Könyvtárak a zsarolóvírusok célkeresztjében – mit tehetnek ellenük a könyvtárak?

A St. Louis Public Libraryt, amelynek több mint kétmillió látogatója van évente, 2017-ben zsarolóvírussal támadták meg. A bajt egy hangpostaszerver sebezhetősége okozta. A bűncselekmény szerencsésen zárult – a könyvtár nem fizetett a zsarolóknak, és adatmentéseiből sikerült visszaállítani a vírus által titkosított adatokat.

Azóta számos hasonló támadás érte a könyvtárakat. Észak-Amerikában például a Daviess County Public Libraryt (Kentucky) 2019-ben, a Kokomo-Howard County Public Libraryt (Indiana), a Contra Costa Couty Libraryt (Kalifornia) és a Volusia County Public Libraryt (Florida) 2020-ban, a Toledo Lucas County Public Libraryt (Ohio) 2021-ben. Legutóbb 2023. december 15-én a kanadai London város könyvtárának számítógépes rendszerét fertőzték meg zsarolóvírussal, használhatatlanná téve a telefonokat, az e-mailezést, a wifit, a weboldalakat, a katalógust, a nyomtatókat, a számítógépeket és digitális forrásokat.

Még súlyosabb incidens történt 2023. október 28-án, amikor a kanadai Toronto Public Library egyik adatszerverére zsarolóvírus került. Az ország legnagyobb könyvtári rendszeréről van szó, melynek 1,2 millió használója, 12 milliós állománya, 100 könyvtárból álló hálózata van. A támadók nagyszámú személyes adatot loptak el, amelyet a – csak speciális böngészővel hozzáférhető – dark weben tettek publikussá. A könyvtár és a Toronto Public Library Foundation (TPLF) jelenlegi és korábbi munkatársainak neve, társadalombiztosítási száma, születési dátuma és lakcíme, valamint személyazonosítási iratok másolatai kerülhettek a kezükbe. Nem kizárt, hogy önkéntesek, adományozók és más ügyfelek adatai is érintettek. Az erre irányuló vizsgálat hónapokig is eltarthat.

Jóformán egy hét sem telt el, és a Rhysida néven ismert zsaroló banda hasonlóképpen támadta meg Nagy-Britannia nemzeti könyvtárát, a British Libraryt. Nemcsak elérhetetlenné tettek számos szolgáltatást, hanem majd 600 gigabájt adatot is elloptak, és feltették eladásra a dark webre. A British Library értesítette használóit, hogy zsarolóvírus blokkolta webhelyét, online rendszerét, telefonvonalait és más szolgáltatásait is. Az olvasói adatok nagy valószínűséggel nem érintettek, mivel a lopás a könyvtári humánerőforrás-adatokból történt, de azt javasolják, hogy azok a regisztrált olvasók, akik máshol is ugyanazokat a bejelentkezési adatokat használják, mint a könyvtárban, feltétlenül változtassák meg ezeket a többi webhelyeken. A rendőrség, a nemzeti kiberbiztonsági központ (National Cyber Security Centre – NCSC) és külső kiberbiztonsági szakértők folytatják a támadás kivizsgálását, a könyvtár pedig a szolgáltatások és a rendszerbiztonság visszaállításán fáradozik. A British Library blogja működik, itt találhatók további információk az elérhető szolgáltatásokról. A kiberbiztonsági központ pedig konkrét útmutatást ad azoknak a személyeknek, akiket esetleg érintett az adatvédelmi incidens.

Mik azok a zsarolóvírusok, és hogyan működnek?

Ezek olyan kártékony kódok, amelyek titkosítják vagy zárolják a számítógépes adatokat, vagy akár egész számítógépes rendszereket. A feloldó kódért a kiberbűnözők pénzt kérnek. Manapság szinte kizárólag a nyomozó hatóságok által követhetetlen kriptovalutát, főként bitcoint. A British Library esetében 20 bitcoin volt a váltságdíj, ami kb. 590 000 fontnak, azaz kis híján 263 millió forintnak felel meg. Fontos megjegyezni, hogy nincs rá garancia, hogy a váltságdíj kifizetése után a zsarolók elküldik a feloldó kódot.

