NIC Cloud Connect

Oslo Spektrum
November 7 - 9

Cloud Connect

Sami Laiho

Forward to the Past and Back to the Future - Cybercrime in 2022/2023

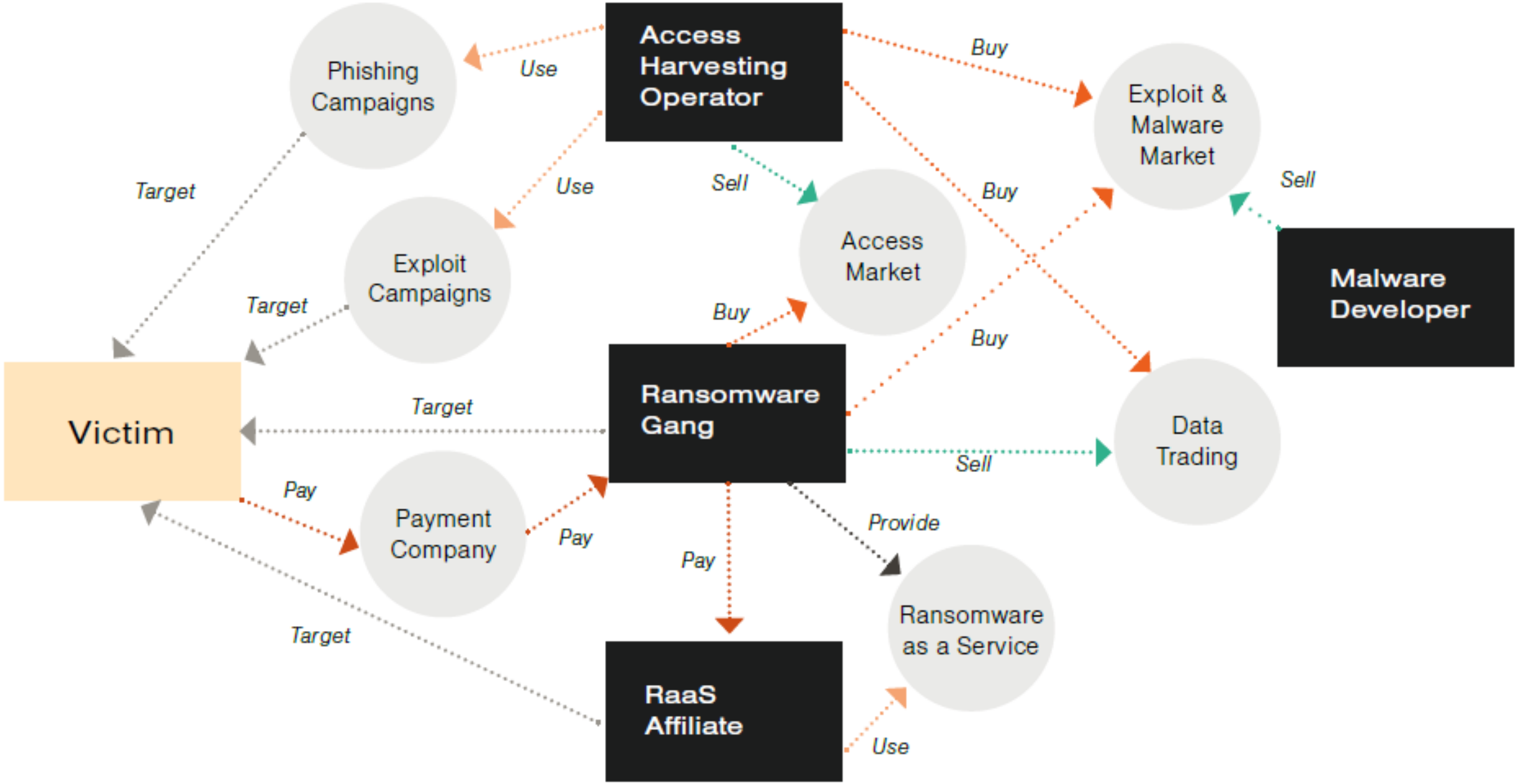
Sami Laiho
Chief Research Officer / MVP

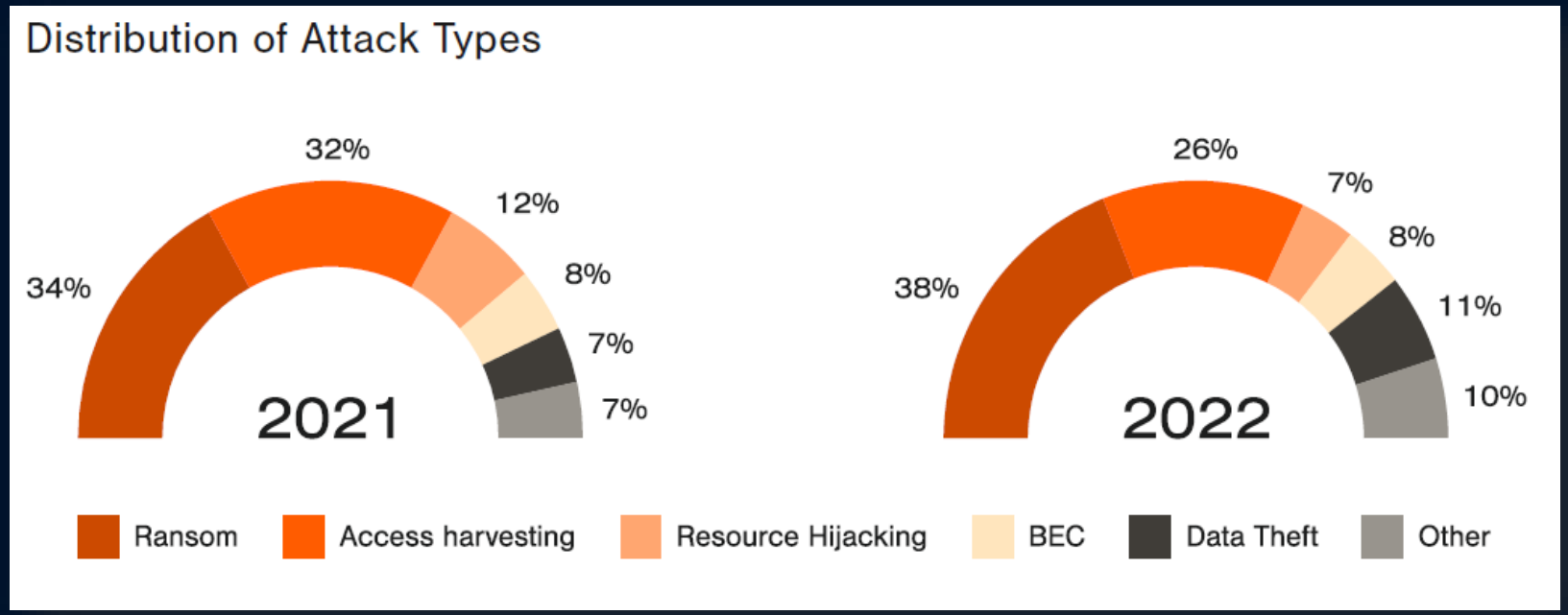
- IT Admin since 1996 / MCT since 2001
- MVP in Windows OS since 2011
- ”100 Most Influencal people in IT in Finland” – TiVi’2019→
- Specializes in and trains:
  - Troubleshooting
  - Windows Internals
  - Security, Social Engineering, Auditing
- Trophies:
  - Best Session at Advanced Threat Summit 2020
  - Best Speaker at NIC, Oslo 2016, 2017, 2019, 2020 and 2022
  - 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

