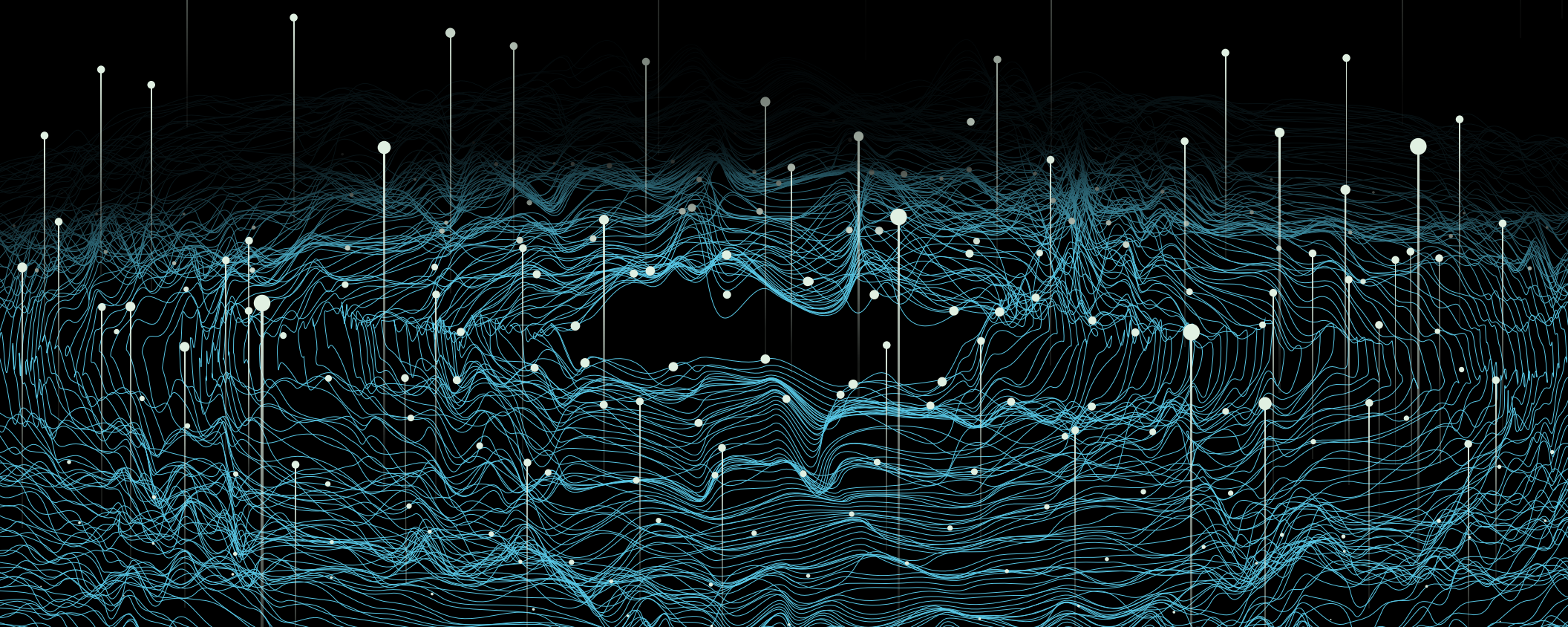
Microsoft

A MICROSOFT BIZTONSÁGI INFORMÁCIÓS JELENTÉSE

24. KÖTET
2018. JANUÁR–DECEMBER



Tartalom

Ez az dokumentum kizárólag tájékoztatásul szolgál. A MICROSOFT NEM VÁLLAL SEMMILYEN KIFEJEZETT, VÉLELMEZETT VAGY JOGSZABÁLYBAN ELŐÍRT GARANCIÁT A JELEN DOKUMENTUMBAN SZEREPLŐ INFORMÁCIÓKRA VONATKOZÓAN.

Ez a dokumentum tájékoztató jellegű. Az itt megjelenő információk és a vélemények, beleértve az URL-címeket és más internetes webhelyhivatkozásokat, értesítés nélkül megváltozhatnak. A használatukért az olvasót illeti a felelősség.

A kiadványban említett valós vállalatok és termékek nevei a vonatkozó tulajdonosaik védjegyei lehetnek.

Szerzők és közreműködők

Abhishek Agrawal
Információvédelem

David Fantham
Információvédelem

Debraj Ghosh
Microsoft biztonságmarketing

Diana Kelley
Kiberbiztonsági megoldások csoport

Elia Florio
Windows aktív védelem

Eric Avena
Windows Defender kutatócsoport

Eric Douglas
Windows Defender kutatócsoport

Francis Tan Seng
Windows Defender kutatócsoport

Jonathan Trull
Kiberbiztonsági megoldások csoport

Joram Borenstein
Kiberbiztonsági megoldások csoport

Karthik Selvaraj
Windows Defender kutatócsoport

Kasia Kaplinska
Microsoft biztonságmarketing

Kristina Laidler
Biztonsági incidenskezelés

Matt Duncan
Windows aktív védelmi adatok elemzése

Mark Simos
Kiberbiztonsági megoldások csoport

Paul Henry
Wadeware LLC

Pragya Pandey
Microsoft biztonságmarketing

Ram Pliskin
Azure Security

Ryan McGee
Microsoft biztonságmarketing

Seema Kathuria
Kiberbiztonsági megoldások csoport

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Windows Defender kutatócsoport

Volv Grebennikov
Bing

Yaniv Zohar
Azure Security

Előszó

Üdvözöljük a Microsoft biztonsági információs jelentés (SIR) 24. kiadásának olvasóit! Szakemberként és biztonsági mérnökként azért olvasok hasonló jellegű jelentéseket, hogy jobb rálátást kapjak az aktuális helyzetre, és gyakorlati tanácsokat kaphassak arra vonatkozóan, hogyan tudom felhasználni ezt a tudást a szervezetek hatékonyabb védelme érdekében.

A SIR csapata a jobb kibervédelem elérését célzó tájékoztatást állította e jelentés középpontjába, és egy évnyi adat alapos átvizsgálásából vonta le a legfontosabb következtetéseket.

A jelentésben található információk egy évnyi biztonsági adat elemzésének és a saját tapasztalatainknak az eredményei. Az adatelemzés során felhasználtuk a Microsoft felhőjén naponta áthaladó közel 6,5 billió fenyegetési jelet, valamint világszerte több ezer biztonsági kutatónk és szakemberünk kutatásait és gyakorlati megfigyeléseit. 2018-ban a támadók számos piszkos trükköt alkalmaztak, amelyek között voltak újak (kriptobányászat) és régiek (adathalászat) is, hogy az ügyfelektől és a szervezetektől adatokat és más erőforrásokat lopjanak el. A hibrid támadások, például az Ursnif kampány, a közösségi és a technikai módszerek kombinációját alkalmazták. Ahogy a „zajos és romboló" zsarolóprogramokkal szembeni védelem egyre jobb lett, a bűnözők a rejtett, de mégis jövedelmező támadási forma, a kriptobányászat felé fordultak.

Ez a váltás nyugtalanító lehet, mivel olyan, mintha a támadók mindig egy lépéssel előrébb járnának. Más szempontból viszont pozitív a történet. Az Önhöz hasonló biztonságvédelmi és kiberbiztonsági szakemberek védelmi módszereinek köszönhetően a támadóknak fel kellett adniuk kedvenc zsarolóprogramjaikat, és más módszerek után kellett nézniük.

A kiberbűnözők az ellátási lánc területén is aktívabbak lettek. Az egyik legjelentősebb támadás, a Dofoil kriptovaluta-bányászó program 2018. március 6-i kitörése, egy megfertőzött P2P-alkalmazásból indult. Az ellátási láncnak nemcsak az alkalmazások jelentettek problémát: a fertőzések érintették a felhőt is, és kártékony böngészőbővítményeket, feltört Linux-repókat és számos hátsó kapuval ellátott modult hagytak maguk után. A fenyegetések kezelése érdekében a zervezetek egyre inkább egy átlátható és megbízható ellátásilánc-modellre törekednek.

Az adatok önmagukban is hasznosak, de segítenek megfejteni azt is, hogy mi történt valójában egy szervezetnél. Ezért az incidensek észlelésével és kezelésével foglalkozó DART csapatunk gyakorlati tapasztalatait is felhasználtuk a jelentésben. Ezek közé tartozik például, hogy egy nagy gyártóvállalat hogyan tudta blokkolni a megfelelő intézkedésekkel a több hónapja tartó, többfázisú adathalász-támadásokat, továbbá hogy egyes pénzügyi szolgáltatók hogyan tudták végül kiiktatni a támadókat a rendszereikből fejlett vizsgálati eszközök és végpontfelügyelet segítségével.

Végül, de nem utolsósorban, bár az adathalász célú webes hivatkozások száma tovább növekedett, a gépi tanulási modellek egyre hatékonyabban tudják kiszűrni ezeket, még mielőtt elérnék a felhasználók postaládáit, és segítenek megelőzni a károkat, ha a felhasználó mégis rájuk kattintana. További jó hír még, hogy egyre több vállalat alkalmaz többfaktoros megoldásokat, amelyekkel korlátozni tudják a hitelesítő adatok ellopására szolgáló adathalász e-mailek sikerességét.

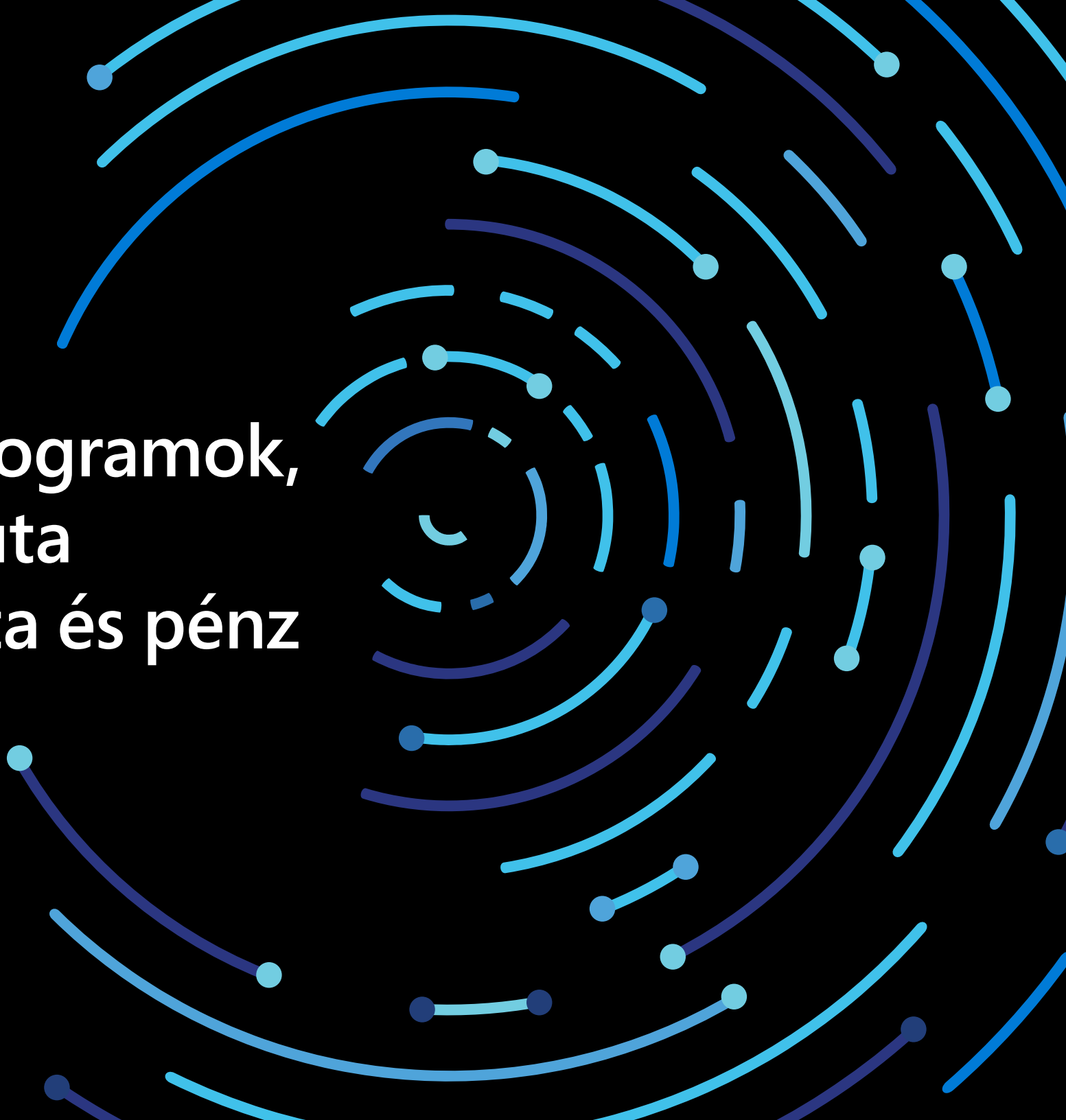
A támadók mindig új lehetőségeket keresnek, ezért minél többet tudunk a módszereikről és a fortélyaikról, annál felkészültebben tudunk védekezni, és annál gyorsabban tudjuk kezelni a problémát. Az apró, de fontos lépések nagy javulást hozhatnak egy vállalat kiberbiztonságában. Éppen ezért a folyton változó kártevők és támadások részletes elemzésén túl a jelentés javaslatokkal és gyakorlati útmutatással is szolgál. Mert szakemberként pontosan erre volt szükségem ahhoz, hogy le tudjam győzni a rosszfiúkat. Reméljük, Önnek is hasznára válik majd!

Diana Kelley
A Microsoft kiberbiztonsági részlegének technológiai vezetője

Ui. A SIR folyamatos fejlesztésére törekszünk. Ha észrevétele van, kérjük, ossza meg velünk.