A British Library rendszerét a Rhyshida nevű zsaroló-banda vette célba. Ennek a 2023 májusában működésbe lépett bűnözői csoportnak a neve hamar jól ismertté vált világszerte, mivel számos országban követtek el bűncselekményt az oktatási, ipari, informatikai és kormányzati szektorban. Kettős zsarolás jellemző rájuk, vagyis pénzt kérnek a feloldó kódért, de egyúttal adatokat is lopnak, melyeket megvételre kínálnak a dark weben. Ezenkívül rosszindulatú programjaikat bűnözőknek adják bérbe, akikkel osztoznak a váltságdíjból származó bevételeken.

Manapság elsősorban nem egyéni használókat céloznak a zsarolók, hanem nagy cégektől próbálnak bezsebelni óriási összegeket. A Covid-járvány – amikor sokan végeztek otthonról számítógépes munkát, rossz esetben sebezhető eszközökön, hálózatokon – és a lenyomozhatatlan kriptovaluták elterjedése sokszorosára növelte a támadások számát. Jól illusztrálja a kiberbűnözők „vállalkozó kedvét" a 2021 májusában történt támadás, amely az USA keleti partvidékének egyik legnagyobb olajvezeték-üzemeltető vállalatát érte. A hekkerek az egyik dolgozó VPN-kódját szerezték meg, és megbénították a számlázó rendszert, amivel benzinkúthálózatok és repülőterek működését lehetetlenítették el. Mindez óriási közlekedési fennakadásokat és az évtized legmagasabb benzinárát eredményezte. A vállalat kénytelen volt kifizetni a kb. 4 millió dollárnak megfelelő bitcoin váltságdíjat a feloldó kódért. 2021-ig ez volt a kritikus infrastruktúra elleni legnagyobb támadás az Egyesült Államok történetében.

A fenti eset is jól érzékelteti, milyen súlyos lehet egy vírusfertőzés, és miért fontos, hogy a cégek, az informatikus szakemberek és a munkatársak mindent megtegyenek ellenük.

Mit érdemes tudni a vírusok terjedéséről?

- A legjellemzőbb az e-mail útján terjesztett vírus. Akár a megnyitott csatolmány, akár az e-mailben szereplő link a kártékony kódot terjesztő webhelyre vezethet.
- Az adathalász e-mailekkel a hitelesítő adatok megszerzésére, felhasználói fiókok feltörésére pályáznak a hekkerek.
- Különböző weboldalakon megtévesztő hirdetések tűnnek fel, amekyekre kattintva szintén rosszindulatú webhely felé vezet az út. A káros hirdetések teljesen megbízható weboldalakon is felbukkanhatnak.

- A rosszindulatú weboldalra vezető linkeket SMS-ben vagy instant üzenetküldővel történő megosztással is terjesztik.
- Vírussal fertőzött külső eszköz (pl. USB) csatlakoztatása is okozhat kárt.
- Természetesen a mobil és az IoT- (Internet on Things) eszközök szintén ki vannak téve a fertőzésnek.

Bejutás után a vírus telepíti magát a megfertőzött számítógépre, a mobil vagy IoT-eszközre. Kiépíti a kapcsolatot azzal a szerverrel, amelyet a vírusgazda használ. Innentől a hekker már meghatározhatja, hogy mikor aktivizálódjon a fertőzés, milyen fájlokat érjen el a zárolás vagy titkosítás és/vagy milyen adatok eltulajdonítására kerüljön sor.

