



**SECURITY
DAYS**

NORDSTELLAR – PROAKTYVUS GRĖSMIŲ VALDYMAS

Laurynas Janušonis,
Nord Security verslo vystymo vadovas

Kas yra Dark Web?

Liet. tamsusis internetas

Ar jūsu verslo informācija gali atsidurti dark web'e?

Ticketmaster Hacked: Customer Data Stolen and Shopped on Dark Web by 'Criminal Threat Actor,' Live Nation Discloses

AT&T data breach: Millions of customers caught up in major dark web leak

With hundreds of Snowflake credentials published on the dark web, it's time for enterprises to get MFA in order

User data stolen from genetic testing giant 23andMe is now for sale on the dark web

Data from 3m Avast users on dark web

Hospital system to pay \$65 million for dark web data leak,

Kas yra Dark Web?

10%

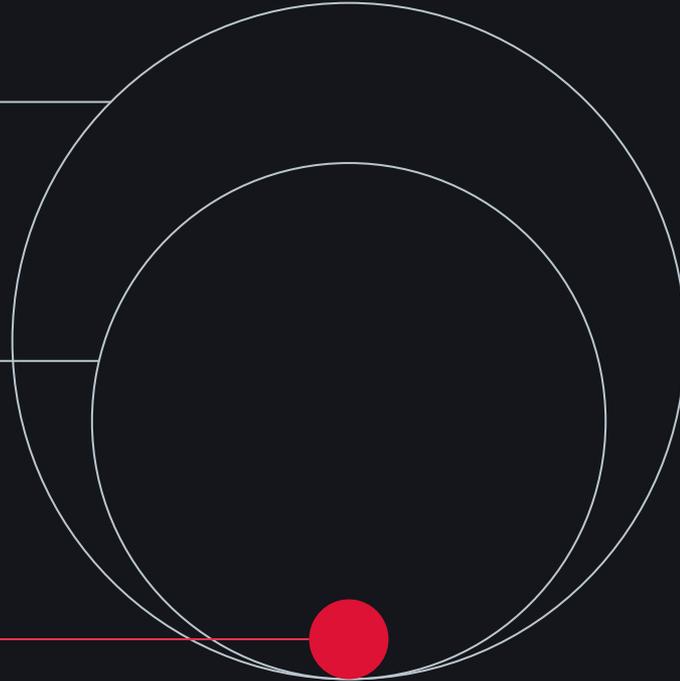
Surface web

90%

Deep web

<1% of deep web

Dark web



Kə galıma rasti **Dark Web**'e?



Tor network



Dark web marketplaces



Forums and social networks



Whistleblower platforms



Cryptocurrency exchanges and wallets

NordStellar turi prieigą prie vienos didžiausios pavogtų duomenų bazės

36k+

Nutekėjusių duomenų bazių

60m+

Malware infostealers

90bn+

Nutekėjusių prisijungimų

90bn+

Slaptažodžių

80bn+

El. paštų

77bn+

Cookies

Deep & Dark Web Underground



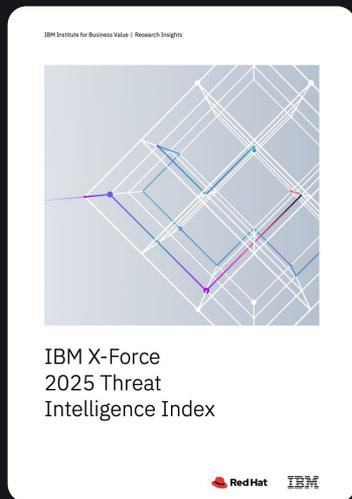
Nutekėjusi informacija

- El. paštai
- Slaptažodžiai
- Sesijų slapukai
- Kreditinės kortelės
- Tel. Nrs
- Tapatybės ID
- Failai
- Kita

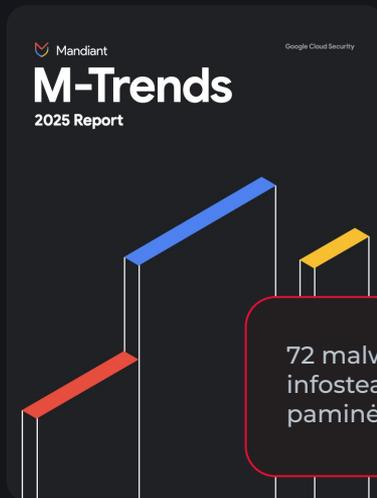
Karščiausia tema dark web'e: Infostealer malware

