INFOSTEALERJI

Aktualna kibernetska grožnja

Programska oprema, ki prikrito krade poverilnice, piškotke in druge občutljive podatke iz računalniških sistemov.

Our Space Appliances d.o.o.

Kazalo

Povzetek za vodje

Infostealerji so zlonamerna programska oprema, namenjena kraji občutljivih podatkov iz naprav — predvsem uporabniških imen in gesel, piškotkov brskalnikov, kriptodenarnic, vsebin datotek, konfiguracij VPN odjemalcev in drugih poverilnic. V zadnjih letih so ti programi doživeli eksplozivno rast zaradi dostopnosti (malware-as-a-service), nizkih stroškov ter velike potencialne koristi za napadalce (preprodaja poverilnic, podpora pri ransomware-u, BEC – business email compromise).

Ta whitepaper obravnava: tehnično delovanje infostealerjev, kanale distribucije, vzorce zbiranja podatkov, vpliv na podjetja, praktične in tehnične metode zaznave in mitigacije ter priporočila za tehnične in organizacijske ukrepe.

Oktober 2025
Our Space Appliances d.o.o.

Kaj so **infostealerji?**

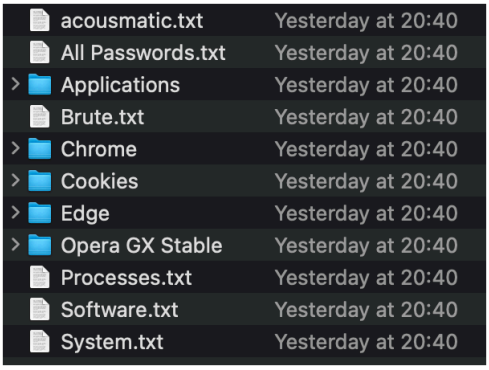
Aktualna kibernetska grožnja

Infostealerji niso novo tveganje, a so postali ključno orodje sodobnih kibernapadalcev zaradi svoje učinkovitosti pri pridobivanju poverilnic, dostopa do računov in pridobivanju surovih podatkov, ki jih je mogoče takoj monetizirati ali pa uporabiti kot vhodno točko za naprednejše napade (ransomware, lateral movement, BEC). Za organizacije, še posebej tiste, ki uporabljajo delovno okolje z mešanico osebnih in službenih naprav, predstavljajo visoko stopnjo tveganja.

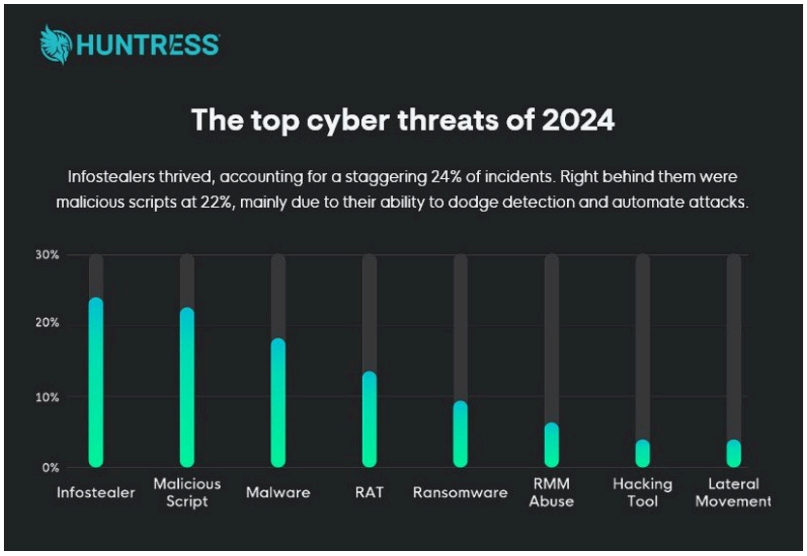
Infostealerji so programi, ki se lahko na videz obnašajo kot legitimna aplikacija, v ozadju pa prikrito zbirajo podatke. Njihova glavna značilnost je usmerjenost v zbiranje (krajo) informacij, v nasprotju z izsiljevalsko programsko opremo (ransomware), ki šifrira podatke ali trojanskimi konji, ki omogočajo oddaljeno upravljanje s sistemom.