1. FEJEZET

Zsarolóprogramok, kriptovaluta bányászata és pénz



2017-ben a biztonsággal kapcsolatos jelentősebb események főszereplői leginkább a zsarolóprogramok voltak. A hírhedt WannaCrypt és Petya világszintű elterjedésével a zsarolóprogramok – azaz az olyan kártevők, amelyek zárolják vagy titkosítják a számítógépeket, majd pénzt kérnek a hozzáférés visszaszerzéséért – bekerültek a köztudatba, és sokan arra számítottak, hogy a jövőben egyre nagyobb teret nyernek majd. Ehelyett 2018-ban a zsarolóprogramok előfordulása jelentősen csökkent.

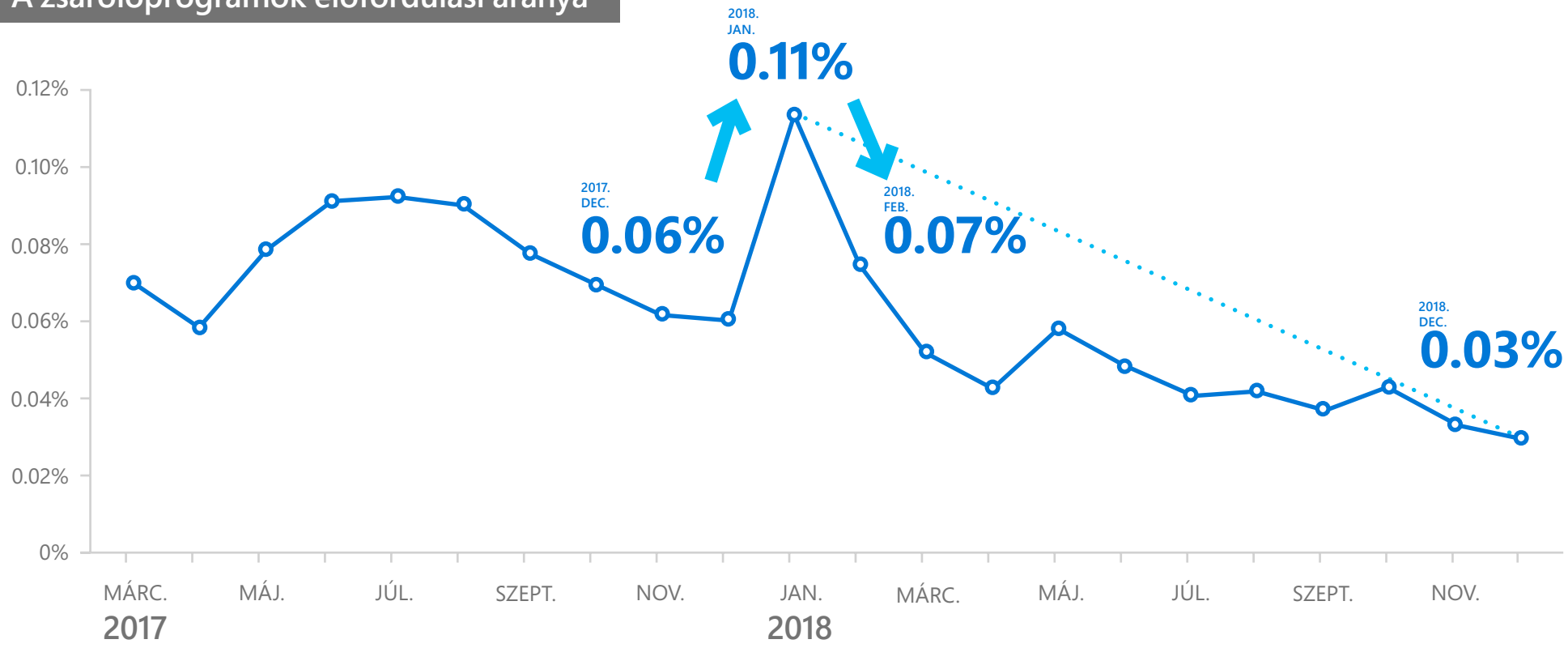
Ez a csökkenés részben a hatékonyabb észlelésnek és a tájékoztatásnak köszönhető, ami megnehezítette a támadók számára, hogy profitáljanak a támadásokból. Ennek következtében a támadók elkezdtek áttérni más módszerekre, például a kriptovaluta-bányászatra, amelynek során az áldozatok számítási erőforrásait használják fel arra, hogy digitális pénzhez jussanak. Ez a változás jól mutatja, hogy a legtöbb profitorientált kiberbűnöző alapvetően opportunista természet: a legkönnyebben megszerezhető pénzt keresik, és ha a kiberbűnözés ökonómiája megváltozik, ők gyorsan alkalmazkodnak hozzá.

KEVESEBB ZSAROLÓPROGRAMOS TÁMADÁS

Több mint tíz évvel ezelőtt a korai kártevők világát meghatározó hackereket kiszorította a szervezett bűnözés és a hozzá kapcsolódó egyéb profitorientált érdekek. Míg az első kártevők terjedése gyakran feltűnő és nyilvánvaló volt, a profitorientált kártevők inkább csendben, figyelemfelkeltés nélkül dolgoztak, hogy a lehető legtovább végezhessék feladatukat: levélszemét küldését, bizalmas adatok ellopását, szolgáltatásmegtagadásos támadások végrehajtását és egyéb kártékony tevékenységeket.

A zsarolóprogramok szembefordultak ezzel a trenddel. Ahelyett, hogy észrevétlenek próbálnának maradni, nyíltan megtagadják az áldozattól a számítógépéhez és a fontos fájljaihoz való hozzáférést, amíg az meg nem fizeti a váltságdíjat (és gyakran még azután is; sokszor előfordul, hogy a támadók a váltságdíj kifizetése után sem adják vissza a számítógépek feletti irányítást). 2017-ben, amikor a zsarolóprogramok virágkorukat élték, úgy tűnt, hogy a nyílt támadás e formája a támadói módszerek új szakaszát jelenti. A legújabb adatok azonban azt sugallják, hogy a zsarolóprogramok hanyatlásnak indultak, és számos támadó visszatér a korábban alkalmazott rejtettebb módszerekhez – nem szeretnének ugyanis rivaldafénybe kerülni, hogy eredményesebb támadásokat tudjanak indítani, mint például a kriptovaluta-bányászat esetében is. Bár a zsarolóprogramok előfordulási aránya csökkent, ez nem feltétlenül jelenti azt, hogy a támadások súlyossága is csökkent volna.

A zsarolóprogramok előfordulási aránya

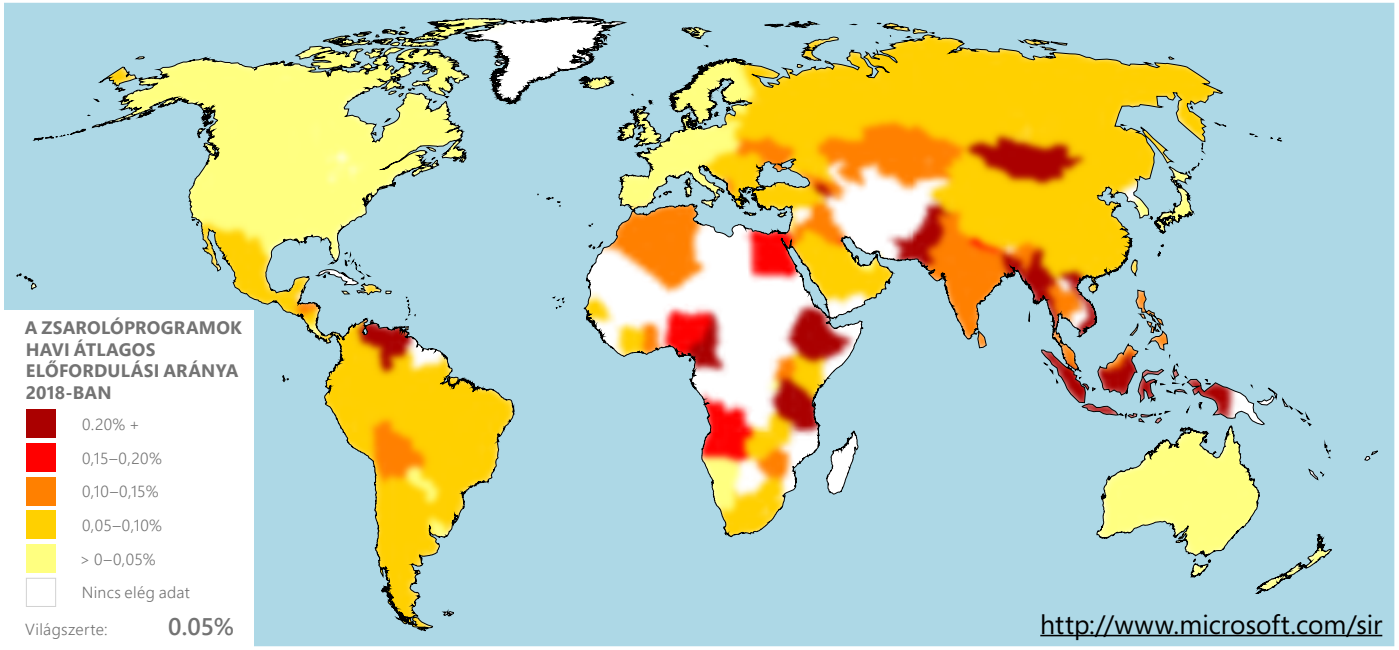


A zsarolóprogramok előfordulási aránya körülbelül 60 százalékkal csökkent 2017 márciusa és 2018 decembere között, átmeneti növekedési szakaszokkal.

1. ÁBRA

Zsarolóprogramok előfordulása 2017 márciusa és 2018 decembere között

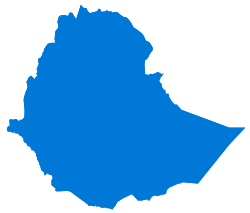
Bár valószínűleg több dolog is áll az általános csökkenés mögött, a Microsoft biztonsági kutatói úgy vélik, hogy ennek elsődleges oka az, hogy a felhasználók és a szervezetek egyaránt tájékozottabbak, és hatékonyabban kezelik a zsarolóprogramok jelentette fenyegetéseket. Például elővigyázatosabbak, és biztonsági mentést készítenek a fontos fájlokról, így azok akkor is helyreállíthatók, ha egy zsarolóprogram titkosítja őket. És ahogy korábban már említettük, a kiberbűnözők opportunista természetek.



2. ÁBRA.

A zsarolóprogramok havi átlagos előfordulási aránya világszerte ország/régió szerint 2018-ban

A ZSAROLÓPROGRAMOK ÁLTAL LEGINKÁBB ÉRINTETT ORSZÁG: ETIÓPIA



Havi átlagos előfordulási arány: **0.77%**

2018-ban az öt legmagasabb havi átlagos zsarolóprogram-előfordulási aránnyal rendelkező ország Etiópia (havi átlagos 0,77%-os zsarolóprogram-előfordulási arány), Mongólia (0,46%), Kamerun (0,41%), Mianmar (0,33%) és Venezuela (0,31%) volt, ahol mindegyik országban legalább 0,31% volt a zsarolóprogramok havi átlagos előfordulási aránya.[1] Néhány évvel ezelőtt a zsarolóprogramok leginkább a gazdag országokban, Európában és Észak-Amerikában tömörültek, de ahogy a zsarolóprogramok népszerűsége csökkent a támadók körében, az előfordulásuk mintázata egyre jobban hasonlítani kezdett a kártevők mintázatára.

A zsarolóprogramok előfordulási aránya 2018-ban Írországban (0,01%), Japánban (0,01%), az Egyesült Államokban (0,02%), az Egyesült Királyságban (0,02%) és Svédországban (0,02%) volt a legalacsonyabb. Ezekben az országokban tehát 0,02% vagy alacsonyabb volt a havi átlagos zsarolóprogram-előfordulási arány ebben az időszakban. Az alacsony előfordulási aránnyal rendelkező országok fejlett kiberbiztonsági infrastruktúrával és a kritikus infrastruktúrák védelmére szolgáló jól kidolgozott programokkal rendelkeznek, a lakosság pedig tájékoztatást kap az alapvető biztonsági kérdésekről.

LÁBJEGYZET

[1] Az előfordulási arány a Microsoft valós idejű biztonsági termékeit futtató számítógépek közül azoknak a gépeknek a százalékos aránya, amelyek kártevők előfordulását jelentik. A fenyegetés előfordulása nem jelenti azt, hogy a számítógép megfertőződött volna. Az előfordulási arányok számításában csak az olyan számítógépeket vesszük figyelembe, amelyeknek felhasználója úgy döntött, hogy adatokat szolgáltat a Microsoftnak.

A KRIPTOVALUTA-BÁNYÁSZAT VIRÁGZIK

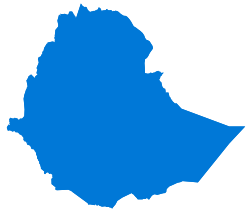
A kriptovaluta olyan virtuális pénzt jelent, amely névtelenül használható fel termékek és szolgáltatások vásárlására és eladására az online és a fizikai világban egyaránt. Sok különböző kriptovaluta létezik, de mindegyik alapja a blokklánc-technológia, ahol minden egyes tranzakciót rögzítenek egy elosztott főkönyvben, amelyet a világ több ezer vagy millió számítógépe tart nyilván. Új érmét úgy lehet létrehozni vagy „bányászni", hogy a számítógépek összetett számításokat végeznek, amelyek a blokklánc-tranzakciók ellenőrzésére is szolgálnak.