X (ex-Twitter) @samilaiho
Bluesky: @samilaiho.com
LinkedIn

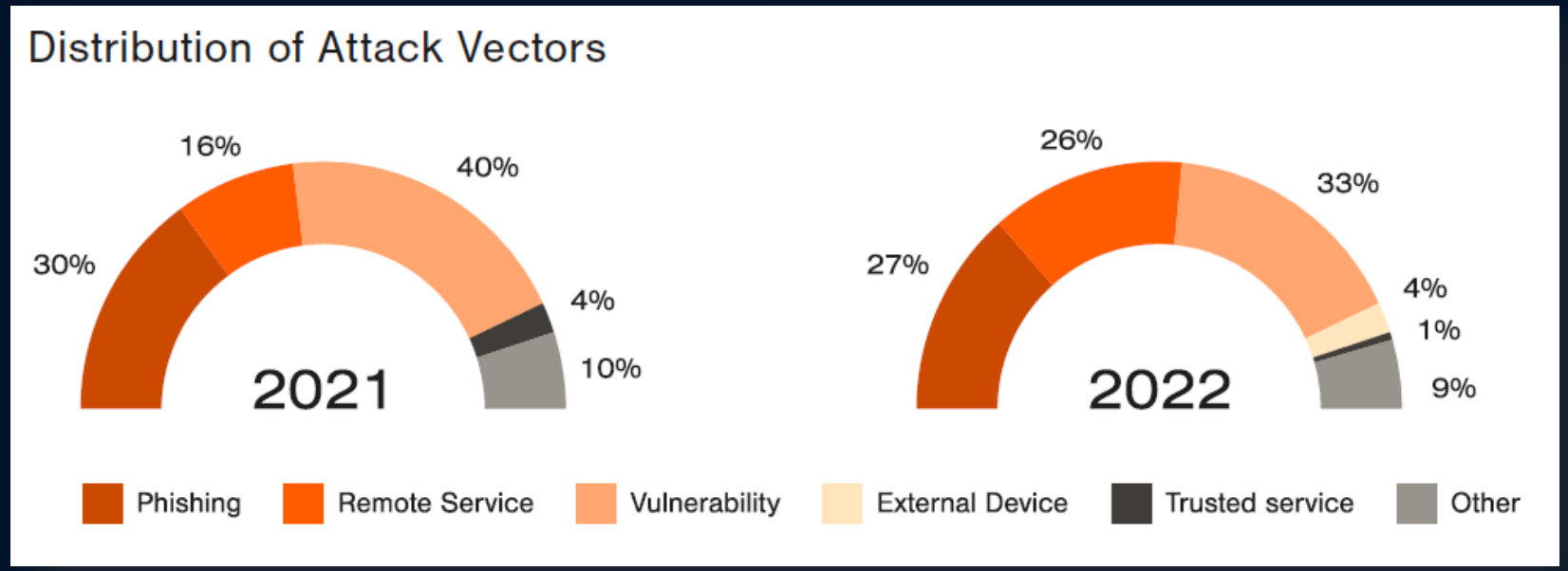
2022

- Magic Numbers:
  - 2 hours
  - 180 days
  - 2% of victims


Phishing Campaigns
Access Harvesting Operator
Exploit & Malware Market
Malware Developer
Exploit Campaigns
Access Market
Victim
Ransomware Gang
Data Trading
Payment Company
Ransomware as a Service
RaaS Affiliate
Use
Buy
Sell
Target
Pay
Provide

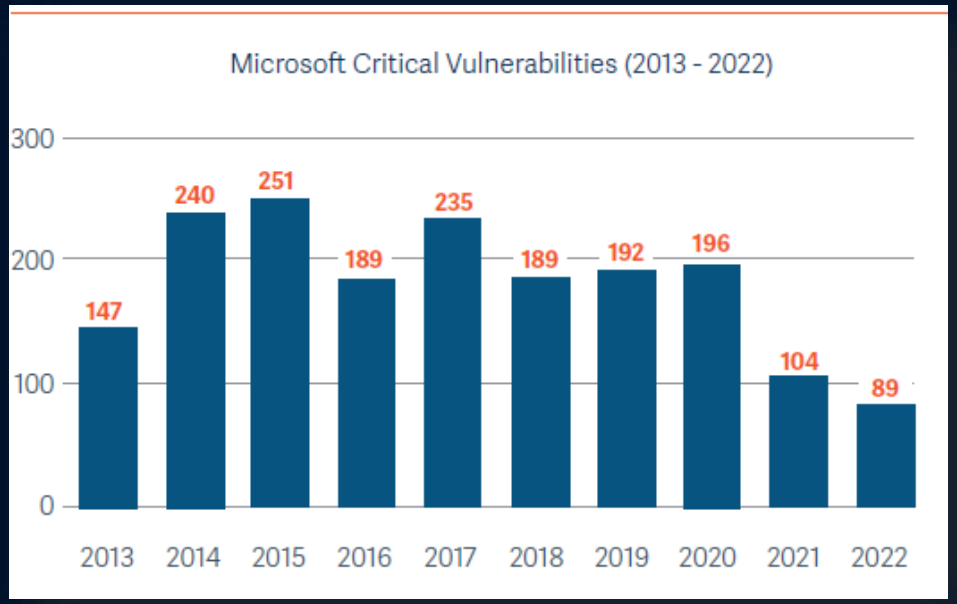


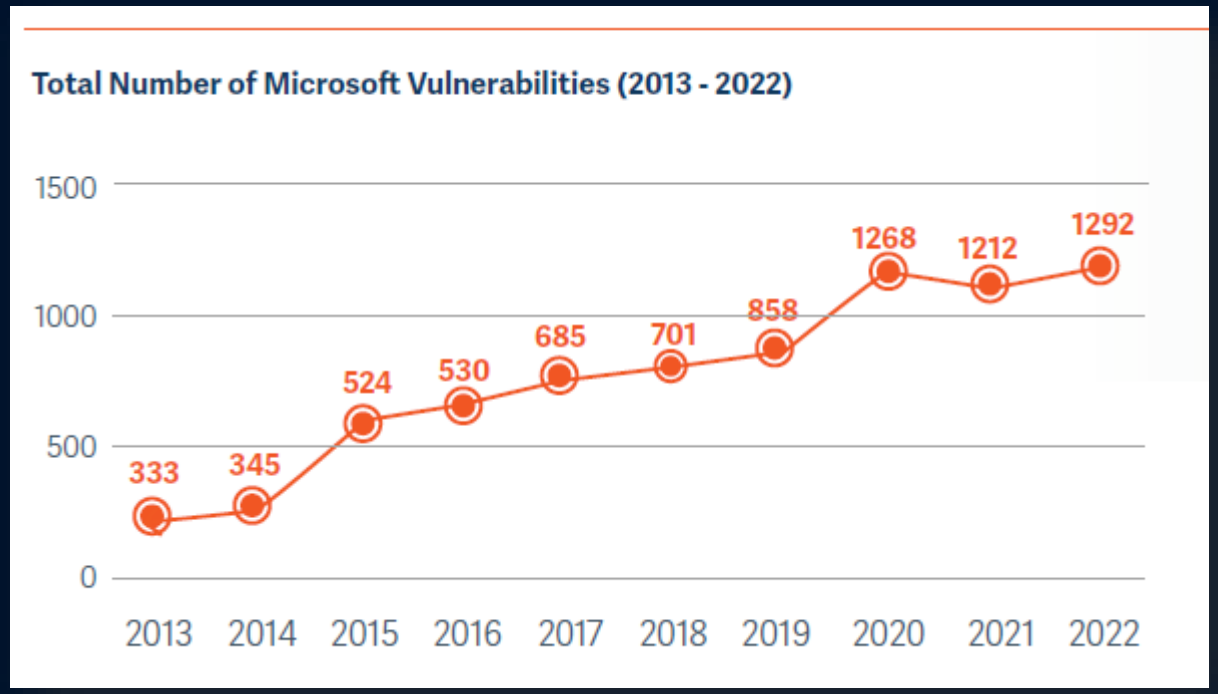
RaaS



*Truesec Threat Intelligence Report 2023

Year 2022





- All time high on Vulnerabilities – 10 year low on Critical Vulnerabilities
- Around 20000 patches for an enterprise

* BeyondTrust Microsoft Vulnerabilities Report

Finland in 2022

- 32,4 M€ scammed from people
  - Romance scams: 9 M€
  - Business Email compromise: 4,9 M€
  - Investment scams: 8,5 M€
- 14,5 M€ prevented by officials

- More than RansomWare…

PANKKIEN TIETOON TULLEET HUIJAUKSET

01-06 / 2022 ja 2023

Huijauksien kokonaismäärä: 35,7 milj. eur

Suomalaiset menettäneet verkkorikollisille

10,8 → 19,8 milj.eur (82 %)

Pankkien estämät ja palauttamat maksut

6,7 → 15,9 milj.eur (139 %)

Dokumentti- ja rakkaus-huijaukset

3,8 → 4,9 milj.eur (29%)

Sijoitus-huijaukset

3,3 → 8,2 milj.eur (155%)

