Patch More, Test Less

— Blocking the Most Common Attack Vector in 2023!

Sami Laiho

Chief Research Officer, MVP

Adminize

Sami Laiho

Chief Research Officer /
Senior Technical Fellow, MVP

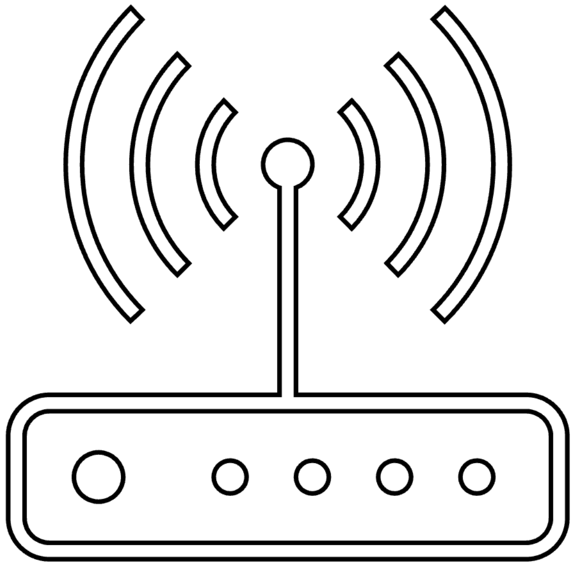
- IT Admin since 1996 / MCT since 2001
- MVP in Windows OS since 2011
- **”100 Most Influencal people in IT in Finland” – TiVi’2019, 2020, 2021**
  - **Among Top 10 most followed techies on Twitter in Finland**
- Specializes in and trains:
  - Troubleshooting
  - Windows Internals
  - Security, Social Engineering, Auditing
  - Centralized Management, Active Directory
- Trophies:
  - Best Speaker at Nordic Virtual Summit 2021
  - 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
  - TechEd Europe 2013 - Best Session by an external speaker

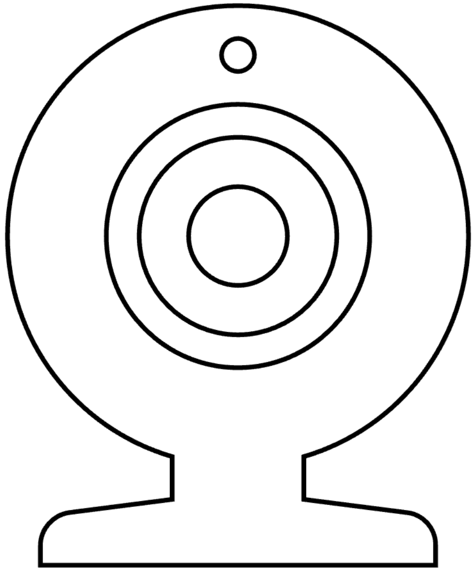
Twitter(X)/Bluesky: @samilaiho

LinkedIn

2022

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





First Vector

Read: “Linux”

Shodan

„Every Year is Someone's Year of the Linux Desktop”