A titkosító (encrypting) támadás eredménye, hogy az eszközre belépve megtalálhatók a korábbi fájlok, de olyan új, az adott vírusvariánsra jellemző kiterjesztéssel, hogy semmilyen alkalmazással nem lehet megnyitni őket. Általában egy új szöveges dokumentum is feltűnik, amelyben a titkosítás megszüntetésének feltételeit közlik az áldozattal. A lezáró (locker) típusú vírusok megakadályozzák az eszközhöz való hozzáférést. Leggyakrabban a képernyőt zárolják. Legkellemetlenebbek az MRB (master boot record) vírusok, amelyek az operációs rendszer betöltését akadályozzák meg. A zsarolók utasításai általában a képernyőn jelennek meg.

Mi a teendő a vírusfertőzés okozta károk megelőzése érdekében?

- Fontos az erős jelszó használata: legalább 12 karakter, vegyesen használt nagy- és kisbetűk, speciális karakterek. Kerülni kell a triviális, „password”, „jelszó”, „vendég”, „12345” típusú jelszavakat. Az erősséget érdemes ellenőrizni, például a Nemzeti Kibervédelmi Intézet oldalán: https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/jelszo-ellenorzo.
- Ne használja ugyanazt a jelszót több helyen!
- Rendszeresen változtassa jelszavait!
- Ne ossza meg hozzáférését másokkal!
- Ne hagyjon leírt jelszavakat az IT-eszközök közelében!
- Ne hagyja felügyelet nélkül IT-eszközeit! Zárolja számítógépét, ha nem tartózkodik a közelében! Munkája befejeztével kapcsolja ki a számítógépet!
- Semmiképpen se használjon lejárt vagy nem támogatott szoftvereket!

Az e-mailek és a web biztonságos használata érdekében:

- Ellenőrizze az e-mailek feladójának valódiságát!
- Ne kattintson ismeretlen helyről vagy gyanús e-mailben érkező linkekre!
- Ne nyissa meg ismeretlen feladójú vagy gyanús e-mailek mellékleteit!

- Az egyéni felhasználók számára is alapvető védelmi teendő a vírusirtó programok és a biztonsági frissítések telepítése.
- Kerülje a gyanús weboldalakat!
- Csak biztonságos (https://) kapcsolatokat használjon a böngészés során!
- Zárja be böngészőjét, ha már nem használja!
- Használjon biztonságos internetkapcsolatot, kerülje a nyilvános wifihálózatokat!
- A Windows-felhasználók ne engedélyezzék az „ismert fájltípusok kiterjesztésének elrejtése" opciót a beállításokban, hogy könnyebben észrevegyék a gyanús kiterjesztésű fájlokat!

Munkahelyi adatvédelem:

- Munkahelyi IT-eszközeit ne használja személyes célra!
- USB-eszközöket kellő elővigyázatossággal alkalmazzon!
- A munkatársak figyelmét fel kell hívni, hogy azonnal kapcsolják ki a hálózatra csatlakoztatott munkaállomást vagy mobil eszközt, ha úgy vélik, hogy azt zsarolóvírussal fertőzték meg, és azonnal értesítsék az informatikust vagy az informatikai részleget!
- Az informatikai részlegek úgy állítsák be rendszereiket, hogy kiszűrjék a futtatható állományokat (executable files) a bejövő és kimenő e-mailekből, letiltsák a makró szkripteket az e-mailben továbbított irodai fájlokból!
- A webes munkameneteket titkosítani kell.
- A könyvtáraknak különösen figyelniük kell tartalomkezelő rendszerükre. A sérülékeny Wordpress például nagyon gondos telepítést és a biztosági javításokkal való gyakori frissítéseket igényel.
- Csak akkor rendeljenek rendszergazdai jogosultságokat az egyes alkalmazottakhoz, ha feltétlenül szükséges!
- Távoli vagy rendszergazdai hozzáférésekhez csakis kétlépcsős azonosítást alkalmazzanak!
- Alapvető a rendszeres adatmentés felhőbe vagy külső, hálózathoz nem kapcsolódó eszközre.
- Fontos a szervezeten belüli információbiztonsági képzési program vagy információs kampányok indítása.
- A külső szolgáltatók kiválasztásánál az információbiztonsági szempontokat is figyelembe kell venni. (Alkalmaznak-e érvényben lévő biztonsági szabványokat és protokollokat, van-e SOC2 – System and Organization Controls, version 2 – auditjuk?).
- A könyvtár külső szolgáltató igénybevételekor szerződéskötéssel biztosítsa a maga számára a megfelelő kiberbiztonsági gyakorlatot a másik fél részéről!
- Az előfizetéses információforrásokhoz történő hozzáféréshez az IP-cím-alapú azonosítás helyett szabványos, központosított azonosításra kell áttérni (pl. OpenAthens, InCommon).