taloudellisesti suurin, 37 % kaikista huijauksista

Toimitusjohtaja-huijaukset

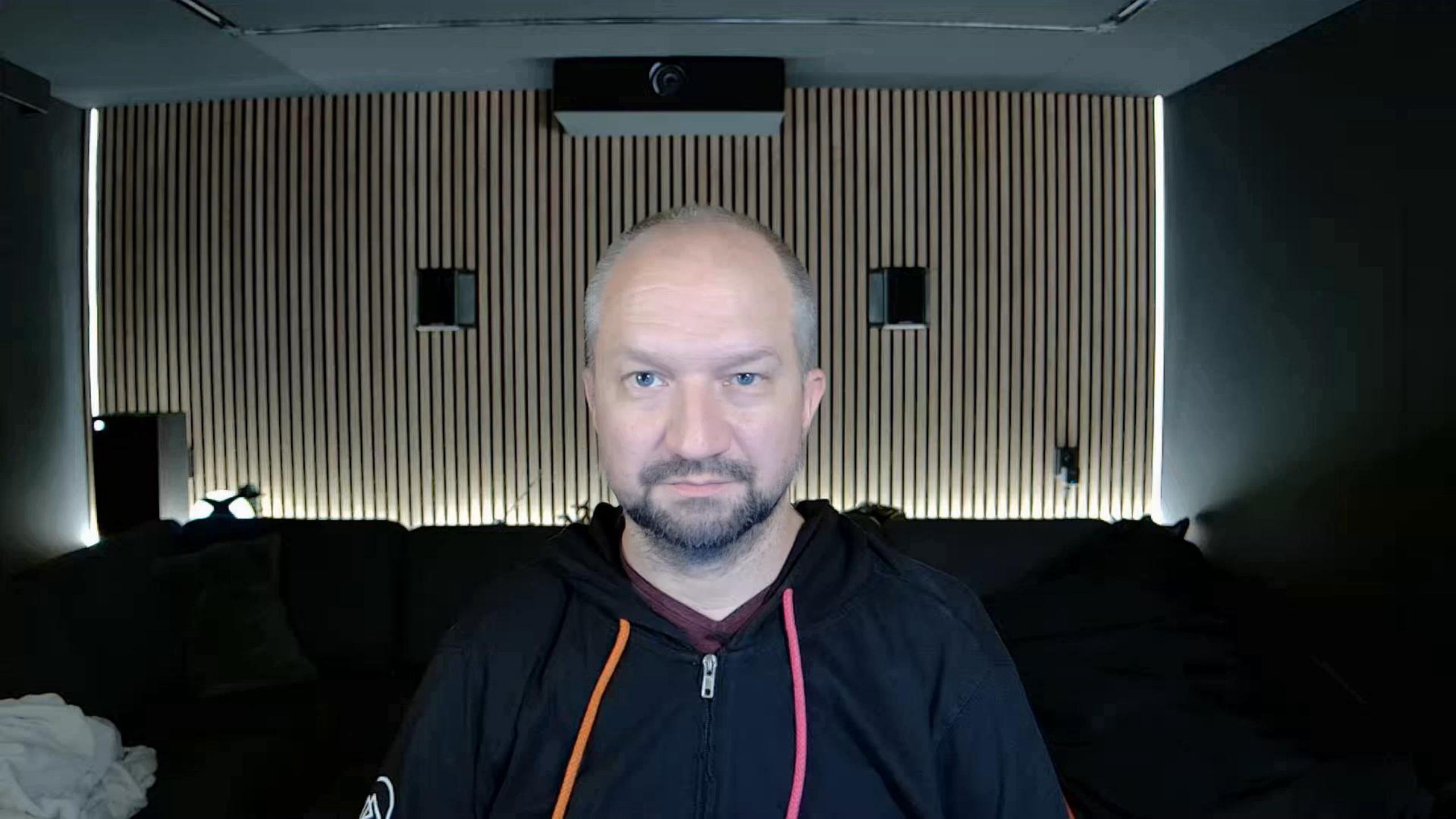
1,1 → 1,9 milj.eur (31 %)

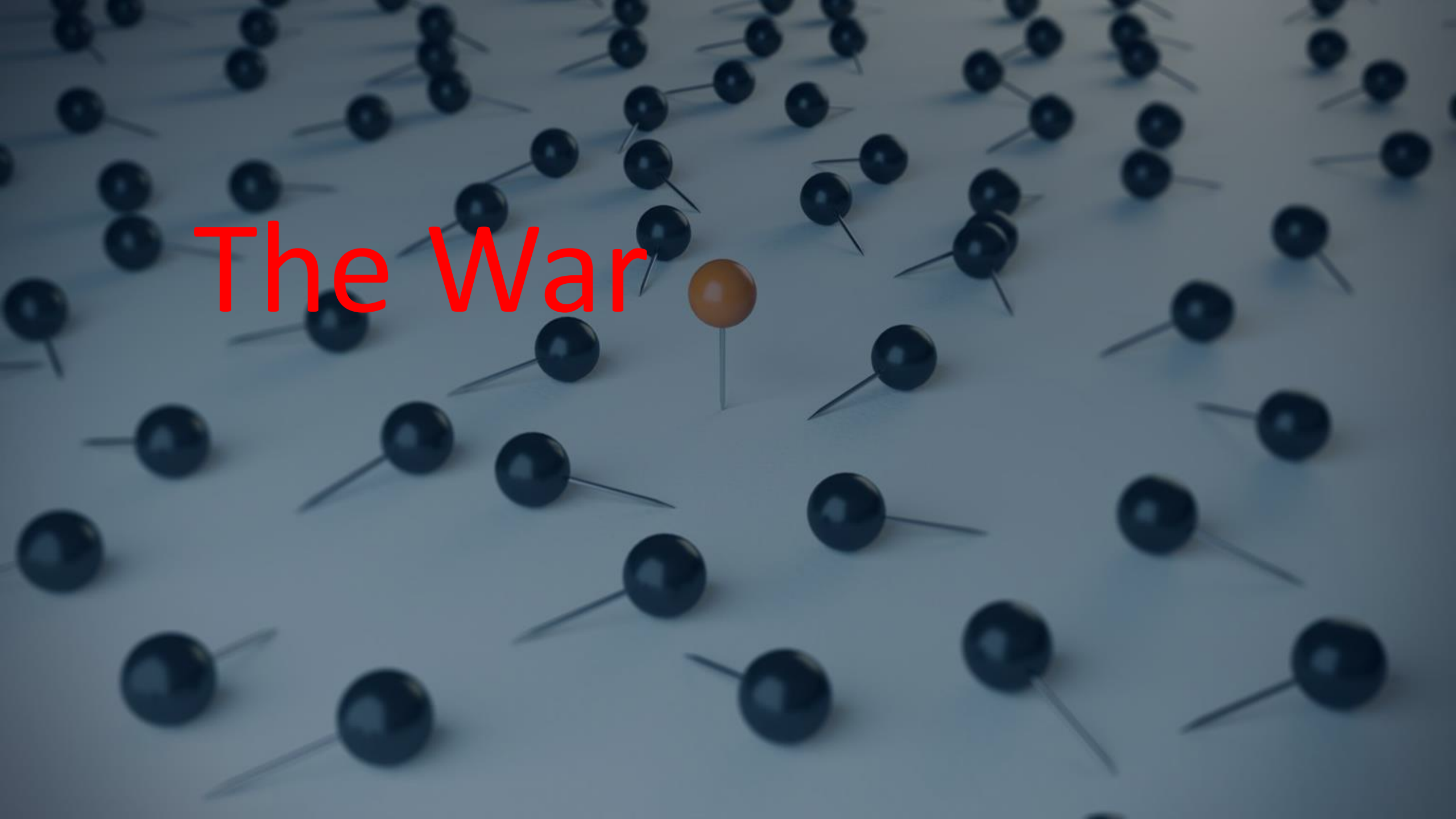
Valepoliisihuijaukset ja tietojen kalastelu

2,6 → 5 milj.eur (93%)

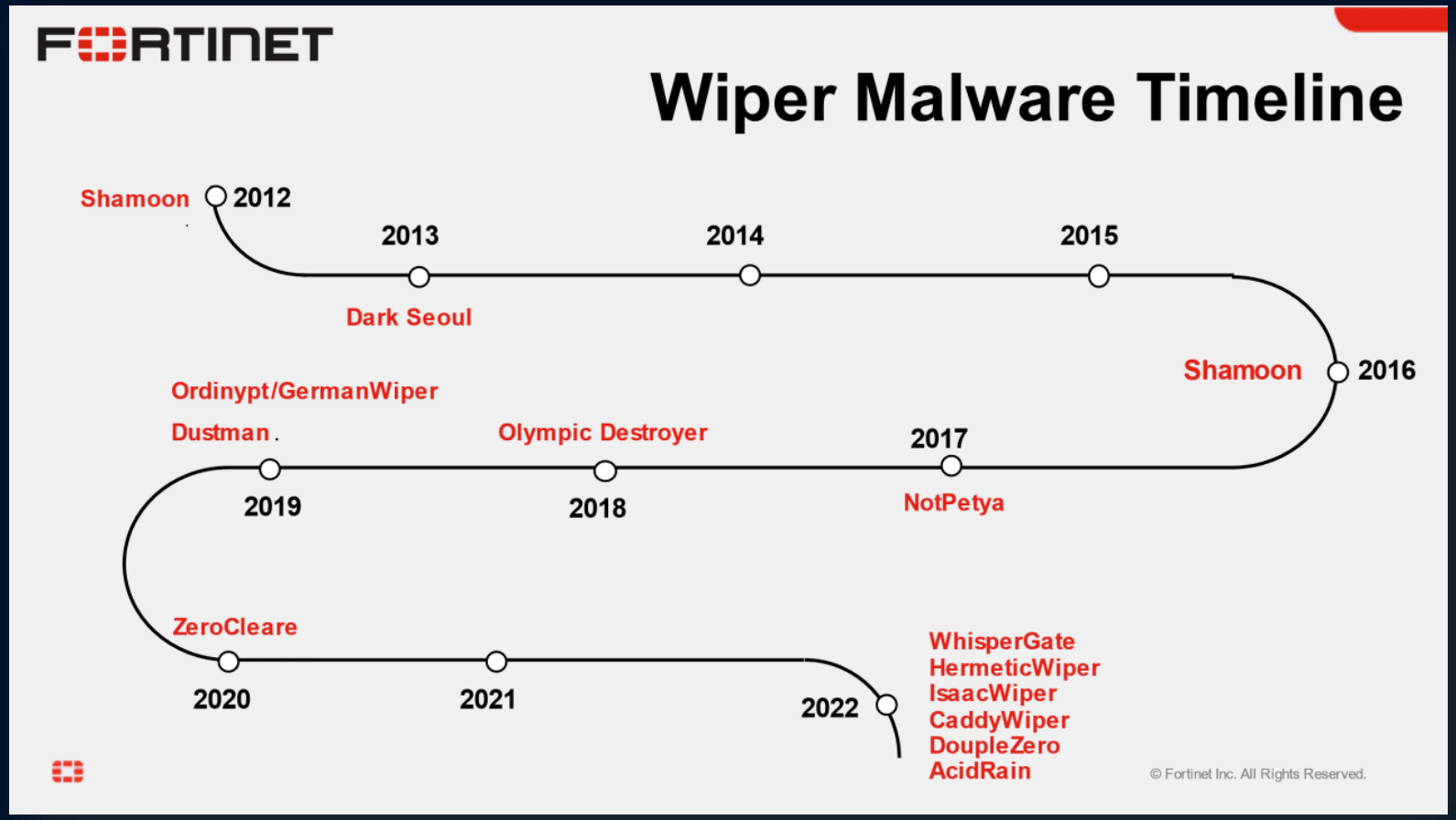
kappalemäärällisesti suurin, 78 % kaikista huijauksista