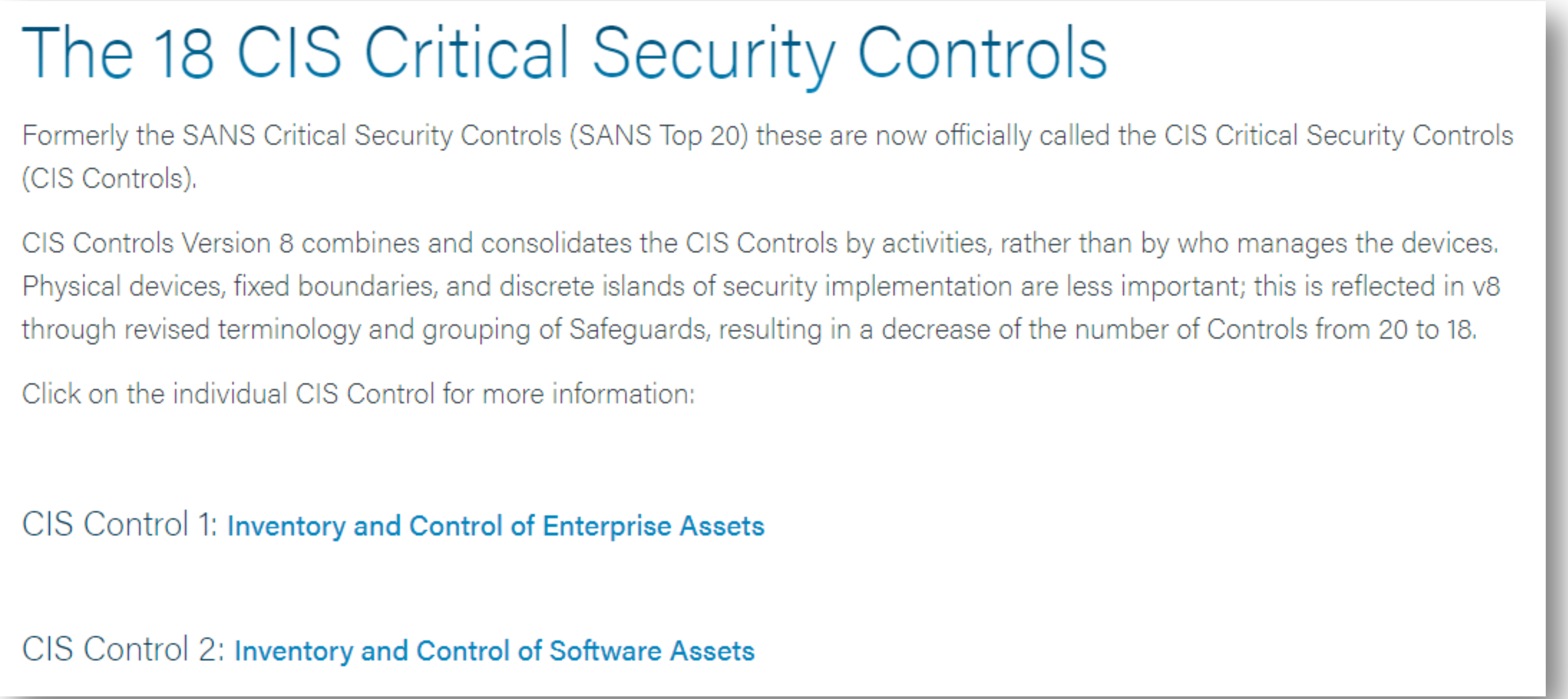
Getting in (and they will) doesn’t get you on the news!

We need Windows to do that!

Vulnerabilities

Patch More, Test Less!

You can’t Patch Unless you know what to Patch



The 18 CIS Critical Security Controls

Formerly the SANS Critical Security Controls (SANS Top 20) these are now officially called the CIS Critical Security Controls (CIS Controls).

CIS Controls Version 8 combines and consolidates the CIS Controls by activities, rather than by who manages the devices. Physical devices, fixed boundaries, and discrete islands of security implementation are less important; this is reflected in v8 through revised terminology and grouping of Safeguards, resulting in a decrease of the number of Controls from 20 to 18.

Click on the individual CIS Control for more information:

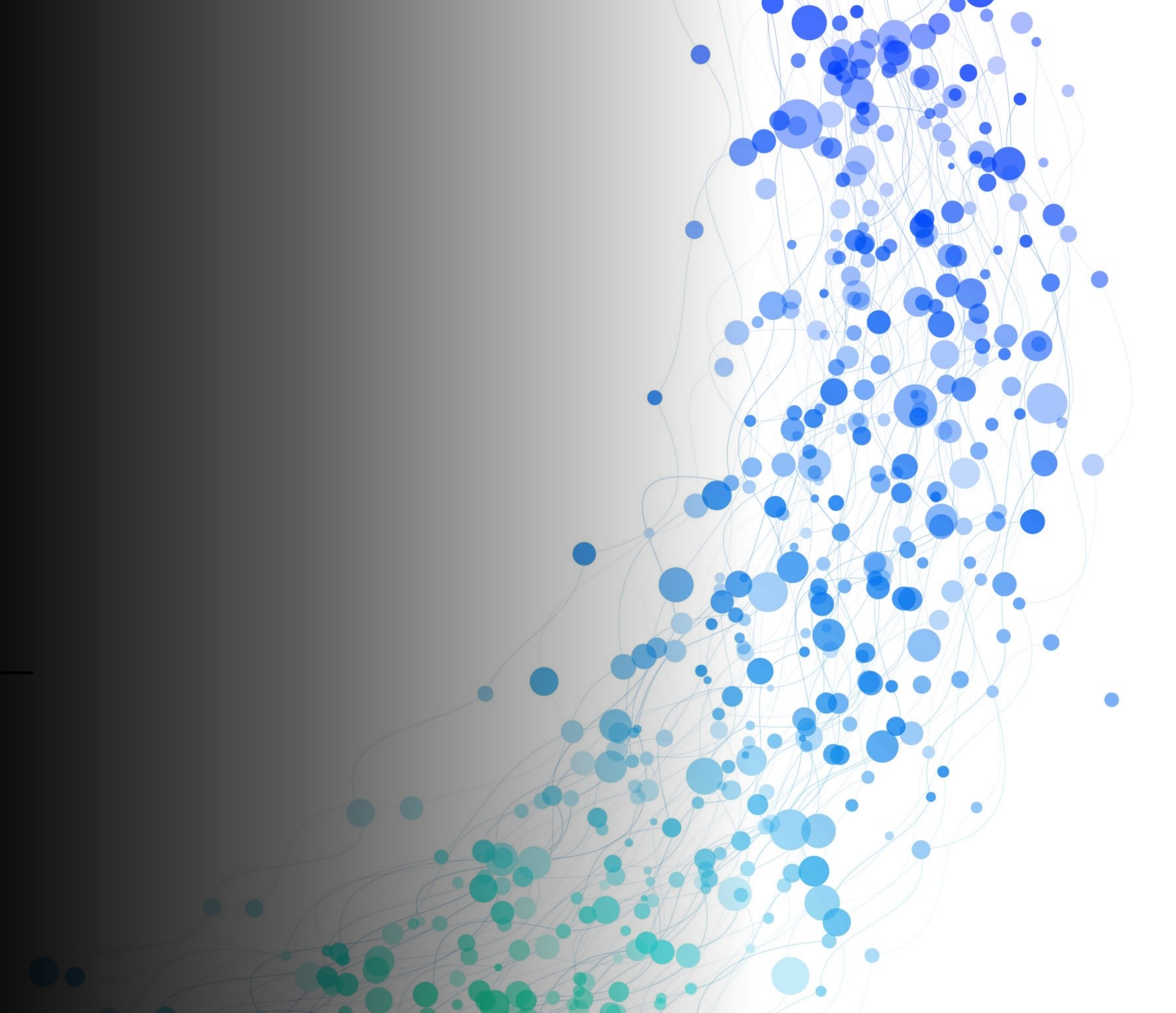
CIS Control 1: **Inventory and Control of Enterprise Assets**

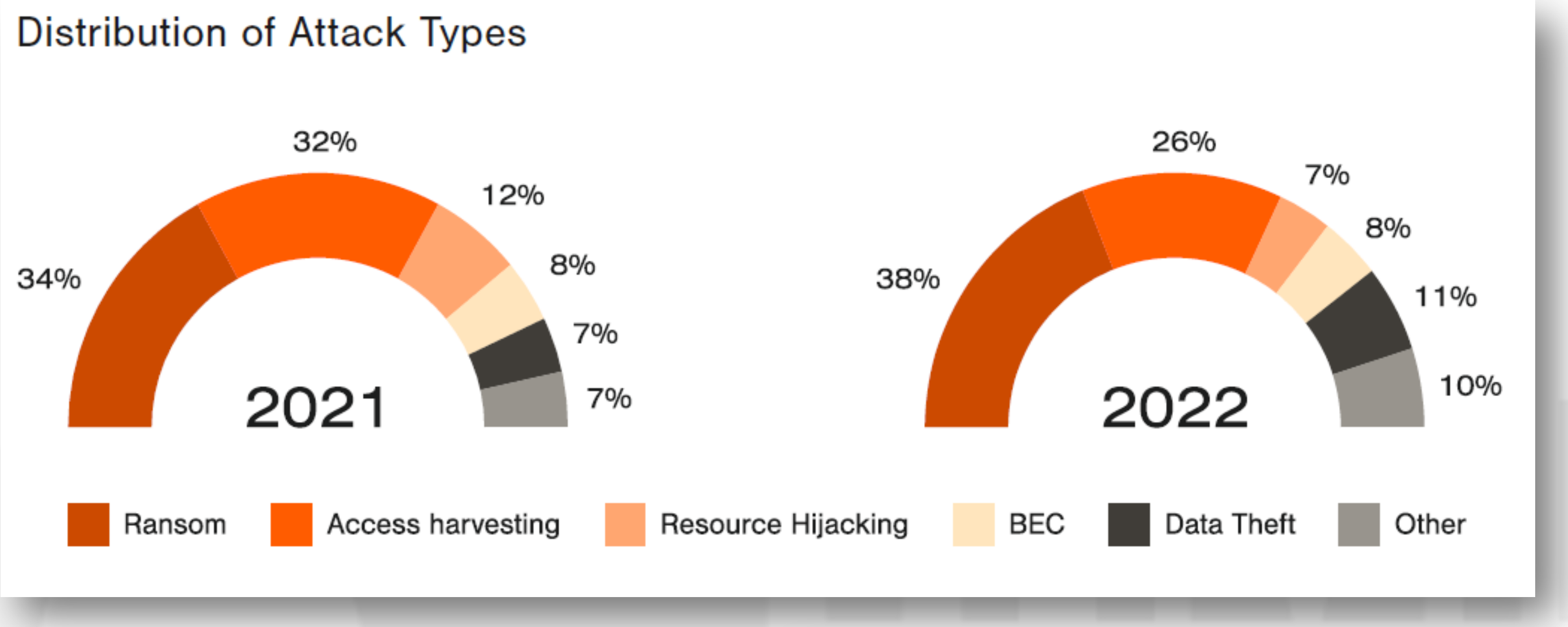
CIS Control 2: **Inventory and Control of Software Assets**

