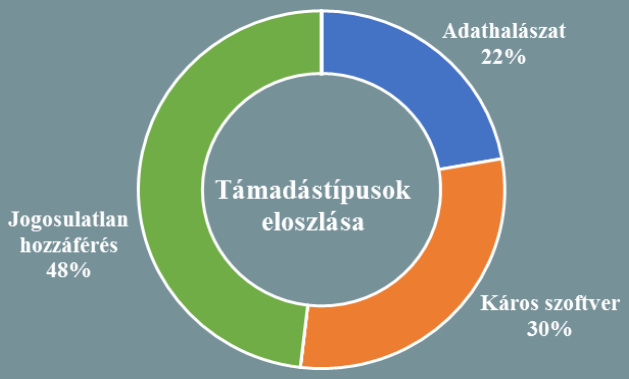
Nemzetközi IT-biztonsági sajtószemle

2017. 32. hét

Incidens adatok:
2017.08.09. — 2017.08.15.



APT28: Kémkedés WiFi hálózaton

(www.infosechotspot.com)

Az APT28 más néven Fancy Bear egy orosz hacker csoport, amelyről kiderült, hogy világszerte a vendéglátóipari szektor WiFi hálózatát használja fel a vendégek adatainak (felhasználó nevek, jelszavak) megszerzésére. Most először használták az NSA-nek tulajdonított EternalBlue exploitot, hogy megkönnyítsék a támadott rendszerekhez való hozzáférést. A FireEye kutatásai szerint a célzott adathalász támadás során alkalmazott dokumentumot — amelynek segítségével hozzáférést szereztek a hotelek WiFi rendszereihez — eddig hét európai és egy közel-keleti országban azonosították. **Bővebben...**

GDPR képzést indítanak a felelős személyek részére

(www.itgovernance.co.uk)

A GDPR felméréseinek eredményei alapján a szervezetek GDPR-nak való megfeleléséért felelős személyek nem rendelkeznek megfelelő képzettséggel és adatvédelmi minősítéssel, ezért az Egyesült Királyság több helyszínen is biztosít egynapos képzést, amely átfogó képet ad a GDPR-ról, segít megérteni annak jogi követelményeit és következményeit. A tanfolyam főleg az adatvédelmi törvényre és az információbiztonsági szabványokra, például az ISO 27001 szabványra épül. **Bővebben...**

IoT eszközökön keresztül támadnak a kiberbűnözők

(www.helpnetsecurity.com)

A Trend Micro legfrissebb jelentése szerint az elmúlt hat hónapban 1,8 millió internetes támadás történt az otthoni router-eken keresztül. Az IoT eszközöket célzó támadások leginkább az Egyesült Államokat, Kínát és az Egyesült Királyságot érintették. A kutatás rávilágít az IoT eszközök három legfőbb kockázatára, mint a nem védett hálózatokhoz történő csatlakozás, az alapméretezett jelszavak használata a készülékeken, valamint a firmware és a szoftver ritka frissítése, amelyek mind hozzájárulnak a biztonsági kockázatok növekedéséhez. **Bővebben...**

Átfogó kibertámadás érte Venezuelát

(www.digitaljournal.com)

Ennek során a múlt héten több ezer kormányzati és magán weboldal vált elérhetetlenné – többek között támadásokat intéztek a legfelsőbb bíróság és a parlament alsó háza ellen is, valamint kilenc helyen elvágták az ország optikai kábeleit, ami jelentős hálózati kiesést okozott hét régióban. Az internetes hálózati problémák mellett azonban Hugbel Roa tudományos és technológiai miniszter szerint az ország egy fontos mobil szolgáltatóját (Movilnet) is érintette a cselekmény, amelynek következtében mintegy 7 millió felhasználó számára megszűnt a GSM kapcsolat. Az eseményekért a magát 'The Binary Guardians'-nak nevező csoport vállalt felelősséget. A vizsgálatok jelenleg is tartanak, de a miniszter úgy véli, a támadások hátterében idegen állami érdekek állnak. **Bővebben...**

Zsaroló támadás az Apple eszközei ellen

(www.thestar.com)

Az elveszett, illetve ellopott készülékek távoli zárolására és törlésére szánt Find My iPhone funkciót kihasználva, a támadók képesek zárolni az eszközöket, hogy váltságdíjat követelhessenek a készülékek feloldásáért cserébe. A funkció eléréséhez és a sikeres támadáshoz valódi Apple ID adatokat (felhasználó név, jelszó) kell megadni, melyeket a támadó egy korábban meghackelt adatbázisból, vagy egy adathalász támadásból szerezhetett meg. Amennyiben ezt a támadási formát tapasztalja, tiltsa le a blokkolási funkciót az eszközön és módosítsa Apple ID-ját. **Bővebben...**

IT biztonsági Tanács

Alkalmazzunk kétlépcsős azonosítást, amennyiben az általunk használt online szolgáltatások azt lehetővé teszik (pl.:Facebook, Gmail).