A kriptobányászat nagyon jövedelmező lehet – 2018-ban egyetlen Bitcoin, a legrégebbi és legnépszerűbb kriptovaluta, több ezer amerikai dollárt ért –, ám a szükséges számítások elvégzése nagyon erőforrás-igényes lehet, és egyre inkább az lesz minden egyes új kibányászott érmével. Az olyan népszerű valuták, mint a Bitcoin, a legtöbb személy és kis csoport számára elérhetetlenek, ugyanis rendkívüli számítási erőforrás nélkül szinte lehetetlen nyereségesen bányászni őket. Ezért azok a támadók, akik jogtalan nyereségre próbálnak szert tenni, gyakran olyan kártevők segítségével teszik azt, amelyek az áldozatok számítógépeit használják fel kriptovaluta-bányászatra. Ezzel a módszerrel számítógépek százezreinek a feldolgozási kapacitását tudják felhasználni, nem pedig csak egy vagy kettőét. Ha egy apróbb fertőzést fel is fedeznek, a kriptovaluta névtelensége megnehezíti a felelősök felkutatását.

2018-ban világszinten a kriptovaluta-bányászat havi átlagos előfordulási aránya 0,12% volt, ehhez képest a zsarolóprogramok előfordulási aránya mindössze 0,05%. Sok tényező hozzájárul a kártevő kód használatával történő bányászat népszerűségének megnövekedéséhez. A zsarolóprogramokkal ellentétben a kriptovaluta-bányászathoz nincs szükség felhasználói tevékenységre: a kártevő a háttérben dolgozik, míg a felhasználó más feladatokat végez vagy nincs a számítógépénél, és addig nem is veszik észre, amíg a számítógép teljesítménye jelentősen le nem csökken. Ezért kisebb az esélye annak, hogy a felhasználók bármit is tesznek a fenyegetés eltávolítása érdekében, így előfordulhat, hogy a kártevő kód hosszabb ideig is tud tevékenykedni a támadó javára.

A trendet szintén elősegítik a számos kriptovaluta rejtett bányászatára használható „késztermékek" is. A kriptobányászati szoftverek széles körű elérhetősége miatt a belépési korlát alacsony – a kiberbűnözők ezeket a szoftvereket csomagolják újra, hogy a gyanútlan felhasználók gépeire telepítsék őket. A fegyverré alakított bányászati eszközöket ezután eljuttatják az áldozatokhoz, gyakran ugyanazokat a módszereket alkalmazva, mint más fenyegetések esetén, például pszichológiai manipulációval, biztonsági rések kihasználásával és „drive-by" letöltésekkel. A bányászszoftver a telepítést követően a háttérben fut az áldozat számítógépén, hogy blokklánc-számításokat végezzen, és ezáltal a támadó nyereséghez jusson

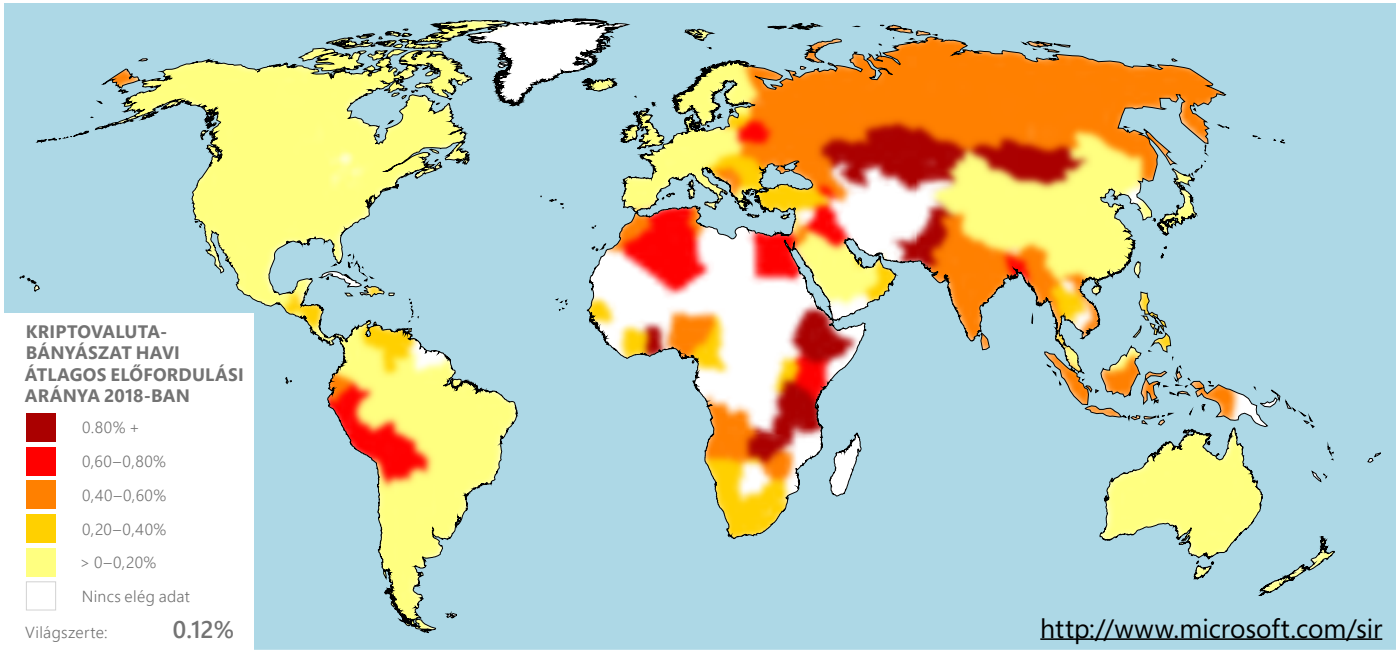
HAVI ÁTLAGOS ELŐFORDULÁSI ARÁNY A KRIPTOVALUTA-BÁNYÁSZAT ÁLTAL LEGINKÁBB ÉRINTETT ORSZÁGOKBAN



Etiópia: **5.58%**

Tanzánia: **1.83%**

Pakisztán: **1.47%**



3. ÁBRA.

A kriptobányász kártevők havi átlagos előfordulási aránya világszerte ország/régió szerint 2018-ban

HAVI ÁTLAGOS ELŐFORDULÁSI ARÁNY A KRIPTOVALUTA-BÁNYÁSZAT ÁLTAL LEGKEVÉSBÉ ÉRINTETT ORSZÁGOKBAN

Írország: 0.02%

Japán: 0.02%

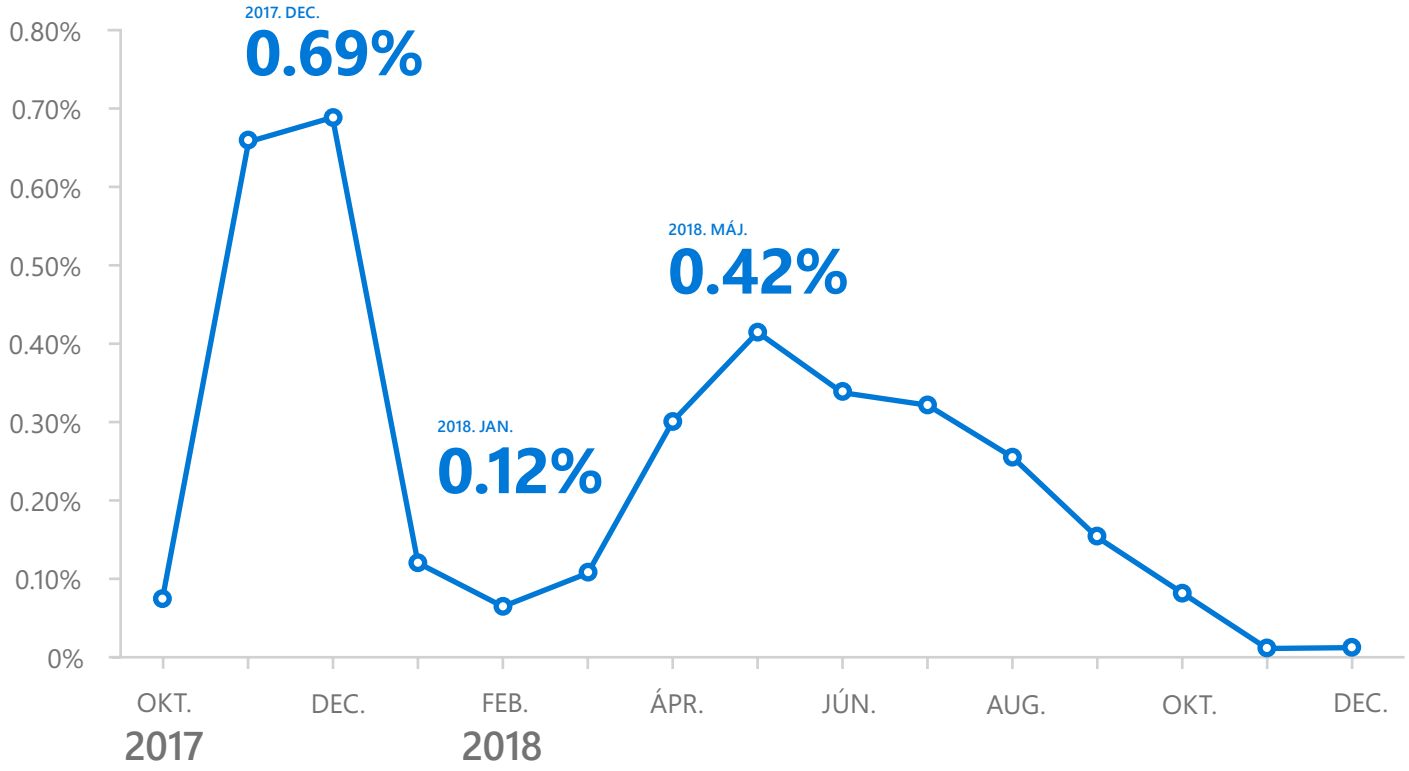
Egyesült Államok: 0.02%

2018-ban az öt legmagasabb havi átlagos kriptobányászat-előfordulási aránnyal rendelkező ország Etiópia (5,58%), Tanzánia (1,83%), Pakisztán (1,47%), Kazahsztán (1,24%) és Zambia (1,13%) volt, ahol mindegyik országban legalább 1,13% volt a kriptobányászat havi átlagos előfordulási aránya ebben az időszakban. A kriptobányászat előfordulási aránya 2018-ban Írországban, Japánban, az Egyesült Államokban és Kínában volt a legalacsonyabb. Ezekben az országokban 0,02% vagy alacsonyabb volt a kriptobányászat havi átlagos előfordulási aránya ebben az időszakban.

BÖNGÉSZŐALAPÚ KRIPTOVALUTA-BÁNYÁSZOK: EGY ÚJ TÍPUSÚ FENYEGETÉS

Az ebben a fejezetben bemutatott statisztikák olyan kártékony kriptovaluta-bányászokat mutatnak be, amelyeket arra terveztek, hogy kártevőként telepítsék őket az áldozatok számítógépein. A legjelentősebb kriptovaluta-bányászati fenyegetések közül néhány azonban teljes egészében egy webböngészőben működik, és egyáltalán nem kell telepíteni őket. Számos szolgáltatás hirdet böngészőalapú kriptovaluta-bányászatot, ami lehetővé teszi a weboldal-tulajdonosok számára, hogy hirdetések nélkül jussanak bevételhez az oldalukra irányuló forgalomból. Az oldaltulajdonosoknak egy JavaScript-kódot kell elhelyezniük az oldalon, amely a háttérben kriptovalutát bányász, miközben a felhasználó az oldalon tartózkodik, és az ebből származó bevétel megoszlik az oldal tulajdonosa és a szolgáltató között. A támadók

A Brocoiner előfordulási aránya



4. ÁBRA.

Előfordulási arány a legelterjedtebb böngészőalapú kriptovaluta-bányász, a Brocoiner esetében

sajnos gyorsan rájöttek arra, hogyan használhatják ki ezeket a szolgáltatásokat kriptopénz bányászatára a felhasználók beleegyezése nélkül. Ehhez sokszor törvényes webhelyeket törnek fel, és kriptovalutát bányászó kártevő kódot illesztenek be a forráskódjukba. A böngészőalapú bányászathoz egyáltalán nincs szükség a felhasználó számítógépének feltörésére, és bármilyen platformon képes működni egy JavaScript-kompatibilis böngésző segítségével. Akárcsak a kriptovaluta-bányászó trójaiak esetében, a böngészőalapú bányászok is jelentősen csökkenthetik a számítógép teljesítményét és megnövelik az áramfogyasztást, amíg a felhasználó ezeken a weboldalakon tartózkodik.

