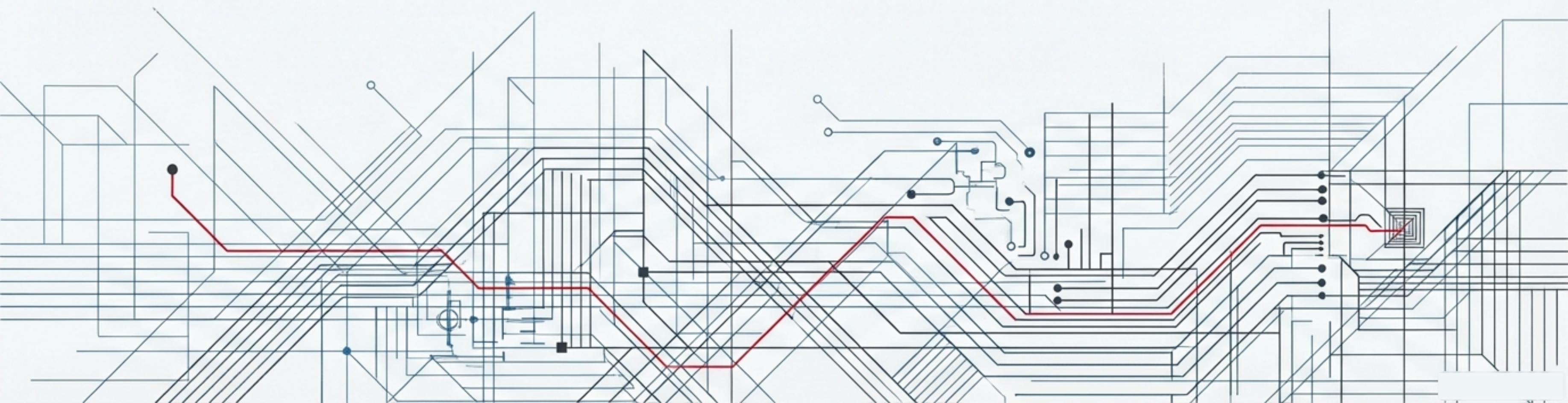


Atakos Anatomija

Išsami „Užkrečiamo Interviu“ kampanijos analizė

Kaip Šiaurės Korėjos programišiai paverčia „LinkedIn“ darbo pasiūlymus sudėtinga tiekimo grandinės ataka, nukreipta prieš programuotojus.



**Tai nebuvo pavienis incidentas.
Tai buvo platus masto operacija.**

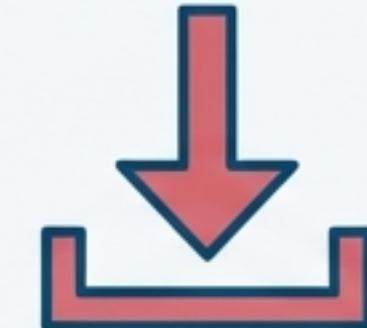
338

Kenkėjiški npm paketai,
sukurti ir išplatinti.



50,000+

Kartu šie paketai buvo
atsisiųsti programuotojų
visame pasaulyje.



Priešas ir jo taikinys: valstybės remiamas tikslumas



Veikėjas

Kas: Šiaurės Korėjos valstybės remiami grėsmių veikėjai.

Tikslas: Infiltruotis į sistemas, kuriose tikėtina rasti vertingus prisijungimo duomenis, privačius raktus ir kitas paslaptis, kurias galima paversti pinigais.

Taikinys

Kas: Web3, kriptovaliutų ir „blockchain“ programuotojai.

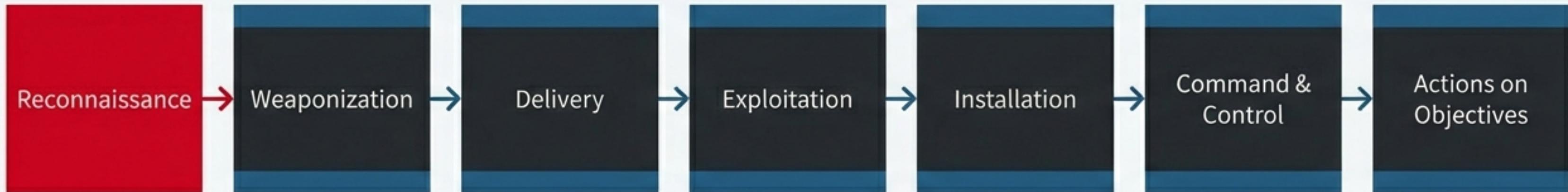
Kodėl: Didelės vertės asmenys, turintys prieigą prie finansinės infrastruktūros ir decentralizuotų sistemų.

