Yritysten tehokas suojaaminen kyberrikkollisuudelta

Sami Laiho, Chief Research Officer / MVP

Adminize Oy

10.4.2025

Sami Laiho

Chief Research Officer / MVP

- IT Admin since 1995 / MCT since 2001
- MVP in Windows OS since 2011
- ”100 Most Influencial people in IT in Finland” – TiVi’2019→
- Specializes in and trains:
  - Troubleshooting
  - Windows Internals
  - Security, Social Engineering, Auditing
- Trophies:
  - Best Session at Advanced Threat Summit 2020
  - Best Speaker at NIC, Oslo 2016, 2017, 2019, 2020, 2022, 2023 and 2024
  - Ignite 2018 – Session #1 and #2 (out of 1708) !
  - TechEd Europe and North America 2014 - Best session, Best speaker
  - TechEd Australia 2013 - Best session, Best speaker


Bluesky: @samilaiho.com
X (ex-Twitter): @samilaiho
LinkedIn 🙏
Jos haluat slaidit → LinkedIn-kontakti ja viesti

Aiheet

1

Miten yritykset todennäköisimmin murretaan – Realistiset uhat

2

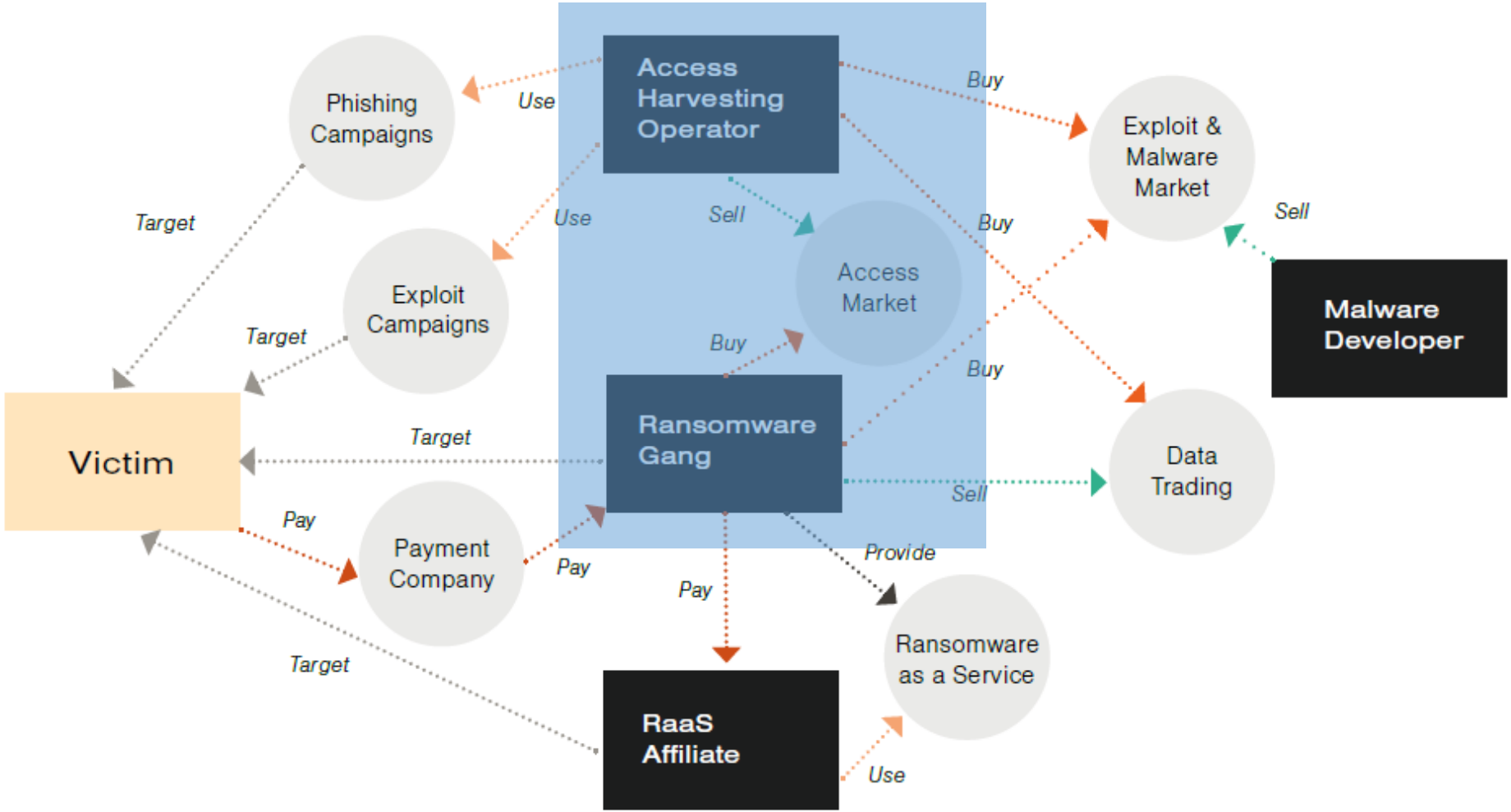
Miten estetään 95% kaikista uhista

3

Mitä voidaan muuttaa, ilman kalliita lisenssejä

2024

- Maagiset numerot:
  - 2 tuntia
  - 180 päivää
  - < 5%



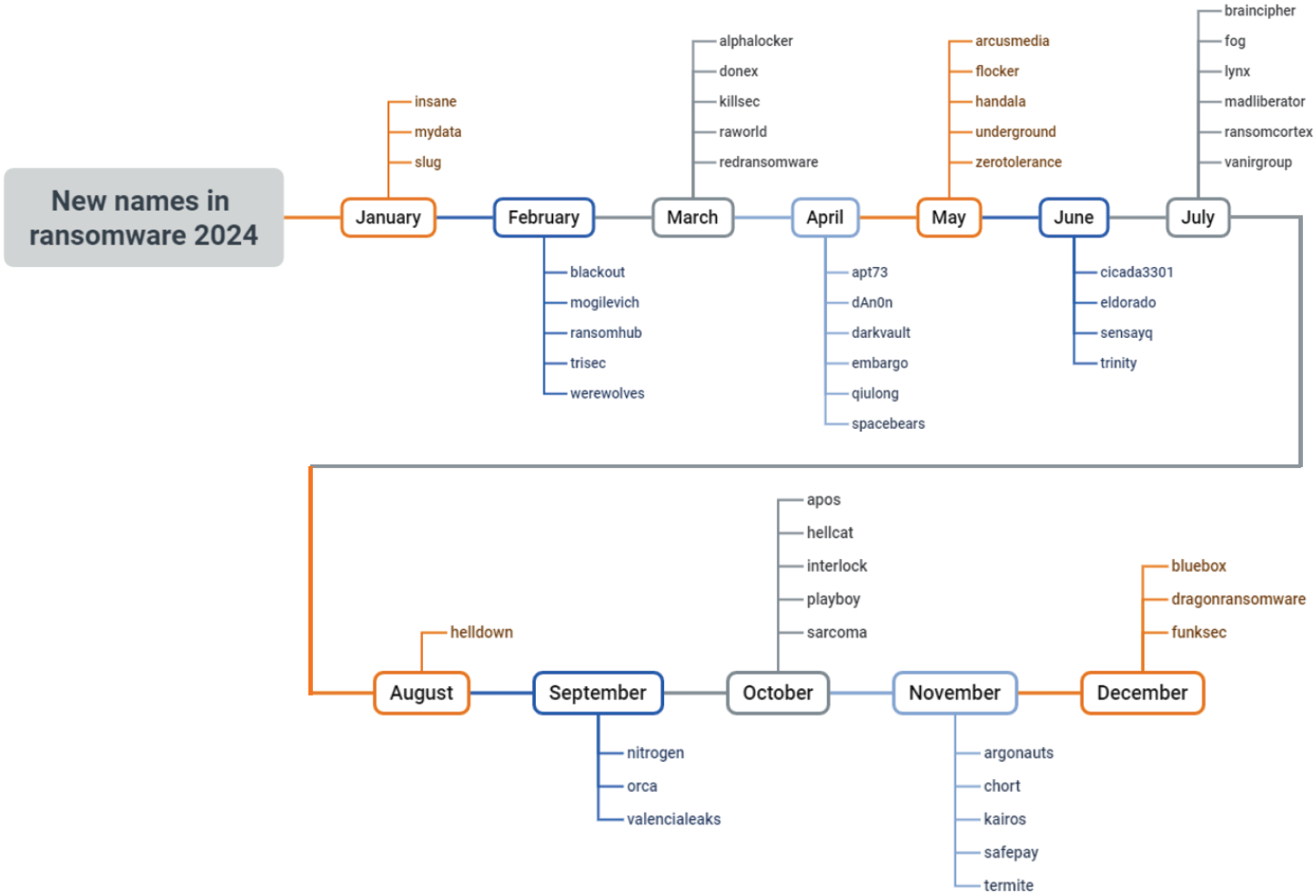
Source: Truesec

Comparison of ransomware attacks globally between 2022-2024

	2022	2023	2024
Total number of attacks	2684	4559	5602
