Szembesülés a modern alattomos támadással

Kiberbiztonsága fájl nélküli fenyegetések, célzott támadások és APT-k korában

kaspersky MŰKÖDÉSBE HOZZUK A JÖVŐT

Bevezetés

Visszapillantás: bűnözés a kiberbűnözés előtt

1963. augusztus 8. korai óráiban egy tolvajokból álló banda feltartotta a Royal Mail vonatot, és 120 zsáknyi bankjegyet lopott el – akkoriban ez körülbelül 7 millió dollárt jelentett (ami ma 50 millió dollárnak felel meg). Az egyesült királyságbeli rablás a világ minden táján megragadta az emberek képzeletét, és (anti) hősöket gyártottak a tolvajokból, valamint temérdek filmet, tv-műsort, könyvet, dalt és még videojátékot is készítettek ennek hatására (ideértve a **Runescape** egy küldetését is). A 15 férfi közül mindössze négyet tudtak elfogni, letartóztatni, majd elítélni.

A legendás „nagy vonatrablás”:
50 millió dollár (a mai pénzben kifejezve)

A NotPetya támadás (2017–):
10 milliárd dollár

A kiberbűnözés mellett eltörpülnek a régi bűnözési formák

2017. június 27-én a Kaspersky globális kutatási és elemzési csapatának (GReAT) kutatói bejelentettek egy zsarolóvírus-szerű törlőtámadást, amelyet **NotPetya** névvel láttak el, hogy megkülönböztessék azt a 2016. évi Petya-változatoktól. A támadás módosított EternalBlue biztonsági rést használt a vállalati hálózatokban való terjedéshez. A NotPetya támadásból eredő teljes kárt 10 milliárd dollárra becsülik, néhány áldozat több száz milliós kárral rendelkezik a térségben. A Merck 870 millió dollárt, a FedEx 400 millió dollárt, a Maersk pedig 300 millió dollárt veszített el. Azóta eddig csak egy letartóztatást hajtottak végre.

Kiberbűnözés: a tökéletes távoli rablás

A bűnözőknek nem kell többé feltartaniuk vonatokat: nagyon távoli és kényelmes ergonomikus irodai székeikből tervezhetik meg és hajthatják végre a pusztító (és nagyon jövedelmező) támadásokat.

Bármilyen kiberbűnözés természetes módon csökkenti a bűnözők által a helyszínen hátrahagyott lábnyomokat, és ami az ujjlenyomatokat illeti, a kiberbűnügyi szakértők csak álmodhatnak ilyen bizonyítékokról. Még magát a bűncselekmény helyszínét is nehéz lehet meghatározni, mivel a kibertámadások átívelnek a nemzeti határokon, és egyetlen pisszenés nélkül törik át a vállalati informatikai peremeket.

Eltűnő lábnyomok

A bűncselekmény evolúciója – kezdve a „nagy vonatrablástól" egészen a NotPetya támadásig – az eltűnő lábnyomokról, illetve a távolról végrehajtott rosszindulatú cselekményekről szól. Ennek a történetnek azonban még nincs vége. Néhány éven belül a NotPetya támadók által alkalmazott technikák ugyanúgy elavultnak tűnhetnek, mint a „nagy vonatrablók" által alkalmazottak.

Az új alattomos támadás

Ebben a dokumentumban megvizsgáljuk az „új alattomos támadás" néhány aspektusát – a kiberbűnözés technikái kifinomultságának szédítő eszkalációját, ami azzal fenyeget, hogy lehetővé teszi a bűnözők számára, hogy behatoljanak a hagyományos kiberbiztonsági megoldások páncélzatába, hogy aztán ott pusztító károkat okozzanak, miközben alig hagynak maguk mögött digitális lábnyomot. Felfedünk néhány olyan erőteljes (és egyértelmű) módszert is, amellyel hatékonyan megvédheti szervezetét a kiszámíthatatlan támadásokkal szemben, és ez nem kerül extra erőfeszítésekbe csapata számára – még a kiberbiztonsági tehetségekkel kapcsolatos válság idején sem.