Atakos dekonstravimas pagal „Cyber Kill Chain“ metodiką

Norėdami suprasti šios sudėtingos operacijos eiga, naudosime „Lockheed Martin Cyber Kill Chain“ modelį. Kiekvienas etapas atskleidžia skirtinę puolėjų taktiką ir mūsų galimybes apsaugoti.



1 etapas: Žvalgyba – auka stebima professionalioje aplinkoje



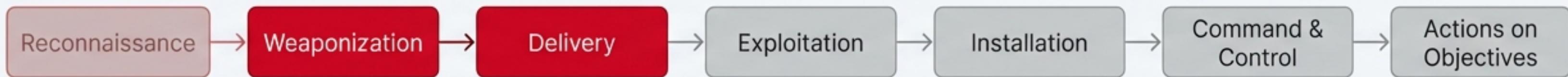
Vardas Pavarde
Profesionalus Pareigos

Skills

Java Python Web3 Cloud Computing Blockchain
Machine Learning Cryptocurrency Wallets
Data Analysis Solidity

- Puolėjai apsimeta įdarbinimo specialistais arba samdančiais vadybininkais „LinkedIn“.
- Jie kruopščiai analizuoją potencialių aukų profilius, ieškodami specifinių techninių įgūdžių ir patirties.
- Atranka vykdoma pagal sąsajas su kriptovaliutų pininėmis, „blockchain“ infrastruktūra ir Web3 aplikacijomis.

2 etapas: Jaukas – „Užkrečiamas Interviu“



HR Recruiter

Exclusive Job Opportunity - Technical Lead

Hello [Name],

We were impressed by your profile and would like to invite you to a **technical assessment** for the Technical Lead role. This is an exciting opportunity to join our innovative team.

Please complete the **technical assessment** as soon as possible. You will need to **install** the required packages using '**npm install**' to run the test environment. We look forward to your submission.

Best regards,
The Recruitment Team

- Su potencialia auka susiekiama su patraukliu darbo pasiūlymu.
- Proceso dalis – **techninė užduotis arba kodo testas**, kuriam reikia įdiegti specifines priklausomybes („dependencies“).
- Ši užduotis sukuria **pretekstą ir skubos jausmą**, priverčiantį programuotoją greitai įvykdysti „npm install“ komandą.

3 etapas: Ginklas – „Typosquatting“ ir npm ekosistemos išnaudojimas



Legitimate		Malicious
express	→	epxre _{so}
express	→	epxre _{sso}
express	→	epxre _{ssoo}
dotenv	→	dote _{vn}
body-parser	→	bo _b y_parser

Taktika

Kenkėjinių paketų yra užmaskuoti kaip populiarū, kasdien naudojamų bibliotekų versijos su nedidelėmis rašybos klaidomis.

Psichologija

Ataka išnaudoja techninių interviu metu kylančį spaudimą ir laiko trūkumą, kai kandidatai linkę neatidžiai tikrinti įdiegiamų paketu pavadinimų.