Top 5 groups	lockbit2/3: 899 attacks alphv: 391 attacks hive: 180 attacks blackbasta: 155 attacks conti: 152 attacks	lockbit3: 1028 attacks alphv: 424 attacks clop: 381 attacks play: 316 attacks 8base: 256 attacks	lockbit3: 538 attacks ransomhub: 538 attacks play: 364 attacks akira: 314 attacks hunters: 235 attacks
The top groups' percentage of the grand total	66%	53%	35%

Source: NetNordic


LockBit?


New names in ransomware 2024
January
insane
mydata
slug
February
blackout
mogilevich
ransomhub
trisec
werewolves
March
alphalocker
donex
killsec
raworld
redransomware
April
apt73
dAn0n
darkvault
embargo
qiulong
spacebears
May
arcusmedia
flocker
handala
underground
zerotolerance
June
cicada3301
eldorado
sensayq
trinity
July
braincipher
fog
lynx
madliberator
ransomcortex
vanirgroup
August
helldown
September
nitrogen
orca
valencialeaks
October
apos
hellcat
interlock
playboy
sarcoma
November
argonauts
chort
kairos
safepay
termite
December
bluebox
dragonransomware
funksec

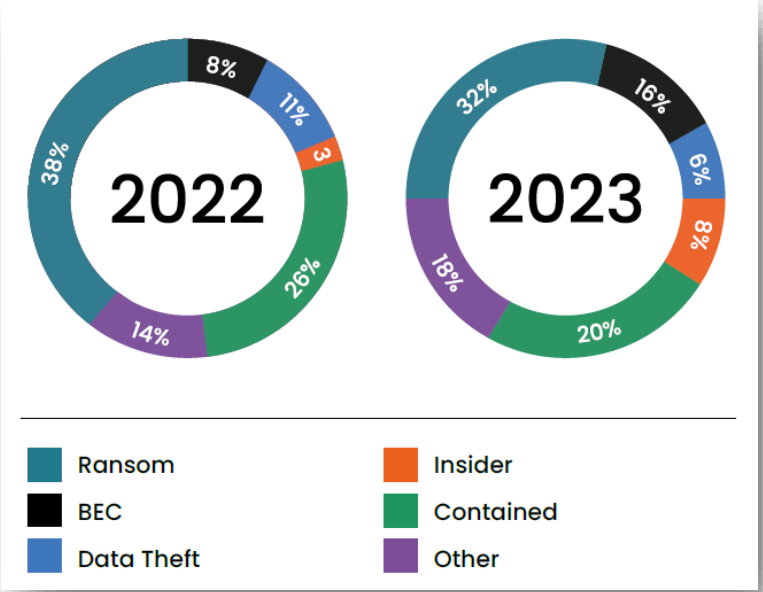
Average Ransoms Paid in US

- 2018 = 5.000$
- 2024 = 2.730.000$

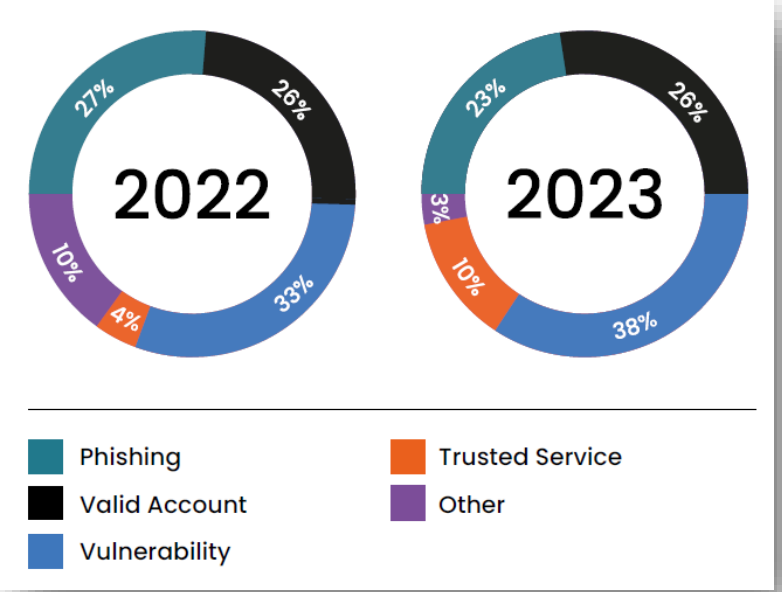
Last year VmWare 0-day vulnerability

- Price: 1,7M$
- When Criminals get more money their budget for the next attacks increase → 0-Day attacks become more common
- Sadly, the enemy is also becoming more bold and cruel…