A KÉRETLEN KRIPTOVALUTA-BÁNYÁSZAT HATÁSA

A legnyilvánvalóbb fenyegetés, amely az áldozatokat éri a kártékony kriptovaluta-bányászat miatt, a számítási erőforrások jelentős fogyasztása, ami árampazarláshoz vezethet, valamint jelentősen csökkentheti a számítógép teljesítményét. A felhasználók és a szervezetek más kockázatokkal is szembesülnek a kriptobányászat miatt:

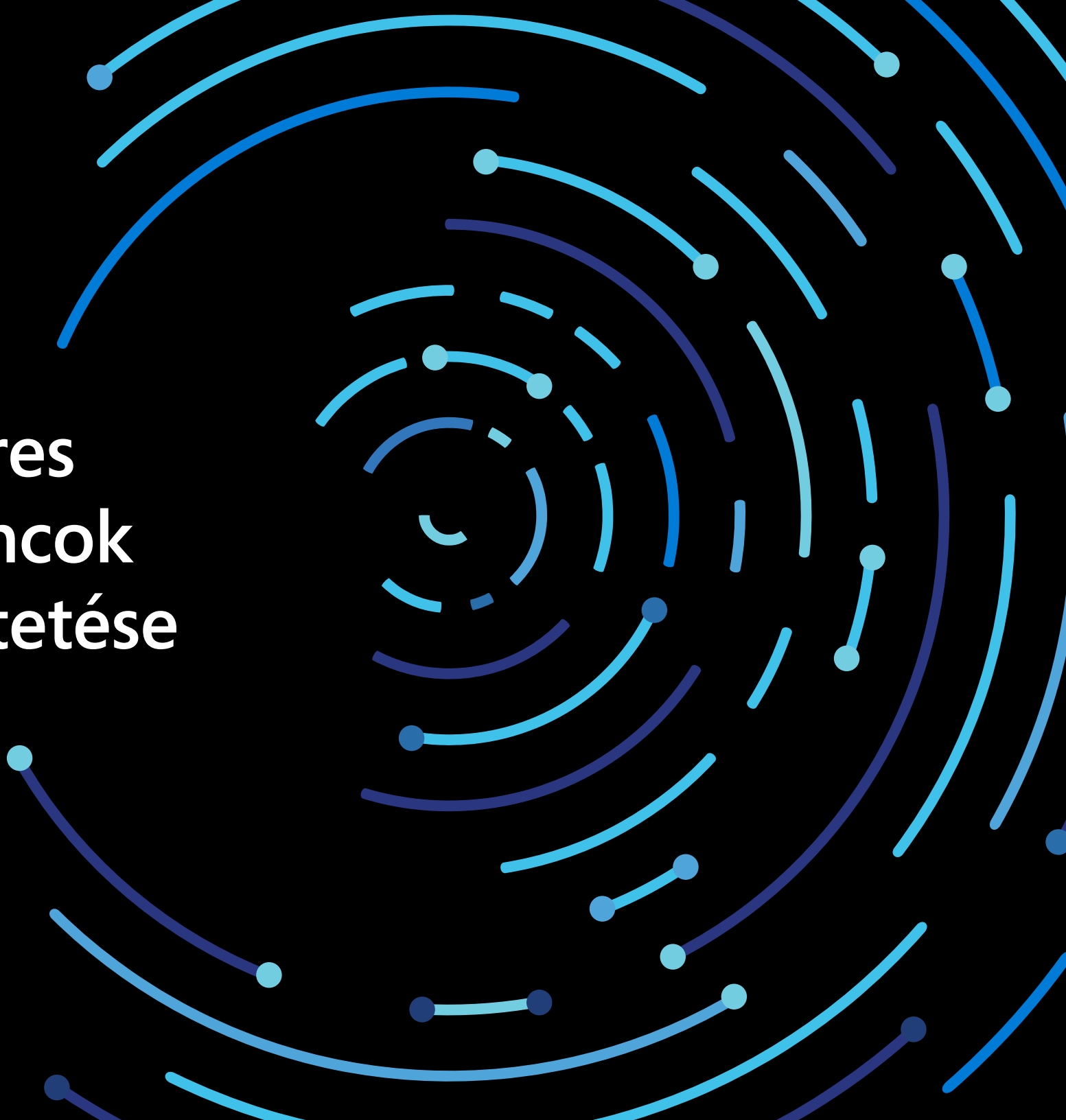
- **A támadók beférkőznek a rendszerbe, így a jövőben nagyobb kárt okozhatnak.**
  Akárcsak más kártevők, a kriptovaluta-bányászat is hozzáférési pont lehet a támadók számára. Míg a számítógép a háttérben kriptopénzt bányászik, a kiberbűnözők megismerhetik a környezetet, és biztonsági réseket fedezhetnek fel, amelyeket más célokra is kihasználhatnak.

- **Az internethez kapcsolódó eszközöket feltörhetik, és kriptovalutát bányászó robotokká alakíthatják.**
  Ezekből az eszközökből gyakran hiányzik a beépített védelem, például a kártevők észlelése, így könnyen a támadók célpontjává válhatnak.

- **Ártanak a gépeknek.**
  Ha a kriptovalutát bányászó szoftverek hónapokon keresztül vagy hosszabb ideig folyamatosan futnak, az ronthat a teljesítményen, a túlzott áramfogyasztás és CPU-használat miatt keletkezett hő pedig ártalmas lehet a számítógépre.

2. FEJEZET

A szoftveres ellátási láncok veszélyeztetése



A Microsoft évek óta nyomon követi azokat a támadókat, akik az ellátási lánc biztonságának sérülését használják fel bejutási pontként a támadásokhoz. Az ellátási láncra irányuló támadásoknál a támadók egy legitim szoftvergyártó fejlesztési vagy frissítési folyamataiba férkőznek be.

Ha ez sikerül, a támadó egy legitim alkalmazásba vagy frissítési csomagba építi be a veszélyes elemet, amely ezután a terjesztési csatornákon keresztül eljut a szoftver felhasználóihoz. A kártékony kód ugyanolyan megbízhatónak tűnik, és ugyanolyan engedélyekkel rendelkezik majd, mint a szoftver. Az elmúlt években megnövekedett számú, szoftveres ellátási láncokat érintő támadások a kiberbiztonság fontos témájává váltak, és számos IT-részleg elsődleges problémájává nőtték ki magukat.

A SZOFTVERES ELLÁTÁSI LÁNCOKAT ÉRINTŐ JELENTŐS TÁMADÁSOK 2017-BEN

▲ 5. ÁBRA.

Szoftveres ellátási láncot érintő támadások 2017-ben és 2018-ban

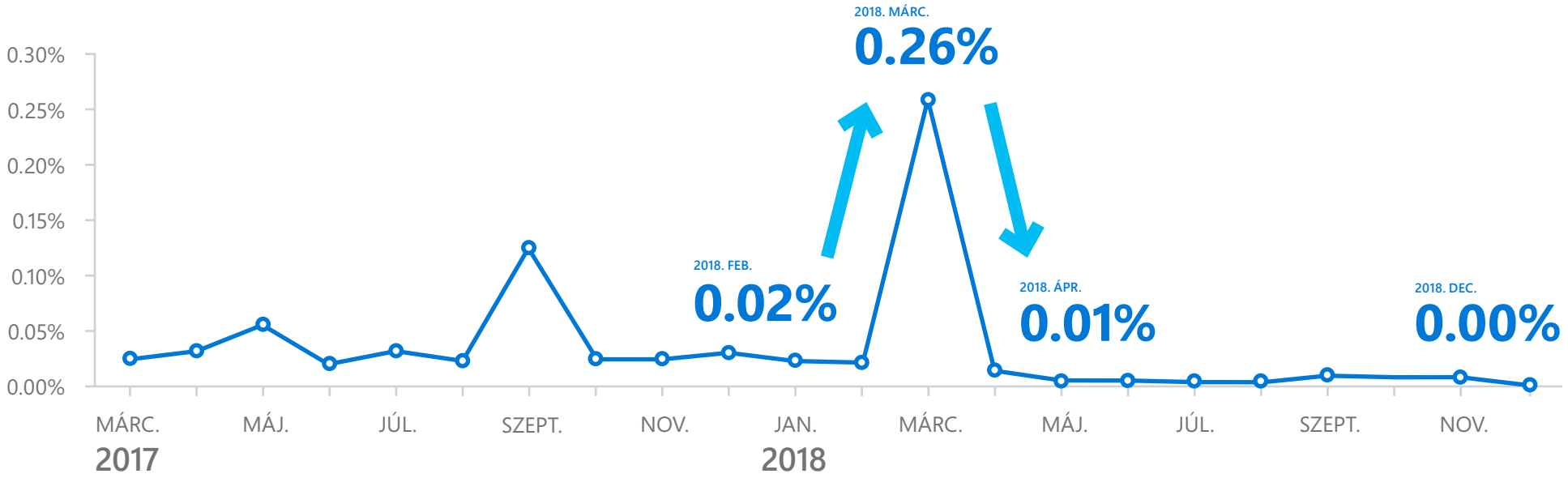
2017-ben az ellátási láncot érintő támadások voltak felelősek számos jelentős biztonsági incidensért, amelyek közül a legismertebb a Petya zsarolóprogram volt júniusban. Ezt egy népszerű ukrajnai számviteli alkalmazás feltört frissítési folyamata okozta, majd a fertőzés onnan terjedt tovább. Májusban az Operation WilySupply egy szövegszerkesztő szoftverfrissítését támadta meg, és hátsó kaput telepített a pénzügyi és az informatikai szektorban megcélzott szervezeteknél. Júliusban a ShadowPad nevű hátsó kaput rejtették el egy szerverfelügyeleti szoftvercsomagba, így a támadók további kártevő kódokat tudtak telepíteni, amelyekkel adatokat lophattak el, és egyéb kártékony tevékenységeket folytathattak. Szeptemberben a népszerű freeware eszköz, a CCleaner esett áldozatul, és egy hátsó kapuval ellátott verzió jutott el a felhasználókhoz.

A szoftveres ellátási láncot érintő támadások 2018-ban – alapvető kiváltó okok és hatás2018-ban a szoftveres ellátási láncokat érintő első jelentős támadás március 6-án történt, amikor a Windows Defender ATP blokkolt egy súlyos kampányt, amely elterjesztette volna a Dofoil trójait (Smoke Loader-nek is nevezik). A súlyos kártevő kampány visszavezethető volt egy megfertőzött P2P-alkalmazásra. Az alkalmazás frissítési csomagját lecserélték egy rosszindulatúra, az sérült biztonságú kódot töltött le, amely később telepítette a Dofoil kártevőt. A kifinomult trójai kriptobányászati terhelést jelentett, és fejlett folyamatközi injektálási technikákat, adattárolási mechanizmusokat és elkerülési módszereket alkalmazott.

6. ÁBRA.

A Dofoil (Smoke Loader) előfordulására vonatkozó 2018-as adatok alapján márciusban jelent meg a legtöbb blokkolt példány

A Dofoil előfordulási aránya



A kampány első 12 órájában a Windows Defender Antivirus több mint 400 000 fertőzési kísérletet akadályozott meg világszerte. Az összes előfordulás 73%-a Oroszországban, 18%-a Törökországban, 4%-a pedig Ukrajnában volt.

2018-ban számos további támadást is észleltek, amelyek a szoftveres ellátási láncok biztonságának sérülését használták ki, többek között az alábbiakat:

Időszak	Támadás	Leírás	Érintett szoftverek
2018. március	Dofoil kriptobányászati kampány (a Microsoft jelentette)	A támadók egy P2P-alkalmazás frissítési folyamatát fertőzték meg a Dofoil telepítéséhez, amely ezután kriptovalutát bányászó kártevőt telepített.	P2P-alkalmazás.
2018. július	Egy ellátási láncon belüli ellátási lánc biztonságának sérülése (a Microsoft jelentette).	A támadók egy PDF-szerkesztő alkalmazás gyártója és annak egyik szoftverszállító partnere közötti megosztott infrastruktúrát támadták meg.	PDF-szerkesztő alkalmazás és külső beszállító partner.
2018. augusztus	Távoli támogatási program biztonságának sérülése (Operation Red Signature – a Trend Micro és az IssueMakersLab jelentette).	Egy távtámogatási megoldásszolgáltató frissítési szerverét törték fel, hogy az ún. „9002 RAT" távelérési eszközt terjessze a felhasználóknak.	Távtámogatási program.
2018. október	Webtárhely-kezelő rendszert ért támadás (az ESET jelentette).	Egy webtárhely-kezelő rendszer telepítőszkriptjét megváltoztatták, hogy hitelesítő adatokat lopjanak el.	Webtárhely-kezelő rendszer.

7. ÁBRA.

Egyéb szoftveres ellátási láncot érintő támadások 2018-ban

VESZÉLYBEN A BIZALOM

Az ellátási lánc elleni támadások azért nagyon alattomosak, mert a felhasználók és az IT-szakemberek általuk használt szoftverekbe vetett bizalmát használják ki. A feltört szoftverek gyakran a szállító digitális aláírásával és hitelesítésével rendelkeznek, és gyakran nincs jele annak, hogy probléma lenne velük, ami miatt jelentősen nehezebb a fertőzés észlelése. Az ellátási láncok és az ügyfelek közötti kapcsolat megromolhat, függetlenül attól, hogy vállalati vagy otthoni felhasználókról van szó. A szoftverek megfertőzésével és a telepítési vagy a frissítési infrastruktúrák aláásásával az ellátási láncot érintő támadások hatással lehetnek a szervezetek által biztosított termékek és szolgáltatások sértetlenségére és biztonságára.

Az ellátási láncokat érintő támadások számos szoftvert, valamint különböző ágazatokban és régiókban működő cégeket is érintettek. Az ellátási láncot érintő támadások az egész ágazatra kiterjedő problémát jelentenek, amelyre számos érintettnek figyelnie kell, ideértve azokat a szoftverfejlesztőket és -szállítókat is, akik a kódot írják, a rendszergazdákat, akik a szoftvertelepítéseket kezelik, valamint az információbiztonsági közösséget, amely észleli ezeket a támadásokat, és megoldást keres rájuk az emberek és a szoftverek védelme érdekében.

A SZOFTVEREKEN TÚL: AZ ELLÁTÁSI LÁNC BIZTONSÁGÁNAK SÉRÜLÉSE FELHŐALAPÚ OBJEKTUMOKON KERESZTÜL

Az ellátási láncot érintő támadások képessége a bizalom aláásására megerősödött, és a helyzet még összetettebbé vált a felhőben. A felhőalapú objektumok, szolgáltatások és infrastruktúra biztonságának sérülésével kapcsolatos 2018-as incidensek jól mutatják ennek komplexitását:

- Fertőzött Chrome-bővítmények, amelyek kattintással terjedő kártevőt telepítettek (az ICEBRG jelentette)
- Számos Linux-repó feltörése (online fórumok jelentették)
- Kártékony WordPress beépülő modulok használata különböző kártékony tevékenységekhez, ami lehetővé tette többek között azt, hogy a támadók tartalmat tegyenek közzé a WordPress-oldalakon (a Wordfence jelentette)
- Egy Docker Hub-fiókba feltöltött kártékony Docker-rendszerképek, amelyek kriptovaluta-bányászathoz használt kártevő letöltésére szolgáló szkriptet tartalmaztak Fortinet és a Kromtech jelentette)
- A hivatalos Python-repóban egy kártékony „typo-squatting" csomag jelent meg; a csomag egy olyan kártevőt letöltő szkriptet tartalmazott, amely a vágólapra másolt kriptovaluta-címeket a támadó címére cserélte ki (a Medium jelentette)
- Feltört szkript a StatCounterben, amely lehetővé tette a támadók számára, hogy kártékony szkriptet helyezzenek el a StatCountert használó weboldalakon (az ESET jelentette)
- Több, hátsó kapuval ellátott npm-modul (The npm Blog, Medium), amelyeket kihasználva egy támadó például tetszőleges kódot helyezhet el egy futó szerveren, és végre is hajthatja azt.