600 milj. maksutapahtumaa, joista n. 6300:ssa väärinkäytöksiä (01-06/2023) / **1,2 mrd.** maksutapahtumaa vuositasolla

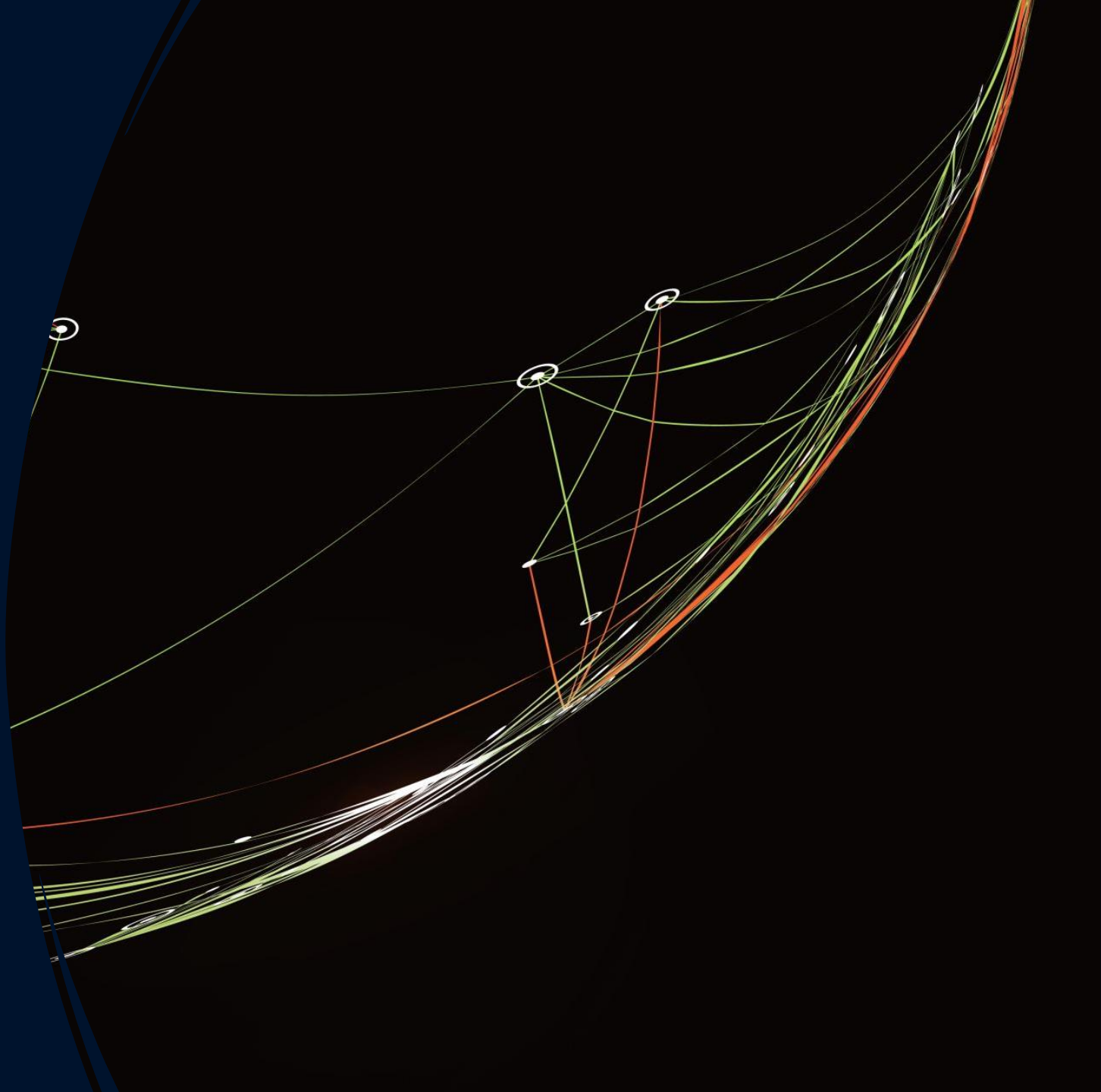



The War

Wipers

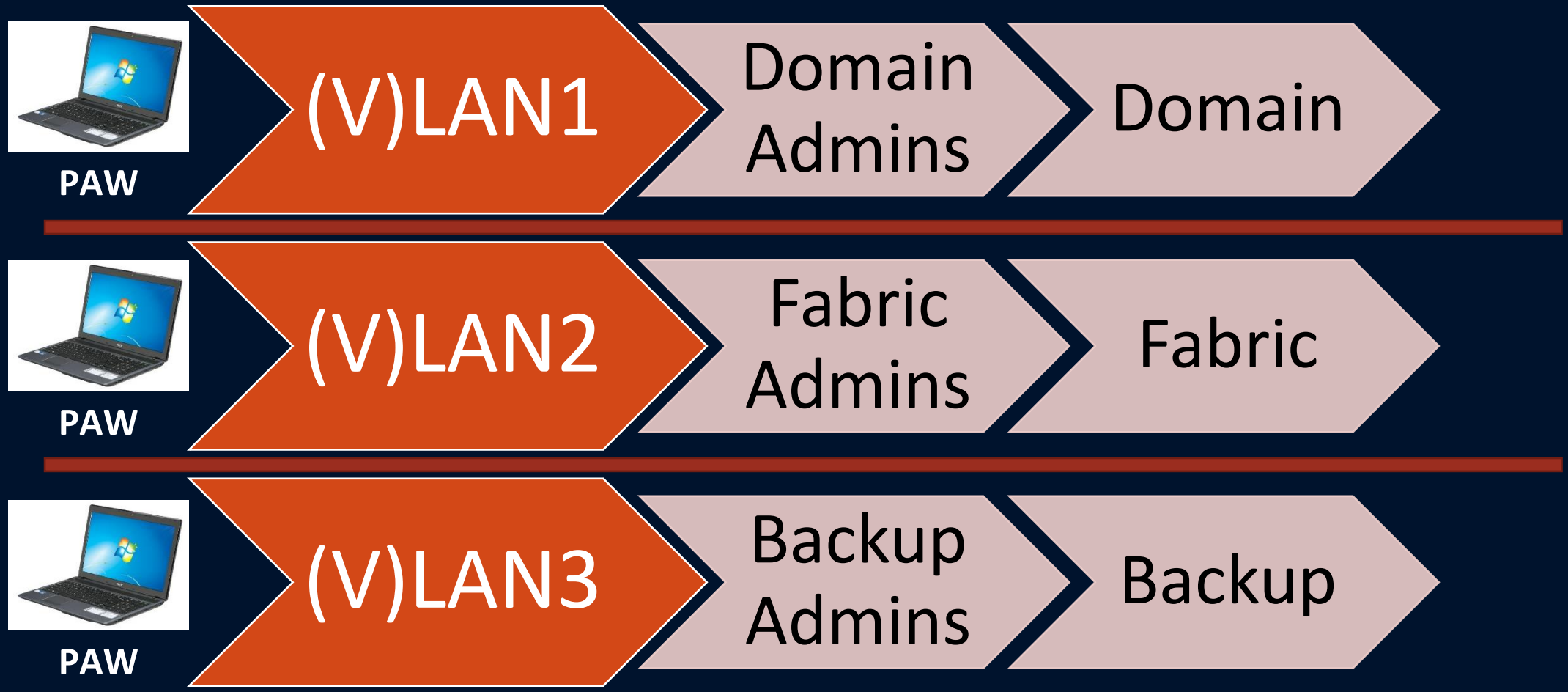

FORTINET
Wiper Malware Timeline
Shamoon
2012
2013
2014
2015
Dark Seoul
Shamoon
2016
Ordinypt/GermanWiper
Dustman
Olympic Destroyer
2017
2019
2018
NotPetya
ZeroCleare
2020
2021
2022
WhisperGate
HermeticWiper
IsaacWiper
CaddyWiper
DoupleZero
AcidRain
© Fortinet Inc. All Rights Reserved.

