PureID

Passwordless Authentication

that is **Secure & Secures** Enterprises

Incumbent solutions fail to protect...

myoffice.com

office.com

Passwords + 2FA/MFA

Authentication & Access channel

Passwords + 2FA/MFA

Attacker gets & relays credentials

***** token
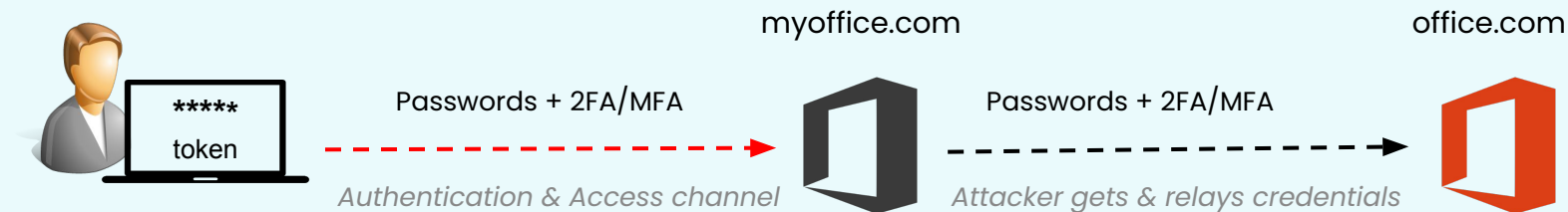
Passwords + MFA/2FA are bypassed using phishing & social engineering

Trend - Cloud/SaaS Adoption

Result - Increase in web based attacks like phishing & credential stuffing

Corben Leo
@hacker_

1/ I used Evilnginx2 to bypass MFA (Okta & Duo)

From Okta, I could access Outlook, Sharepoint, Github, & many more services on behalf of the 50+ employees that fell for the phish.

I was blown away by how easy it was to pull off this "hack" that could've impacted 60M+ people.

11:50 PM · Jan 2, 2023

48.4K Views   20 Retweets   2 Quote Tweets   394 Likes

Authentication Data leaked by Incumbents is abused

Dark Reading Staff
Dark Reading

July 19, 2022

Okta Exposes Passwords in Clear Text for Possible Theft

Researchers say Okta could allow attackers to easily exfiltrate passwords, impersonate other users, and alter logs to cover their tracks.

## Leaked passwords, MFA seeds, Biometrics data triggers next breach

Trend – Rise of Hacking Groups

Result – Data leaked from Vendors is used to attack customers

Hackers breached 2FA accounts of some Authy users, Twilio confirms

The announcement from early August said that 100 Twilio customers had their information accessed by outside sources as a result of Twilio employees being phished. Now the company has announced that 93 Authy app users have also had select information compromised.

Incumbents can verify user, but not the user's device

Only Passwords + 2FA/MFA

device & its security profile is unknown
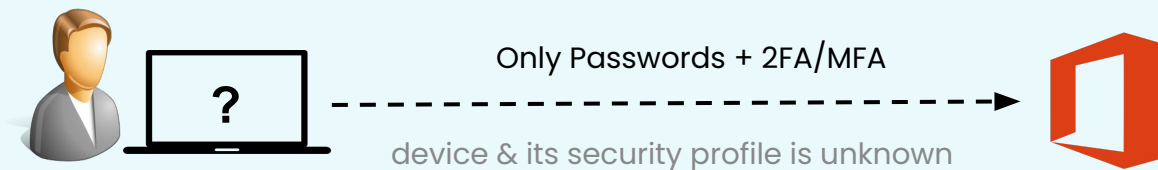
Valid user connecting with untrusted or compromised device, is a RISK

Trend - Remote Working

Result - *use of Personal, Untrusted, Vulnerable devices, helps attackers to get in enterprise systems*

IOTW: Over 77,000 Uber employee details leaked in data breach

The rideshare company's confidential information has been shared to a hacking forum

Previous Lapsus$ hack into Uber's internal systems

On September 15, 2022, a hacker used a compromised Uber EXT account to access the company's internal systems after an employee's personal device became infected with malware and their login credentials posted to the dark web.

PureAUTH Passwordless Authentication

Signatures + Device Profile
Authentication channel

SAML Response
Authentication channel

PureAUTH
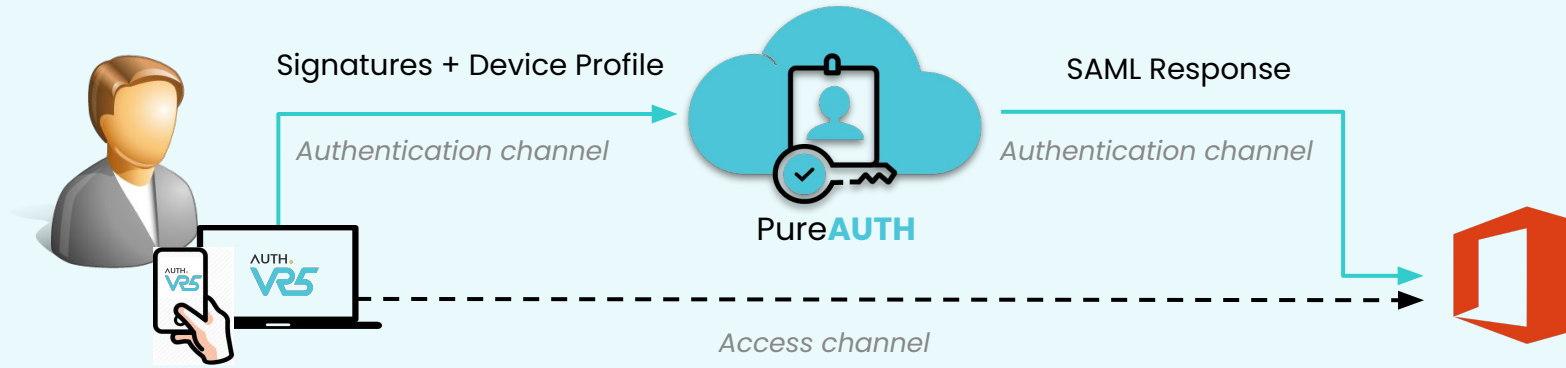
Access channel

Separate Authentication Channel

PureAUTH is designed to eliminate phishing, Identity thefts & frauds.

Digital Signature Verification

AuthVR5 authenticator app uses digital signatures, 0 Risk if leaked

Device Profile & Zero Trust Access

AuthVR5 uses signature & device profile to give *Zero Trust Access Control*

Technology Patented in India, USA & UK

How PureAUTH Works?

Explainer Video

- *https://pureid.io/pureauthdemo*

For More

- hello@pureid.io

THANK YOU

PureID