EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ZLONAMERNA PROGRAMSKA KODA (ANG. MALWARE)

VSEBINA

Kaj je zlonamerna programska koda.

Vrste zlonamerne kode.

Vrste zlonamerne kode in kako se vnese v sistem in kako deluje.

Zaščita pred napadom.

ZAKAJ GOVORIMO O ZLONAMERNI PROGRAMSKI KODI?

Večina incidentov vključuje zlonamerno programsko kodo (ang. malware)

Finančni in poslovni vplivi

Taktično–strateška grožnja

Vir: https://euro-systems.co.uk/news/what-is-the-difference-between-a-virus-and-malware/

KAJ JE ZLONAMERNA PROGRAMSKA KODA?

Vir: https://www.malwarebytes.com/malware

Zlonamerna programska koda je programska koda, namenoma ustvarjena za:

- škodovanje sistemom, podatkom ali uporabnikom,
- nepooblaščen dostop ali prevzem nadzora,
- povzročanje motenj, sabotaže ali finančne škode.

KAKO DELUJE?

1. Prenos okuženih datotek ali aplikacij
2. Neželena e-pošta
3. Zlonamerne spletne strani
4. Slabo zaščitene naprave in ranljivosti
5 Omrežni napadi

ZAKAJ USPEVA?

Previsoki privilegiji v organizaciji

Uporabniki imajo pogosto admin pravice — nepotrebno.

Zlahka prevzame celoten sistem ali AD.

Slabo segmentirani privilegiji omogočajo hiter preboj po omrežju.

Nezakrpane ranljivosti

Veliko organizacij še vedno zakasni posodobitve za 30–90 dni.

Napadalci aktivno zlorabljajo CVE ranljivosti v nekaj urah po objavi.

VPN, požarne pregrade (ang. Firewalli), izmenjeve dokumento (ang. Exchange) so med najpogostejšimi točkami vstopa.

Kompleksna in slabo segmentirana omrežja

Sistemi + OT + IoT → velika površina napada.

Ko malware vstopi, se brez segmentacije hitro širi.

Napadalec najde „najšibkejše vozlišče“ in gre dalje.

Človeški faktor (lažna e-pošta + socialni inženiring)

91 % uspešnih vdorov se začne s klikom na lažno e-pošto.

Napadi so izjemno prepričljivi (MFA fatigue, Direktorska(CEO) prevara, lažna IT-supp).

Uporabniki pogosto kliknejo preden preverijo.

USPEVA TUDI ZARADI:

01

Dobavna veriga in nezavarovane naprave

02

Zlonamerne posodobitve, lažni mobilni APK-ji.

03

IoT naprave (kamere, senzorji) pogosto brez gesel ali posodobitev.

04

Napadalec lahko preko ene naprave okuži celotno omrežje.

TER…

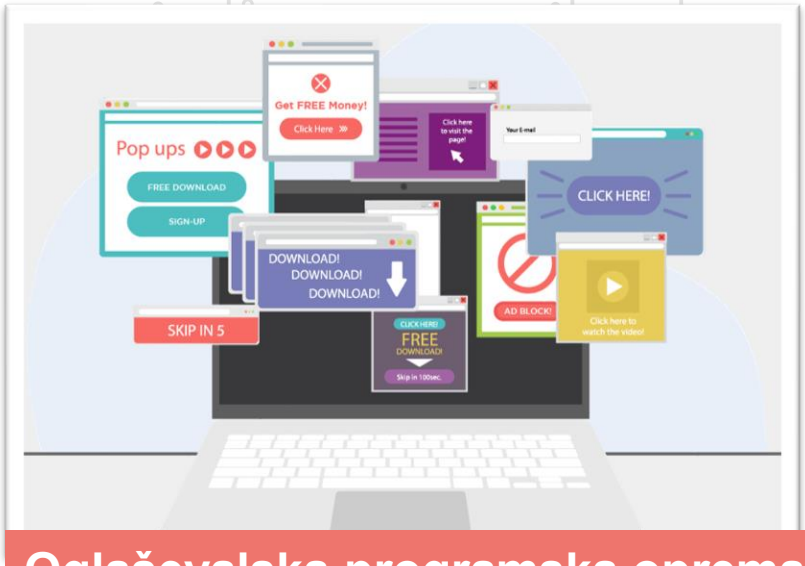
Nezadostna detekcija (EDR/XDR ni povsod)

Veliko organizacij se še vedno zanaša na klasični antivirus.