Attack types



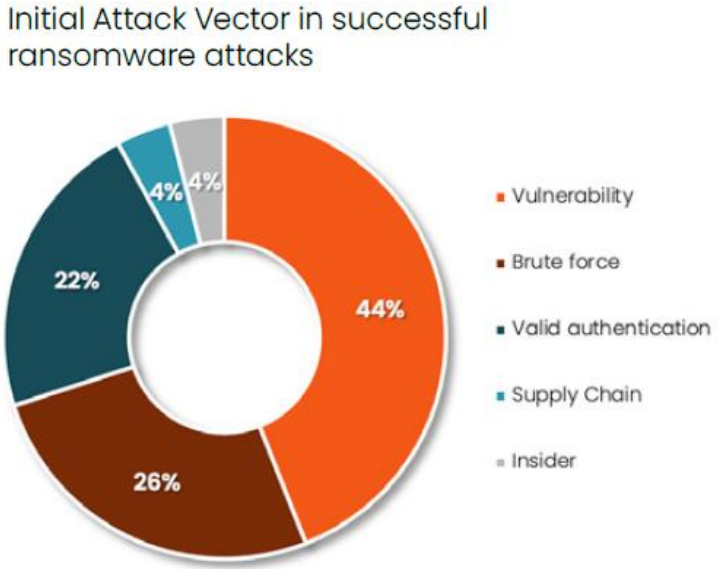
Attack vectors

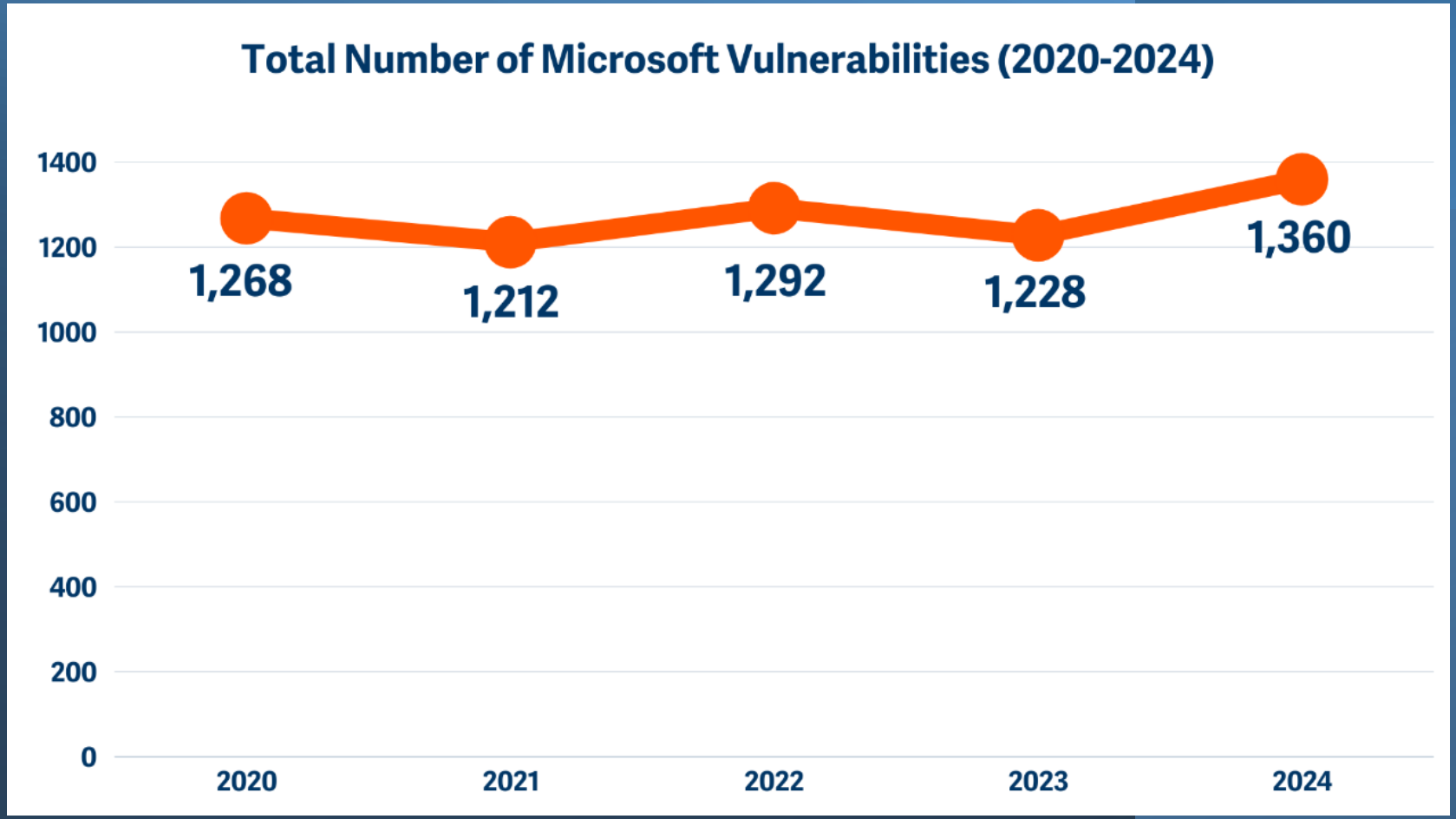


*Truesec Threat Intelligence Report

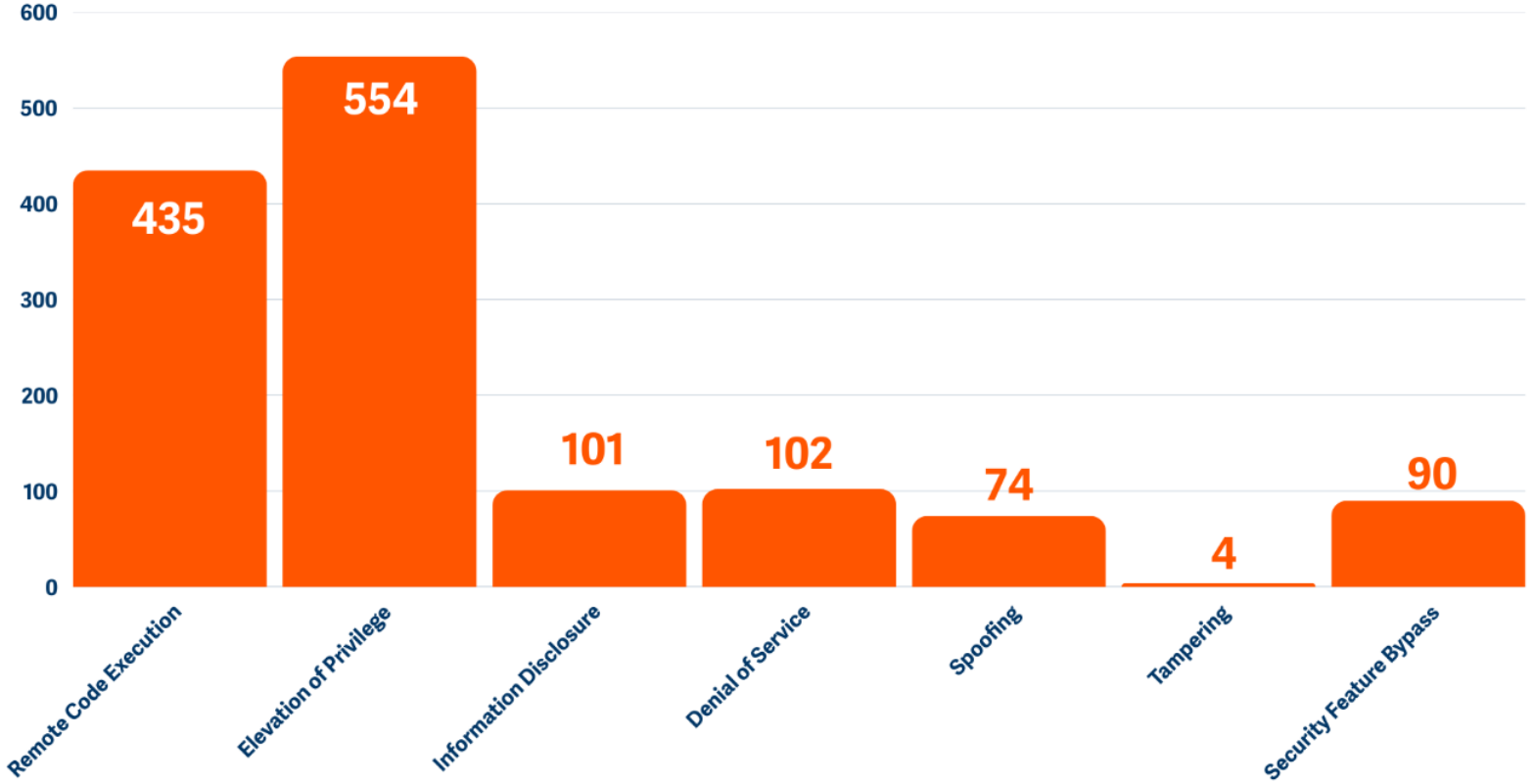
Miten hyökkäys alkaa?

