čudnim lokacijama, može ukazivati na LotL napad.

Ključne Preporuke:

1. Implementirajte slojevitu zaštitu
2. Kontinuirano unapređujte detekcijske mehanizme
3. Automatizujte response procedure
4. Održavajte ažurnu dokumentaciju
5. Redovno trenirajte security tim

Living off the Land napadi zahtevaju sofisticirane strategije detekcije. Kako bi se oduprli napadima, IT timovi moraju koristiti kombinaciju analize logova, bihejvioralne detekcije, i stalnog nadzora nad korišćenjem alata kao što su PowerShell, WMI i PsExec.

Primenom ovih metoda, kompanije mogu značajno smanjiti rizik od neprimetnih LotL napada i zaštititi kritične sisteme od kompromitacije.

Budite korak ispred napadača

Kontaktirajte naš tim za procenu bezbednosti vašeg sistema i saznajte kako možemo pomoći u detekciji i sprečavanju LotL napada.

KONTAKT INFORMACIJE

NET++ TECHNOLOGY

+381-11-3699-967

office@netpp.rs

Otokara Keršovanija 11/39,
Beograd

RADNO VREME

Pon - Pet 8:00 - 16:00

www.netpp.rs

www.it-klinika.rs