NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023.1-2. hét

HÍREK

- Holnaptól végleg megszűnik a Windows 7 és a Windows 8.1 támogatása
- Proxy-támogatást vezet be a WhatsApp
- A GitHub megkönnyíti a kódokban található sérülékenységek felfedezését
- Elavult bővítményeket használó WordPress oldalakat vett célba egy új malware
- Ismét lecsap a SpyNote androidos kémprogram, ezúttal pénzintézeteket vett célba

Heti IT biztonsági tipp

- 6 egyszerű lépés, hogy biztonságos legyen a 2023-as év

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK,

Riasztás Microsoft termékeket érintő sérülékenységekről – 2023. január

Tájékoztatás Adobe szoftverek sérülékenységeiről – 2023. január

PODCAST

Kiber az egészségügyben, avagy a kibertér egészsége
[aktuális]

CTI ELEMZÉS

A Mozi malware áttekintése

További érdekességekért, látogasson el **weboldalunkra**!

NEWS

IT biztonsági
HÍREK

Holnaptól végleg megszűnik a Windows 7 és a Windows 8.1 támogatása

(bleepingcomputer.com)

2023. január 10-től nem kapnak biztonsági frissítéseket a Windows 7 Professional és Enterprise kiadásai, továbbá ezzel egyidőben a Windows 8.1 is eléri életciklusa végét. **Bővebben....**

Proxy-támogatást vezet be a WhatsApp

(thehackernews.com)

A WhatsApp azonnali üzenetküldő alkalmazás új Proxy-támogatás funkciója lehetővé teszi az Android és iOS felhasználóknak, hogy megkerüljék a kormányok által bevezetett internetes kommunikációra vonatkozó szigorú előírásokat és korlátozásokat. **Bővebben...**

A GitHub megkönnyíti a kódokban található sérülékenységek felfedezését

(bleepingcomputer.com)

A kódellenőrzéshez az újonnan bevezetett alapértelmezett beállítás opcióval a GitHub lehetővé teszi a fejlesztők számára, hogy csupán néhány kattintással konfigurálhassák azt. Bár ez az új lehetőség még csak Python, JavaScript és Ruby nyelvű repositoryk esetén érhető el, a GitHub a következő hat hónapban több nyelvre is igyekszik majd kiterjeszteni a támogatást. **Bővebben...**

Elavult bővítményeket használó WordPress oldalakat vett célba egy új malware

(thehackernews.com)

WordPress alapú weboldalakat vett célba egy eddig ismeretlen Linux malware, amely több mint két tucatnyi bővítmény és téma biztonsági réseit használja ki a weboldalak támadásához. **Bővebben...**

IT biztonsági
TIPP

Ismét lecsap a SpyNote androidos kémprogram, ezúttal pénzintézeteket vett célba

(thehackernews.com)

2022 októberétől ugrásszerűen nőtt az androidos kártevő új verziójával történő fertőzések száma, ami részben annak köszönhető, hogy a kártevő fejlesztője nyilvánosságra hozta a malware forráskódját, derült ki a ThreatFabric jelentéséből. Ezzel más rosszindulatú szereplők is szabadon terjeszthették és fejleszthették a kémprogramot, célba véve olyan bankokat mint például a Deutsche Bank, a HSBC U.K., a Kotak Mahindra Bank és a Nubank. **Bővebben...**

IT biztonsági Tipp

Az NBSZ NKI weboldalán hasznos tippeket talál egy biztonságos 2023-as évhez.

Statisztikai adatok

2022.12.22-2023.01.12.

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes

Incidensek eloszlása típus és kockázati besorolás szerint

További információkért, látogasson el **weboldalunkra**!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Riasztás Microsoft termékeket érintő sérülékenységekről – 2023. január

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztást** ad ki **Microsoft** szoftvereket érintő **kritikus kockázati besorolású** sérülékenységek kapcsán, azok súlyossága, kihasználhatósága, és a szoftverek széleskörű elterjedtsége miatt.

A Microsoft 2023. január havi biztonsági csomagjában összesen **98** különböző biztonsági hibát javított, köztük **11 kritikus** kockázati besorolású, amelyek kihasználása távoli kódfuttatást vagy jogosultság kiterjesztést tesznek lehetővé. A javított sérülékenységek között **egy nulladik napi (zero-day)** sebezhetőség is található. Ez a CVE-2023-21674 (**Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability**) azonosító alatt került nyilvántartásba.

Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítéssel, valamint manuálisan is letölthetők a gyártói honlapokról.

Elolvasom

Tájékoztatás Adobe szoftverek sérülékenységeiről – 2023. január

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **tájékoztatót** ad ki az **Adobe** szoftverfejlesztő cég **termékeit érintő sérülékenységekkel kapcsolatban**, azok súlyossága, valamint az egyes biztonsági hibákat érintő aktív kihasználások miatt.

Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítésen keresztül, valamint manuálisan is letölthetők a gyártói honlapokról.

Elolvasom

Aktuális tartalmak

KIBERTÁMADÁS!
PODCAST

Kiber az egészségügyben, avagy a kibertér egészsége [aktuális]

Egy kibertámadás bármilyen cégnél nagyon tud fájni, de egy egészségügyi ellátónál egy sor extra probléma és szempont adódik. Adásunkban az egészségügyi szektor kiberbiztonságát boncolgattuk.

Meghallgatom

A Mozi malware áttekintése

CTI jelentés

A Mozi egy Peer-To-Peer (P2P) kapcsolat alapú botnet káros kód, amely elosztott hash táblákat (DHT – Distributed Hash Table) használ fel a kommunikáció során. Sok hasonlóságot mutat a már korábban felbukkant Gafgyt, IoT Reaper és Mirai malware karakterisztikáival. Hasonlóan a nagy népszerűségnek örvendő Torrent hálózatokhoz, a Mozi malware is elosztott hash táblák segítségével alakítja ki a P2P felépítést. Ennek segítségével lehetőség nyílik a központi koordinátort, mint például egy centralizált irányító szervert vagy más néven C2 szervert teljesen mellőzni.

Jelen kiberbiztonsági elemzésünkben a Mozi malware kerül részletesebben bemutatásra.

Elolvasom