Recommendations for 2023→



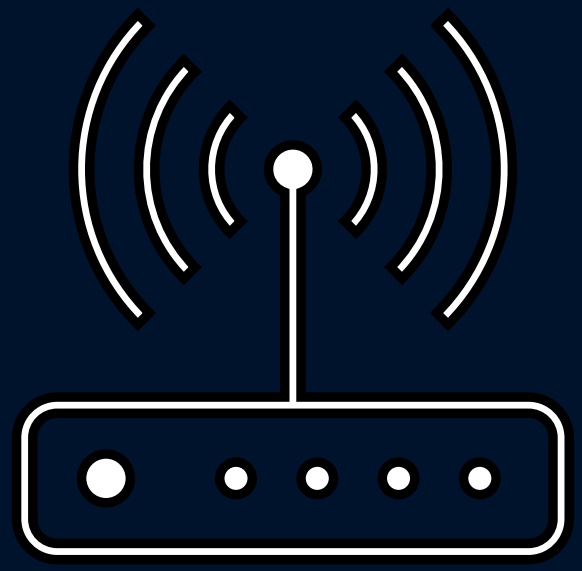
Recommendations for 2023

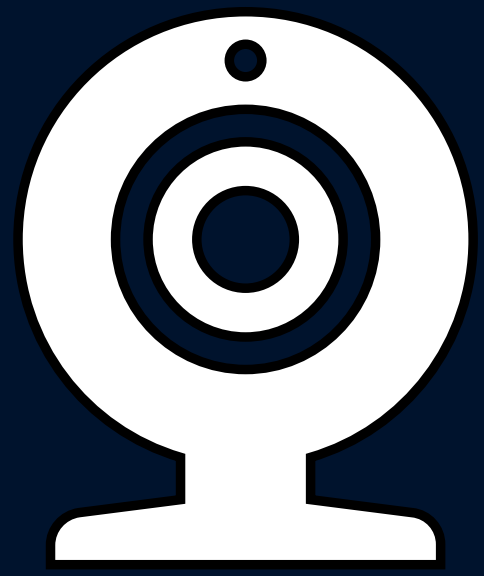
- Tier Domain / Fabric / Backups
- Patch more, test less – as hard as it sounds
- Remove end-user Admin-rights
- Deploy Application Control
- Enforce MFA
- Invest in user awareness
- Tier your Directories
- Implement Privileged Access Workstations (PAW)
- Establish or outsource a SOC



You need IMMUTABLE backups!!!


Vulnerabilities

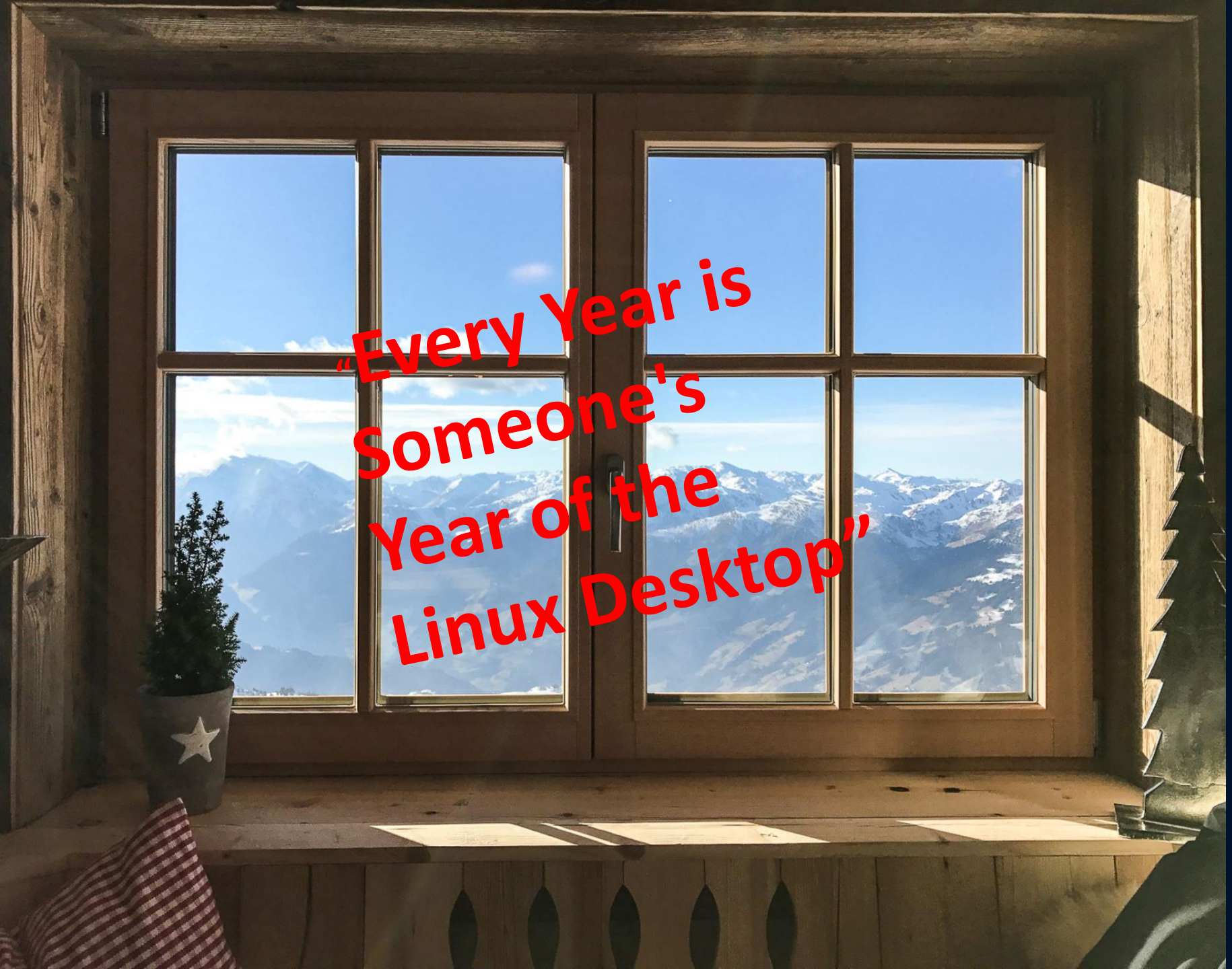




First Vector

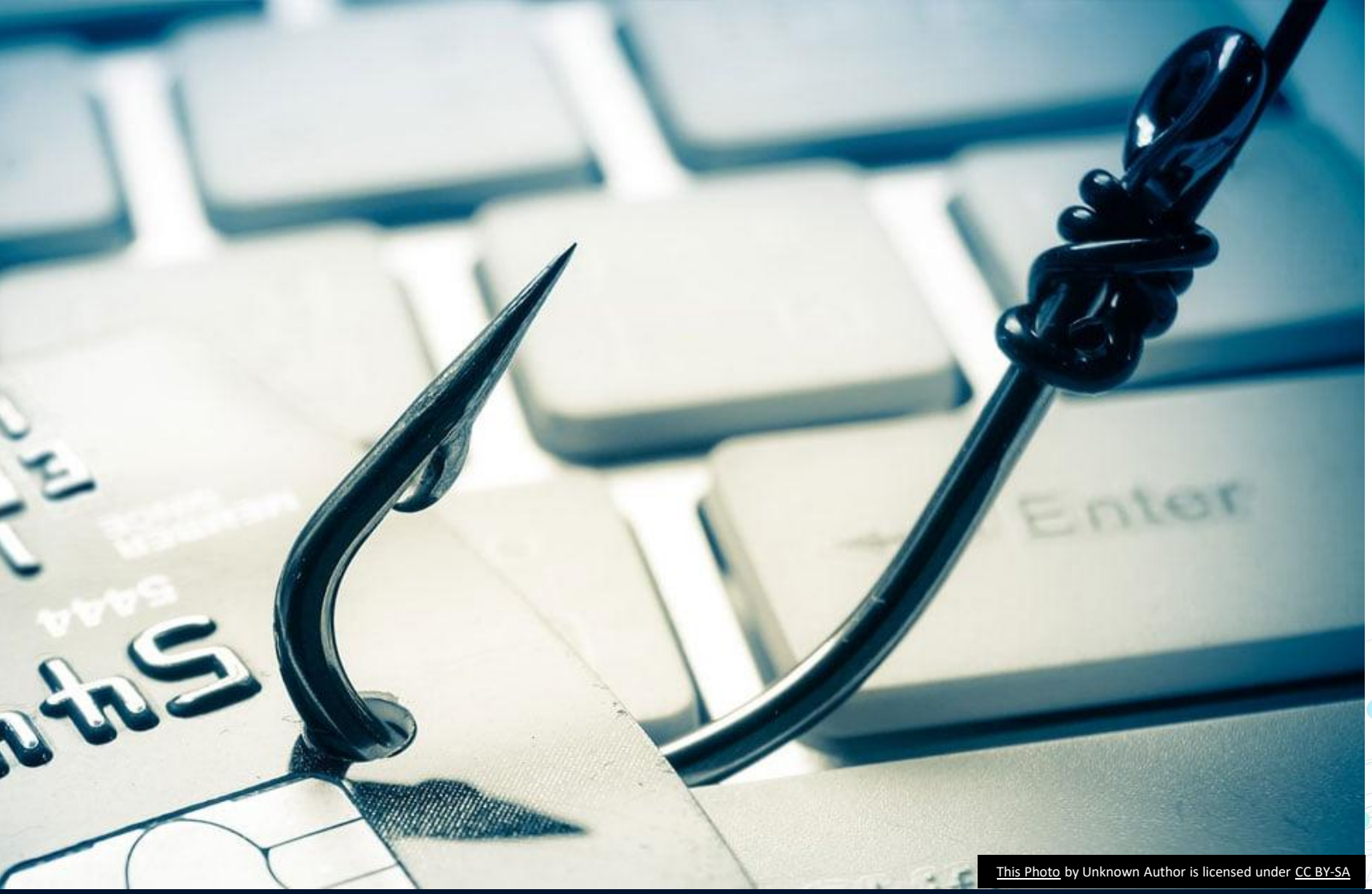
Read: “Linux”