Supply Chain Attacks

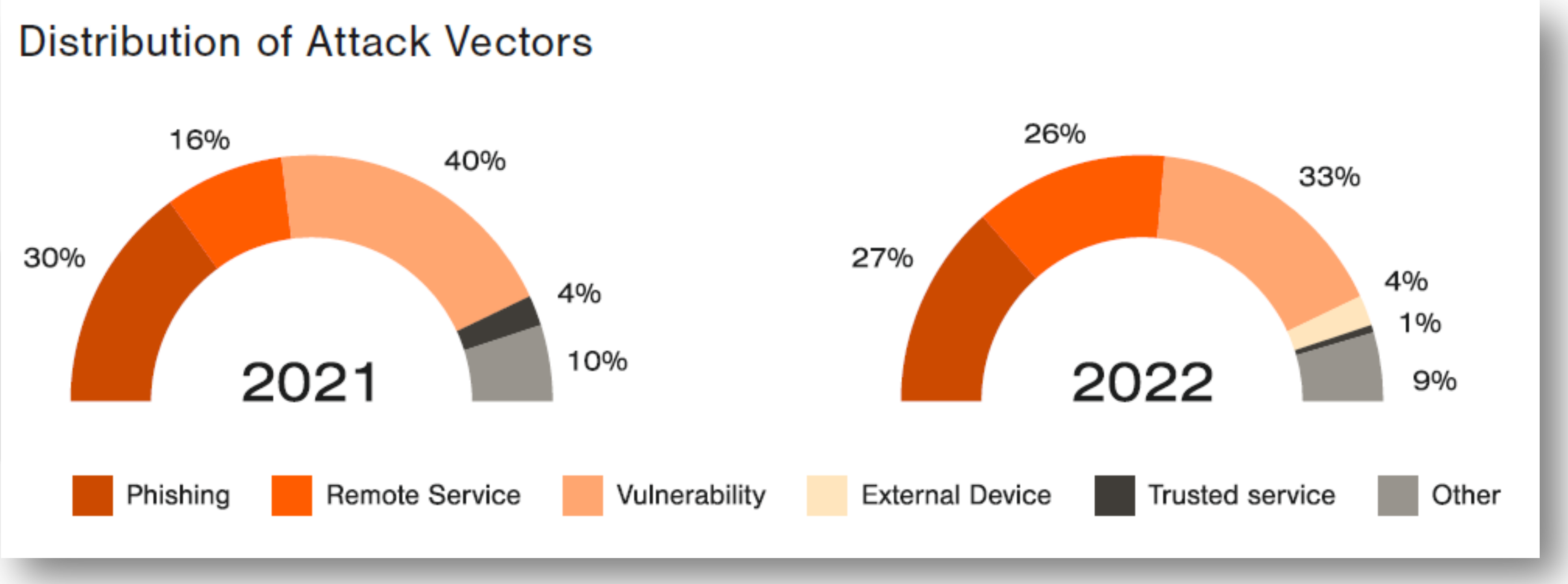
- *"In fact, Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021."*