4 etapas: Vykdymas – nuo tiesioginių paleidiklių iki užšifruotų operacijų



Evoliucija



Dabartinė Karta

Užšifruoti paleidikliai

HexEval
technika

XORIndex
technika

Tikslas

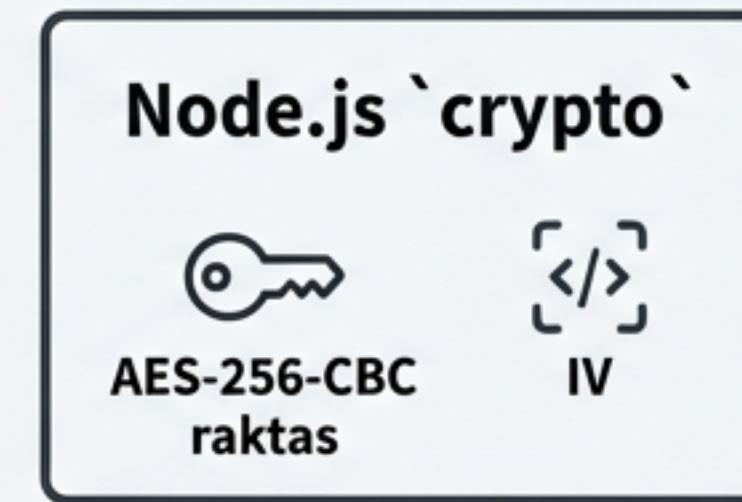
Vengti statinės analizės ir tradicinių saugumo įrankių aptikimo.