Ezek az incidensek jól szemléltetik, hogy az ellátási lánc biztonságának sérülése rendkívüli módon megnövelheti a támadási felületet. Ha a felhőben lévő objektumok nem védettek, váratlan támadási pontot jelenthetnek. A Docker Hub incidens például egy kártékony fiókot használt a Docker-rendszerképek feltöltésére, amelyek rejtett, kriptobányászatra használható hátsó kaput tartalmaztak. A Docker-rendszerképeket a Docker Hubon tárolták majdnem egy évig, és a gyanútlan rendszergazdák és felhasználók több milliószor letöltötték és használták őket.

Az ellátási láncot érintő kockázatok kiterjednek a felhőben futó kódra, a nyílt forráskódra, a webes függvénytárakra, a konténerekre és más felhőbeli objektumokra is. Ezek a kockázatok a szoftveres és hardveres ellátási láncok eddig kiderült biztonsági sérüléseinek sokféleségével párosulva az ellátási láncot érintő fenyegetések széles skáláját képviselik. Bár nem létezik univerzális megoldás e támadástípusok teljes spektruma ellen, a szervezeteknek ki kell építeniük a szükséges megelőző védelmet és incidensek utáni detektálási képességet, hogy védekezni tudjanak a megtámadott hardver- és szoftvergyártók, a beszállítóik, a felvásárolt cégek, a nyílt forráskódú szoftverfejlesztők, valamint a felhőszolgáltatók és az infrastruktúra-szolgáltatók ellátási láncát érintő támadások ellen.

Az informatikai támadások kivizsgálása a DART segítségével

A Microsoft incidenssészleléssel és -kezeléssel foglalkozó csapata (DART) kiberbiztonsági szakemberekből és incidenskezelőkből álló globális csapat, amely segít a szervezeteknek észlelni, kivizsgálni és kezelni a kiberbiztonsági incidenseket. Ebben a fejezetben a DART által a tavalyi évben kezelt ügyfélesetek közül vizsgálunk meg néhányat. Ezek általános képet adnak a támadói trendekről, és arról, hogy a Microsoft és az ügyfelek hogyan tudják azokat meghiúsítani.

ÁLLAMILAG SZERVEZETT INFORMÁCIÓSZIVÁROGTATÓ TÁMADÁSOK PROFESSZIONÁLIS SZOLGÁLTATÓSZERVEZETEK ELLEN

Egy professzionális szolgáltatószervezetet kifinomult, államilag finanszírozott, összetett, tartós fenyegetés (APT) általi támadás ért, amellyel hozzáférést nyertek a szervezet kiemelten fontos hitelesítő adataihoz. A támadók szórásos jelszófeltöréses támadással szereztek hozzáférést a hálózathoz gyenge vagy sokak által használt jelszavak segítségével (például „p@ssword" vagy „123456"), hogy nagyszámú felhasználói fiókot célozhassanak meg, és megszerezzék az Office 365 rendszergazdai hitelesítő adatait. (A lebukás elkerülése érdekében szórásos jelszófeltöréses támadásokkal korlátozták a bejelentkezési kísérletek számát az egyes fiókoknál.) A hálózatba való beszivárgást követően az APT precízen, automatizált módon kiszivárogtatta az adatokat az alkalmazottak postaládájából. Annak ellenére, hogy voltak belső próbálkozások a kizárására, a támadó több mint 200 napig a hálózatban maradt. A támadók a támadás keretében kihasználták a szervezet ellátásilánc-kezelő szoftverét, és automatizált módon szivárogtatták ki az adatokat.

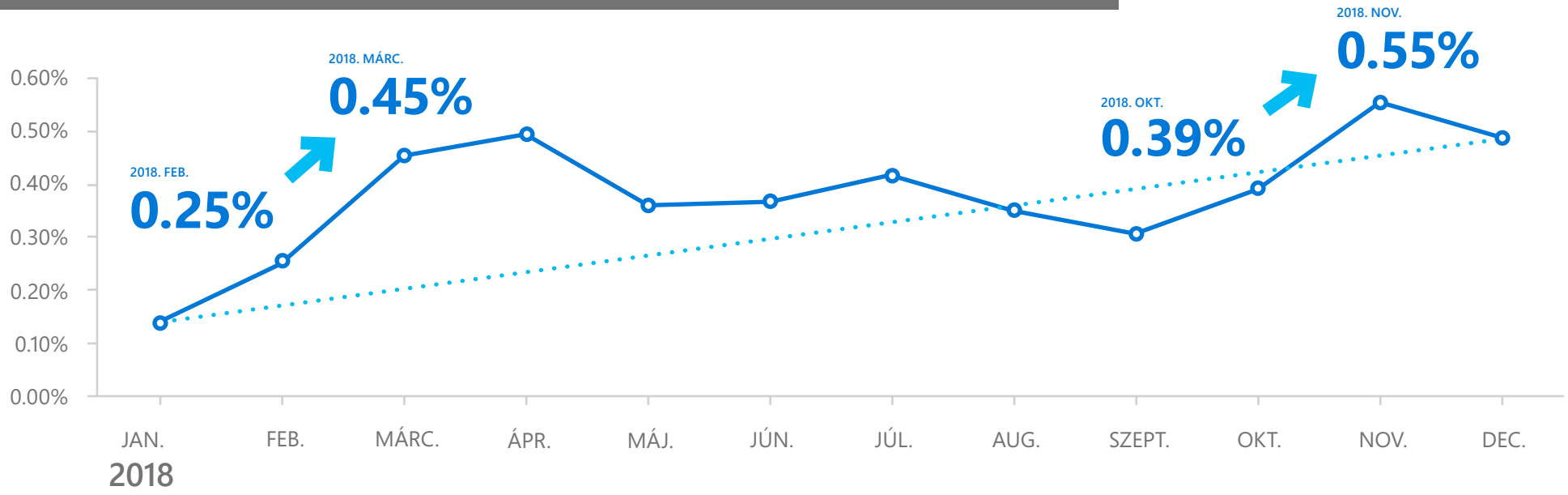
Mivel sejtették, hogy ügyféladatok szivárogtak ki, a szervezet felkérte a DART csapatát, hogy vizsgálja ki a helyzetet, és segítsenek megelőzni a további károkat. A DART azonosította a célzott kereséseket az Office 365-postaládákban, a feltört fiókokat és a támadó irányítási csatornáit. A legfontosabb tanulság ebből az incidensből az, hogy a felhőszolgáltatások azonosításalapú fenyegetésekkel és támadókkal szembeni védelme érdekében ellenőrzésekre van szükség. A szervezet többfaktoros azonosítást (MFA), bizonyos felhőalkalmazásokhoz feltételes hozzáférési szabályzatot és Office 365-naplózást vezetett be. Ahhoz, hogy a jövőben nagyobb védelmet élvezzen a hasonló fenyegetésekkel szemben, a szervezetnek végponti fenyegetésészlelő és -kezelő (EDR) megoldást kell alkalmaznia azon támadók azonosítására, akik megpróbálhatják kihasználni a hálózatot. Javasoltuk továbbá, hogy a szervezet nevezzen ki egy felhőért felelős irányító testületet vagy egy globális azonosításért felelős csapatot, akik kezelni és biztosítani tudják a megfelelő felhasználó-azonosítási szabályokat, így a szervezetnek rálátása lesz a biztonságra, és hatékonyabban tudja csökkenteni a kockázatot.

3. FEJEZET

Az adathalászat nem vesztett népszerűségéből

2018-ban a Microsoft fenyegetésekkel foglalkozó szakértői úgy látták, hogy a támadók kedvenc módszere továbbra is az adathalászat maradt. Úgy tűnik, hogy az adathalászat a belátható jövőben is problémát fog jelenteni, mivel a kiberbűnözők folyamatos erőfeszítéseivel szemben az emberi döntések és ítélőképesség állnak.

Az adathalászat aránya változatlanul magas.
Adathalász e-mailek százalékos aránya az összes beérkező e-mailhez képest



2018-BAN IS AZ ADATHALÁSZAT MARADT A LEGNÉPSZERŰBB TÁMADÁSI FORMA.

▲ 8. ÁBRA.

Adathalász e-mailek 2018-ban

A Microsoft havonta több mint 470 milliárd e-mail-üzenetet elemez és vizsgál meg az Office 365-ben adathalász és kártevő tevékenység után kutatva, így a szakértőknek nagy rálátása van a támadói trendekre és módszerekre. A beérkező levelek között megjelenő adathalász üzenetek száma 250%-kal nőtt 2018 januárja és decembere között. Az adathalászat továbbra is a leggyakoribb támadási forma, amelyet arra használnak, hogy teljesen új kártékony kódokat küldjenek a felhasználóknak, a Microsoft pedig a felhasználók biztonsága érdekében az adathalászat elleni védelemre szolgáló észlelési, vizsgálati és incidenskezelési lehetőségek kidolgozásával folyamatosan próbálja megerősíteni a támadásokkal szembeni védelmét.

Az adathalász módszerek fejlődése

Az adathalászattól védő eszközök és módszerek fejlődéséhez a támadóknak is alkalmazkodniuk kellett. Az adathalász támadások rendkívül sokfélék lettek, ami azt jelenti, hogy a támadók nem egyetlen URL-címet, tartományt vagy IP-címet használnak e-mail-küldésre, hanem változatos infrastruktúrát használnak, több támadási ponttal. A támadások jellege is megváltozott; a modern adathalász kampányok között vannak olyan rövid távú támadások, amelyek csak pár percig aktívak, és sokkal hosszabb, nagy volumenű kampányok is. Léteznek támadássorozat-jellegűek is, ahol a támadók kis mennyiségű e-mailt küldenek több egymást követő napon keresztül.

A Microsoft ezenkívül megfigyelte, hogy a támadók egyre több szolgáltatott infrastruktúrát és egyéb nyilvános felhőinfrastruktúrát használnak, ezáltal nehezebb az észlelés, hiszen legitim oldalak és eszközök mögé rejtőznek. A támadók például egyre nagyobb számban használnak népszerű dokumentummegosztó és együttműködési webhelyeket és szolgáltatásokat kártevő kódok és hamis bejelentkezési űrlapok terjesztésére, hogy ellopják a felhasználók hitelesítő adatait. Emellett gyakrabban vesznek igénybe feltört fiókokat további kártékony e-mailek küldésére a szervezeteken belül és kívül egyaránt.

Az adathalász kampányok lehetnek célzottak és általánosak.

Akárcsak a kártevők terjesztése általában, az adathalász kampányok is lehetnek célzottak vagy szélesebb körű, általánosabb támadások. Habár a kifinomultabb támadások esetén feltört fiókonként nagyobb a nyereség, az általánosabb támadások fiókonként kevesebb pénzt hoznak, de szélesebb felhasználói kört céloznak meg.

Kifinomult, célzott kampány például az Ursnif, amelynek során a támadók honosították a dokumentumneveket, hogy az a célzott szervezethez hasonló szervezetre vagy ágazatra jellemző legyen. Ezek a támadások nagyon különböznek az általános kampányoktól, sokkal hitelesebbnek és megbízhatóbbnak tűnnek.

2018-ban az általánosabb kampányok vállalati levelezések feltörésével (BEC) és a célszervezeteken belül ismert márkák, tartományok vagy felhasználók megszemélyesítésével voltak kapcsolatosak, illetve kifinomult családkampányok voltak. A tartomány megszemélyesítése egy bevett támadói módszer, amelyet arra használnak fel, hogy meggyőzzék velük a cégeket, hogy az e-mail megbízható, ezért megnyitható.

Az adathalász csalik sokféle formát ölthetnek.

A Microsoft kutatóinak megfigyelése szerint az adathalász csaliknak vagy a kampányok során alkalmazott kártevő kódoknak sok különböző típusa van, például:

- **Tartománynév-hamisítás** (az e-mail-üzenet tartománya pontosan megegyezik az eredeti tartománynévvel)
- **Tartomány megszemélyesítése** (az e-mail-üzenet tartománya hasonlít az eredeti tartománynévre)[2]
- **Felhasználó megszemélyesítése** (úgy tűnik, hogy az e-mail-üzenet megbízható személytől érkezik)
- **Szöveges csalik** (úgy tűnik, hogy a szöveges üzenet hiteles forrásból származik, például egy banktól, kormányhivataltól vagy más vállalattól, így a címzett azt hiszi, jogosan kérnek tőle valamit, általában bizalmas adatokat – felhasználóneveket, jelszavakat vagy bizalmas pénzügyi adatokat)
- **Hitelesítő adatok halászatára használt hivatkozások** (az e-mail-üzenet olyan oldalhivatkozást tartalmaz, amelynek a bejelentkező oldala nagyon hasonlít a hiteles oldaléra, így a felhasználók megadják a hitelesítő adataikat)
- **Adathalász csatolmányok** (az e-mail-üzenet olyan kártevő fájlcsatolmányt tartalmaz, amellyel a küldő ráveszi az áldozatot, hogy megnyissa azt)
- **Hamis felhőtárhelyre mutató hivatkozások** (úgy tűnik, hogy az e-mail-üzenet hiteles forrásból származik, ezzel ráveszi a felhasználót, hogy engedélyt adjon és/vagy olyan személyes adatot adjon meg, mint a hitelesítő adatai, cserébe pedig egy hamis felhőtárhelyhez fér hozzá)

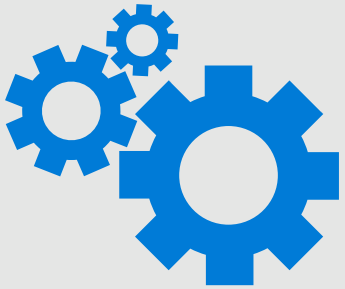
Ezek a támadók által használt változatos csalik még komplexebbé teszik az adathalász fenyegetéseket, amelyekkel a szervezeteknek meg kell küzdeniük.