Patching vs Phishing





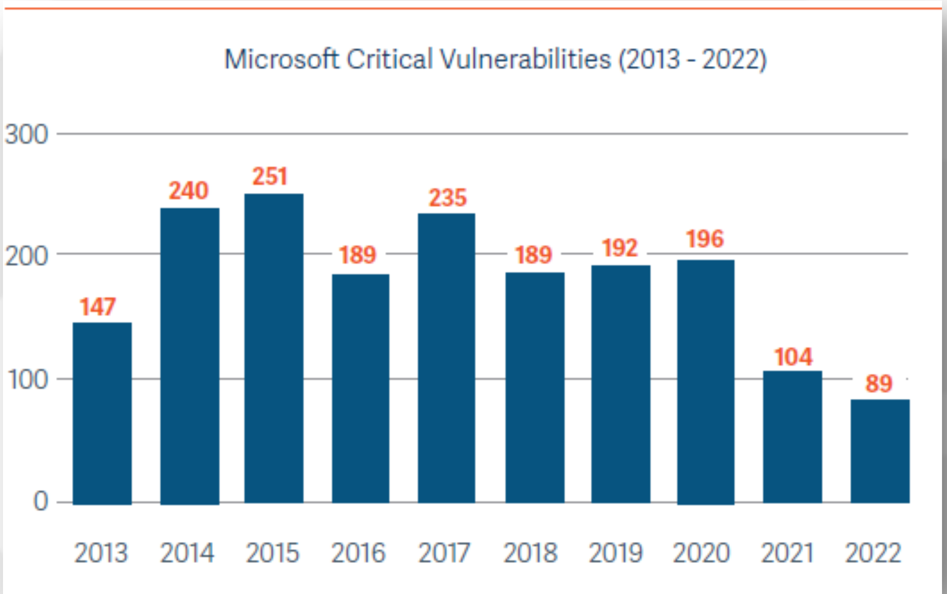
Distribution of Attack Types

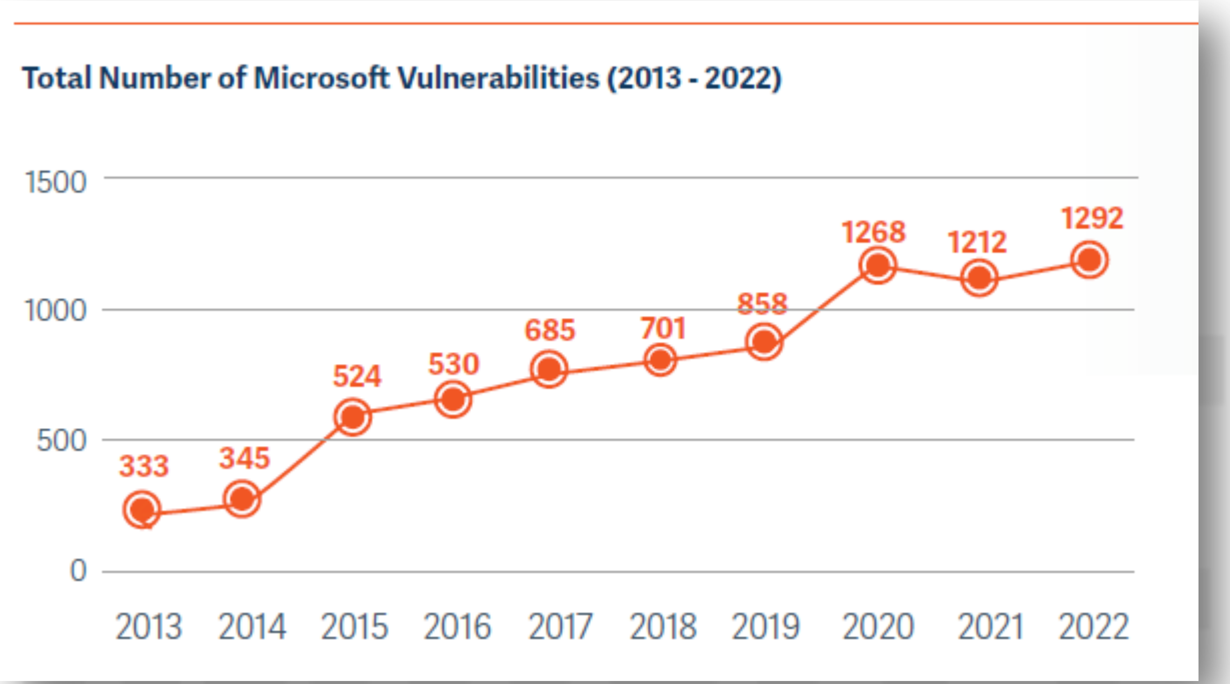


Distribution of Attack Vectors

*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

Your job is not to
Stop the enemy but
to Slow them down