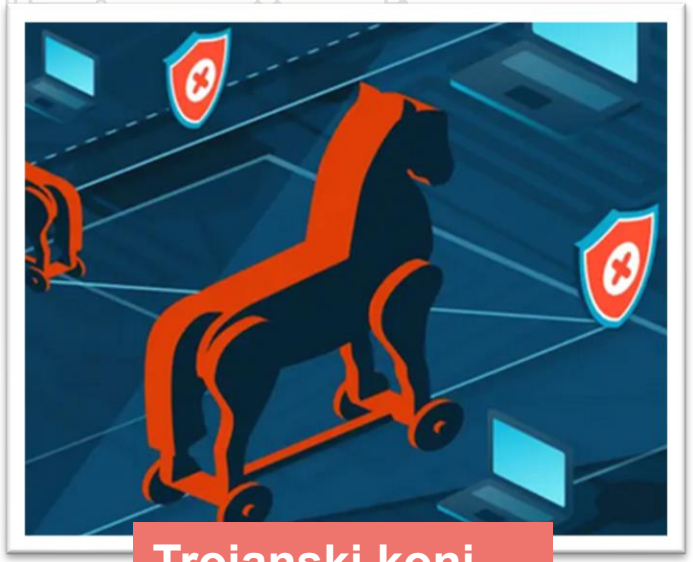
Napad brez datotek (ang. Fileless), PowerShell-based in RAM-only napadi se ne zaznajo.

Zelo malo podjetij spremlja **abnormalno vedenje** (ang. behavioral detection).