A célzott támadások anatómiája

A célzott támadások az új alattomos támadási mód sólyomszemű gazemberei: kiválasztják az áldozatokat, és finomítják a nem megfelelően védett rendszerek (és a nem megfelelően tájékozott felhasználók) ellen irányuló fegyvereiket, hogy aztán térdre kényszerítsenek vállalkozásokat. A módszerek és jellemzők a következők:

- A kiberbűnözők a támadás megkezdése előtt megvizsgálják az áldozat végpontvédelmi rendszerét annak érdekében, hogy kialakítsanak egy mechanizmust, amely automatikusan megkerüli azt.
- „Nulladik napi" biztonsági rések és feltört fiókok: a nem megfelelően védett vállalkozások rajtakapása teljesen váratlanul.
- Testreszabott rosszindulatú szoftverek, amelyeket kifejezetten egy adott vállalkozásnak való károkozásra fejlesztettek ki.
- Megfertőzött objektumok, amelyek normálisnak tűnnek, és megkerülik a nem megfelelő végpontvédelmet, vagy a nem létező Endpoint Detection and Response (EDR) rendszert.
- Többvektoros támadások: a lehető legtöbb végpont megtámadása egyszerre.
- Rendkívül rosszindulatú **pszichológiai manipuláció** és támadások, amelyeket konkrét és személyes bennfentes adatok segítenek, és amelyek az idősebb személyzetre irányulhatnak.

Téves riasztások – elmerülés a (rosszul elhelyezett) figyelmeztető jelzésekben

A téves riasztás aránya 30% és 99% között mozog, és halálos kétélű kard. Az egyik él felől nézve a téves riasztások kimerültséget okoznak: az informatikai személyzet értékes órákat pazarol az egyes riasztások kivizsgálására, míg a valódi pozitív riasztások észrevétlenül maradhatnak a potenciálisan nem megfelelő kibervédelmi eszközök által. A másik él felől nézve pedig az informatikai személyzet által alkalmazott egyik leggyakoribb mód ennek a kimerültségnek enyhítésére és a téves riasztások áradatának megfékezésére az, hogy csökkentik a kiberbiztonsági megoldásaik érzékenységét, hogy kevesebb riasztás jelenjen meg. Mindkét esetben a téves riasztások pusztítóak lehetnek.

A jó hír az, hogy teljes mértékben eltüntetheti a téves riasztásokat, és így kizárólag a releváns fenyegetésekre tud összpontosítani. Amikor az **AV-Test** megvizsgálta a Kaspersky Endpoint Security for Business szolgáltatást (14 másik forgalmazó végpontvédelmi megoldásaival együtt), termékünk lenyűgöző eredményt ért el: nem volt téves riasztás vagy téves blokkolás.

Fájl nélküli fenyegetések

A kiberbűnözők egyre inkább a fájl nélküli támadások kezdeményezését részesítik előnyben, így kihívás elé állítják azokat a vállalkozásokat, amelyek mindig is kizárólag a hagyományos végpontvédelmi megoldásokra hagyatkoztak.

Másnap, miután közzétettük a NotPetya támadás híreit, tanácsot adtunk vállalkozásoknak világszerte arra vonatkozóan, hogyan kell biztonságban maradni. Nagyon világos utasításokat tudtunk adni arról, hogyan kell a perfc.dat nevű fájl futtatását letiltani a Kaspersky Endpoint Security for Business programcsomag Akalmazásfelügyelő funkciójának használatával. A fájl nélküli támadásokhoz nem adhatunk ilyen utasításokat: más megközelítésre van szükség, amelyet az alábbiakban ismertetünk.