Liet. informaciją vagianti kenkėjiška programa

Infostealer Malware: augimas ir naminių įrenginių pažeidžiamumas



84% malware infostealer užsikrėtimų augimas



Viena didžiausia šiuolaikinio kibernetinio saugumo problema



Nutekėjusios informacijos augimas dėl užsikrėtimų naminiuose įrenginiuose

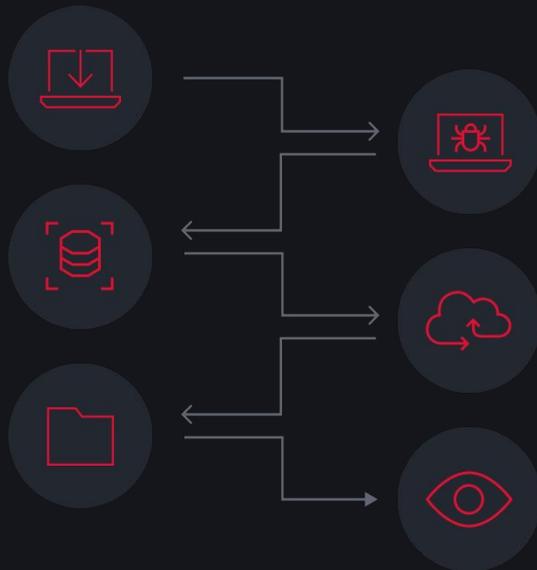
Infostealer malware: kenkėjiška programa apie kurią (ne) girdėjote

Vartotojas atsisiunčia
nulauztą programinę įrangą

Infostealer pavogia:

- Prisijungimo duomenis
- Naršyklės duomenis
- Failus...

Atskiri incidentai sujungiami į
paketus



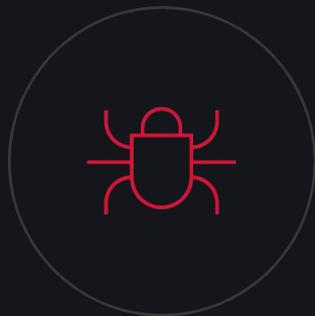
Užkrėsta programa
paleidžiama vartotojo
kompiuteryje

Duomenys išsiunčiami į C2
infrastruktūrą

Incidentų failai platinami
deep ir dark web'e

Admin teisės NEREIKALINGOS ir programa nepastovi

Infostealer malware pavogiami duomenys



*** Credentials (emails, passwords, URLs)

👁 Cookies and session tokens

💳 Credit cards and crypto wallets

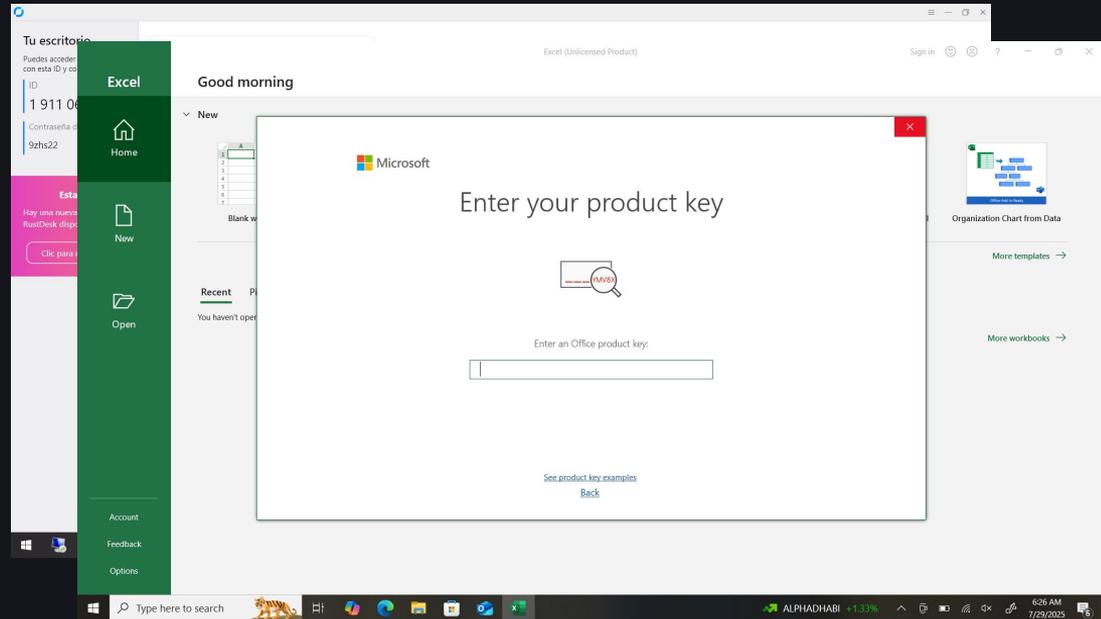
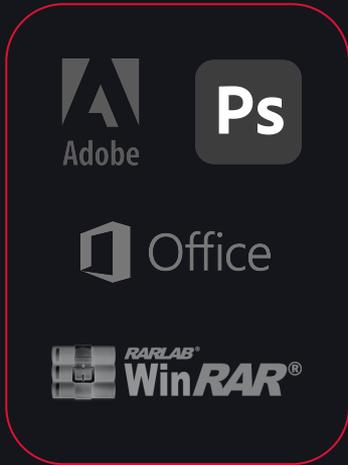
🖼 Screenshots and webcam pictures