Tarče infostealerjev:

- Brskalniki: shranjena gesla, piškotki, zgodovina brskanja, autofill podatki.
- Kriptodenarnice: datoteke wallet.dat in seed fraze.
- VPN in RDP poverilnice: konfiguracijske datoteke in shranjeni ključi.
- FTP/SFTP odjemalci: poverilnice za dostop do strežnikov.
- E-poštni odjemalci: shranjena gesla e-mail računov.
- Datoteke in dokumenti: .xls(x), .doc(x) ali .txt z občutljivimi podatki.



Primer strukture zbranih podatkov



Vir: Huntress 2025 Cyber Threat Report"

- **Infostealer je prva faza napada**

  Infostealer je lahko prva faza resnega napada na organizacijo.

- **Kraja identitete**

  Ukradene poverilnice in piškotki napadalcem omogočijo nepooblaščen dostop do sistemov.

- **Monetizacija**

  Ukradene poverilnice in ostali podatki se običajno prodajajo na temnem spletu za nekaj EUR.

Trg infostealerjev

Velik porast v zadnjih letih

Vir: https://www.infostealers.com

Raziskava projekta Brimsec je pokazala, da je bilo v Sloveniji okuženih 15.500 naprav.

Razlogi za veliko porast infostealerjev

1. Malware-as-a-service:

Napadalci lahko najamejo Infostealerje in pripadajočo infrastrukturo z minimalnim tehničnim znanjem. Mesečna naročnina znaša od 200 dolarjev dalje.

2. Avtomatizacija in učinkovitost

Programska oprema izvaja krajo piškotkov, shranjenih gesel v brskalnikih in datotekah. Vsi zbrani podatki se samodejno zapakirajo in posredujejo na upravljavski (C2) strežnik.

3. Nizki stroški širjenja

Infostealerji se najpogosteje širijo s pomočjo phishing sporočil, lažnega oglaševanja in nelegalne programske opreme.

4. Slaba ozaveščenost

O napadih z izsiljevalsko programsko opremo lahko vsakodnevno beremo v dnevnem časopisju. Phishing sporočila nas bombandirajo na vsakem koraku. Premalo pa je govora o infostealerjih in njihovih posledicah.

Neuspešno razbijanje kriminalnih združb

Poročila varnostnih podjetij kažejo na to, da so nekatere družine — kot so RedLine, Vidar, Raccoon, Lumma in novejše kot Poseidon ali ACRStealer — zelo razširjene. Mednarodne organizacije so v preteklih letih pristopile k organiziranemu razbijanju organiziranih kriminalnih združb, ki upravljajo infostealer projekte, a Lumma stealer se je nekaj tednov po uradnem razbitju ponovno pojavil.

Delovanje infostealerja

Tehnična anatomija

1. Okužba

Naprava žrtve se okuži preko:

- Phishing e-poštnih sporočil z zlonamernimi priponkami ali povezavami.
- Lažnih programskih "crackov" ali goljufivih programov (cheatov).
- Zlonamernih oglasov (malvertising).
- Fake CAPTCHA.
- Kompromitiranih spletnih strani, ki ponujajo prenose.
- Samodejnih prenosov (drive-by downloads) preko "exploit" kitov ali lažnih posodobitev brskalnika ...

2. Izvedba

Ob zagonu infostealerja:

- Infostealer teče v ozadju.
- Aktivira mehanizme za persistenco (samodejni zagon, sistemski register...)
- Cilja določene aplikacije (npr. brskalnike, klepetalnike, kriptodenarnice, upravljalnike gesel).
- Pobira shranjene poverilnice, sejne piškotke, samodopolnitve obrazcev in zgodovino obiskov spletnih strani.