A fájl nélküli támadások során alkalmazott technikák a következők (de nem korlátozódnak kizárólag ezekre):

- **A WMI-előfizetésekben tárolt rosszindulatú parancsfájlok**
- **A rosszindulatú parancsfájlok parancssori paraméterekként kerültek át közvetlenül a PowerShell-hez**
- **A rosszindulatú parancsfájlok a beállításjegyzékben és/vagy az operációs rendszer feladatkezelőjében vannak tárolva, és az operációs rendszer ütemezője hajtja végre őket**
- **A rendszer a rosszindulatú futtatható fájlt közvetlenül a memóriában bontja ki, majd a .Net-tükrözésen keresztül futtatja anélkül, hogy a lemezre mentené**

Lopakodó jellegük miatt a fájl nélküli támadások tízszer nagyobb valószínűséggel járnak sikerrel, mint a fájlalapú támadások. Az egyik legjelentősebb fájl nélküli támadás az Equifax amerikai fogyasztói hitelintézetnél történt jogsértés volt 2017-ben, ami 146,6 millió személyi nyilvántartás ellopását eredményezte.

Viselkedés – nem csak fájlok – elemzése a Kaspersky Endpoint Security for Business segítségével

Ha nincs észlelhető gyanús fájl, akkor az egyetlen módszer a gyanús viselkedés észlelése. Valójában egy teljesen reménytelen törekvés a fájl nélküli támadások megelőzése viselkedés-észlelési technológia nélkül.

A Kaspersky viselkedés-észlelési technológiája folyamatos, proaktív gépi tanulási folyamatokat futtat, amelyeket a Kaspersky Security Network adattudományon alapuló adatfeldolgozása és a globális, valós idejű statisztikák elemzése által összegyűjtött, fenyegetésekkel kapcsolatos bőséges információ támogat.

A biztonsági réseket megelőző technológiánk blokkolja a rosszindulatú programoknak a biztonsági rések kihasználására tett kísérleteit, az adaptív anomália-ellenőrzés pedig képesblokkolni azokat a folyamatműveleteket, amelyek nem felelnek meg a betanult mintának (például akadályozzák a PowerShell indulását).

A kiberbiztonsági tehetségválság

Az új alattomos támadás mellett az is veszélyes, hogy kiberbiztonsági tehetséghiány áll fenn. A kiberbűnözők bámulatosan képesek felvértezni magukat, miközben az őket elfogni képes kiberbiztonsági szakértők egyre ritkábbak a munkaerőpiacon (mind a toborzás, mind pedig a megtartás örökös kihívást jelent).

2019 elején a **Forbes magazin** beszámolt arról, hogy „a be nem töltött kiberbiztonsági pozíciók várhatóan 2022-re elérik az 1,8 milliót, ami 20%-os növekedést jelent a 2015-ös 1,5 millióhoz képest”. **A Security Magazine** bejelentése még ennél is drámaibb volt: „Háború zajlik a kiberbiztonsági tehetségek megszerzéséért.”

Tragikus módon túlságosan sok vállalat jutott arra a keserédes sorsra, hogy végül toboroznia kellett, majd be kellett tanítania egy házon belüli informatikai biztonsági szakértőt, aki aztán továbbállt, hogy – nagyobb fizetésért cserébe – máshol hasznosítsa a felbecsülhetetlen értékű szakértelmét.

A kiberbiztonsági tehetségválságtól eltekintve a teljes munkaidős belső kiberbiztonsági szakértelem meglehetősen drága lehet azon vállalatok számára, amelyeknek az informatikai csapatokra se jut elegendő pénz ahhoz, hogy boldoguljanak a folyamatos digitális átalakulás korában.

Amíg a kiberbiztonsági tehetségválság nem oldódik meg, a technológia az egyetlen módja annak, hogy a jövőbiztos kibervédelem szerte a világon elérhetővé tudjon válni a vállalatok számára, költségvetéseiken és képességeiken belül. Az emberi kompetencia továbbra is nélkülözhetetlen, de a megfelelő informatikai biztonsági technológia kritikus hidat jelenthet a nyomás alatt álló informatikai csapatok és az iparágvezető biztonsági elemzés között.