LÁBJEGYZET

[2] A tartománynév megszemélyesítése abban a különleges esetben hasonlít a tartománynév-hamisításhoz (amikor az eredeti tartománynévvel teljesen megegyezik a hamis), amikor a tartomány megjelenik az e-mail megjelenítendő nevében.

Az informatikai támadások kivizsgálása a DART segítségével

CÉLZOTT ADATHALÁSZAT EGY NAGY GYÁRTÓVÁLLALAT ELLEN

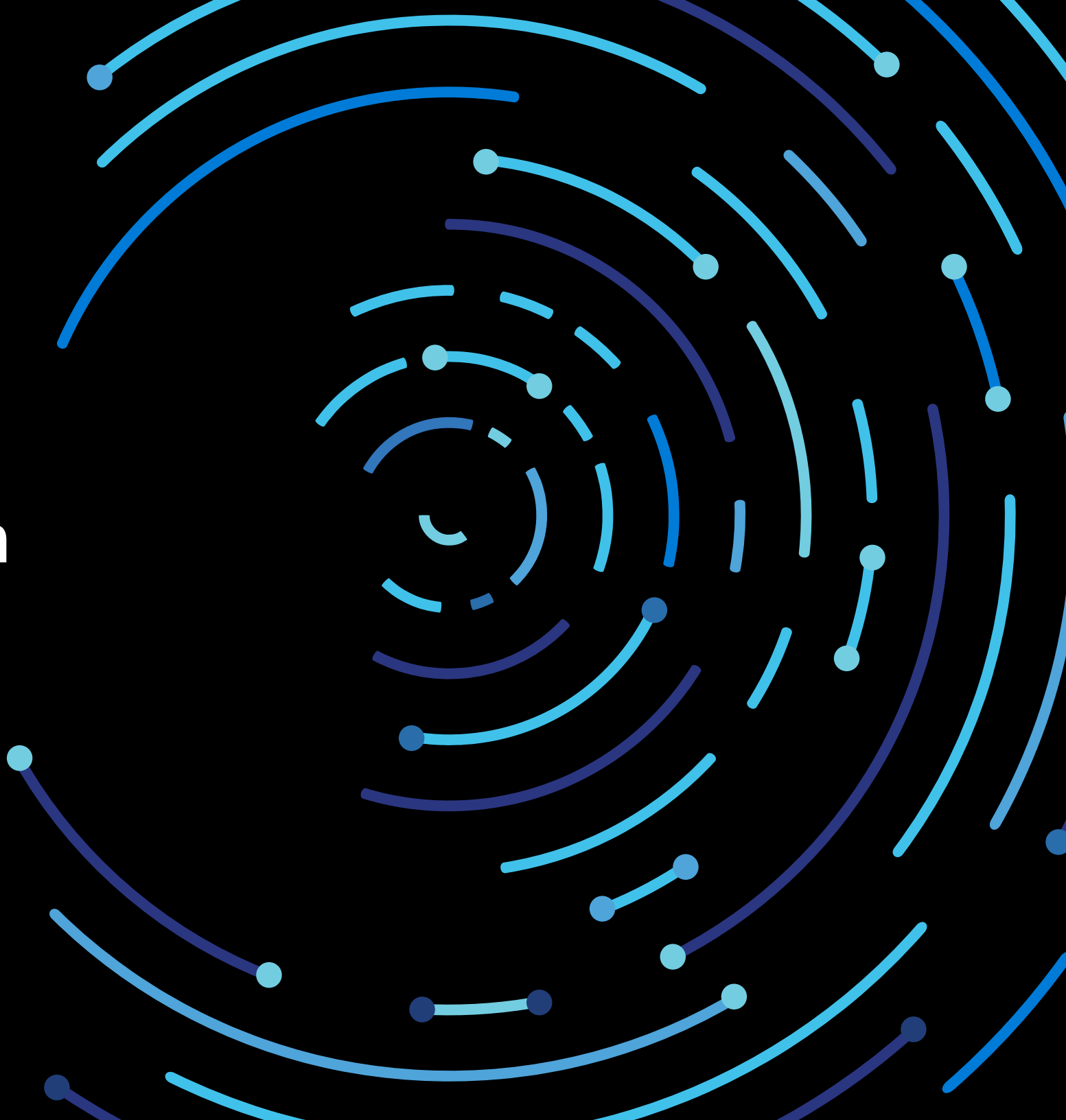


Egy gyártóvállalat ellen többfázisú adathalász kampányt indítottak néhány hónap leforgása alatt. Ez nem szokatlan módszer. Az első fázis során a támadó felderítést végez, a második fázisban pedig célba veszi az értékes célpontokat. A kampány első szakaszában azt a jól ismert adathalász csalást alkalmazták, amikor beágyazott weboldal-hivatkozást tartalmazó e-mailt küldenek a szervezeten belül egy kisebb célzott csoportnak. Az e-mail szerint a célszemélynek egy fontos elektronikus dokumentumot kell átolvasnia, és csak meg kell adnia a hitelesítő adatait a hozzáféréshez. A célszemély számára készített hamis kezdőlap, ahol az ún. „fontos dokumentumot" meg tudja tekinteni, igazából begyűjtötte a hitelesítő adatokat, és lehetővé tette a támadó számára, hogy hozzáférjen az Office 365-fiókokhoz a világon bárhonnan. Az adathalász kampány második fázisában hasonló adathalász e-maileket terveztek küldeni a gyártóvállalat magasabb rangú munkatársainak, annak reményében, hogy értékesebb adatokhoz kapnak hozzáférést.
A Microsoft az adathalász kampány második fázisában került kapcsolatba az ügyféllel. Az ügyfél számára a legnagyobb tanulság az volt, hogy az adathalászat továbbra is az egyik leghatékonyabb támadási mód, és a felhasználók jelentik a leggyengébb láncszemet. A felhasználók adathalász kísérletek felismerésével kapcsolatos képzése, a támadók azonosítására alkalmas eszközök és lépések biztosítása, valamint a rendszerek folyamatos frissítése mind fontosak; ha a szervezet akár csak az egyiket is figyelmen kívül hagyja, sérülékeny lehet.

Ebben az esetben az ügyfélnek az volt a legfontosabb, hogy azonnal megszüntessék a feltört fiókok külső hozzáférését. Az Azure Identity és az Office 365 csapatai segítségével a DART tervet dolgozott ki arra vonatkozóan, hogyan lehetne a támadókat kizárni a hálózatból, és felügyelni a parancscsatorna és a vezérlőcsatorna felé irányuló forgalmat az újonnan telepített Microsoft Azure Log Analytics megoldás segítségével. A csapat alig három óra alatt megoldotta a helyzetet. A támadó hozzáférése megszűnt, a szervezet pedig a kárfelmérésre és a helyrehozásra tudott koncentrálni. A DART az Azure Log Analytics eszközeit használta a támadói viselkedés felkutatására, amely segített felfedni számos konfigurációs kihívást a szervezet számára. A DART azonosította, hogy javítani kell a kritikus fontosságú kiszolgálók biztonságán, kiderítette, hogy vannak olyan számítógépek a hálózaton, amelyek köztudottan rosszindulatú gazdagépekkel kommunikálnak az interneten, valamint több kiszolgálót is talált, amelyek nem rendelkeztek kártevők elleni védelemmel.

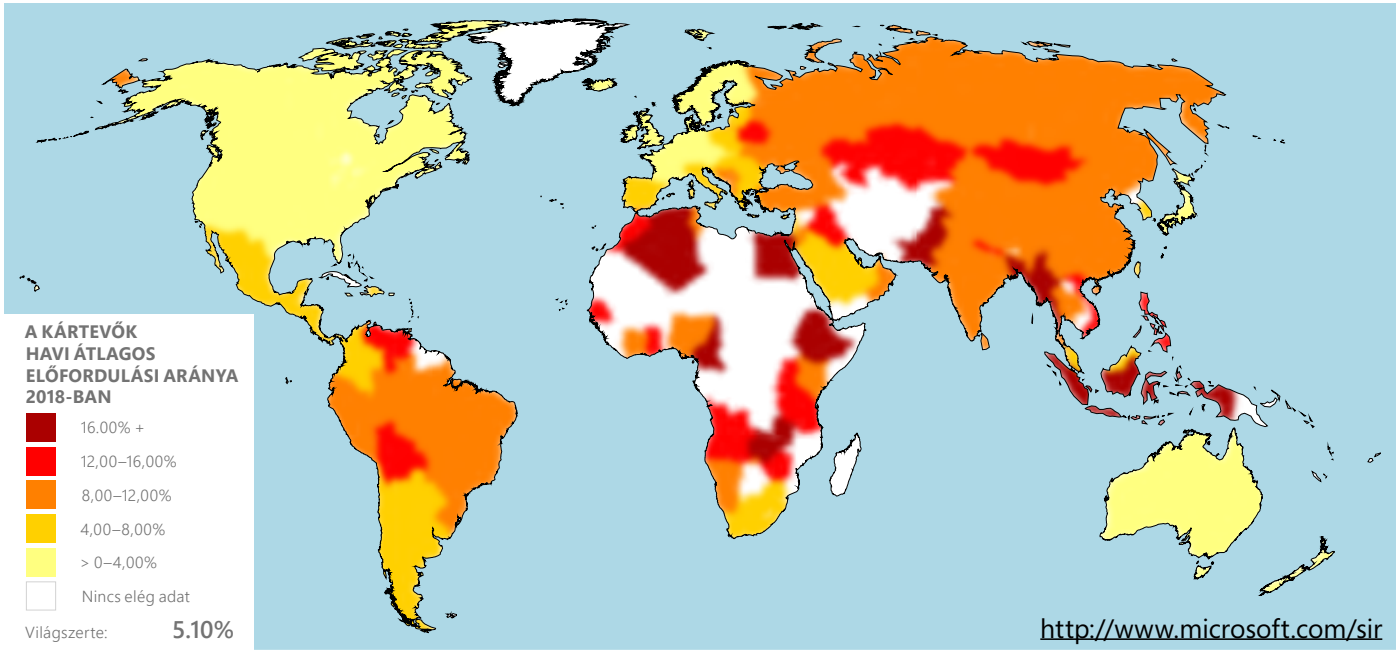
4. FEJEZET

Kártevők a világban



A kártevők a szervezetek és az egyének számára is kockázatot jelentenek, károsíthatják a használhatóságot, adatveszteséget okozhatnak, szellemitulajdon-lopást eredményezhetnek, pénzügyi veszteséget, szorongást okozhatnak, és akár emberéleteket is veszélyeztethetek. A Microsoft sokféle eszközt és módszert alkalmaz a kértevők által okozott fertőzések beazonosítására, megakadályozására és kiiktatására.

A kártevők előfordulási aránya 2017-ben 5% és több mint 7% között mozgott. 2018 elején először megnövekedett, majd az év többi részében 4 százalék fölötti értékre csökkent ez az arány. A kártevők előfordulási arányának 2018-as csökkenése összességében talán a Windows 10 bevezetésének növekedésére és a Windows Defender védelmi megoldás szélesebb körű használatára vezethető vissza. Az előfordulási arány azoknak a számítógépeknek a százalékos száma, amelyeken Windows Defender víruskereső fut, és amelyek a hónap során kártevő-előfordulást jelentettek, ideértve azokat a kísérleteket is, amelyeket a Defender kivédett.



9. ÁBRA.

A kártevők havi átlagos előfordulási aránya világszerte ország/régió szerint 2018-ban

2018. január és december között az öt legmagasabb havi átlagos kártevő-előfordulási aránnyal rendelkező ország Etiópia (a havi átlagos előfordulási arány 26,33%), Pakisztán (18,94%), Palesztina (17,50%), Banglades (16,95%) és Indonézia (16,59%), ahol mindegyik országban legalább 16,59% volt a havi átlagos előfordulási arány ebben az időszakban. A fertőzési arány általában szoros összefüggésben áll az emberi fejlettségi tényezőkkel és az adott társadalom technológiai felkészültségével. Azok az országok, ahol 2018-ban a legmagasabb volt az előfordulási arány, az Egyesült Nemzetek Nemzetközi Távközlési Uniója által publikált 2017-es Információs és kommunikációs technológiák (ICT) mutatójának utolsó 40 százalékában találhatók.

A kártevők előfordulási aránya ebben az időszakban öt helyen volt a legalacsonyabb: Írországban (1,26%), Japánban (1,51%), Finnországban (1,74%), Norvégiában (1,79%) és Hollandiában (1,82%). Ezekben az országokban 1,82% vagy alacsonyabb volt a havi átlagos előfordulási arány ebben az időszakban. Ezek az országok jellemzően érett kiberbiztonsági infrastruktúrával és a legfontosabb infrastruktúrák védelmére szolgáló jól kidolgozott programokkal rendelkeznek, valamint ezekben az országokban a lakosság tájékoztatást kap az alapvető biztonsági kérdésekről.

HAVI ÁTLAGOS ELŐFORDULÁSI ARÁNY A KÁRTEVŐK ÁLTAL LEGINKÁBB ÉRINTETT ORSZÁGOKBAN

Etiópia: **26.33%**

Pakisztán: **18.94%**

Palesztina: **17.50%**

Az informatikai támadások kivizsgálása a DART segítségével

TÖBB PÉNZÜGYI SZOLGÁLTATÓ SZERVEZETET ÉRT A MŰKÖDÉSÉT AKADÁLYOZÓ, ÁLLAMILAG TÁMOGATOTT TÁMADÁS.