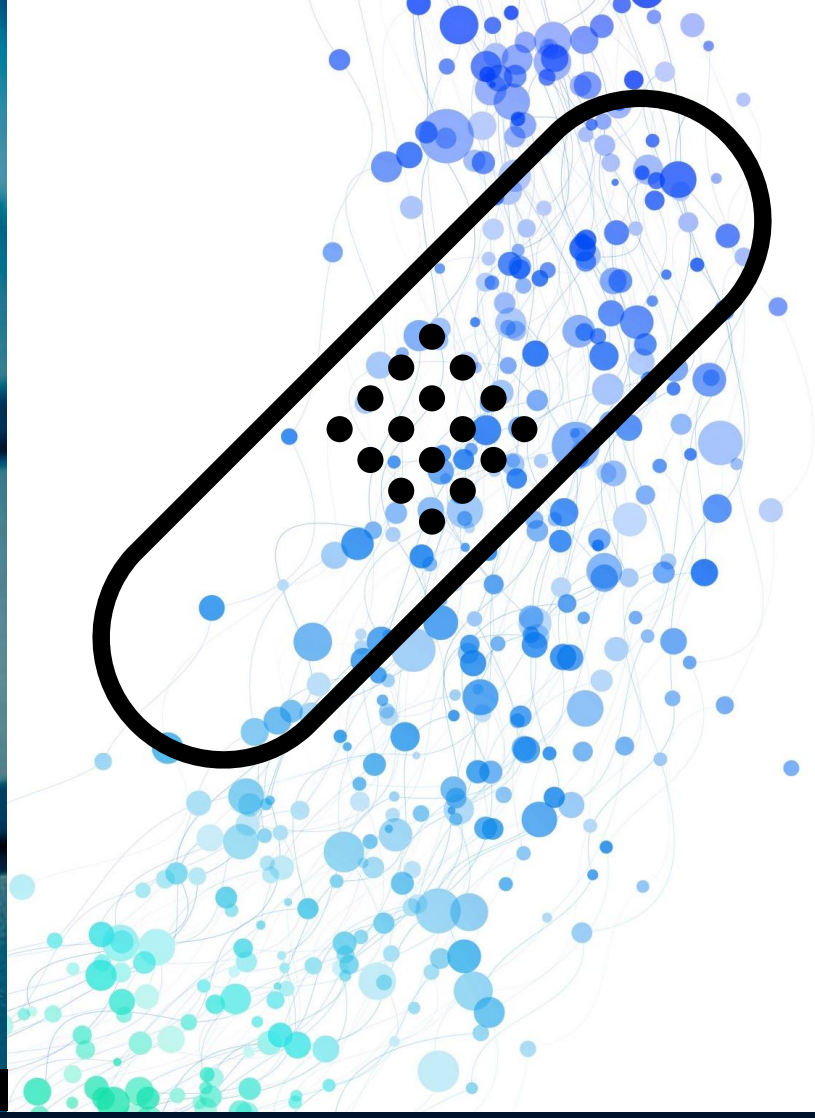

Shodan



Getting in (and they will) doesn’t get you on the news!

We need Windows to do that!





Phishing vs Vulnerabilities


Vulnerabilities
Patch More, Test Less

Principle of Least Privilege

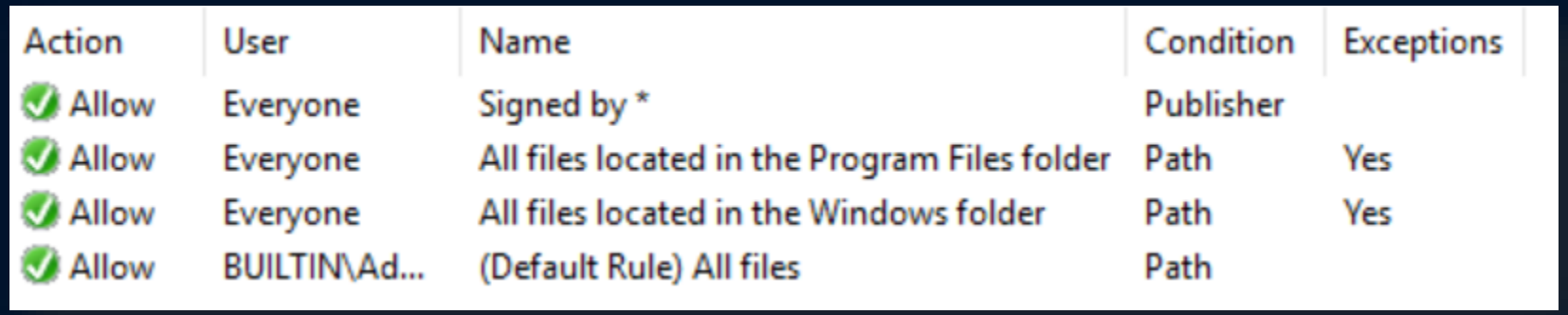
- In Windows there is no Security if you logon as an admin
- The security subsystem was not built to withstand the use of admin rights
- With “No-Admin” approach
  - We get better performance
  - We get less tickets
  - We get less reinstallation
  - We get more productive users!
  - We get less malware
  - We get to be lazier as admins!

Admin Rights are not Human Rights

https://www.zazzle.com/store/adminize/products

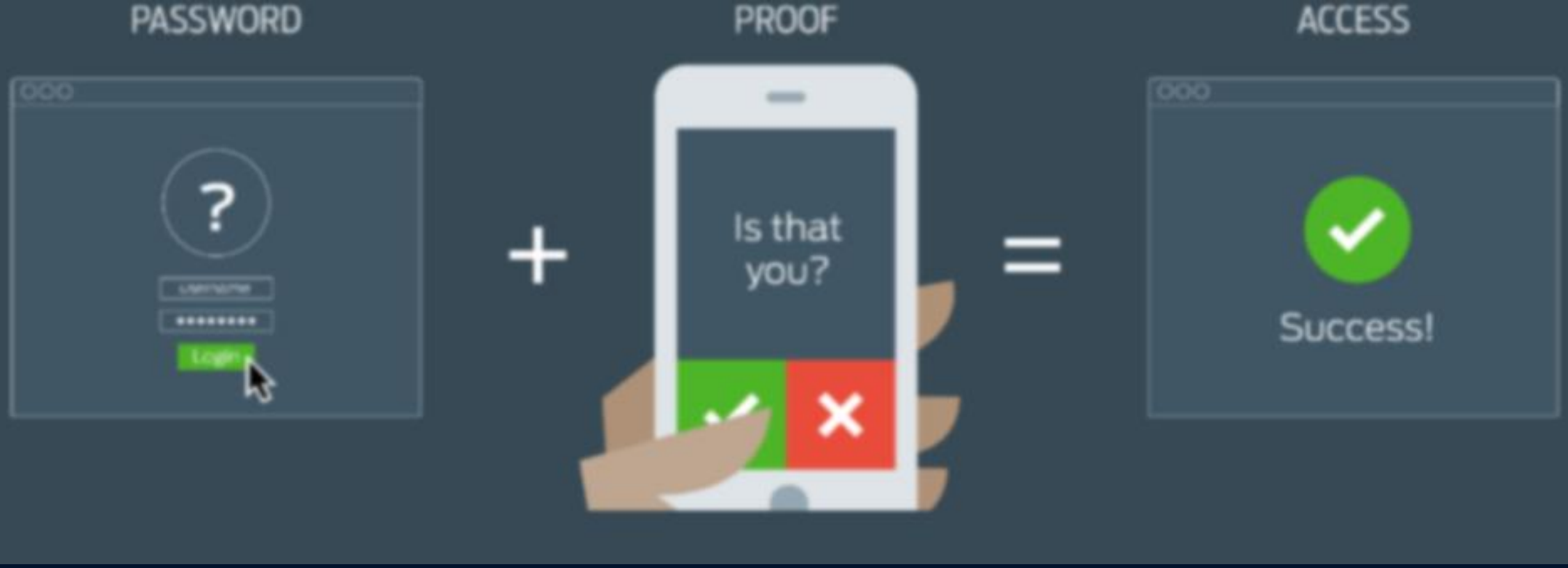
Simplest AppLocker

- THIS KILLS 950000+ PIECES OF MALWARE PER DAY!! With no Anti-Malware ☺



Action	User	Name	Condition	Exceptions
Allow	Everyone	Signed by *	Publisher	
Allow	Everyone	All files located in the Program Files folder	Path	Yes
Allow	Everyone	All files located in the Windows folder	Path	Yes
Allow	BUILTIN\Ad...	(Default Rule) All files	Path	