3. Eksfiltracija

Zbrane podatke posreduje iz sistema

- Pridobljene podatke zapakira in pošlje na strežnik napadalca za ukazovanje in nadzor (C2), Telegram bota ali Steam platforme.
- Podatki se pogosto prodajo na temnem spletu, telegram kanalih ali pa jih uporabijo za širjenje infostealerjev.
- Pogosto se infostealer po eksfiltraciji pobriše.

4. Zloraba informacij

Informacije se uporabijo za

- Dostop do korporativnih sistemov (kar vodi do razkritja podatkov, namestitev izsiljevalske zlonamerne programske opreme).
- Prevzem elektronske pošte, oblačnega shranjevanja ali razvojnih portalov.
- Izvedbo prevar, prevzemov identitete ali za nadaljnjo namestitev zlonamerne programske opreme.

Kraja, ki je ne opazimo

Žrtev napada z izsiljevalsko programsko opremo o tem nedvoumno izve, ko kmalu po uspešnem napadu ne more dostopati do svojih datotek. Žrtev infostealerja pa o odtujitvi občutljivih informacij včasih še dolgo ne izve. Sumljivi indici so lahko avtentikacije iz nenavadnih lokacij in ob nenavadnih urah.

Žrtve in posledice

Profil okužene osebe iz Slovenije*

- Moški, starost med 15 in 25 let.
- Okužba z infostealerjem preko “cracka” ali “cheata” za igrico.
- Igralec igric (Steam, Riot Games, Roblox, Ubisoft Connect …).
- Uporabnik socialnih omrežij (Discord, Facebook, Instagram …).
- Slaba kakovost gesel, ponavljajoča se gesla.

Posledice za souporabnike sistema

Ne le, da je infostealer pridobil občutljive podatke uporabnika, ki se je okužil, pridobil je tudi podatke iz drugih uporabniških profilov / računov na istem sistemu. V primeru družinskega računalnika so to lahko dostopi do spletnih bank staršev, partnerjev ipd.

Posledice za organizacijo

Pogosto se zgodi, da sodelavci v spletnih brskalnikih hranijo gesla in imajo omogočeno sinhronizacijo brskalniškega profila v oblak. Ta profil zaradi priročnosti aktivirajo tudi na domačem računalniku. V primeru, da se na domačem računalniku požene infostealer, bodo nepridipravi pridobili poverilnice za dostop do organizacijskih storitev.

Kaj bi moral početi vsakdo?

- Skrb za osnovno informacijsko higieno.
- Uporaba opreme za zaščito končnih točk.
- Uporaba namenskega upravljalnika gesel.
- Težnja k uporabi večfaktorske avtentikacije, kjer je le mogoče.
- Prenosi datotek le iz zaupanja vrednih virov.
- Uporaba preverjene (in legalne) programske opreme.
- Redno posodabljanje sistemov (in brskalnikov).
- Preudarnost pri uporabi vtičnikov v spletnih brskalnikih.

* raziskava projekta Brimsec

Zaznavanje in preprečevanje

Tehnološki pristopi za boj proti infostealerjem

EDR

Uporaba EDR (Endpoint Detection and Response) rešitev je ključna pri obrambi pred infostealerji. EDR rešitve lahko spremljajo in analizirajo delovanje aplikacij in procesov na napravah. Njihova naloga je (tudi) zaznavanje in preprečevanje aktivnosti infostealerjev kot so poizkus deaktivacije varnostnih mehanizmov, poganjanje skript, iskanje občutljivih podatkov in prenos podatkov na upravljavske (C2) strežnike.

EDR rešitve pogosto vključujejo sezname znanih distribucijskih in komunikacijskih točk nezaželene programske opreme. Komunikacijo s takšnimi entitetami preprečujejo.

SIEM

Dobra implementacija SIEM rešitve lahko zazna infostealer na sistemu in nas obvesti o anomaliji še preden se podatki pojavijo na podzemnih kanalih.

Na podlagi podatkov o procesih lahko spremljamo ali so se na sistemih pojavili vzorci aktivnosti, ki so značilni za infostealerje. Zaznavamo lahko tudi komunikacijo sistemov z entitetami iz seznamov groženj.