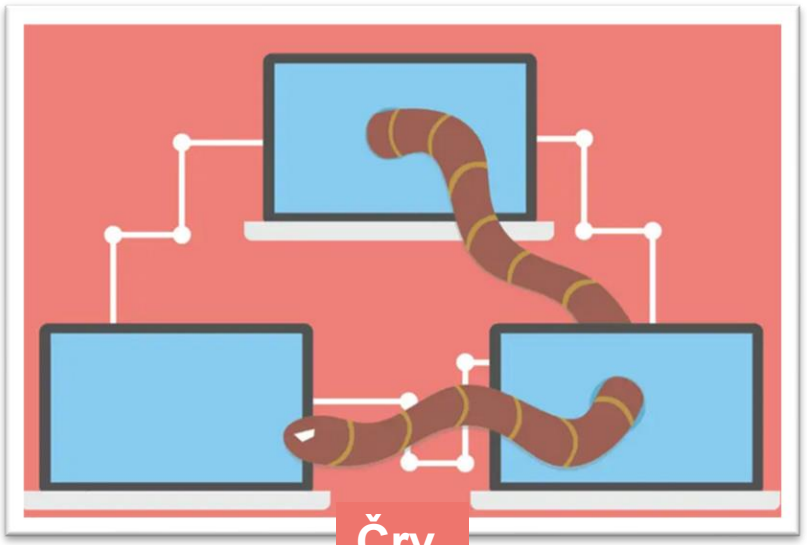
Vohunska programska oprema



Oglaševalska programska oprema



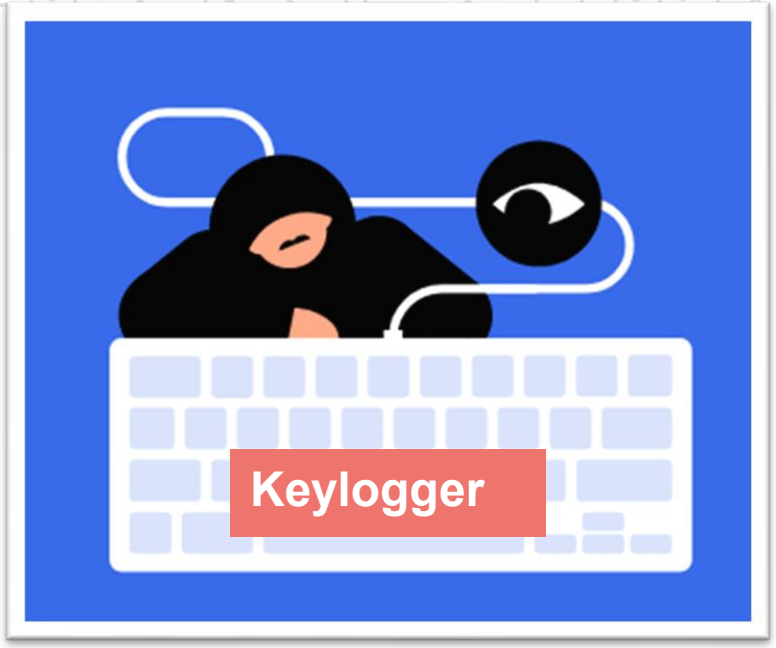
Trojanski konj

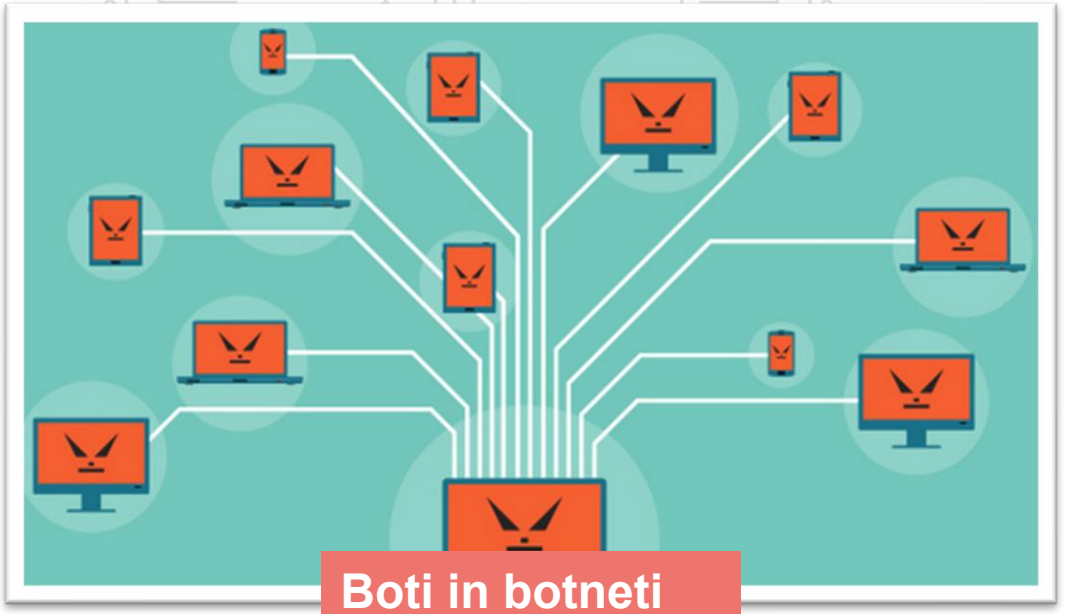


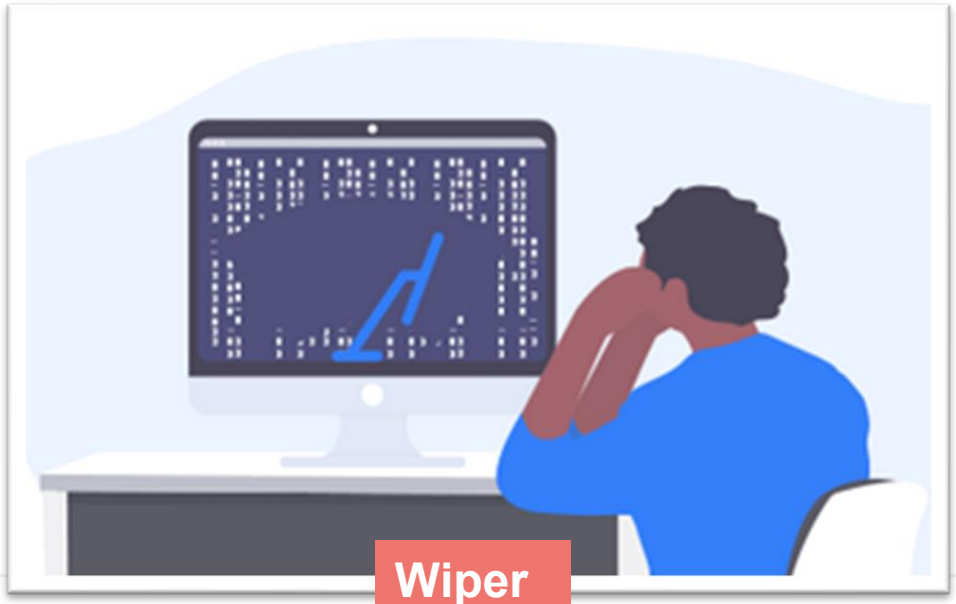
Črv

Virus

Rootkit


Keylogger


Boti in botneti


Wiper


Izsiljevalska programska oprema

NAJPOGOSTEJŠI PRIMERI

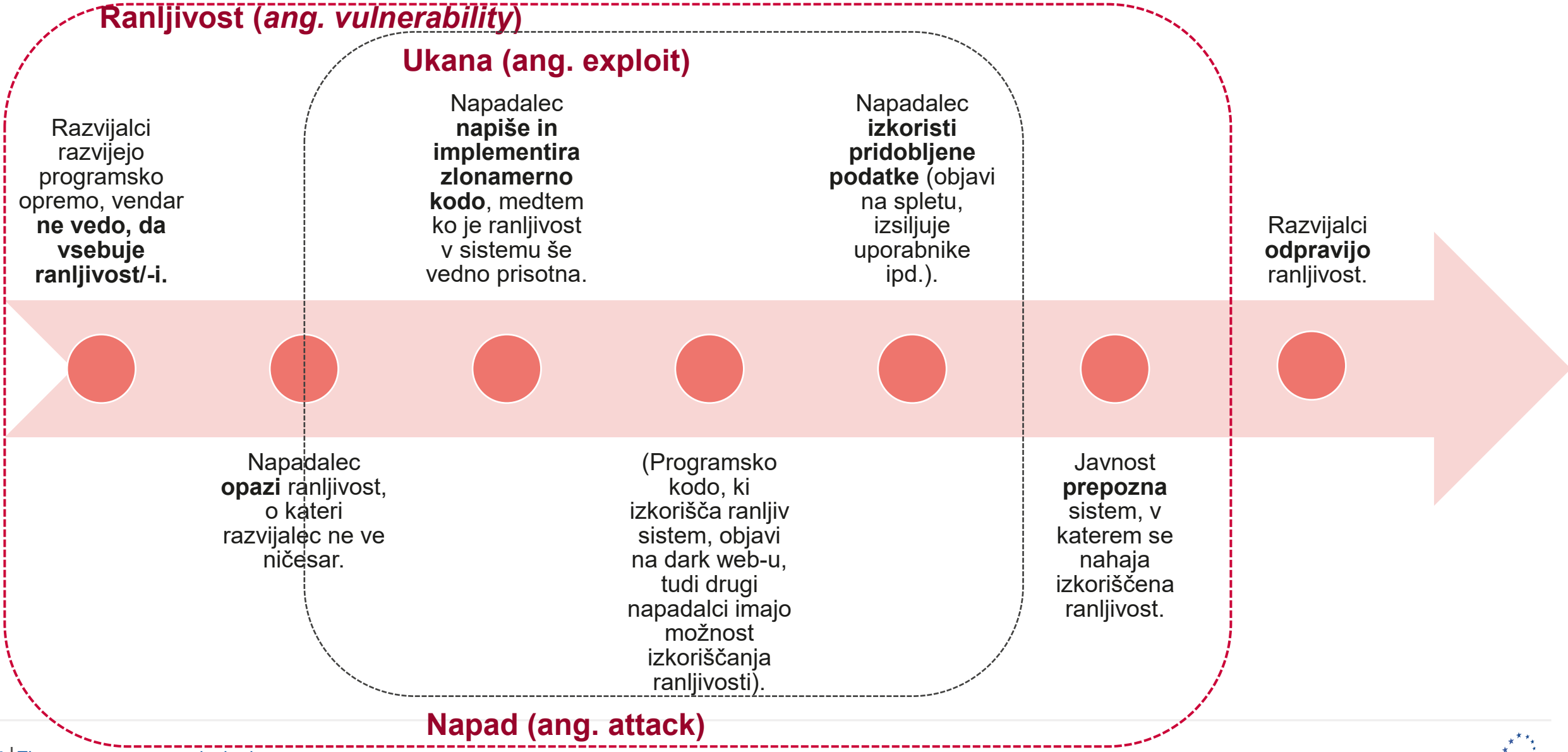
Vohunska programska oprema (ang. Spyware)	• Prikrito zbiranje informacij o aktivnostih uporabnika, • gesla, PIN, plačilni podatki, sporočila, • *DarkHotel*.
Ogleševalska programska oprema (ang. *Adware)*	• Sledenje brskanju, ne namesti programske opreme, ne zajame tipkanja, • profil uporabnika in prodaja teh informacij naprej brez privolitve.
Trojanec	• Se predstavlja kot legitimna, želena programska oprema, • nadzor nad sistemom za različne zlonamerne aktivnosti, • *Emotet, TrickBot.*
Črv	• Izkoriščanje ranljivosti OS, da pridejo do omrežja (nepooblaščen dostop), • DDoS napadi, kraja podatkov, *ransomware* napadi, • *Stuxnet.*
Virus	• Kraja podatkov, DDoS napadi, *ransomware* napadi, • potreben zagon aplikacije (drugače od trojanca in črva).