👤 Autofills and Personal Identifiable Information (PII)

📁 Files

They don't just steal passwords—they steal access

Kaip užsikrečiama infostealer malware: nušaužta programinė įranga



Kaip užsikrečiama infostealer malware: žaidimų “cheats & mods”



A screenshot of a Windows desktop environment. In the foreground, a YouTube video player is open, displaying a video titled "[LULU UPDATE] Fortnite Hack 2025 - Safe & Undetected Legit Cheats [Download Now]". The video player shows a colorful, abstract graphic. Below the video, the video description is visible, including the channel name "BK FF" and a list of features such as "Legit Aimbot & ESP", "Wallhack & Radar", and "No Ban & Undetected". To the right of the video player, a file explorer window is open, showing a folder named "ModCore" with several files, including "Loader", "PASS-2025", "server.dll", and "updater". In the background, a game window is partially visible, showing a character in a blue and white outfit. The desktop taskbar at the bottom shows the time as 9:55 PM on 7/27/2025.

Kaip užsikrečiama infostealer malware: Google Ads

The image displays two side-by-side screenshots of a Google search for 'midjourney'. The left screenshot shows the search results page with a sponsored ad for 'ai mid-journey org' titled 'Get The Latest Updates - MidJourney'. A red box highlights the word 'Sponsorisé' above the ad, and another red box highlights the ad's title and description. A yellow award ribbon with the number '1' is placed below the ad. Below the ad, there are search suggestions for 'midjourney image', 'midjourney bot', 'midjourney ai', 'midjourney #macron', 'midjourney gratuit', 'midjourney how to use', 'midjourney discord', and 'midjourney prix'. A red box highlights the search suggestion 'midjourney ai'. The right screenshot shows the search results page with a sponsored ad for 'Switch to Java - Java Download'. A red box highlights the word '광고' (Advertisement) above the ad, and another red box highlights the ad's title and description. A yellow award ribbon with the number '1' is placed below the ad. Below the ad, there are search suggestions for '한국소프트웨어인재개발원 - java - ikosmo.co.kr' and 'Java 다운로드'. A red box highlights the search suggestion 'Java 다운로드'. The screenshots illustrate how search results are manipulated to promote specific content, which in this case is related to malware distribution.

Infostealers – statistika iš 2024

Populiariausios duomenų kategorijos

Cookies	51,058,866,236
Autofills	5,939,861,393
Credentials	1,537,226,295
Passwords	346,453,140
Emails	216,519,234
Grabbed Files	66,888,742
Credit Cards	1,448,471

Populiariausi prisijungimų domenai

Rank	Credential domain	Count
1	Facebook	13,695,693
2	Microsoft	11,763,108
3	Google	9,229,057
4	Instagram	5,658,990
5	Netflix	5,203,901

NordStellar - Threat exposure management platform

Liet. Kibernetinių grėsmių valdymo platforma

Kibernetinių grėsmių valdymo platforma

Aptikite ir užbėkite už akių kibernetinėms grėsmėms, kurios kelia pavojų jūsų įmonei.

Su NordStellar pagalba galite realiu laiku stebėti grėsmes, kylančias dark web'e ir apsaugoti darbuotojus, vartotojus, prekės ženklą bei infrastruktūrą.



Kaip NordStellar padeda kibernetinio saugumo ir IT komandoms

Leaked data management

Darbuotojų ir vartotojų apsauga

Dark web monitoring

Įmonės ir prekės ženklų apsauga

Attack surface management

Infrastruktūros apsauga

Cybersquatting detection

Reputacijos apsauga



Live DEMO