AppLocker now on Pro



Laiho’s Law

“If you RDP, you MFA”

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]

Ransomware Deployment Protocol

Password Quality

Passwords – Top 100 Breached Passwords

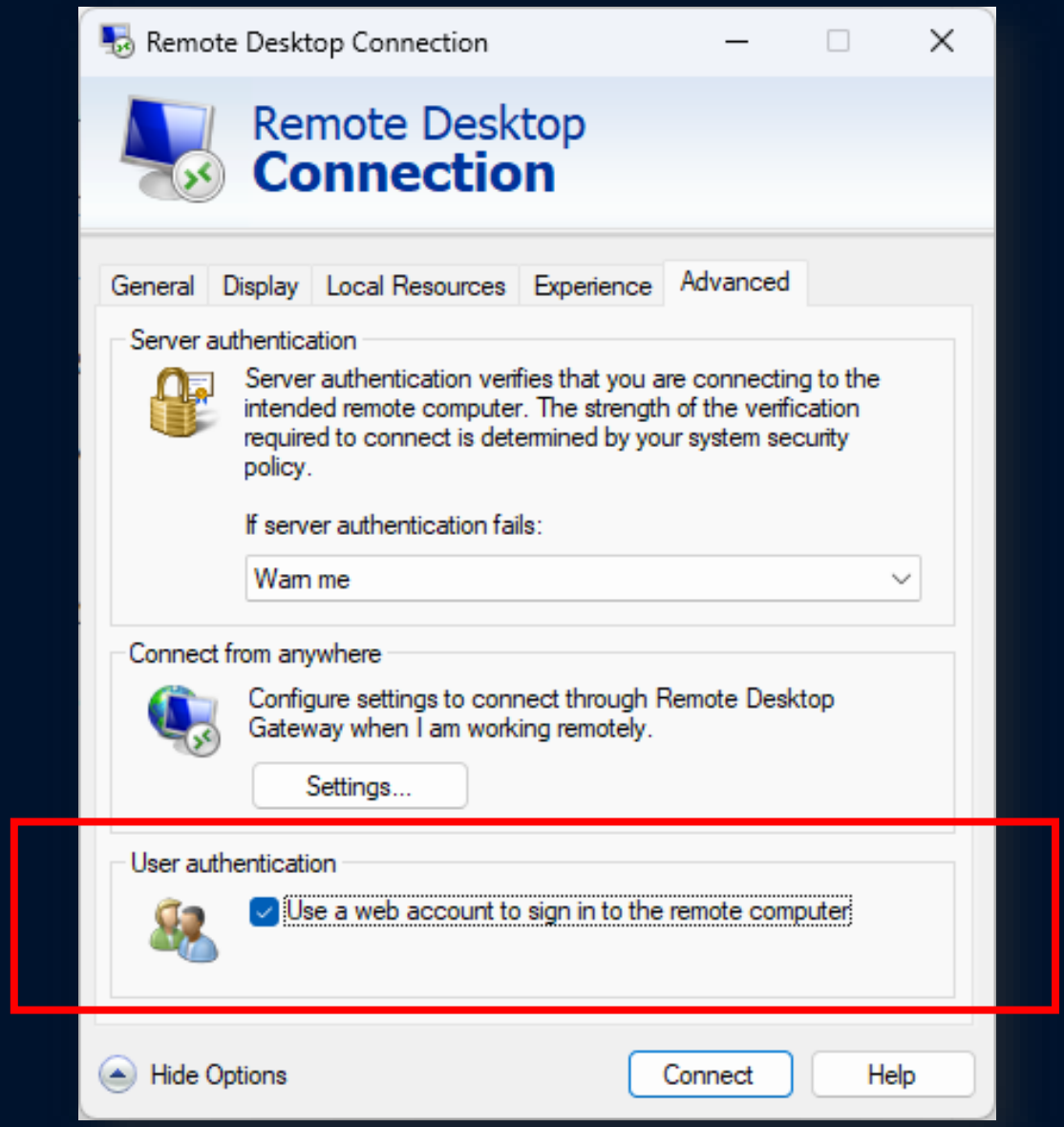
- 014745880
- 1804090178Ds
- 1q2w3e4r
- aleksi
- antero
- asdasd11
- aurinko
- banaani
- Finlandia
- greippi13
- hemuli
- jalkapallo
- Jipijaije1
- **kikkeli**
- **koira123**
- Mohammadkhizar1
- moimoi
- None
- ohe1ohe
- oong6aet
- Qpa9Zm1o
- Qvidja123
- samuli
- SZ9kQcCTwY
- tiikeri
- Tk0pljes
- **trustno1**
- 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

Swedes

- 812057bk
- hammarby
- Hejhej123
- hemligt
- jalojalo77
- LCalice9
- losenord
- Mamma123
- marcus
- quinty1980
- qwe123
- sixten
- staffan
- BpdQfeF1
- cocacola
- morris
- N55k0ba31u@
- qwertyuiop
- rasmus
- skrotnisse08
- Sommar2019
- Sommar21
- thaimiNoop
- fotboll123
- Hejsan123
- johanna
- linnea
- Max1234
- Skolan4a
- Tradera77
- 666666
- amanda
- daniel
- Ekeby2020@@@
- Ekeby2021@@@
- fotboll
- smulan
- Teater13
- 111111
- Cerwinvega@11
- guntles1999
- helloo
- Pelikan1
- 1234567
- 1234567890
- Sommar2020
- 46530011
- abcd1234
- anders
- blomma
- hejhej123
- mormor
- skola123
- Sommar19
- mamma123
- scania142
- manjari77
- MicMusic67
- hej123
- LLq45b93###
- lol123
- Pakistan@123
- scania
- Skola123
- Welcome1
- asdfghjkl
- Failad123
- deqasdQ
- Sommar20
- 1234
- bajskorv
- m9a98ckq
- zinch
- 123123
- jayajaya
- jablko96
- luckydayel
- zebraman
- klumpf0t
- lj1210
- v11scxad12
- marmar
- fuffen
- abc123
- hejhej
- hejsan123
- qwerty
- sommar
- password
- hejsan
- 12345
- Asptuna14144
- Manjari77
- None
- NULL
- 123456789
- 66456xyz
- 123456
- 12345678
- hugo526205