Az azonosítás lényege, hogy a bejelentkezéshez egy általunk megadott jelszó valamint egy változó jelszó (SMS-ben kapott adat, kódgenerátor) szükséges.

Kína kvantumkommunikációval kísérletezik

(www.chinadaily.com)

A Quantum Experiments at Space Scale (QUESS) a világ első kvantum műholdján végzett kísérletei szolgálnak alapul egy globális, feltörhetetlen kommunikációs hálózat kiépítéséhez. Kvantumszámítással magas a feltörés kockázatának lehetősége a hagyományos nyilvános kulcsú kriptográfia esetén, ezzel szemben a kvantumszámítási technológián alapuló titkosítás csökkenti ennek tényét, ezáltal növelve a biztonságot. **Bővebben...**

iPhone kábellel kémkedhetnek a támadók

(www.forbes.com)

A harmadik féltől származó (online webshopok), nem az Apple által forgalmazott eredeti adatkábelek olyan rejtett SIM kártya fogadására alkalmas nyílással rendelkezhetnek, amely lehetővé teszi, hogy a „kábel” egy GSM hálózathoz csatlakozzon. A kábelt áramforráshoz csatlakoztatva lehetőség van audio és helyadatok továbbítására, valamint arra, hogy egy megadott zajszint felett a készülék automatikusan egy előre programozott telefonszámot hívjon, ezáltal a kábel környezetében történő beszélgetéseket továbbítsa. A kábeleken felül forgalomban vannak olyan hálózati töltők, amelyek alkalmasak SIM kártya fogadására, ami szintén lehetővé teszi a kémkedést. **Bővebben...**

Kína tovább figyeli az online médiaoldalakat

(www.techcrunch.com)

A kínai kormány tovább vizsgálja a három legnépszerűbb közösségi média szolgáltatót (WeChat, Weibo és Baidu Tieba), melyeket azzal vádol, hogy nem szűrik kellőképpen a trágár, pornográf és terrorizmussal összefüggő, a "nemzetbiztonságra veszélyes" tartalmakat. A VPN szolgáltatások tiltásával a kormány a Great Fire Wall internetes cenzúrázási rendszer megkerülését korlátozta, továbbá blokkolta a Facebook, a Twitter és a Google, valamint a The New York Times és a Wall Street Journal elérését. Ezen felül új funkcióval bővítette a cenzúrázási rendszert, ami képes megzavarni a WhatsApp és a WeChat kommunikációját. **Bővebben...**

A kvantumszámítás veszélyei

(www.forbes.com)

A kvantumszámítás technológiai háttere olyan figyelemreméltó számítási kapacitást képvisel, ami drasztikusan megváltoztatja az aktuális kibervédelmi és mesterséges intelligencia technológiákat. Ez a számítási kapacitás lehetővé teszi a napjainkban alkalmazott titkosítási rendszerek feltörését, legyen szó banki rendszerekről vagy üzenetküldő szolgáltatásokról. A bűnözői réteg számára feltehetően nem lesz megfizethető a technológia, de a kormányok számára a kibervédelem terén kulcsfontosságú lehet. **Bővebben...**

DDOS szolgáltatást nyújtó izraeli fiatalokat tartóztattak le

(ehackingnews.com)

18 hónapos nyomozást követően Izrael Sharon tartományában letartóztattak két tinédzsert, akik világszerte több ezer internetes támadásért tehetőek felelőssé. A fiatalok csomagokban értékesítették DDOS szolgáltatásaikat, amelyek ára 19,99$-tól 499,99$-ig terjedt. A gyanúsítottak megközelítőleg 613 ezer dollárt nyertek tevékenységükkel, amely több millió dollárra becsült anyagi kárt okozott. A bankszámlák beazonosítását követően a számlákat zárolták és a pénzt lefoglalták. **Bővebben...**