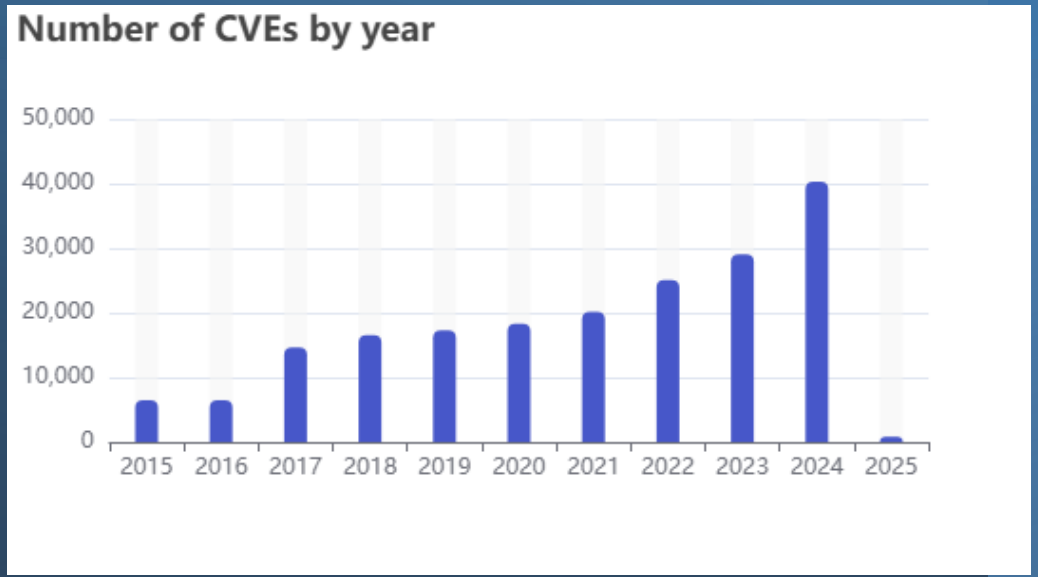
2024




Total Number of Microsoft Vulnerabilities (2020-2024)
1400
1200
1000
800
600
400
200
0
1,268
1,212
1,292
1,228
1,360
2020
2021
2022
2023
2024

Breakdown of Microsoft Vulnerability Categories (2024)

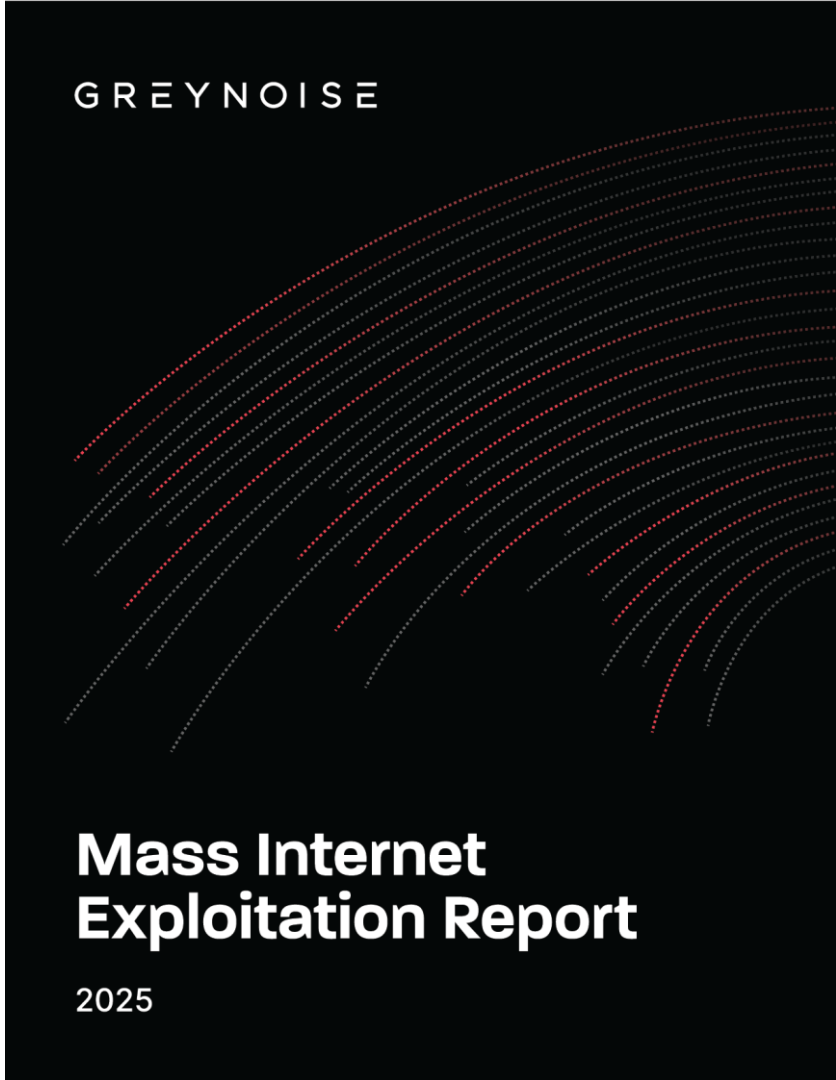




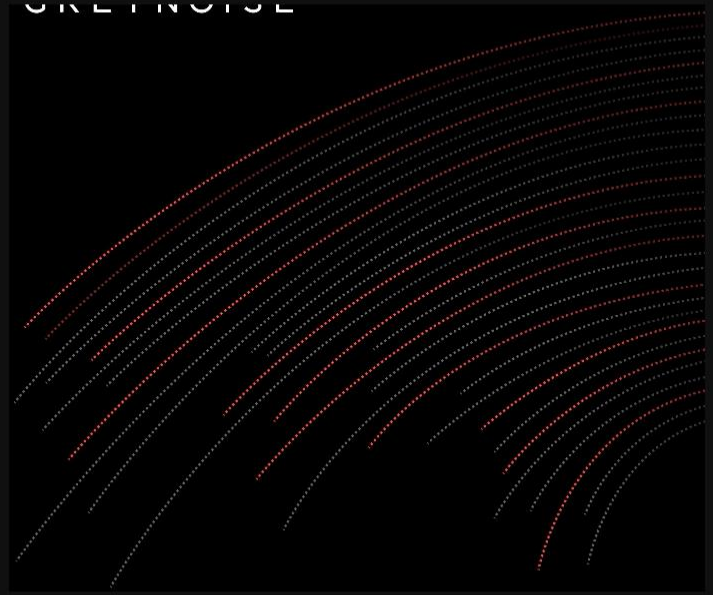
Cumulative Yearly CVE publication, via Cyberpress

GREYNOISE 2025 REPORT

- The most exploited vulnerability of 2024 targeted home internet routers, fueling massive botnets used in global cyberattacks.
- 40% of exploited vulnerabilities in 2024 were from 2020 or earlier — some dating back to the 1990s.
- Attackers are exploiting vulnerabilities within hours of disclosure, making real-time defense more critical than ever.
- Ransomware groups leveraged 28% of the CVEs in CISA's Known Exploited Vulnerabilities catalog that GreyNoise tracked in 2024.
- A surge in May 2024 was traced to 12,000+ hacked Android devices, showing mobile threats are growing.
- D-Link and Ivanti devices were among the most heavily exploited in 2024, posing critical security risks for businesses and governments.



Mass Exploitation Overview



GreyNoise 2025 report insights.

Windows Version	Market Share (%)
Windows 10	62.73
Windows 11	34.1
Windows 7	2.4
Other Windows versions	0.7

Ransomware is Inevitable. Plan Ahead.

We surveyed 350 CISOs, information security professionals, and backup administrators from a variety of organizations via an independent research firm to unpack how they were attacked by ransomware and what they learned from it.