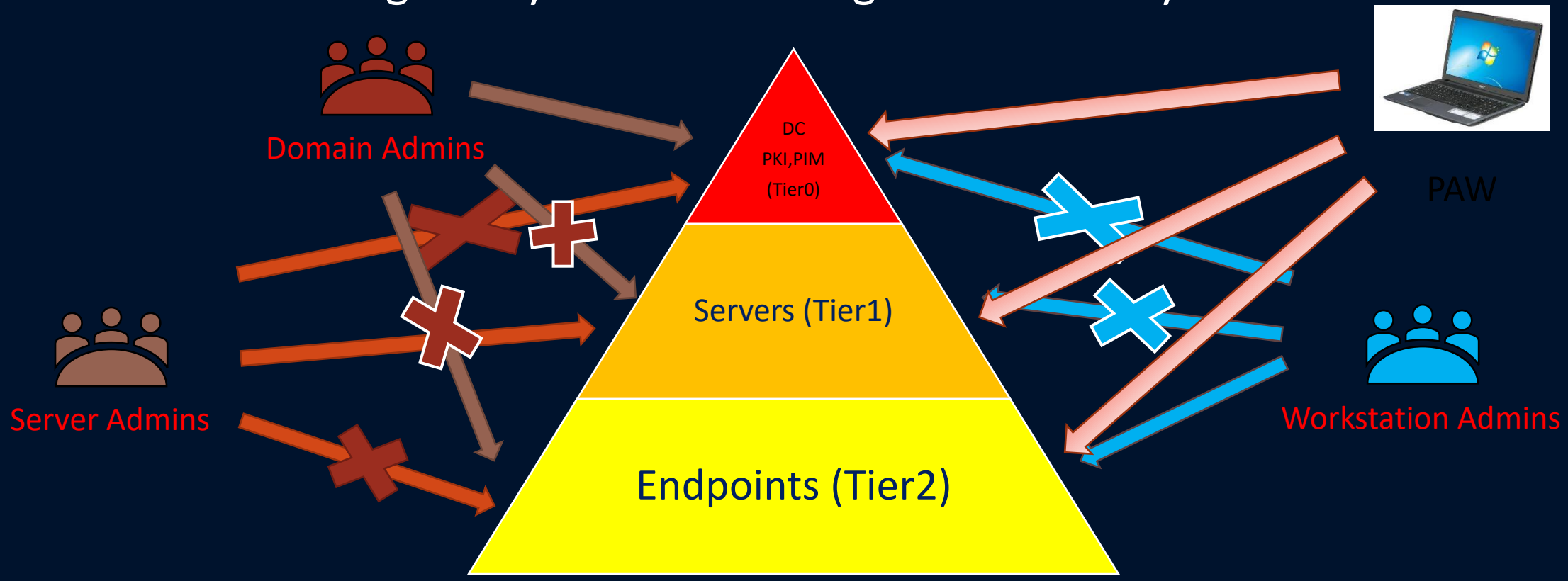
Yubikeys

https://swjm.blog/the-complete-guide-to-rdp-with-yubikeys-fido2-cba-1bfc50f39b43



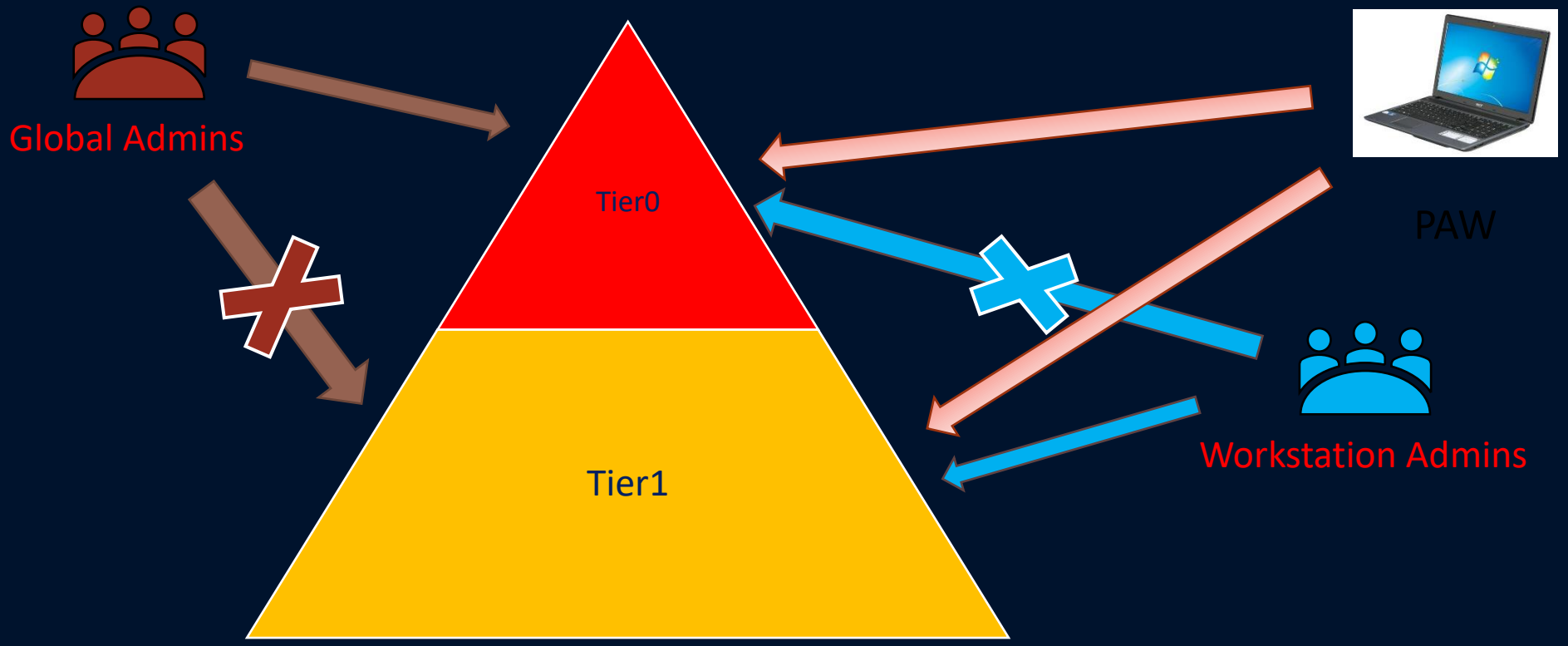
Tier your Directories on-prem…

- Split your environment into three tiers
- Never allow higher layer admins to logon to lower layers



… or in the Cloud

- Split your environment into two layers
- Never allow higher layer admins to logon to lower layers



Limit the Attack Surface

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…

Baselines

- Remember, Windows OS is the same for companies and homes. Settings are based on the weakest link. If you buy Pro or Ent version, it doesn’t change the security policy… So, if you haven't installed the baselines from Microsoft or CIS etc., you are running Corporate Computers with security settings for a Home Computer...
- https://www.cisecurity.org/benchmark/microsoft_windows_desktop
- https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines

Local Group Policy Editor

File Action View Help

Local Computer Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Privilege Management Settings
  - Administrative Templates
    - Control Panel
    - Microsoft Edge
    - Microsoft Edge - Default Settings (users
    - Microsoft Edge Update
    - Microsoft Edge WebView2
    - Network
    - Printers
    - Server
    - Start Menu and Taskbar
    - System
      - Access-Denied Assistance
      - App-V
      - Audit Process Creation
      - Credentials Delegation
      - Device Guard
      - Device Health Attestation Service
      - Device Installation
        - Device Installation Restrictions

13 setting(s)

Device Installation Restrictions

Prevent installation of devices using drivers that match these device setup classes

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for driver packages that Windows is prevented from installing. By default, this policy setting takes precedence over any other policy setting that allows Windows to install a device.

NOTE: To enable the "Al
installation of devices th
any of these device IDs"
and "Allow installation c
that match any of these
instance IDs" policy sett

Extended Standard

Setting	State
Allow administrators to override Device Installation Restriction policies	Enabled
Apply layered order of evaluation for Allow and Prevent device installation policies across ...	Not configured
Allow installation of devices using drivers that match these device setup classes	Not configured
Prevent installation of devices using drivers that match these device setup classes	Enabled
Display a custom message when installation is prevented by a policy setting	Enabled
Display a custom message title when device installation is prevented by a policy setting	Enabled
Allow installation of devices that match any of these device IDs	Not configured
Prevent installation of devices that match any of these device IDs	Not configured
Allow installation of devices that match any of these device instance IDs	Not configured
Prevent installation of devices that match any of these device instance IDs	Not configured
Time (in seconds) to force reboot when required for policy changes to take effect	Not configured
Prevent installation of removable devices	Not configured
Prevent installation of devices not described by other policy settings	Not configured

Prevent installation of devices using drivers that match these device setup classes

Prevent installation of devices using drivers that match these device setup classes

Previous Setting | Next Setting

Not Configured
Enabled
Disabled

Comment:

Supported on: At lea

Options:

Prevent installation of devices using drivers fo
these device setup classes:

Show...

To create a list of device classes, click Show. In
Show Contents dialog box, in the Value colum

type a GUID that represents a device setup cla

(for example, {25DBCE51-6C8F-4A72-8A6D-
B54C2B4FC835}).

Also apply to matching devices that are already installed.

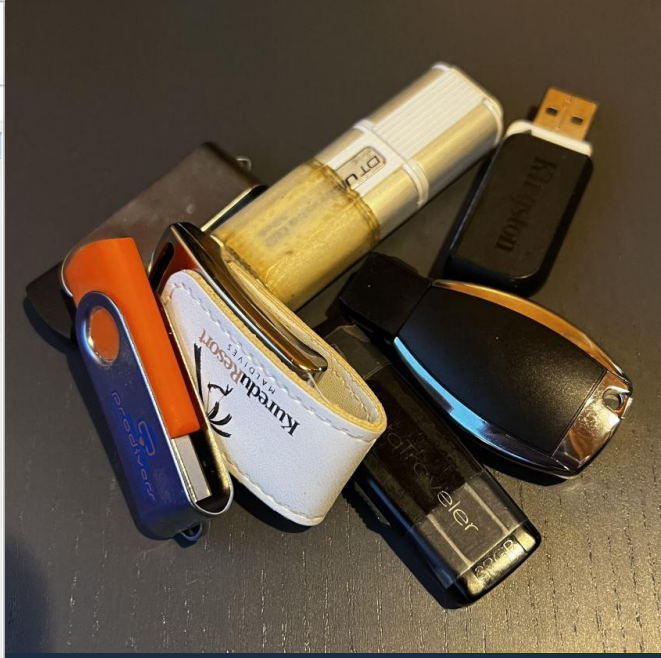
If you enable this policy setting, Windows is prevented from installing or updating driver packages whose device setup class

Show Contents

Prevent installation of devices using drivers for these device setup classes:

Value
{4d36e967-e325-11ce-bfc1-08002be10318}

OK



Settings

BLOCKED DEVICE!

If you need access to USB driver, contact SD!

2°C Pilvistä ENG 11.55 8.3.2022

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

Contact

- sami@adminize.com
- Twitter: @samilaiho
- Free newsletter: http://eepurl.com/F-Goj

- My trainings:
  - https://corellia.fi/sami-laiho-courses/
- https://win-fu.com/dojo/
  - Free for one month!!
    - Promo Code: TRIAL2023