Ofenzivna sigurnost

Operacije bliskog pristupa u kibernetičkom prostoru

Diego Mišetić, 22.12.2025

Pregled predavanja

- Motivacija
- Pitanja za ispite
- Osnovni koncepti i definicije
- Taksonomija operacija bliskog pristupa
- Primjeri iz prakse
- Izazovi i rizici
- Zaključak

Motivacija (1/2)

- Kritični sustavi su sve češće izolirani
- Udaljeni kibernetički napadi su često nemogući
- Bliski pristup je jedini način kompromitacije takvih meta
- Rast državnih/specijaliziranih napadača koji koriste fizički pristup
- Standardna kibernetička obrana ne pokriva ove prijetnje

Motivacija (2/2)

- Koristi
  - Bolje razumijevanje ranjivosti izoliranih sustava
  - Izrada obrane protiv fizičkih infiltracija
  - Predviđanje naprednih i nevidljivih napada
- Problemi
  - Potreban fizički pristup i složena izvedba
  - Teško prikriti aktivnosti i eksfiltrirati podatke

Pitanja za ispite

1. Što su kibernetičke operacije bliskog pristupa i kako se razlikuju od udaljenih operacija?
2. Koje tri komponente taksonomije operacija bliskog pristupa i koja je njihova uloga?
3. Koje sposobnosti moraju imati uređaji za infiltraciju u operacijama bliskog pristupa?
4. Koji su ključni tehnički i operativni izazovi u provedbi operacija bliskog pristupa?
5. Kako se organizacije mogu učinkovito braniti od operacija bliskog pristupa?

Osnovni koncepti

- Kibernetički napadi i kibernetičko iskorištavanje su dvije odvojene kategorije kibernetičkih operacija
- SIGINT metode su povijesni temelj za modernu fizičko-kibernetičku infiltraciju
- Ograničena primjenjivost udaljenih napada u fizički izoliranim sustavima
- Integracija fizičke sigurnosti, obavještajnog rada i kibernetičkih tehnika
- Implantati i kompromitirana oprema su sastavni dio suvremenih kibernetičkih operacija
- Infrastruktura fizički izoliranih sustava je ključna meta za operacije bliskog pristupa

SIGINT pozadina

- Povijesne infiltracije fizičkih objekata tijekom hladnog rata su pokretači modernih metoda
- Postavljanje prislušnih uređaja i manipulacija komunikacijskom opremom u operacijama obavještajnih službi
- Prijelaz s analognog prisluškivanja na digitalne nadzore i infiltracijske sustave
- Kontinuitet strategije usmjeren na kompromitaciju uređaja umjesto komunikacijskog kanala

Udaljene prema bliskim operacijama

- Udaljene operacije – skalabilne, niskog rizika, ali ovise o dostupnosti mreže
- Bliske operacije – fizički zahtjevnije, visokog rizika, ali jedine moguće za izolirane sustave
- Operacije bliskog pristupa su primarni način djelovanja nad fizički izoliranim i visoko zaštićenim sustavima
- Fizička blizina je preduvjet za pasivno nadziranje i manipulaciju uređaja
- Fizička blizina omogućuje pasivno presretanje, manipulaciju uređaja ili ubacivanje implantata
- Državni akteri preferiraju bliski pristup protiv meta visoke vrijednosti

Taksonomija operacija bliskog pristupa

- **Okruženje** - fizički prostor, elektroničke barijere, nadzorne mjere, protokoli pristupa
- **Entitet uređaja** - alati za pasivno presretanje, isporuku implantata i eksfiltraciju
- **Entitet pristupa** - operativci, dronovi, robotske platforme,...

