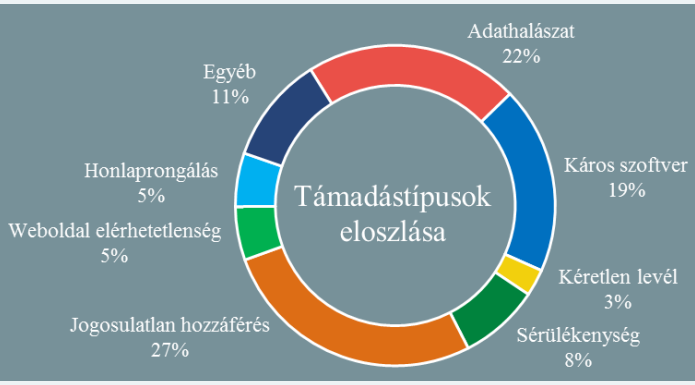
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 11. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.03.06. - 2020.03.12.



Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Vigyázat: újabb koronavírus malspam kampányokat fedeztek fel

(securityaffairs.co)

Újabb koronavírus témájú csaló levél kampányokat fedeztek fel szakértők. A levelek látszólag a WHO-tól érkeznek, azonban valójában információ lopó trójai programok terjesztését végzik. A MalwareHunterTeam szerint az egyik kampány felismerhető arról, hogy a káros e-mailek tárgy mezőjében „Coronavirus Updates" szerepel, a csatolmányban pedig egy ZIP fájl található. Ez tartalmazza a „MyHealth.exe" nevű fájlt, ami valójában egy downloader, ami a tényleges információlopást végző malware, a FormBook letöltéséért felel. **Bővebben...**

Évek óta ellophatóak a Google Authenticator által generált egyszer használatos jelszavakat

(zdnet.com)

A ThreatFabric kutatói előző hónapban felfedezték az első olyan androidos kártevőt (Cerberus), amely képes a Google Authenticator applikáció által generált egyszer használatos jelszavak (OTP) megszerzésére. (A Google Authenticator a kétfaktoros hitelesítés (2FA) második lépcsőjeként alkalmazható többféle online szolgáltatás esetén.) A malware készítői ugyanis felfedezték, hogy az alkalmazás egy hibás konfiguráció következtében – a „FLAG_SECURE" paraméter hiányából fakadóan – engedélyezi más appok számára, hogy azok képernyőmentést készítsenek az alkalmazás felületéről. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat az utóbbi hetekben elszaporodott egészségügyi témájú rosszindulatú levelekkel kapcsolatban.

Ha minden jól megy, a Microsoft felszámolja a Necurs botnetet

(microsoft.com)

A Microsoft és partnerei összehangolt jogi és technikai lépéseket tettek, hogy felvegyék a harcot a világ egyik legtermékenyebb robothálózata, a Necurs ellen, amely többek között spam és különböző malware-ek tömeges terjesztésről ismert, világszerte pedig már több, mint kilencmillió számítógépet fertőzött meg. Március 5-én egy több éves folyamat eredményeként létrejött határozat végre lehetővé tette a Microsoft számára, hogy átvegye az irányítást az USA-ban működő infrastruktúra felett. **Bővebben...**

Záporoznak az egészségügyi témájú adathalász kampányok

(bleepingcomputer.com)

Ezúttal HIV-teszt eredményekre hivatkozó csaló e-maileket fedeztek fel a Proofpoint biztonsági kutatói, amelyeket látszólag a Vanderbilt Egyetem küld ki egy rosszindulatú Excel fájl kíséretében. Az e-mailhez csatoltan szerepel egy *TestResults.xlsb* nevű fájl, amely megnyitása során arról tájékoztatja az áldozatot, hogy adatai védve vannak, a dokumentum megtekintéséhez azonban még engedélyeznie kell a tartalmat (Enable Content). Amennyiben az áldozat így tesz, a háttérben elindulnak azok a rosszindulatú makrók, amelyek letöltik és telepítik a Koadic nevű, eredetileg sérülékenység vizsgálatra szánt eszközt. **Bővebben...**

Windows rendszerek veszélyben – új SMB sérülékenységre derült fény

(bleepingcomputer.com)

Egy új sérülékenységre derült fény a főképp Windows környezetekben hálózati fájl- és erőforrás megosztásra használt Server Message Block 3.1.1-es verzióját érintően. A biztonsági hibáról nem a Microsoft számolt be, hanem a Microsoft Active Protections Programban (MAPP) résztvevő gyártók kezdtek információkat közölni a sérülékenységről. A hiba kihasználásával autentikáció nélkül, távolról tetszőleges kód futtatható a célrendszeren. Nem ez az első eset, hogy sebezhetőséget fedeztek fel az SMB kapcsán, a Wannacry zsarolóvírus terjedéséért is egy ilyen sérülékenység volt a felelős. **Bővebben...**