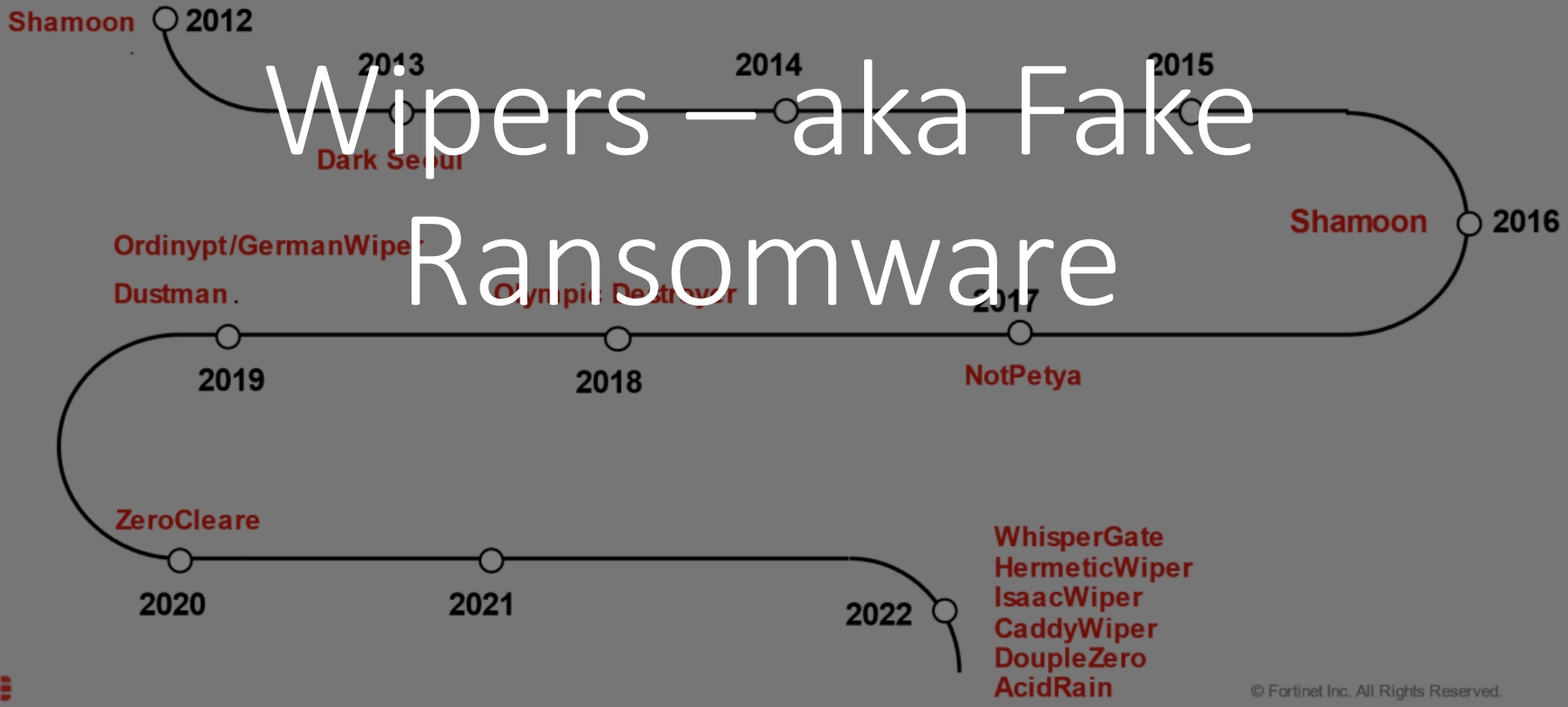
of ransomware attacks targeted backup repositories

were able to recover their data without paying a ransom

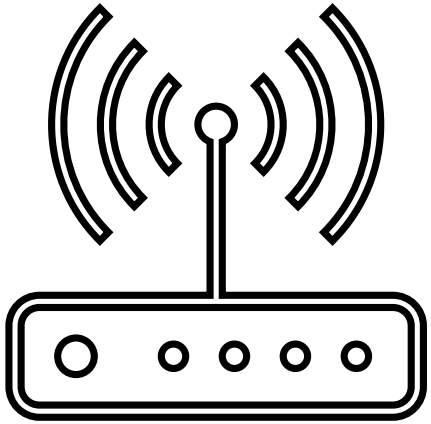
of organizations who paid the ransom still could not recover their data

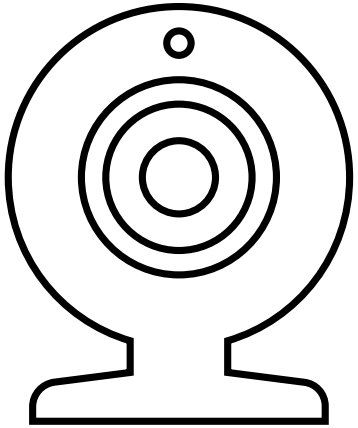
Source: Veeam EMEA

Wipers – aka Fake Ransomware



Eli mitä nyt sitten voidaan tehdä?





First Vector

Read: “Linux”

https://m.ransomware.live/

Shodan skannaa koko Internetin 4 minuutissa…

Päivittäkää kotinne laitteet, älkää osallistuko pankkien tai Ukrainan kaatamiseen…

Ransomware gang encrypted network from a webcam to bypass EDR

By **Bill Toulas**

March 6, 2025 03:31 PM 4


Paikkaa Enemmän – Testaa
Vähemmän!

“Elämä on liian lyhyt uloskirjautumiselle”

- Anonymous Finnish Admin

Top 10 Biggest Cyber Attacks, Data Breaches and Ransomware Attacks of 2024

- Change Healthcare Ransomware Attack
- Snowflake Ransomware Attack
- UK MoD Data Breach
- Ascension Ransomware Attack
- MediSecure Data Breach
- Synnovis-NHS UK Ransomware Attack
- **CrowdStrike Outage**
- TfL Cyber Attack
- Ivanti Mass Zero-Day Exploits
- Salt Typhoon Attacks

Varmuuskopiot

(V)LAN1

Domain Admins

Domain

(V)LAN2

Fabric Admins

Fabric

(V)LAN3

Backup Admins

Backup

You need IMMUTABLE backups!!!

“Backup is nothing, Recovery is everything – Obey your Recovery Testing Plan”


You need immutable logs

Hallintatyöasemat

PAW

Limiting the attack surface

- Administeration is done from a different OS installation than daily driver
- “Don’t mix business with pleasure”
- Privileged Access Workstation (PAW) – implementation is one of the most effective ways to fight breaches

Security is simple at the end… Laiho's Laws

Don't let accounts that can take down your environment logon to devices with access to malware…

Don't let computers that can take down your environment talk to Facebook…

Admin-oikeudet pois käyttäjältä, joka lukee sähköposteja ja surffaa

Why Shouldn't Users Want to Have Administrative Rights?

- Performance of systems is improved without local administrator rights
- Installation of various software causes slowdowns and reliability issues.
- SSD lifespan increases
- Decreases the need for reinstallations.
- Due to more reliable systems productivity is increased
- The attack surface of malware is greatly reduced and helps limit propagation
- Because it decreases the amount of money needed in extra security solutions
- Because it mitigates more vulnerabilities than patching

Kyllä, tähän on ratkaisut, joilla käytettävyys ei heikkene ☺

Salasanat / tunnistautuminen?

Top 100 Finnish passwords in breaches

- 014745880
- 1804090178Ds
- 1q2w3e4r
- aleksi
- antero
- asdasd11
- aurinko
- banaani
- Finlandia
- greippi13
- hemuli
- jalkapallo
- Jipijaije1
- **kikkeli**
- **koira123**
- Mohammadkhizar1
- moimoi
- None
- ohe1ohe
- oong6aet
- Qpa9Zm1o
- Qvidja123
- samuli
- SZ9kQcCTwY
- tiikeri
- Tk0pljes
- **trustno1**
- 12koonee56sei
- aepohg9a
- buzzmachines
- heikki
- iLLo1954
- jaakko
- johanna
- **jokerit**
- **kakka123**
- koira
- **makkara**
- millamagia
- niko99
- **NULL**
- s4a3m0
- **saatana**
- soppa765
- terra25
- tietokone
- 1janina9
- aak31985
- **akuankka**
- **asdasd**
- dominion
- f2Ubyf!1
- juhani
- **kissa**
- kukkanen
- lumina79
- **password**
- rasmus
- sakari
- helena
- matias
- mikael
- terra255
- 12345678
- J0h4nne54591
- mansikka
- **moi123**
- Terra255
- viaplay72
- 171078Pp
- eemeli
- **paska123**
- petteri
- **salasana1**
- YR3f7dSF
- anneli
- Happyhappy2018
- **moikka**
- **paska**
- @rchi128K
- **Salasana123**
- **123456789**
- Archi128K
- **qwerty**
- hbo1972
- jeejee
- oskari
- akuankka93
- F15t1128K
- Pailammas975&&
- sukupuu
- **perkele**
- f5-sso-token
- **kakka**
- ascona79
- 12345
- 123456
- akamari
- **salasana**
- kamari

NIST SP 800-63 standard

- Passwords shorter than eight characters are prohibited, with a minimum of 15 characters recommended.
- Scheduled, mandatory password rotation is considered an outdated practice and therefore prohibited.
- It’s also prohibited to impose requirements on password composition (such as “your password must contain a letter, a number, and a symbol”).
- It’s recommended to allow using any visible ASCII characters, spaces, and most Unicode symbols (such as emojis).
- Maximum password length, if enforced, must be at least 64 characters.
- Using and storing password hints or security questions (such as “your mother’s maiden name”) is prohibited.
- Commonly used passwords must be eliminated through the use of a stop-list of popular or leaked passwords.
- Compromised passwords (for example, appearing in data breaches) must be reset immediately.
- Login attempts must be limited in both rate and number of unsuccessful attempts.

