NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 49. hét

HÍREK

- Új malware kalózszoftvereken keresztül célozza a Mac felhasználókat
- A VMware kritikus Cloud Director sérülékenységet javított
- CISA: A víz- és szennyvízrendszerekben használt Unitronics PLC-k kihasználása
- Egy egyszerű trükkel kinyerhetőek a ChatGPT training adatai
- Több ezer Microsoft Exchange Szerver sebezhető, köztük több magyar is

TÁJÉKOZTATÓ

- Tájékoztatás a Simple elleni támadásról

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági
HÍREK

Új malware kalózszoftvereken keresztül célozza a Mac felhasználókat

(bleepingcomputer.com)

A kiberbűnözők a Mac felhasználókat célozzák meg egy új proxy trójai kártevővel, amelyet népszerű, szerzői jogvédett macOS szoftverekkel együtt kínálnak warez oldalakon. **Bővebben...**

A VMware kritikus Cloud Director sérülékenységet javított

(bleepingcomputer.com)

A **VMware** több mint két hét után kijavította azt a **Cloud Director sérülékenységet**, ami már november 14-óta publikus, és amiről ebben a cikkünkben tájékoztatást adtunk. **Bővebben...**

CISA: A víz- és szennyvízrendszerekben használt Unitronics PLC-k kihasználása

(cisa.gov)

A CISA a víz- és szennyvízrendszerek (WWS) ágazatában használt Unitronics programozható logikai vezérlők (PLC-k) aktív kihasználására reagált. A kiberfenyegetések szereplői a WWS létesítményekhez kapcsolódó PLC-ket, köztük egy azonosított Unitronics PLC-t vettek célba egy amerikai vízügyi létesítményben. **Bővebben...**

Egy egyszerű trükkel kinyerhetőek a ChatGPT training adatai

(securityweek.com)

Egy kutatócsoport, amelynek tagjai a Google és számos rangos egyetem szakemberei közül kerültek ki, **egyszerű módot talált arra, hogy a ChatGPT-ből training adatokat nyerjen ki.** A módszert a csapat „kissé butácskának" titulálta, mivel a lényege az, hogy egy promptban arra kérik a mesterséges intelligenciát, hogy egy szót örökké ismételgessen. **Bővebben...**

Több ezer Microsoft Exchange Szerver sebezhető, köztük több magyar is

(bleepingcomputer.com)

Több tízezer sebezhető Microsoft Exchange e-mail szerver érhető el az internet irányából, amelyek **távoli kódfuttatást** lehetővé tévő hibáktól szenvednek. Az oka az, hogy ezeken a szervereken **régi, már nem támogatott verziók** futnak, amelyek semmilyen frissítést nem kapnak. A hibák között található **kritikus súlyosságú**.
A **Shadowserver** nonprofit kiberbiztonsági csoport felmérése szerint majdnem **20 000 Exchange szerver érintett**, ezeknek több mint a fele európai, 6000 amerikai és 2200 ázsiai. A **magyarországi érintettség körülbelül 100 szerverre** tehető.
Bővebben...

Aktuális tartalmak

Biztonságos jelszókezelés: jelszószéfek [tudatosan]

Ebben az adásban a jelszómenedzserekről beszélgetünk:
Mire jók? Hogyan működnek? Milyen típusaik vannak? Kiknek érdemes használni?

Meghallgatom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el közösségi oldalainkra!

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

TÁJÉKOZTATÁS A SIMPLE ELLENI TÁMADÁSRÓL

A Simple 2023.12.06-ai közleménye szerint:

„December 5-én este, más felület(ek)en eltulajdonított felhasználónév/jelszó kombinációkkal digitális adattolvajok több ezer Simple-felhasználó fiókjához fértek hozzá. Az illetéktelenek fizetési tranzakciót nem tudtak indítani, anyagi kár így nem történt. Az érintett fiókokat haladéktalanul blokkoltuk, a helyreállításról és a szükséges tájékoztatásról gondoskodtunk.

A fiókok védelme érdekében a szükséges lépéseket megtettük. A bűnözők ellen hatósági intézkedést kezdeményezünk."

Az NBSZ NKI az eset kapcsán az alábbiakra szeretné felhívni a figyelmet:

1. Amennyiben Ön érintett a Simple elleni kibertámadásban (erről a fentiek szerint értesítést kapott az alkalmazást üzemeltető OTP Mobil Kft.-től), javasolt minden egyes ilyen szolgáltatásnál **mielőbb lecserélnie a kiszivárgott jelszót**, mert ezeket a fiókokat is támadás érheti.
2. A digitális felhasználói fiókok védelmében elengedhetetlen a szolgáltatásonként különböző, **erős jelszavak használata**. A témában ajánljuk az NBSZ NKI, „Kulcs a digitális élethez – a biztonságos jelszókezelésről" című tájékoztatóját, valamint a Kibertámadás! podcast adását, amelyben a jelszavak biztonságos tárolására adunk tanácsokat.
3. Ha egy szolgáltatás lehetőséget ad a **többfaktoros hitelesítés** használatára, azt javasolt aktiválni. (A Simple esetében bevezetés alatt áll a többtényezős hitelesítés.)
4. Mivel a támadók megszerezhették az érintett ügyfelek a SimplePay rendszerében regisztrált e-mail címeit, várhatóan meg fog szaporodni az ezekre érkező csaló, adathalász levelek száma, ezért az érintett fiókok tulajdonosainak javasolt fokozottan óvatosan kezelniük a hiperhivatkozást vagy csatolmányt tartalmazó üzeneteket.

Statisztikai adatok

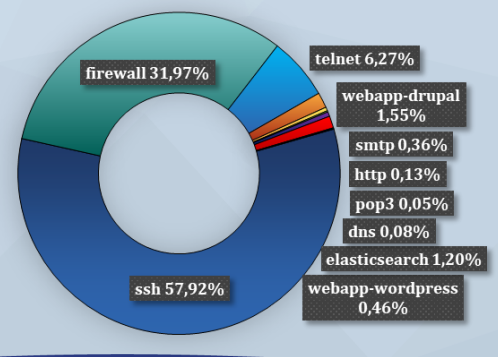
2023.12.01.-2023.12.07.

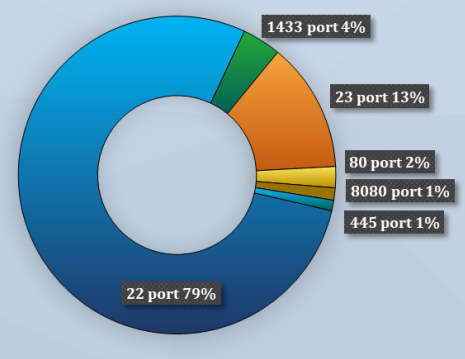
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes

Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:





További információkért, látogasson el **weboldalunkra**!