A nyomás alatt álló informatikai csapatokat és az iparágvezető biztonsági elemzést összekötő hídunk a Kaspersky Sandbox, amely automatikusan blokkolja a komplexebb fenyegetéseket a munkaállomás és a kiszolgáló szintjén. Amikor megalkottuk a Kaspersky Sandbox megoldást, az első számú célunk az volt, hogy enyhítsük az informatikai csapatokra nehezedő nyomást, hogy több idejük legyen a komplexebb – és szükséges – feladatok kezelésére.

A Kaspersky Sandbox éppen ezt teszi, mivel lehetővé teszi a kis szervezeteknek, hogy a modern fenyegetésekkel szembenézhessenek anélkül, hogy teljes munkaidős informatikai biztonsági szakembereket kellene alkalmazniuk, míg a nagyobb vállalatok jelentősen csökkenteni tudják az informatikai biztonsági szakértőkre való ráfordításaikat és a kapcsolódó költségeket azáltal, hogy automatizálják a speciális fenyegetésekkel kapcsolatos megelőzés feladatainak nagy részét, beleértve az osztályozást és az elemzést is.

A dinamikus fenyegetésemulációs (tesztkörnyezet) technológián alapuló Kaspersky Sandbox hasznosítja a komplexebb fenyegetések és az APT-szintű támadások leküzdéséhez alkalmazott legjobb szakértői gyakorlatokat, és szorosan integrálva van a Kaspersky Endpoint Security for Business megoldással. Így működik:

- A Kaspersky Endpoint Security for Business egy objektum ellenőrzésére irányuló kérést küld a Kaspersky Sandbox számára.
- A Kaspersky Sandbox ellenőrzést végez a vállalat igazi infrastruktúrájától elkülönített környezetben, és ezt az ellenőrzést olyan virtuális gépeken futtatja, amelyek a tipikus munkakörnyezetet emuláló eszközökkel vannak felszerelkezve.
- A Kaspersky Sandbox összegyűjti és elemzi az összetevőket, és viselkedési elemzést végez.
- Ha az objektum rosszindulatú tevékenységeket hajt végre, a Kaspersky Sandbox felismeri, hogy az rosszindulatú, és döntést hoz.
- A döntéstől függően a Kaspersky Endpoint Security for Business vagy automatikusan blokkolja a fájlt, vagy tisztaként jelöli meg.
- A rendszer az ítéletet valós időben elküldi az ítéleteket tartalmazó megosztott működési gyorsítótár számára, hogy a Kaspersky Endpoint Security for Business szolgáltatást használó más gazdagépek gyorsan megszerezzék az adatokat a beolvasott objektumról anélkül, hogy újra kellene elemezni a fájlt.

A Kaspersky Sandbox gyors, dinamikus és hatékony, valamint összetett informatikai biztonsági ismeretekkel segíti a vállalatokat mindenütt. A Kaspersky Endpoint Security for Business szolgáltatással való szoros integrációja azt jelenti, hogy a Kaspersky Sandbox nélkülözhetetlen akadályt biztosít a komplex modern fenyegetésekkel szemben, még azon vállalatok esetében is, amelyek még nem foglalkoztatnak házon belüli informatikai biztonsági szakértőket.

A rosszindulatú programok oldalsó mozgása a célzott támadási stratégiákban

Régen a rosszindulatú programok támadásai hasonlóan zajlottak, mint a „nagy vonatrablók” támadása: a kiberbűnözők behatoltak egy rendszerbe, elvették, amit akartak, és amilyen gyorsan csak tudtak, elmenekültek. Az új alattomos támadás korszakában a kiberbűnözők ambíciói a technikáikkal együtt jelentősen növekedtek.