Prikrita zlonamerna programska oprema (ang. Rootkit)	• Oddaljen dostop in nadzor nad okuženo napravo, admin pravice, • vdelan v aplikacije, hipervizorje, *firmware* – težko zaznati, • prikrivanje druge zlonamerne programske opreme, • *Zacinlo.*
Beleženje tipkanja (ang. Keylogger)	• Nadzor aktivnosti uporabnika, zajem tipkanja, • kraja poverilnic, bančnih in drugih občutljivih informacij, • *Snake.*
Zagonsko omrežje	• *Bot* = aplikacija, ki izvaja avtomatizirana opravila na zahtevo, • *Botnet* = skupina povezanih *botov* za izvedbo razširjenih napadov (*DDoS*), • *Mirai Echobot.*
Brisalec (ang. Wiper)	• Izbris uporabniških podatkov brez možnosti obnovitve, • tudi da napadalci izbrišejo svoje sledi, • *WhisperGate.*
Izsiljevalska programska oprema (ang. Ransomware)	• Šifriranje podatkov, zahteva za plačilo odkupnine. • več različic.

NAJPOGOSTEJŠI VEKTORJI NAPADA Z ZLONAMERNO KODO V 2025

- Phishing (e-pošta + socialni inženiring)
- Zloraba legitimnih storitev
- Kompromitirane spletne strani
- Exploiti ranljivosti (0-day)
- Zloraba SSH (šibka gesla, brute force)
- Dobavna veriga(zlonamerne posodobitve, infostealerji)
- Zlonamerni oglasi

RANLJIVOST NIČTEGA DNE (ZERO DAY VULNERABILITY)



KAZALNIKI ZLORAB (IOC)

Kazalniki (IOCs) na končnih točkah, računalniki, naprave.

- Uporabnik nenadoma znotraj 1 ure pošlje 200 e-mailov.
- Račun dostopa iz neobičajn(e) lokacije / naprave.
- Proces deluje v ozadju z administrativnimi privilegiji.
- Nepričakovano ustvarjanje novih admin računov.
- Upravljanje z datotekami, ki jih uporabnik nikoli ne uporablja (npr. backupi, sistemske mape).
- Zazna jih XDR/EDR sistem.

Uporabniški IOCs (nenavadno vedenje sistema ali uporabnika)

- Nenavadni procesi, ki jih uporabnik ni zagnal
- Visoka poraba CPU / RAM brez razloga
- Antivirusi / varnostne storitve izklopljene ali „neodzivne“
- Pojav neznanih programov, map, skript
- Sumljivi ukazni pozivi (ang. Powershell) ali CMD ukazi
- Sistemske datoteke spremenjene / nove izvršljive datoteke

KAKO SE BRANITI

Redno izvajanje varnostnih pregledov in zaščita vseh platform	Zaščita oblačnih okolij – malware se širi prek oblačnih datotek	Uvedba EDR/XDR za zaznavanje vedenjskih anomalij	Segmentacija omrežja + izolacija IoT naprav (ključna zaradi zagonskih omrežij; ang. botnetov)
Minimalne pravice + onemogočanje nepotrebnih skriptnih orodij	Redna izobraževanja glede infostealerjev in beležnikov tipkanja (ang. Keyloggerjev)	Redne varnostne kopije + testiranje obnovitev	Hitro patchanje kritičnih sistemov (VPN, požarne pregrade)

HVALA

+111 123 456 789

info@enisa.europa.eu