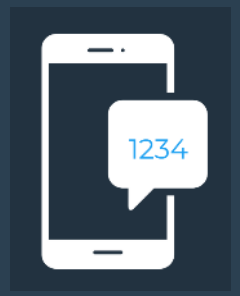
SCIRGE

SHEDDING LIGHT ON SHADOW IT

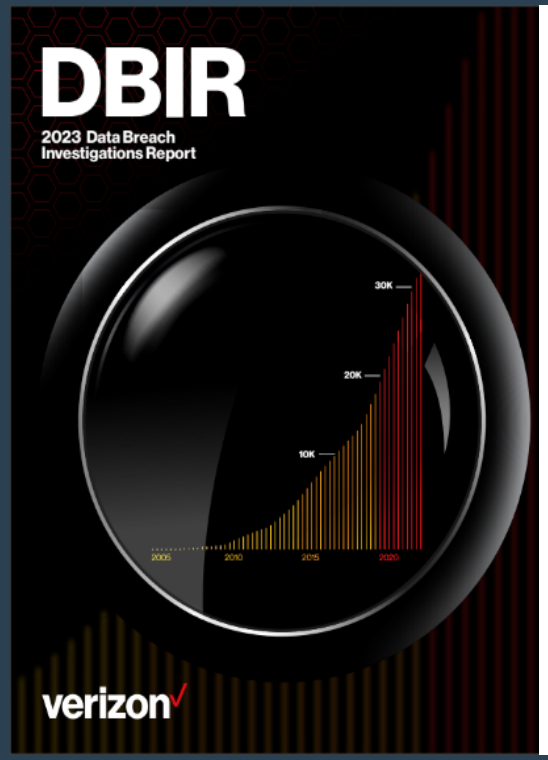
filter:max

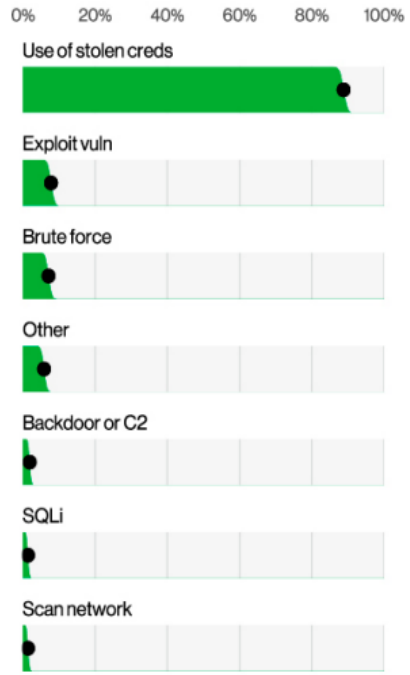

Office 365
aws
SAP S/4 HANA
cisco
zapier
zoom
pipedrive
Quora
650,000,000
Láthatóság
Mennyiség



Integrációk

Felhasználói tudatosság





Initial access

86% of the breaches, as you can see in Figure 39, involve the Use of stolen credentials. And where better to use those credentials than against the various web servers that contain our sensitive information? The other major part of the puzzle within this pattern is the use of exploits. This is where attackers have an exploit and the victims just happen to have a vulnerability (handy for the criminal). This typically occurs in only about 10% of the dataset, and while that may sound like an insignificant number of breaches, unpatched vulnerabilities are still the bread and butter for many attackers, with 50% of organizations experiencing over 39 Web application attacks this year.[39]