A rosszindulatú programok oldalirányú mozgása miatt tekintendőek a perzisztens támadások célzott támadási stratégiáknak (APT). A ki- és becsapódás helyett a kiberbűnözők számos eszközt használnak fegyverként, hogy oldalirányban terjedhessenek egy rendszeren belül, hogy aztán eszközről eszközre mozogjanak. Az ilyen támadások folyamatos visszaélésekhez vezethetnek, és az áldozatnak látszólag végtelen rosszindulatú incidensekkel kell szembenéznie.

A rosszindulatú program oldalirányú mozgása egyre veszélyesebb. A **2019. évi éves APT-vizsgálatunkban** két olyan APT-re hívtuk fel a figyelmet, amelyek nemrégiben a rosszindulatú programok oldalirányú technikáit alkalmazták:

- Új tevékenység a BlueNoroff részéről, amely során a támadók oldalirányban mozogva nagy értékű gazdagépek eléréséhez nyilvános bejelentkezési hitelesítő adatokat és házi készítésű PowerShell parancsfájlokat használnak.
- Az Icefog fenyegető szereplő oldalirányú mozgása a betöltési sorrend eltérítésének nevezett technikával.

„A támadások növekvő bonyolultsága és gyakorisága növeli a támadások észlelésének és az incidensekre való reagálás szükségességét."

Gartner, Inc.

Az APT-k legyőzése a láthatóság, elemzés és a betekintés triumvirátusával

Az APT-k perzisztens elemeinek eltávolítása és a rosszindulatú programok oldalirányú mozgásának megállítása számos nagyon specifikus Endpoint Detection and Response (EDR) képességet igényel, amelyeket két kategóriába lehet sorolni – láthatóság és elemzés:

- **Láthatóság**
  - Az a képesség, hogy az összes végpontot egyszerre és valós időben lehet megjeleníteni és felügyelni egyetlen központi felületről.
  - Környezeti információk az egyedi végponti tevékenységekről, valamint a vállalaton belüli végpontok közötti folyamatokról, ütemtervekről és kölcsönös kapcsolatokról.
  - A felbecsülhetetlen értékű biztonsági információk összegyűjtése az informatikai biztonsági szakértők számára további vizsgálatok és válaszok céljából.

EDR nélkül a rendszerkép alaphelyzetbe állításával kapcsolatos költségek (az időben való hatékony visszatekintéshez) incidens esetén 400–600 dollár között mozognak.

— **Elemzés**
- **A különböző észlelési mechanizmusokból származó több döntés beépített leképezése vagy összekapcsolása egyetlen egységesített incidenssé, hogy érthetőek legyenek a fenyegetés fő taktikái, eljárásai és technikái.**
- **A rosszindulatú programok oldalirányú mozgásának retrospektív elemzése**
- **A „szürke zónában" zajló események elemzése, amelyek a megbízható/törvényes objektumok és folyamatok között helyezkednek el, és amelyek határozottan rosszindulatúak, ideértve főleg az alábbiakat:**
  - „Nulladik napi" biztonsági rések
  - Egyedi rosszindulatú szoftverek (máshol nem látható)
  - Új/ismeretlen rosszindulatú program
  - Kijátszott jogtiszta szoftverek/folyamatok

EDR nélkül a több száz különböző végpont és rendszer incidensekre való reagálásának bizonyítékai összegyűjtése és elemzése rendkívüli: a biztonsági szakértők akár 600 dollárt is elkérhetnek óránként.

„Használja a már meglévő EPP-forgalmazónál elérhető EDR-modulokat."