Ransomware Deployment Protocol

182

Vendors Log into a Typical Org each Week[1]

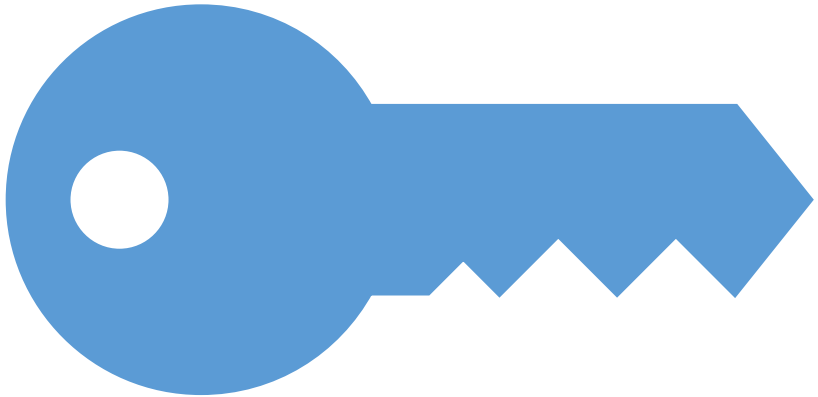
76%

of Cloud Accounts Sold on Dark Web = RDP[2]

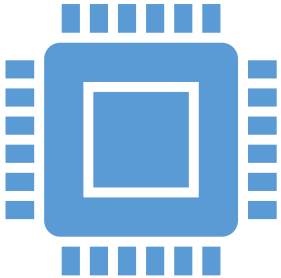
80%

of Ransomware Attacks Exploit RDP[3]

Tunnistustavat



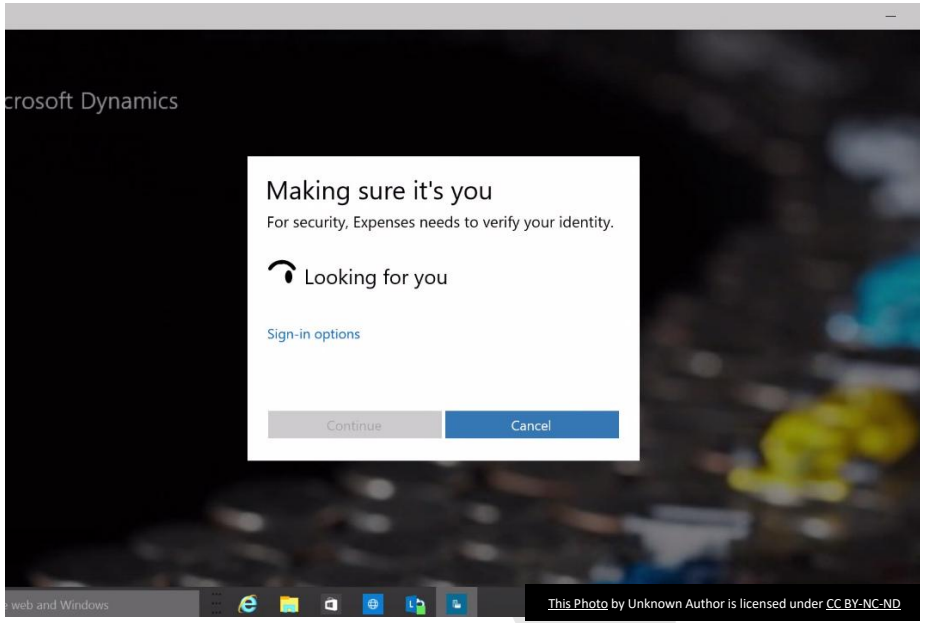
PIN-codes



Windows with PIN is MFA!

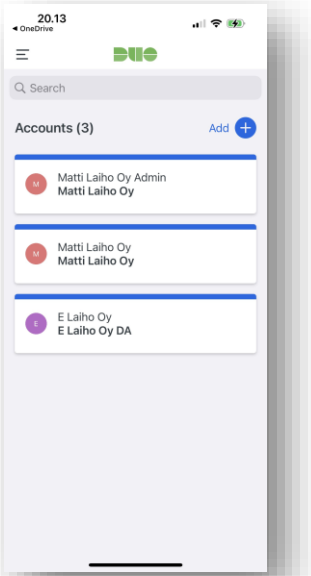
Why a PIN is more secure than a password