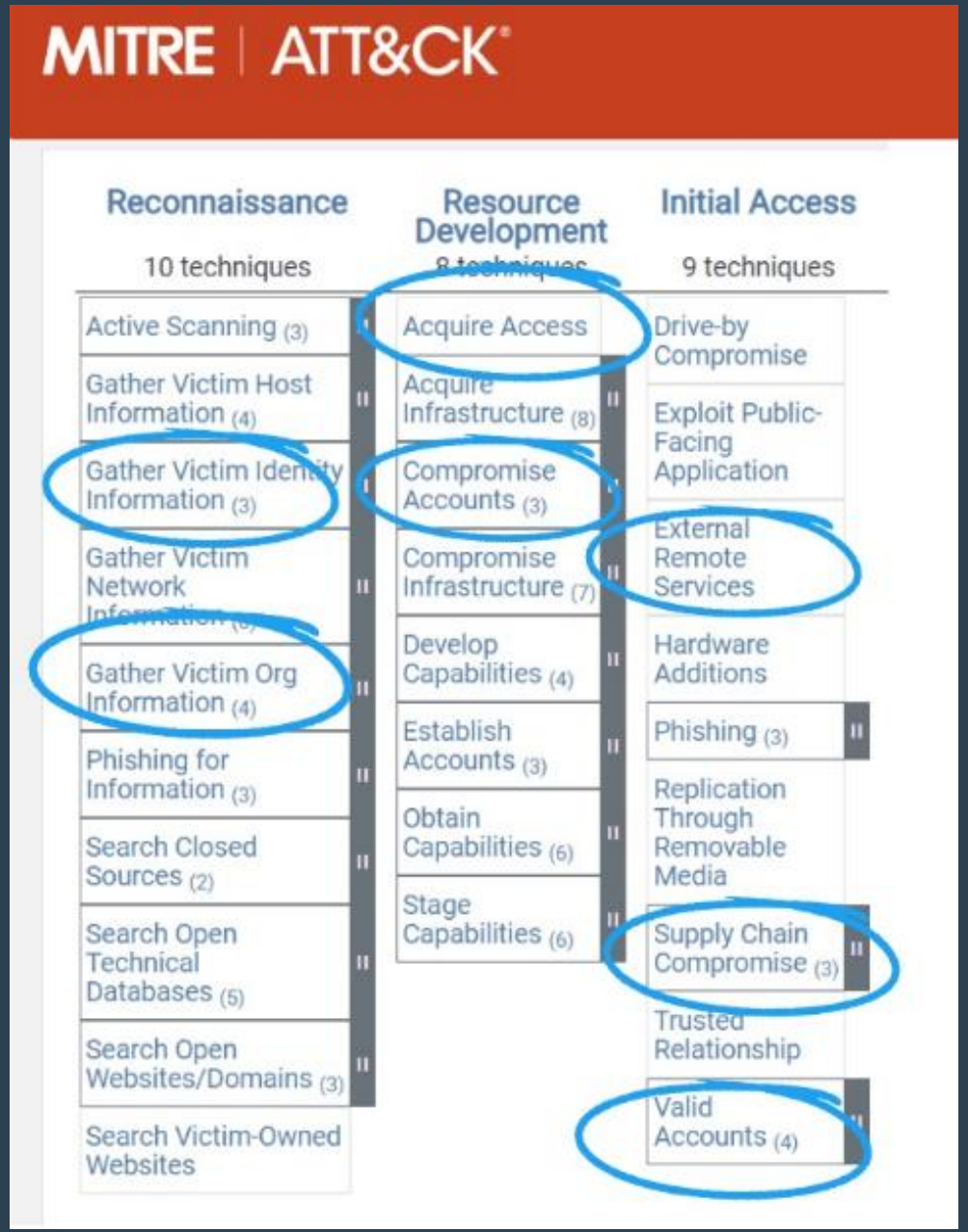
Largest Study of its Kind Shows Outdated Password Practices are Widespread

FRIDAY, NOVEMBER 17, 2023 JOHN POPHAM

SCHOOL OF CYBERSECURITY AND PRIVACY

More than half of the websites in the study accepted passwords with six characters or less, with 75% failing to require the recommended eight-character minimum. Around 12% of had no length requirements, and 30% did not support spaces or special characters.

Only 28% of the websites studied enforced a password block list, which means thousands of sites are vulnerable to cyber criminals who might try to use common passwords to break into a user's account, also known as a password spraying attack.



OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

REPORT FRAUD, WASTE, and ABUSE

ABOUT | COMPLAINTS & REQUESTS | REPORTS | ISSUE AREAS | NEWS | CONTACT US

P@s$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk

What We Found

We found that the Department's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data. Over the course of our inspection, we cracked 18,174 of 85,944—or 21 percent of active user passwords, including 288 accounts with elevated privileges and 362 accounts of senior U.S. Government employees.

dentials

02:41 PM 1

Jogszabályi megfelelés Scirge-el

Előadó: Tóth Ádám

Információbiztonsági tanácsadó, filter:max Kft.

Elektronikus információbiztonsági vezető

GRC terület szakértője

Cél a megfelelés

?

MAGYAR NEMZETI BANK

SCIRGE

Jogi környezet

NIS2 – Kibertantv.

- Programmenedzsment
- Hozzáférés-felügyelet
- Azonosítás és hitelesítés
- Tudatosság és képzés

MNB ajánlások (8/2020)

- Hozzáférési rend kialakítása
- Felhasználói adminisztráció

?

SCIRGE

A gyakorlatban…

- Autentikáció
- Autorizáció
- Adminisztráció, nyilvántartás
- Felhasználói tudatosság

?

SCIRGE

Autentikáció

- **Jelszó policy**
- **Fekete listás jelszavak ellenőrzése**
- **Jelszó frissítések kikényszerítése**
- **Erős jelszavak kiválasztásának támogatása**

Jelszó komplexitás és minőség ellenőrzése,
Tetszőleges jelszó komplexitási szabályok előírása
Ismert, ellopott, vagy újra felhasznált jelszavak felderítése.

Jogosultságkezelés

- Külső rendszerek használata
- Need to know, least privileges elvek, összeférhetetlenségek

Policy alapú monitorozás/blokkolás vállalati online regisztrációk létrehozására és felhasználására.

Adminisztráció

- Leltár nyilvántartások
- Adatkezelők nyilvántartása

Alkalmazásonként és felhasználónként készített leltár a jogosultságokról és azok felhasználásáról
Teljeskörű, felhasználónkénti leltár a külső szolgáltatásokról és abban használt hozzáférésekről

Tudatosítás, képzés

- Biztonságtudatossági képzések
- Gyakorlati feladatok

Felhasználók értesítése a gyenge jelszavakról vagy problémás accountokról.
Egyedileg testre szabható felhasználói tudatossági üzenetek

Köszönöm a figyelmet!

Q&A

filtermax.hu

info@filtermax.hu

+36 20 520 0967


Login
john@business.com
Password123
Sign in
Forgot your password?
https://scirge.local/personal