Techninė analizė: Užšifruoto paleidiklio veikimo principas

1. Talpykla



2. Iššifravimas



3. Vykdymas

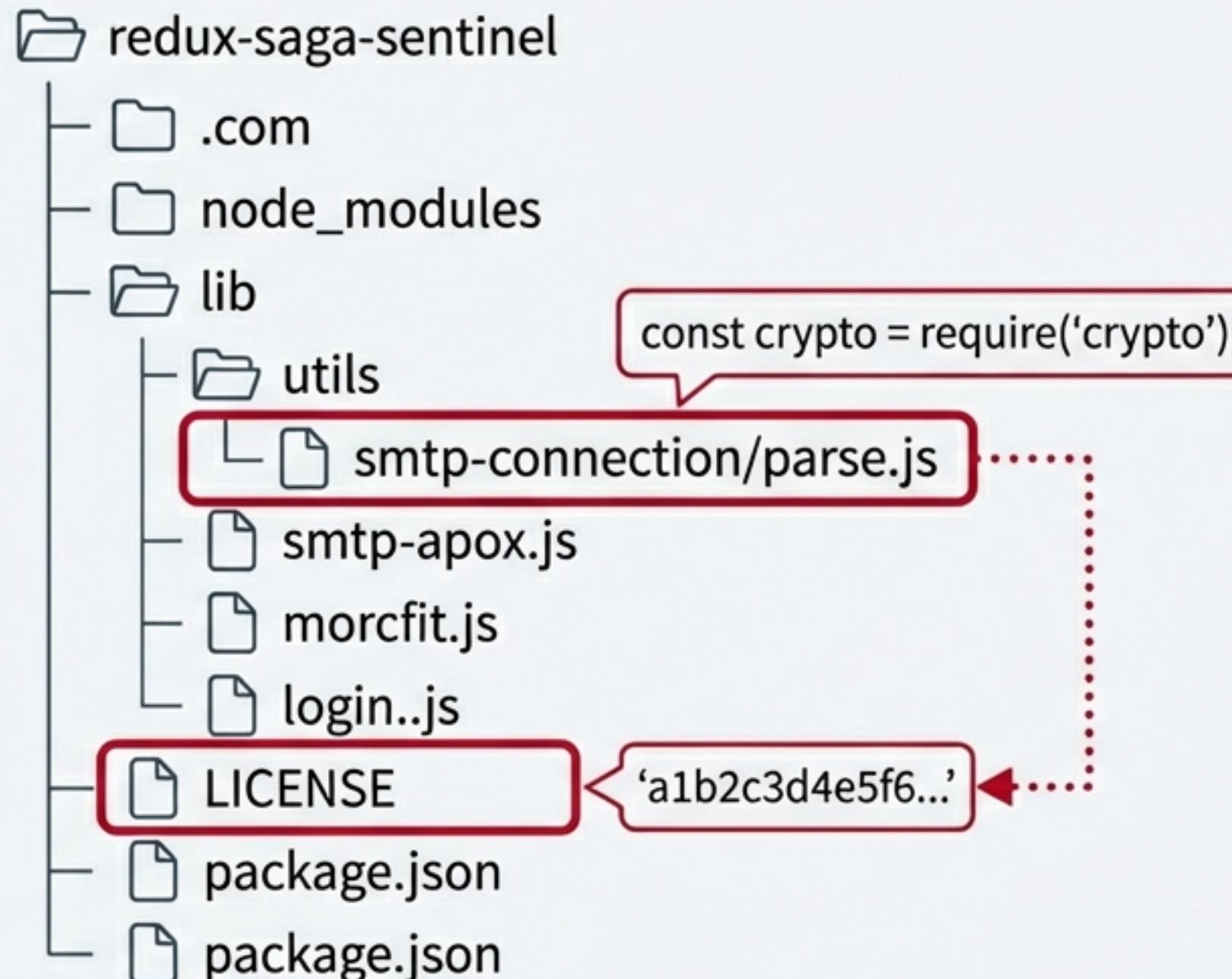


Užšifruotas kenkėjiskas kodas (payload) yra paslėptas nekenksmingai atrodančiuose failuose, pavyzdžiui, 'LICENSE' dokumente.

Vykdymo metu paleidiklis naudoja Node.js `crypto` funkcijas su koduotais AES-256-CBC raktu ir inicializacijos vektoriumi (IV) tam, kad iššifruotų kodą.

Iššifruotas kodas yra atkuriamas ir vykdomas tiesiogiai kompiuterio atmintyje ('in-memory'), nepaliekant jokių pėdsakų diske, kuriuos galėtų aptikti antivirusinės programos.

Atvejo studija: `redux-saga-sentinel` paketo analizė



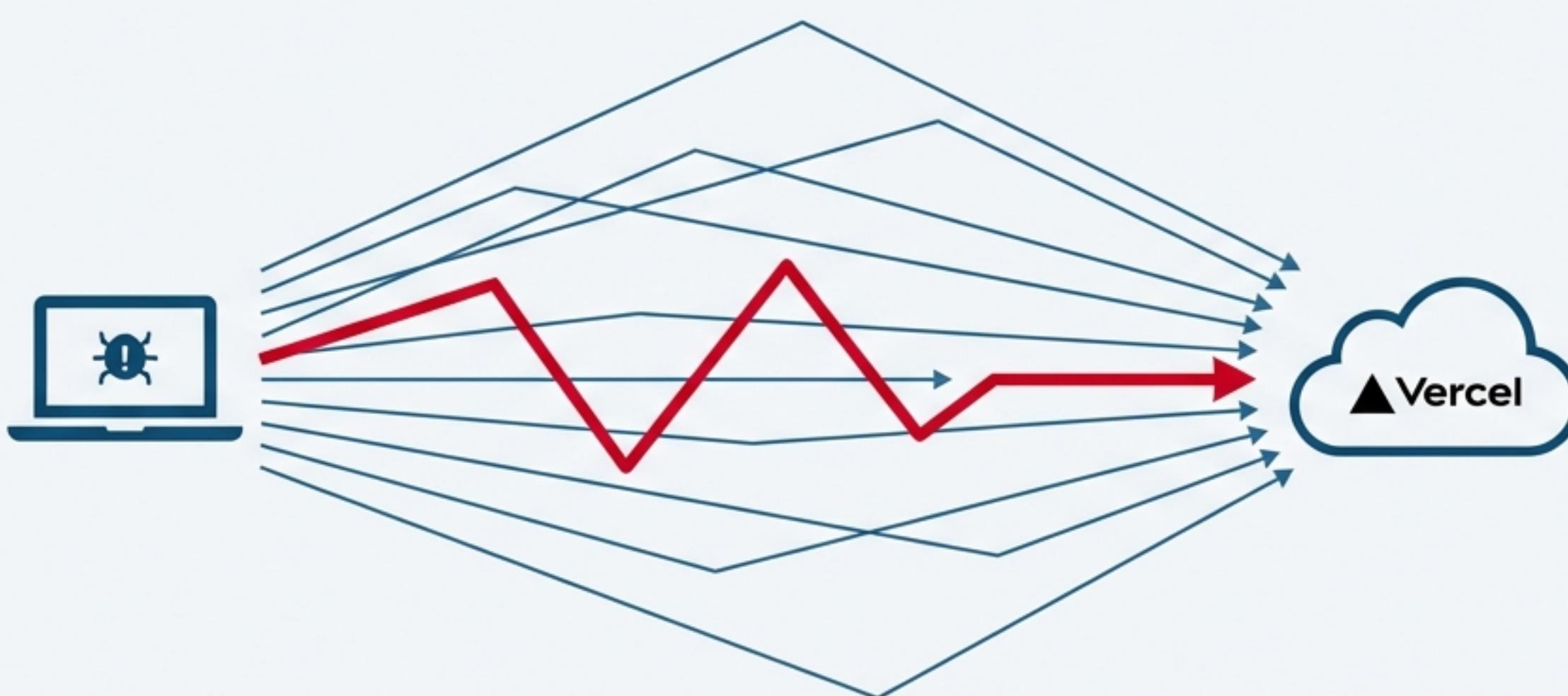
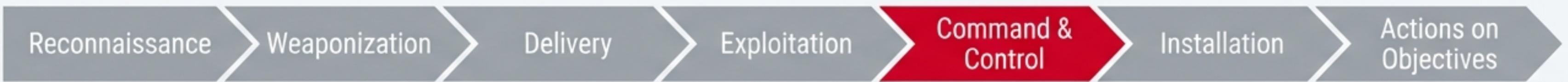
Išskaidyta logika