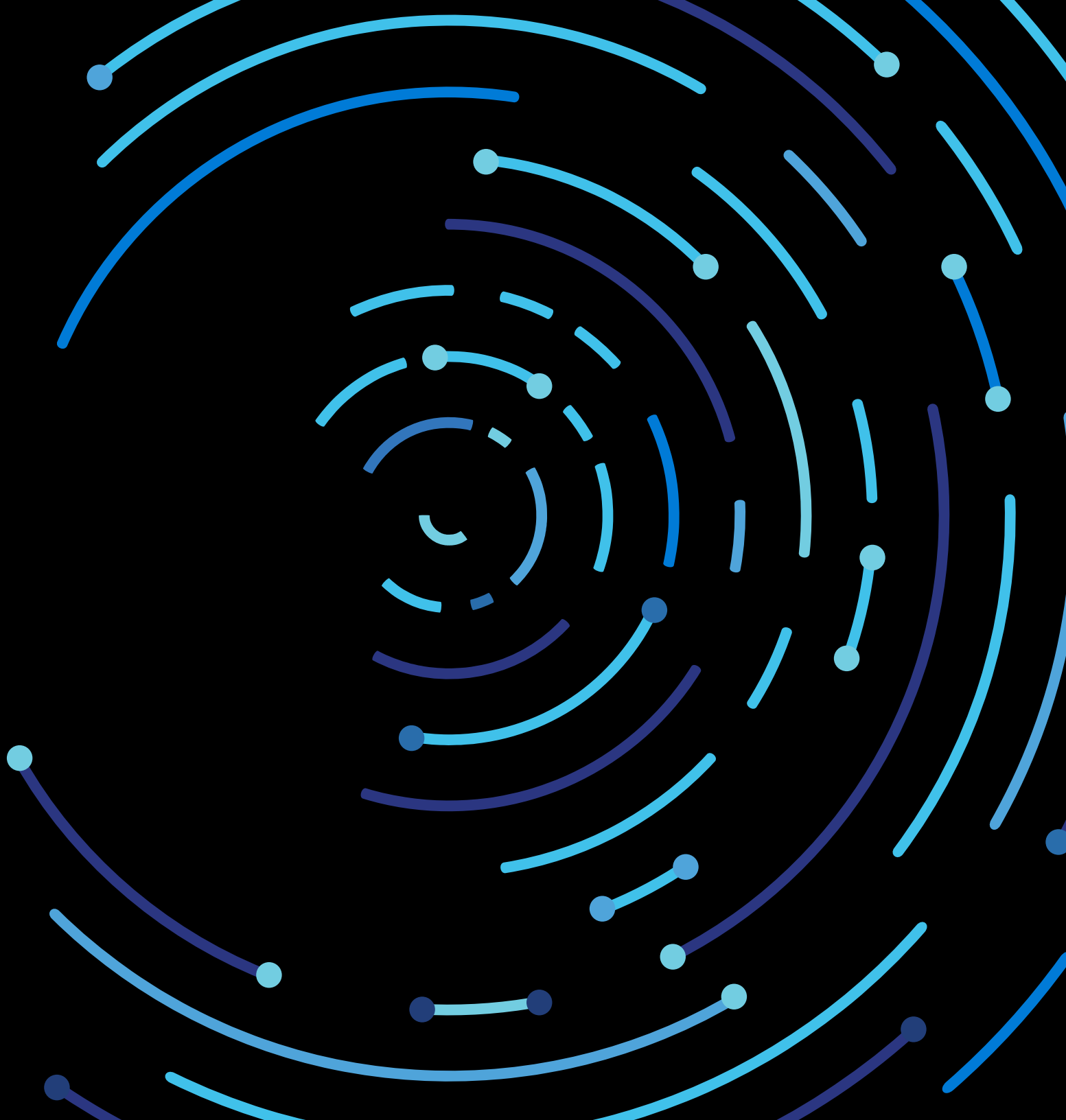
Az egyik legpusztítóbb incidens, amelynek a DART tanúja volt, egy számos pénzügyi szolgáltatót érintő, államilag finanszírozott APT volt (ez a korábban már említett, professzionális szolgáltató szervezeteket támadó csoporttól eltérő társaság), amely hasonló módon zajlott.

Ez az APT rendszergazdai jogosultságot szerzett, miután megfertőzte az első gépet egy jól célzott, rejtjelezett hátsó kapu elhelyezésével, valószínűleg egy célzott adathalász e-mailen keresztül. Ennek eredményeképpen az APT több csalárd tranzakciót is végrehajtott, amelynek során nagy pénzösszegeket utaltak át külföldi bankszámlákra. Néhány esetben a támadó több mint 100 napig észrevétlen maradt. Miután a támadó rájött, hogy észlelték a jelenlétét, gyorsan végrehajtott egy előkészített támadást, és kártevőt telepített a környezetben lévő rendszerek több mint felére. Ezeknek az ügyfeleknek a működése napokra leállt.

Az ügyfelek fontos tanulságokat vonhattak le az esetekből. Az első, hogy a szoftverek életciklus-kezelése különösen fontos, ami magában foglalja a rendszerek (operációs és biztonsági rendszerek) rendszeres frissítését, javítását és ellenőrzését. Az egyik szervezet Linux-rendszerkörnyezete, amelyben rendkívül sok feladat futott, teljesen felügyelet nélkül működött, ezzel pedig hatalmas támadási kockázatnak volt kitéve. A másik tanulság az volt, hogy nagyon fontos biztonsági másolatot tartani egy offline helyszínen a rendszeradatokról arra az esetre, ha az elsődleges adatok elvesznének. Egy másik tanulság pedig az volt, hogy a hagyományos vírusirtó megoldások nem mindig elegendők a támadói tevékenység felismerésére.

Ezeknél a szervezeteknél a legfontosabb dolog a normál működésre való visszaállás volt. A DART azzal segített helyreállítani a szolgáltatásokat, hogy először kivizsgálta a helyzet súlyosságát, majd megtette a szükséges kockázatcsökkentő lépéseket, például eltávolította a kártevőt az érintett rendszerekből, és helyreállította azokat. A csapat képzést tartott az ügyfeleknek a Microsoft fenyegetésvizsgálati eszközeinek használatáról, ideértve az EDR-t és egyéb eszközöket is, hogy észlelhessék a rendellenes jelenségeket, vagy ha támadó tevékenykedik a hálózaton. A DART hangsúlyozta, hogy a végpont-monitorozás nagyon fontos az olyan kifinomult, célzott támadások kivédése érdekében, amelyeket a hagyományos vírusirtó megoldások nem észlelnek.

Útmutató



Útmutató

A szervezeti védelem és a hatékony kockázatcsökkentés kiépítéséhez olyan biztonsági megközelítésre van szükség, amely magában foglalja a megelőzést, az észlelést és a kezelést. Ezekbe a kategóriákba soroltuk a következő bevált biztonsági gyakorlatokat.

MEGELŐZÉS:

A megelőző intézkedések kulcsfontosságú szerepet játszanak a teljes védelmi stratégián belül, mivel a megfelelő befektetéssel megnövelhetők és hosszabb távon is magasan tarthatók a kiberbűnözők támadási költségei (anélkül, hogy szakértő elemzőre lenne szükség az eredmények felügyeletéhez és értelmezéséhez). A megelőző beruházásoknál a legalacsonyabb költséggel járó módszereket érdemes megcélozni, hogy biztosan elhárítsuk az olcsó és hatékony támadási típusokat.

Négy dolgot érdemes megfontolni a megelőzéssel kapcsolatban:

1. **A biztonsági higiénia nagyon fontos. Ahogy a jelentésben szereplő incidensekből láthattuk, hétköznapi problémák is alááshatják a fejlett biztonsági funkciókat, ezek a tippek azonban segíthetnek csökkenteni a kockázatot:**

- Ne használjon ismeretlen ingyenes és/vagy kalózszoftvert. Csak megbízható forrásból származó szoftvert használjon.
- Csökkentse a hitelesítő adatok ellopásának kockázatát, például a rendszergazdai fiók biztonságának növelésével. Erről további információ ezen a blogon olvasható, amely felvázolja, milyen elvek mentén és milyen eszközöket használt a Microsoft a saját biztonságának kezeléséhez és növeléséhez, valamint azokat a távolabbi terveket, amelyek segítenek Önnek megtervezni a saját biztonságát.
- A szoftverszállító által biztosított biztonságos referenciakonfigurációt alkalmazza.
- Tartsa naprakészen számítógépeit, ne késlekedjen az operációs rendszerek és az alkalmazások legújabb frissítéseinek telepítésével, és azonnal telepítse a legfontosabb biztonsági frissítéseket az operációs rendszerhez, böngészőkhöz és e-mailekhez. Különítse el (vagy selejtezze le) azokat a gépeket, amelyeket nem lehet frissíteni vagy megjavítani.
- Alkalmazzon speciális e-mail- és böngészővédelmet. Telepítsen biztonságos e-mail-átjárót, amely speciális védelmet biztosít a modern adathalász fenyegetések ellen.
- Engedélyezze a kártevők elleni és hálózati védelmet a gazdagépeken, hogy közel valós idejű blokkolási válaszokat kaphasson a felhőből (ha elérhető a megoldásai között).

2. **Szabályozza a hozzáférést. Fontolja meg a következőket:**

- Legyen minél kisebb a „jogosultak” köre; használjon hálózatszegmentálást, a végfelhasználóknak ne legyenek helyi rendszergazdai jogosultságaik, és legyen körültekintő, amikor engedélyezi egy alkalmazásnak, hogy a számítógépen fusson.
- Kizárólag megbízható forrásból töltsön le alkalmazást (hivatalos alkalmazásáruházból).
- Vezessen be erős kódintegritási házirendeket, korlátozza a felhasználók által futtatható alkalmazásokat. Ha lehetősége van rá, alkalmazzon olyan biztonsági megoldást, amely korlátozza a rendszermagban (kernel) futtható kódot, és blokkolja az aláírás nélküli parancsfájlokat és a nem megbízható kódok egyéb formáit. Használjon alkalmazásengedélyezési listákat.
- Ha többet szeretne megtudni a szoftveres ellátási láncokat fenyegető támadásokról, és arról, hogy miként védekezhet ellenük, tekintse meg a Microsoft kutatóinak blogját.

3. **Legyenek biztonsági másolatai!**

- Készítsen ellenálló biztonsági másolatot a legfontosabb rendszerekről és adatokról.
- Használjon felhőtárhely-szolgáltatást az online adatok automatikus mentésére. A helyszíni adatok esetében a fontos adatokról rendszeresen készítsen biztonsági mentést a 3-2-1 szabály szerint. Legyen három biztonsági másolata az adatokról, két különböző tárolótípuson, amelyből legalább egy nem a helyszínen van.

4. **Figyeljen, és cselekedjen, ha valami gyanúsat észlel!**

- Tanítsa meg a munkatársaknak, hogy figyeljenek a gyanús üzenetekre, amelyekben bizalmas adatokat kérhetnek tőlük; tájékoztassa őket arról, mi a teendő, ha ez történik; és kérje meg őket, hogy azonnal jelentsék az incidenseket a szervezet biztonsági csapatának. A képzés segíthet elkerülni a pszichológiai manipulációt és a célzott adathalász támadásokat.
- Legyen óvatos, ha webes hivatkozásokra kattint. Ha biztonságosan böngészik, és olyan megoldásokat használ, amelyek figyelmeztetnek a nem biztonságos weboldalakról, vagy blokkolják azokat, lecsökkentheti annak valószínűségét, hogy kriptovaluta-bányászattal foglalkozó weboldalakra jut.
- Ha egy számítógép szokatlanul lassan fut, olyan gyanús fájlok után kutasson, amelyek éppen futnak, és küldjön egy mintát az operációs rendszer szállítójának. A Microsoftnak itt küldhet fájlokat kártevőelemzésre: https://www.microsoft.com/wdsi/filesubmission.

ÉSZLELÉS ÉS REAGÁLÁS:

Az észlelés és reagálás a támadó erőforrásokhoz való hozzáférésének idejét korlátozza, erősítve ezzel a hibatűrést. A támadói költségek növelésével lecsökkenti a támadói megtérülést (újra kell próbálkozniuk vagy módosítaniuk kell a műveleteiket), és csökkenti a nyereségüket (kisebb a valószínűsége, hogy elérik a céljukat).

Az a felhőtechnológia, amely lehetővé teszi a üzleti szervezetek számára, hogy jobban megfeleljenek a piaci igényeknek, a támadókkal is segít megküzdeni.

10. ÁBRA.

A SOC-ok fejlődési pályája

Ahogy a biztonsági központok (SOC) fejlődési pályájára tekintünk, látjuk, hogy a technológiának köszönhetően gyorsabban tudnak jobb döntéseket hozni és cselekedni. Sok ilyen innováció megfeleltethető a „Megfigyelés, tudatosítás, döntéshozatal, cselekvés" (Observe Orient Decide Act, OODA) ciklus egyes szakaszainak, ami az USA légierejénél szolgáló John Boyd ezredes nevéhez fűződik.[3]

MEGFIGYELÉS – A SOC-ok kihasználhatják a rendelkezésre álló (a Microsofttól és egyéb forrásokból származó) hatalmas mennyiségű biztonsági információt, ezzel drasztikusan megnövelve a látóteret a szervezeten belül és a külső környezetben.

TÁJÉKOZÓDÁS – Ahogy ezek az új adatforrások elérhetővé válnak az egyébként is túlterhelt SOC-ok számára, a gépi tanulás (a mesterséges intelligencia egyik része) fontos eszköze lesz a hatalmas adatkészletek elemzésének, és a kivizsgálandó rendellenességek azonosításának. A biztonsági termékek szállítói (például a Microsoft) gépi tanulási technológiát alkalmaztak, hogy gyorsan priorizálni tudják az eseményeket (és segítsék ezeket az egyes eseményeket egy holisztikus incidensként elhelyezni).