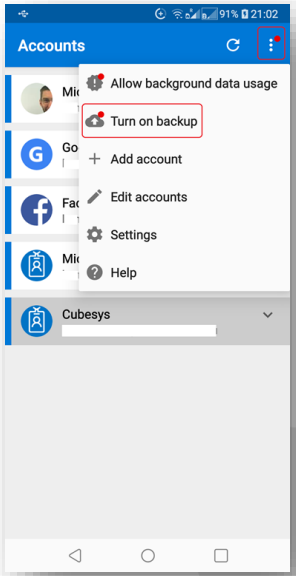
Biometrics



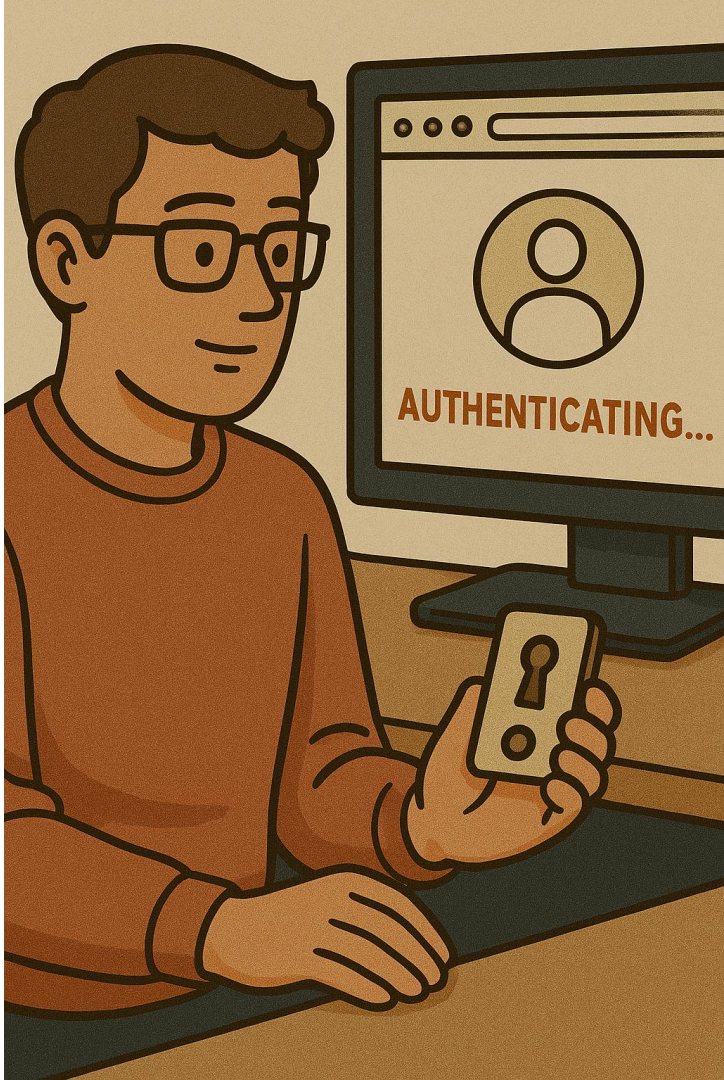
Authenticator Apps

Requires a Smartphone



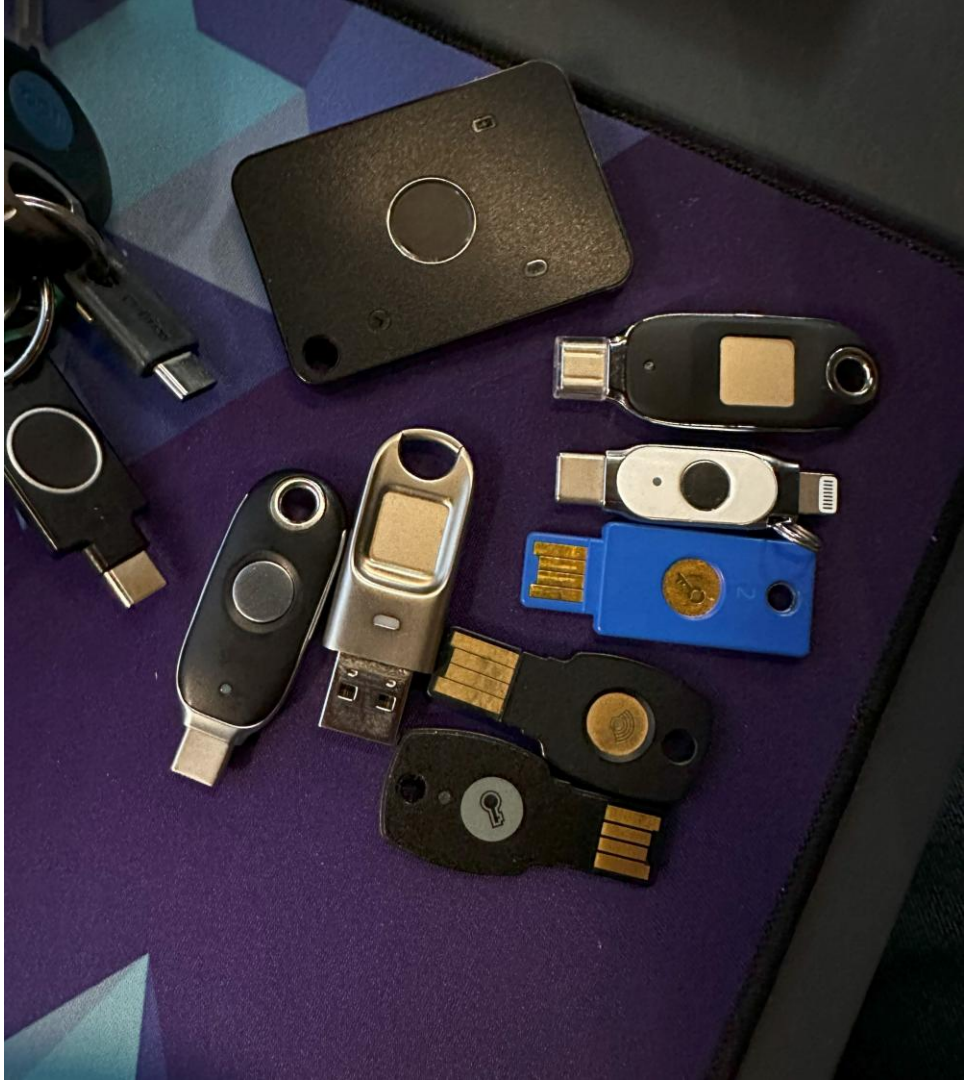


Edelliset yhdistettynä PassKeys:in kanssa = Muy Bien!



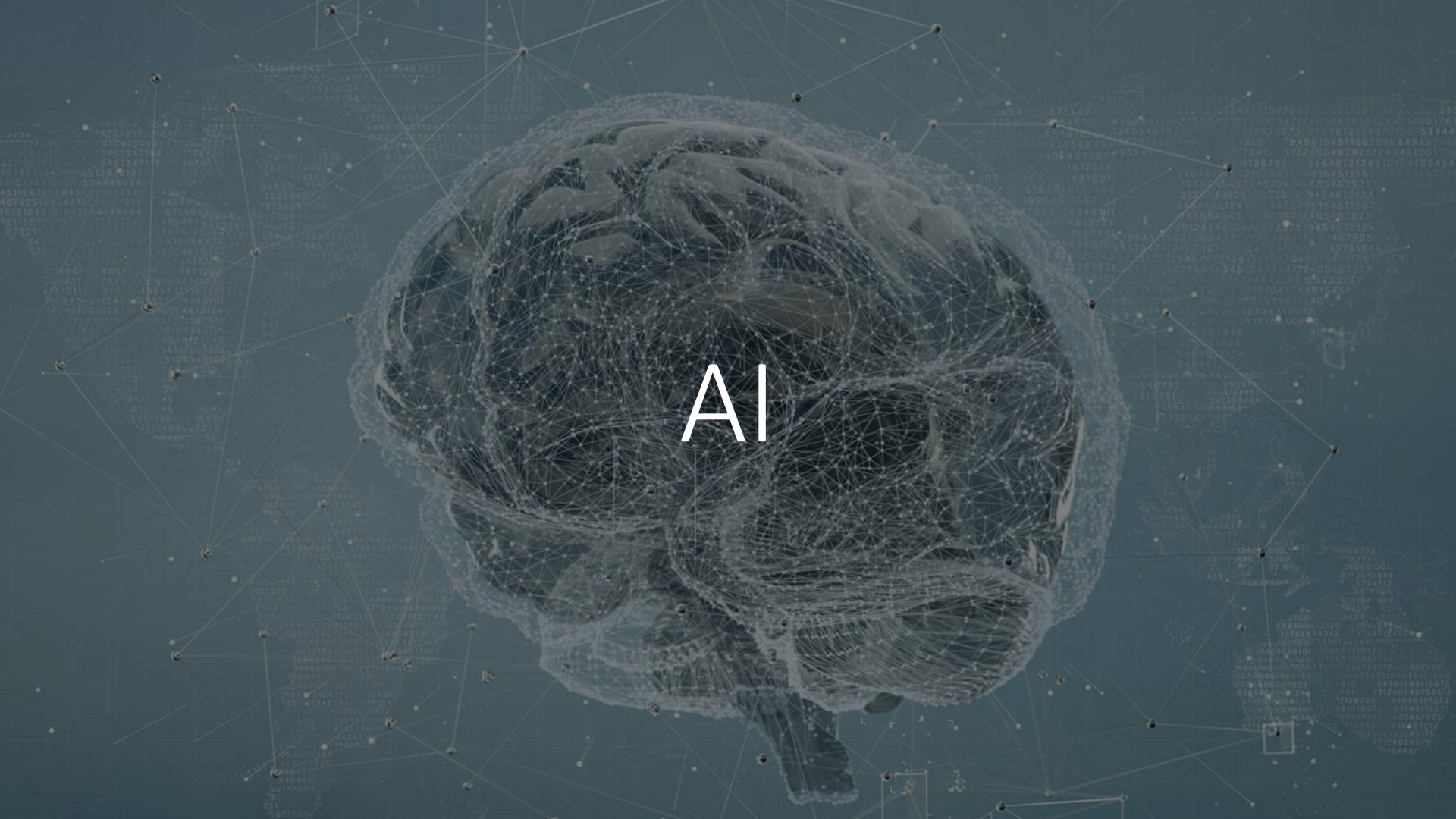
Physical Tokens

- Phishing resistant MFA
  - Plug in or NFC
  - Biometrics or PIN



Jos olet tosissasi ja haluat päästä helpolla → Application Control

AppLocker ei maksa mitään Pro/Enterprise-versioille


AI


Screen Swap Experiment
Share
0:02 / 0:25
YouTube

”Vuonna 2024 raportoitiin 105 120 deepfake-hyökkäystä, mikä tarkoittaa noin yhtä hyökkäystä joka viides minuutti.”