Siekiant išvengti aptikimo, iššifravimo logika yra išskaidyta per kelis failus tame pačiame pakete.

Rezultatas

Vykdymo metu kodas surenkamas, iššifruojamas ir atkuria antrojo etapo užmaskuotą (obfuscated) JavaScript kodą.

5 etapas: Valdymas ir kontrolė (C2) – pasislėpus minioje



Komunikacijos kanalas

Atkurtas kenkėjiškas kodas užmezga ryšį su puolėjų valdymo ir kontrolės (C2) serveriu per standartinius HTTP/HTTPS protokolus.

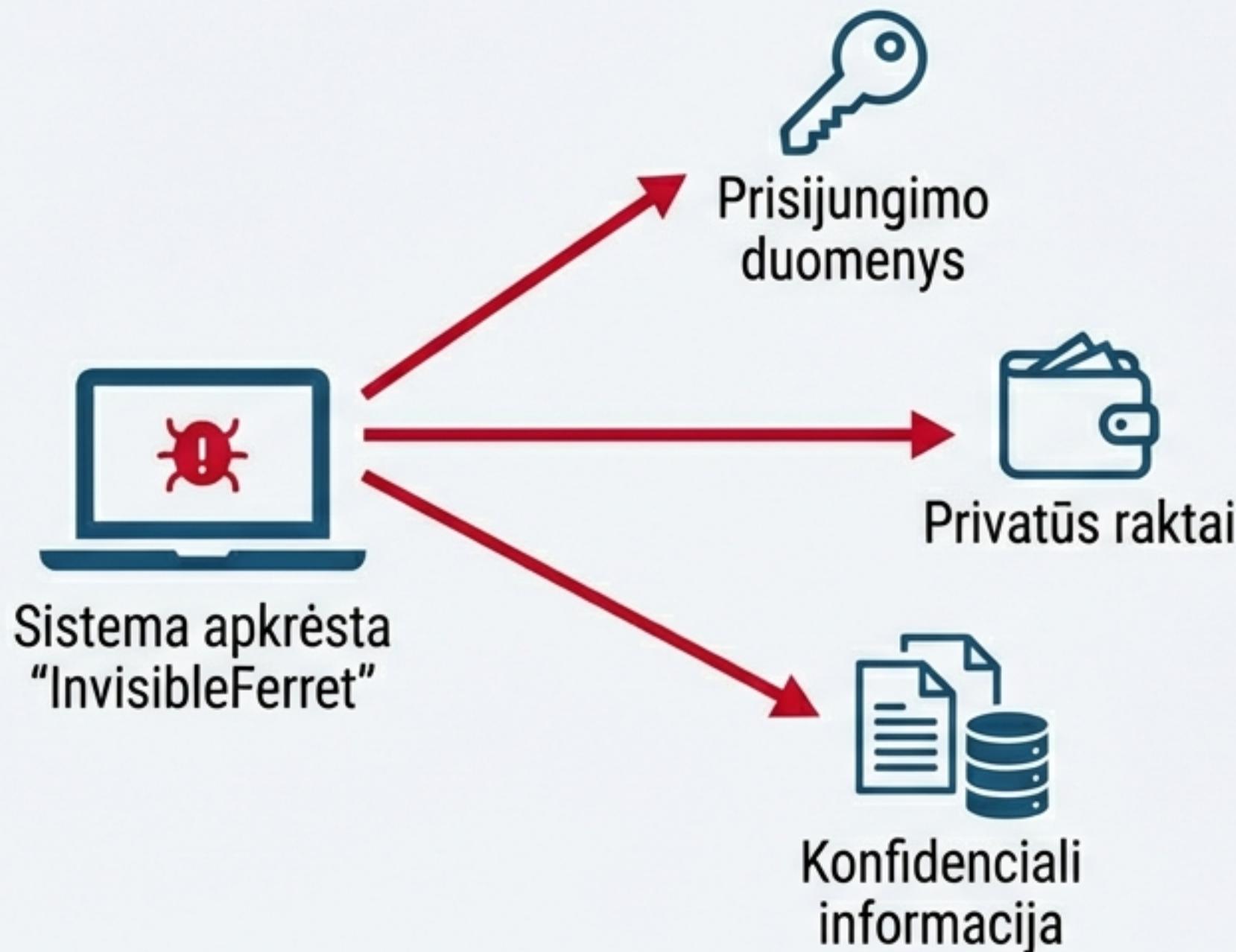
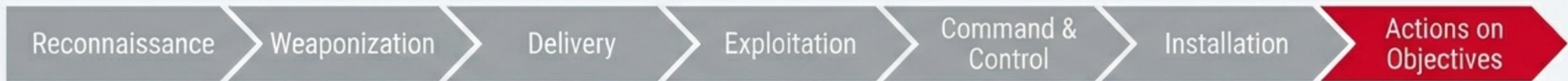
Maskavimosi technika