Entitet uređaja (1/3) - Sustavi za presretanje

- Sustavi za pasivno presretanje bežičnih komunikacija i elektromagnetskih emisija
- Alati za analizu RF spektra i identifikaciju anomalnih signala
- Uređaji za aktivno kreiranje pristupnih točaka i manipulaciju protokolima
- Optički i akustični nadzorni sustavi za izvlačenje informacija iz fizičkog okruženja
- Sredstva koja omogućuju prikupljanje podataka bez izravnog kontakta s uređajem

Entitet uređaja (2/3) - Sustavi za isporuku

- Hardverski implantati ugrađeni u računalne komponente, periferije ili mrežnu opremu
- Prijenosni mediji s prilagođenom programskom opremom ili skrivenim modulima
- Oprema ubačena kroz opskrbni lanac prije instalacije u ciljnu infrastrukturu
- Sustavi dizajnirani za prisutnost uz minimalni energetski otisak

Entitet uređaja (3/3) - Sustavi za eksfiltraciju

- RF sustavi niske snage za bežični prijenos podataka iz izoliranih okruženja
- Optičke metode eksfiltracije putem modulacije svjetlosnih signala ili LED indikatora
- Akustične tehnike prijenosa informacija putem ultrazvučnog spektra
- Fizički prijenos podataka putem uklonjivih medija
- Hibridni modeli koji kombiniraju više kanala radi smanjena otkrivanja

Entitet pristupa (1/2) - Ljudi

- Operativci specijalizirani za infiltraciju visoko osiguranih objekata
- Insajderi s pristupnim ovlastima unutar ciljne infrastrukture
- Osoblje s legitimnim razlogom ulaska
- Metode prikrivenog ulaza i izbjegavanja nadzornih sustava
- Visoka razina rizika i potreba za koordiniranim djelovanjem s tehničkim timovima

Entitet pristupa (2/2) - Uređaji

- Mehanički pristup temeljen na autonomnim platformama
- Dronovi kao primarno sredstvo za blisko pozicioniranje bez ljudske prisutnosti
- Statični nadzorni moduli koji su postavljeni u blizini cilja
- Platforme posebno pogodne u lokacijama s visokim fizičkim nadzorom

Hibridni model pristupa

- Kombinirano korištenje ljudskih operativaca i mehaničkim platformama
- Ljudski operativci postavljaju uređaje, a zatim se povlače
- Uređaji preuzimaju dugotrajni nadzor
- Niži operativni rizik uz visoku učinkovitost
- Model čest u operacijama visokovrijednih ciljeva

Izazovi i rizici

- Fizički pristup zahtjeva visoku koordinaciju i planiranje
- Ograničen pristup lokacijama (pogotovo s nadzorom)
- Tehnička složenost implantata i njihovog postavljanja
- Zahtjev za minimalnom vidljivošću
- Detekcija i izbjegavanje sigurnosnih sustava
- Ovisnost o okruženju i arhitekturi cilja
- Visoki operativni rizik zbog fizičke blizine cilja
- Mogućnost kompromitacije operativaca
- Otkriće implantata tijekom sigurnosnih pregleda
- Detekcija signala
- Operativni tragovi

Obrambene mjere

- Poboljšanje fizičke sigurnosti
- Sustavna inspekcija opreme
- Detekcija anomalnih signala
- Jačanje sigurnosti opskrbnog lanca
- Kontrola pristupnih točaka
- Edukacija osoblja

Zaključak

- Operacije bliskog pristupa kombiniraju fizički pristup i kibernetičke tehnike
- Fizički izolirani sustavi ostaju ključna meta ovakvih operacija
- Razumijevanje pristupa, uređaja i kompromisnih točaka ključno je za obranu
- Tehnički zahtjevne i rizične operacije

Literatura

- **Villalon-Huerta, Antonio, Ismael Ripoll-Ripoll, and Hector Marco-Gisbert. „A survey and characterization of Close Access Cyberspace Operations.” International Journal of Information Security 23.2 (2024): 963-980**
- K. Zetter, „Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon”, 2014
- M. Guri, „Air-Gap Covert Channels”

Hvala!