Lähde: Barracuda Networks

16.1.2024: Suomessa ensimmäinen miljoonaluokan AI-toimitusjohtajahuijaus …

Huijauksia yhteensä 2023 **76,9 milj. €**

Pankkien torjumat huijaukset 2023 **32,7 milj. €**

FA

Suomalaiset menettäneet verkkorikollisille

32,4 → 44,2 milj.eur
36 %

Pankkien estämät ja palauttamat maksut

14,1 → 32,7 milj.eur
132 %

Dokumentti- ja rakkaus-huijaukset

9 → 10,4 milj.eur
15%

Sijoitus-huijaukset

8,5 → 16,2 milj.eur
91%

taloudellisesti suurin, 37 % kaikista huijauksista

Toimitusjohtaja-huijaukset

4,9 → 5,4 milj.eur
10 %

Valepoliisihuijaukset ja tietojen kalastelu

10 → 12,3 milj.eur
22%

PANKKIEN TIETOON TULLEET HUIJAUKSET 2022 ja 2023

HUIJAUKSET JA PETOKSET

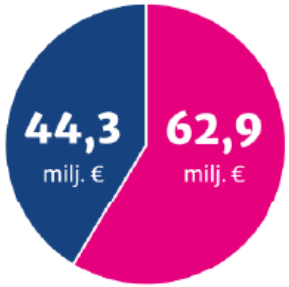
Pankkien tietoon tulleet huijaukset 2024

Huijauksia yhteensä 2024

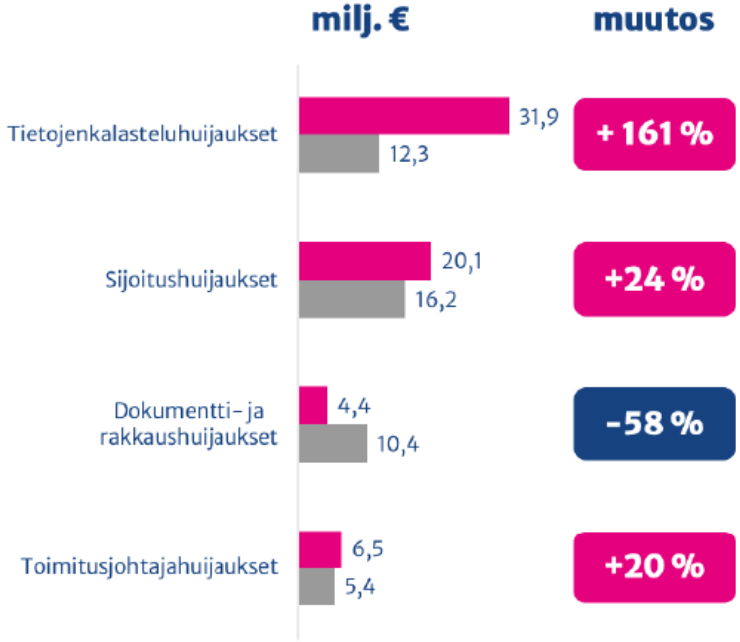
107,2 milj. €

+39 % vrt. 2023

Pankkien pysäyttämät ja palauttamat maksut

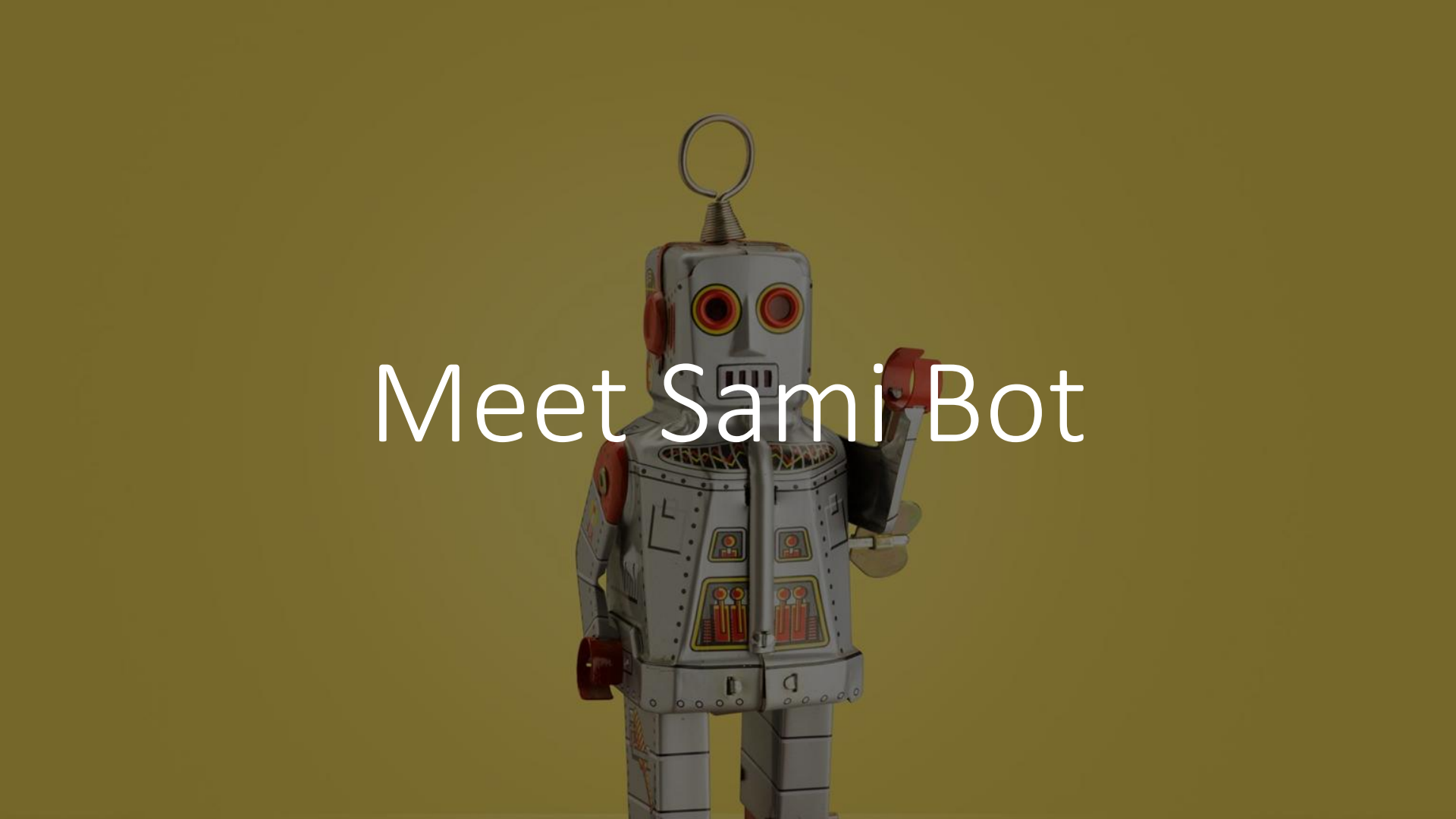


Suomalaiset menettäneet verkkorikollisille



Lähde: FA

Meet Sami Bot




EAT
Lock is not a control to stop a thief that has a key

“Your job is not to stop to enemy, but to slow it down”


clas
son