C2 komunikacijai dažnai naudojamos teisėtos prieglobos platformos, pavyzdžiui, „Vercel“.

Poveikis

Šis metodas leidžia kenkėjiškam srautui susilieti su įprastu programuotojų veiklos srautu, todėl jį ypač sunku aptikti tinklo stebėjimo įrankiais.

6 etapas: Tikslas – nuolatinė prieiga ir vertybių vagystė



Ilgaliaikė prieiga (Persistence)

Užmezgus C2 ryšį, sistema dažniausiai apkrečiama „InvisibleFerret“ „backdoor“ programa, kuri užtikrina nuolatinę prieigą prie pažeistos sistemos.

Galutinis tikslas

- Ieškoti ir vogti prisijungimo duomenis.
- Nuskaityti privačius raktus nuo kriptovaliutų piniginių.
- Rinkti bet kokią kitą konfidentialią informaciją, kurią galima paversti pinigais.

Grėsmės Indikatoriai: Kaip atpažinti „Užkrečiamą Interviu“



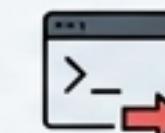
Socialinė inžinerija



Netikėti darbo pasiūlymai per „LinkedIn“, ypač susiję su Web3/kripto sritimi.



Techninės užduotys



Prašymai įdiegti specifinius npm paketus skubiam kodo testui.



Paketų pavadinimai



Atidus priklausomybių pavadinimų tikrinimas ieškant „typosquatting“ klaidų (`epxreso` vietoj `express`).



Neįprasti failai



Kenkėjiškas kodas, paslėptas netikėtose vietose, pavyzdžiui, `LICENSE` failuose.



Tinklo srautas



Neaiškus arba netikėtas ryšys su teisėtomis hostingo platformomis (pvz., „Vercel“) diegimo proceso metu.

Tiekimo grandinė yra naujasis frontas

„Užkrečiamo Interviu“ kampanija yra ryškus pavyzdys, kaip profesionalūs socialiniai tinklai ir atviro kodo ekosistemos tampa pagrindiniai valstybių remiamų kibernetinių operacijų taikiniai. Pasitikėjimas, kuriuo remiasi programuotojų bendruomenė, yra paverčiamas ginklu. Atidumas diegiant kiekvienu priklausomybę tampa nebe geriausia praktika, o būtinybė.