DÖNTÉSHOZATAL – Mivel a támadások mértéke és összetettsége gyorsan túlterhelheti a SOC-ot, az elemzőknek és az incidenskezelőknek gyorsan kell dönteniük és cselekedniük, hogy kezelni tudják a riasztásokat és az észleléseket. A Microsoft és más gyártók automatizált vizsgálati funkciókkal és útmutatással segítik az elemzőket a gyors és helyes döntéshozatalban (például az esetlegesen fertőzött vagy sérült eszközök elkülönítésében). Jelenleg az automatizálás feladata, hogy gyorsan megoldja az alacsony prioritással rendelkező incidenseket, hogy a szakértők összetettebb problémákkal tudjanak foglalkozni.

CSELEKVÉS – A reagáláshoz gyors és pontos, számos technológián és platformon átívelő végrehajtás szükséges – ez válik lehetővé a biztonsági vezényléssel és a válaszautomatizáló technológiákkal. A Microsoft és sokan mások kitartóan fejlesztik ezeket a technológiákat, többek között a modern fenyegetésészlelési és automatikus reagálási megoldásokat.

LÁBJEGYZET

[3] http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/

Egyéb, a modern biztonsági központokra vonatkozó trendek:

- **A riasztáscsatornáknál a minőség fontosabb a mennyiségnél** – Ahogy a szervezetek áttérnek a „nem elég információ” kezeléséről a „túl sok információ” kezelésére, a nagy szakértelemmel rendelkező SOC-elemzők ideje és figyelme egyre értékesebbé válik. Ezáltal egyre nagyobb szükség van a minőségi riasztásokra, amelyek 1. és 2. szintű elemzői közbenjárást igényelnek. Bár az újabb adatcsatornák mindig hasznosak a vizsgálódás és a proaktív „vadászat” szempontjából, a Microsoft központi IT-osztályának SOC-je az elemzői reagálást igénylő riasztási csatornák valós pozitív riasztásainak arányát méri (és jelenleg 90%-os vagy magasabb valós pozitív arányt ír elő).

- Fontos adatok – A nagy adatkészleteket (ideértve a biztonsági adatokat) nehéz elemezni anélkül, hogy hozzáférnénk a mögöttük lévő nyersadatokhoz is. Minél több biztonsági adat áll rendelkezésre, annál gazdaságosabb és célszerűbb a felhőben végezni a biztonsági elemzéseket ahelyett, hogy az adatokat helyszíni rendszerbe vinnénk át. Ez valószínűleg olyan SIEM- és SOC-architektúrák kialakulásához vezet, amelyek hibrid SIEM-módszereket vagy natív felhőalapú, szolgáltatásként kínált SIEM-megoldásokat foglalhatnak magukban.

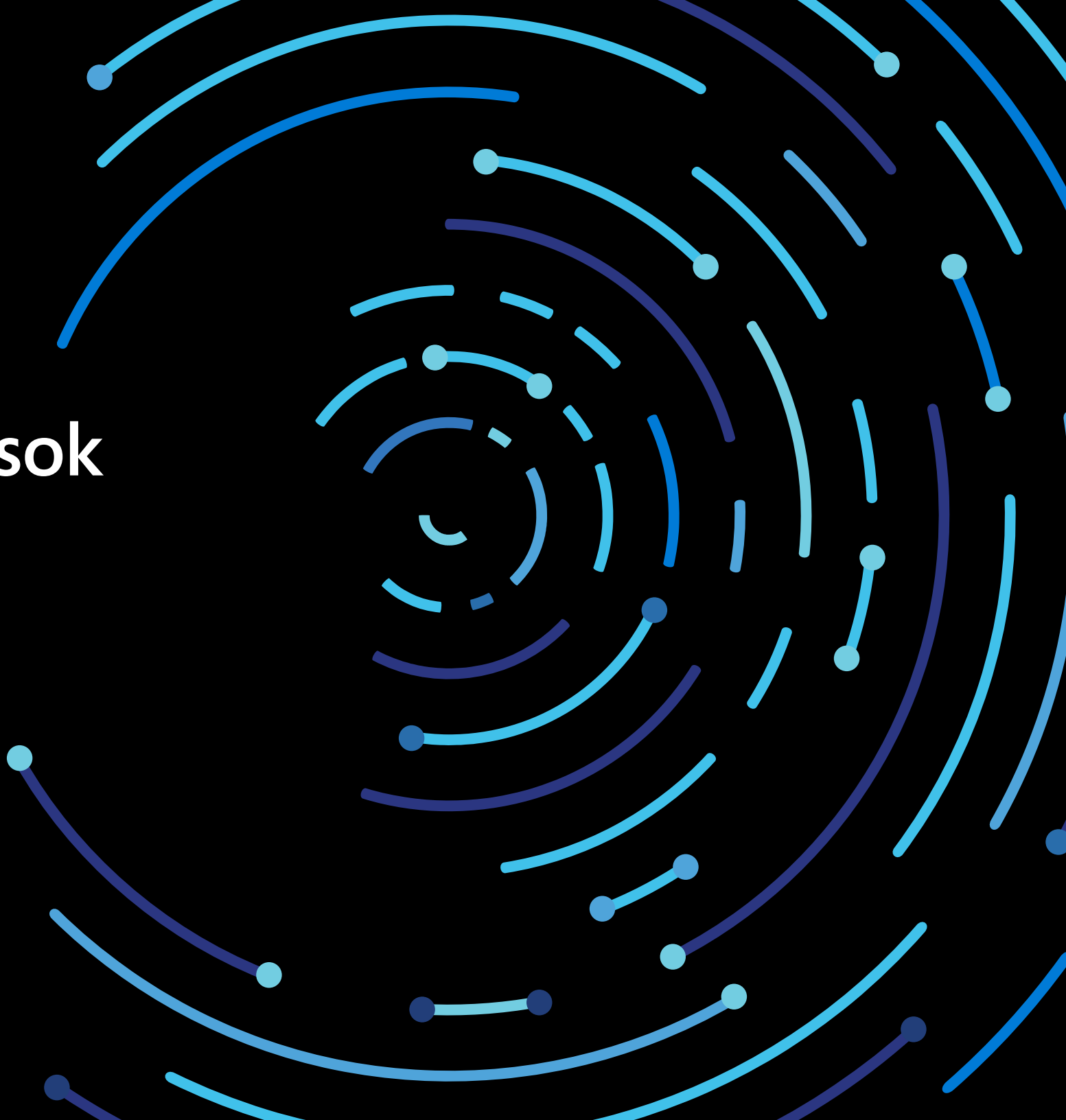
- **Tágabb kontextus** – Ezek az észleléstípusok sokkal hasznosabbak, mivel hatékonyabban tudják összefüggésbe hozni az adatkészleteket. Bár a hálózati forgalomra alapuló hagyományos észleléseknek továbbra is van némi biztonsági értéke, a nyers hálózati forgalom általában nem szolgál kellő kontextussal ahhoz, hogy megkülönböztessük a legitim és a rendellenes tevékenységeket. A SOC-oknak valószínűleg értékesebbek a kontextusgazdag észlelések, mint például:

  - **Végponti észlelési és reagálási (EDR)** megoldások, amelyek mélyreható kontextussal szolgálnak a gazdagép tevékenységéről
  - Identitásalapú észlelések, amelyek a felhasználó szokásos azonosítási mintáiról szolgálnak információval (helyszín, idő, használt szolgáltatások stb.), és viselkedés-elemzést alkalmaznak

Ezeket a kontextusban gazdag észleléseket nehezebb kikerülnie a támadóknak, mert sokkal összetettebb műveleteket kell utánozniuk (szemben az IP-forgalom néhány technikai jellemzőjével).

Az ügyfeleknél történt komoly támadások másik tanulsága az, hogy milyen nehéz gyorsan reagálni az incidensekre, ha az informatikai funkciók részben vagy teljes egészében kiszervezetten működnek. Javasoljuk, hogy tekintse át az IT-kiszervezési és a szolgáltatási szintre vonatkozó szerződéseket (SLA), valamint az ellátási lánc szállítóit, és győződjön meg arról, hogy lehetővé teszik-e a gyors biztonsági reagálást. Ha többet szeretne megtudni az ügyfelek incidenseinek kivizsgálásáról, tekintse meg az incidenskezelési referenciaútmutatót (Incident Response Reference Guide, IRRG): https://aka.ms/IRRG.

Adatforrások



Adatforrások

A Microsoft biztonsági információs jelentésben szereplő adatokat a Microsoft a termékekein és szolgáltatásain keresztül gyűjtötte be a Microsoft adatvédelmi nyilatkozatának megfelelően. Ezek az adatok értékes információkkal szolgálnak a termékek és szolgáltatások biztonságáról és működéséről, valamint betekintést nyújtanak a kiberbiztonsági fenyegetésekről általában. Az adatok az alábbi források elemzéseiből származnak:[4]

- **Az Azure Security Center** olyan szolgáltatás, amely a szervezetek számára a felhőalapú munkafolyamatok jobb láthatóságának megteremtésével teszi lehetővé a fenyegetések megelőzését, észlelését és kezelését, valamint fejlett elemzési funkciókkal és a veszélyforrásokkal kapcsolatos információk szolgáltatásával segíti elő a támadások észlelését.
- A **Bing** kereső- és döntéstámogató motor, amely minden évben weboldalak milliárdjainak átvizsgálásával keresi meg a rosszindulatú tartalmakat. A Bing ilyen tartalmak észlelése esetén figyelmeztetést jelenít meg a felhasználónak, hogy így segítse elő a fertőzések megakadályozását.
- Az **Exchange Online** a Microsoft által üzemeltetett levelező- és hatékonyságnövelő szolgáltatás. Az Exchange Online kártevőirtó és levélszemétszűrő szolgáltatásai évente üzenetek milliárdjait vizsgálják át a kéretlen tartalmak és a kártevők azonosítása és letiltása céljából.
- A **Kártevő-eltávolító eszköz** (MSRT) egy ingyenes eszköz, amelyet a Microsoft azzal a céllal készített, hogy könnyebben azonosíthatók és eltávolíthatók legyenek a konkrét elterjedt kártevőcsaládok az ügyfelek számítógépeiről. Az eszköz elsősorban fontos frissítésként jelenik meg a Windows Update, a Microsoft Update és az Automatikus frissítések szolgáltatásban. Az eszköz egyik verziója a Microsoft Letöltőközpontból is elérhető. Az MSRT nem helyettesíti a naprakész víruskereső megoldásokat.
- A **Microsoft Biztonsági ellenőrzőeszköz** egy ingyenesen letölthető biztonsági eszköz, amellyel igény szerint futtathatók vizsgálatok, és könnyebben eltávolíthatók a kártevők és más rosszindulatú szoftverek. A Microsoft Biztonsági ellenőrzőeszköz nem helyettesíti a naprakész víruskereső megoldásokat, mivel nem kínál valós idejű védelmet, és nem akadályozza meg a számítógépek megfertőződését.

LÁBJEGYZET

[4]Ezek az adatok mindig szigorú adatvédelmi és megfelelőségi ellenőrzéseken esnek át, mielőtt felhasználnák őket biztonsági célokra.

- **A Microsoft Security Essentials** ingyenes, könnyen letölthető és valós idejű védelmet biztosító termék, amely alapszintű, hatékony védelmet nyújt a vírusok és kémprogramok ellen Windows Vista és Windows 7 rendszeren.

- A **Microsoft System Center Endpoint Protection** (korábbi nevén Forefront Client Security és Forefront Endpoint Protection) egy összevont termék, amely a vállalati asztali gépek, laptopok és szerverek operációs rendszerei számára nyújt védelmet a kártevőkkel és a nemkívánatos szoftverekkel szemben. A Microsoft kártevőirtó motorját és a Microsoft vírusdefiníciós adatbázisát használja valós idejű, ütemezett és igény szerinti védelem nyújtására.

- Az **Office 365** a Microsoft Office előfizetéses szolgáltatása üzleti és otthoni felhasználók számára. A csomagok egy része az Office 365 Komplex veszélyforrások elleni védelmét is elérhetővé teszi.

- A **Windows biztonság** a Windows 10-ben a kártevők és a nem kívánt szoftverek valós idejű vizsgálatát és eltávolítását végzi. Ezenkívül a Windows legutóbbi verziója kihasználja a környezettel kapcsolatos részletes információkat, mint például a számítógép-konfiguráció, az eszközteljesítmény és -állapot, valtamint az egyéb hasonló jellegű információkat, amelyek az ügyfelek biztonságát növelik. Ugyanakkor segítünk az ügyfeleknek, hogy tájékozottabbak legyenek adataik védelmével kapcsolatban a Windows 10-ben. Olvassa el a blogot, ha további információkat szeretne találni ennek módjáról.

- A **Windows Defender Komplex veszélyforrások elleni védelem** a Windows 10 évfordulós frissítésébe és újabb verzióiba beépített új szolgáltatás, amellyel a vállalati ügyfelek észlelhetik, megvizsgálhatják és orvosolhatják hálózatukban a fejlett, tartós fenyegetéseket és az adatokkal való visszaéléseket.

- A **Windows Defender Offline** egy letölthető eszköz, amelynek segítségével olyan rendszerindító CD, DVD vagy USB flash meghajtó készíthető, amellyel kártevők és egyéb fenyegetések kereshetők a számítógépeken. Valós idejű védelmet nem kínál, és nem helyettesíti a naprakész kártevőirtó megoldásokat.

- A **Windows Defender SmartScreen** a Microsoft Edge és az Internet Explorer böngészők egyik funkciója; az adathalász és a kártevőket terjesztő webhelyekkel szemben nyújt védelmet a felhasználóknak. A Microsoft adatbázist vezet a Microsoft Edge, az Internet Explorer és a Microsoft más termékeinek és szolgáltatásainak felhasználói által jelentett adathalász és kártevőterjesztő webhelyekről. Amikor egy felhasználó a szűrő bekapcsolt állapotában megkísérli egy olyan webhely felkeresését, amelyik szerepel az adatbázisban, a böngésző figyelmeztetést jelenít meg, és leállítja az oldal megnyitását.