Hkrati pa lahko spremljamo tudi spremembe v dinamiki ali izvoru avtentikacij uporabnikov. V primeru, da pride do porasti avtentikacij (po možnosti iz tujine) je to lahko indikator, da je bil uporabnik žrtev infostealerja.

Nadzor poverilnic

Rešitev za nadzor nad poverilnicami nam omogoča, da smo o nelegalno pridobljenih poverilnicah naših uporabnikov obveščeni takoj, ko se te pojavijo na temnem spletu ali drugih kanalih za prekupčevanje s poverilnicami.

Takšne rešitve brez prestanka skenirajo temni splet, telegram kanale in ostale vire. Pogosto se ponudniki infiltrirajo tudi v podzemne skupnosti, za katere ve le malokdo.

Tovrstno alarmiranje nam omogoča zmanjševanje škode v primeru neljubega dogodka. Takoj, ko poverilnice zaznamo, moramo računu zamenjati geslo, preklicati vse sejne piškotke in preveriti zgodovino avtentikacij. Vsekakor pa moramo o tem obvestiti tudi žrtev.

A pri obrambi ne pozabimo na človeški požarni zid!

Še tako dobrim tehnološkim rešitvam zmanjka sape, če je varnostna kultura v organizaciji postranskega pomena.

Priporočljivi ukrepi za organizacije v boju proti infostealerjem

- Gradnja varnostne kulture mora biti ena izmed prioritet sodobnih organizacij.
- Redno izvajanje ozaveščanj.
- Prepoved hranjenje gesel v brskalnikih in uvedba namenskih upravljalnikov gesel.
- Prepoved sinhronizacije brskalniških uporabniških profilov med napravami.
- Upravljanje ranljivosti in skrb za redno posodabljanje programske opreme.
- Sledenje principu najnižjih pravic in skrb za utrjevanje (hardening) sistemov.
- Uvedba tehničnih ukrepov.

OUR SPACE APPLIANCES

Vaš partner v boju proti infostealerjem

Zavedamo se resnosti grožnje, ki jo predstavljajo infostealerji. V naši ponudbi lahko najdete nekaj rešitev, ki vam bodo pomagale v boju proti infostealerjem.

- **SIEM: Splunk Enterprise Security**

  Od leta 2013 smo partnerji podjetja Splunk, kjer smo se specializirali za implementacijo SIEM rešitve Splunk Enterprise Security. Na slovenskem trgu nam je implementacijo in vzdrževanje Splunka zaupalo že več kot 20 organizacij.

- **Rešitve za nadzor ukradenih poverilnic**

  Smo pooblaščeni partner za prodajo rešitev podjetja RecordedFuture, ki nudi različne pakete informacij o grožnjah. Med njimi tudi informiranje o zaznanih ukradenih poverilnicah.
  Vključeni pa smo tudi v razvoj slovenske rešitve za nadzor nad ukradenimi poverilnicami Brimsec.

- **Rešitve za zaščito končnih točk**

  V naboru rešitev, ki jih nudimo, so tudi različne rešitve za zaščito končnih točk.

- **Upravljanje ranljivosti**

  Za upravljanje ranljivosti v vaši organizaciji lahko poskrbimo s priznano rešitvijo Rapid7 InsightVM. Ta nudi celovit in kontinuiran pristop k upravljanju ranljivosti in ni namenjena zgolj enkratnemu iskanju ranljivosti.

- **Izvajanje usposabljanj in ozaveščanj o kibernetski varnosti**

  Naši izkušeni sodelavci z žarom v očeh predavajo na usposabljanjih o kibernetski in informacijski varnosti. Da vsebina ni suhoparna, jo predstavijo na realnih primerih. Držimo pa se načela, da usposabljanja izvajamo le v živo, saj je učinek takšne delavnice bistveno večji.

Our Space Appliances d.o.o.

Stegne 11c, 1000 Ljubljana
email: info@ourspace.si | web: www.ourspace.si
telefon: 01 8100343

Our Space Appliances
I Enostavno obvladovanje podatkov I