- A belső rendszerek alakításakor törekedni kell a széles körben elterjedt biztonsági szabványok bevezetésére (ISO/IEC 27001).
- Az ellenőrzési naplók minden rendszeren legyenek bekapcsolva, mert ezek incidens esetén a történtek rekonstruálásában, az okok felderítésében nélkülözhetetlenek. A naplóknak független kiszolgálókon kell működniük.

Ha mégis megtörtént a baj

- Az incidenst jelenteni kell a Nemzeti Kibervédelmi Intézetnél (https://nki.gov.hu/).
- A könyvtárnak haladéktalanul értesítenie kell használóit a történtekről, illetve arról, hogy mennyi és milyen jellegű adat kerülhetett illetéktelen kezekbe.
- Jó tudni, hogy a Nemzeti Kibervédelmi Intézethez magánszemélyek is fordulhatnak segítségért, ha adatbiztonsági incidensben érintettek.

Balla Attila, Fazokas Eszter, Kormány Milán
Országos Széchényi Könyvtár

2024. január 8.

Felhasznált irodalom:

Albrecht, Steve: *Keeping libraries safe from DIGITAL ATTACKS.* In: Computers in Libraries, vol. 43, no. 5, pp. 8–12. https://www.proquest.com/trade-journals/keeping-libraries-safe-digital-attacks/docview/2825236662/se-2

Banfield-Nwachi, Mabel: *British Library suffering major technology outage after cyber-attack*. In: The Guardian. 2023. nov. 16. https://www.theguardian.com/books/2023/oct/31/british-library-suffering-major-technology-outage-after-cyber-attack

Breeding, Marshall: *How to secure library systems from malware, ransomware, and other cyberthreats*. Computers in Libraries, vol. 42, no. 1, pp. 20–23. https://www.proquest.com/trade-journals/how-secure-library-systems-malware-ransomware/docview/2617716823/se-2

Cervone, H. Frank: *Top recommendations for updating your library's IT security plan*. In: Computers in Libraries, vol. 42. no. 1, pp. 4–8. https://www.proquest.com/trade-journals/top-recommendations-updating-your-librarys/docview/2617717216/se-2

Cybersecurity incident. Last updated: 2023. nov. 29. https://torontopubliclibrary.typepad.com/tpl/cybersecurity-incident.html
Enis, Matt: *Ransomware hackers target government offices, libraries*. In: Library Journal, 2017. ápr. 4. https://www.libraryjournal.com/story/ransomware-hackers-target-government-offices-libraries

Greig, Jonathan: *Ontario public library shuts down most services due to cyberattack*. In: The Record. 2023. dec. 15. https://therecord.media/ontario-public-library-shuts-down-services?&web_view=true

Halász Viktor: *Zsarolóvírusok és a No More Ransom projekt*. In: Belügyi Szemle, 2022. no. 9. https://doi.org/10.38146/BSZ.2022.9.9

Milmo, Dan: *Rhysida, the new ransomware gang behind British Library cyber-attack*. In: The Guardian. 2023. nov. 24. https://www.theguardian.com/technology/2023/nov/24/rhysida-the-new-ransomware-gang-behind-british-library-cyber-attack