Gartner, Inc.: Végpontvédelem és a reagálás (Endpoint Detection and Response – EDR) architektúra és üzemeltetési gyakorlatok

Néhány szó a macOS kiberellenálló mítoszáról

A macOS eszközök itt külön említést érdemelnek a veszélyes mítosz miatt, amely szerint az operációs rendszereik valamiért eredendően ellenállnak a kibertámadásoknak. Az egyetlen ok, amiért a macOS rendszerű eszközök ritkábban esnek áldozatul a kibertámadásoknak az az, hogy kevesebb ilyen eszköz van, és a bűnözők rosszindulatukat a tömegre összpontosítják (általában Windows rendszerre). Az eredetileg – a központi rendszerekhez csökkentett hozzáféréssel és kevesebb jogosultságokkal rendelkező – tervezők és más alkotók számára fenntartott macOS eszközök egyre népszerűbbek, különösen a startup vállalkozások és más innovatív cégek körében, amelyeket az informatikai fogyasztás befolyásol (ez az a jelenség, amikor a fogyasztói informatikai viselkedés befolyásolja az üzleti döntéseket).

A kiberbűnözők egyre inkább a nem megfelelően védett macOS eszközök Achilles-sarkára koncentrálnak. 2019 első felében **közel 6 millió olyan adathalász támadást észleltünk,** amely a macOS felhasználók ellen irányult, és ennek 11,8%-a vállalati felhasználókat célzott meg. Találtunk két trójai családot is, amelyek a macOS felhasználókat célozták meg: Trojan.OSX.Spynion és Trojan-Downloader.OSX.Vidsler. Az előbbi tartalmaz egy kiskaput, amely lehetővé teszi a támadók számára, hogy távolról csatlakozzanak a felhasználó macOS eszközéhez, és több ingyenes macOS-alkalmazással együtt terjesztik, az utóbbit pedig a szalaghirdetések hivatkozásain keresztül juttatják el a felhasználó eszközébe.

Az eszközök kakofóniája: modern fenyegetések, vegyes környezet és BYOD

A tökéletes informatikai környezet kiépítése azt jelenti, hogy ki kell használni az eszközök, operációs rendszerek, hálózati protokollok és technológiák teljes skáláját. A Bring Your Own Device (BYOD, saját eszköz használata) népszerűsége nem mutatja a csökkenés jelét, így az informatikai környezet gyakran nem csupán vegyes, hanem kiszámíthatatlan is.

Egy tipikus informatikai beállítás magában foglal egy Windows és/vagy egy Linux operációs rendszert a háttérrendszerekhez; az alkalmazottak az irodában Windows vagy macOS rendszerű eszközöket használnak. A mobil telepítés egyre összetettebb, és gyakran tartalmaz dedikált táblagépeket vagy más eszközöket a célkitűzések szempontjából létfontosságú műveletekhez és szolgáltatásokhoz.

Az új alattomos támadás korszakában a vegyes környezet különösen vonzó vadászterületet jelent a kiberbűnözők számára. A különböző technológiák és eszközök nyomon követése óriási informatikai kihívást jelenthet, és a vállalat kiberpáncélzatában gyakran előfordulhatnak potenciális rések. A rendkívül összekapcsolt világban egy nem megfelelően védett végpont elegendő egy fenyegetés behatolásához, amely aztán – amint azt fentebb láthattuk –, oldalirányban mozoghat az áldozat IT-parkjában.

Nyilvánvaló, hogy a vállalatoknak intuitív, részletgazdag, bárhol elérhető megoldásra van szükségük az integrált kibervédelem kezeléséhez, de ez már nem lehet elegendő a vegyes környezet védelméhez. Az ÚJ Kaspersky Security Console Cloud

szolgáltatással egy lépéssel előrébb léptünk, és figyelembe véve ügyfeleink vegyes környezetének egyedi textúráját, ingyenes dedikált telepítést (és frissítést) nyújtunk.

Az ÚJ Kaspersky Security Console Cloud egy eszköz- és felhasználó-központú szolgáltatás, amely szerepkör alapú hozzáférés-vezérléssel (RBAC) és szerverhierarchia-támogatással rendelkezik. Megkönnyíti a Kaspersky biztonsági alkalmazások kezelését Windows, Linux és macOS környezetben, és hipervizor, valamint központosított automatikus felderítési és telepítési funkcióval rendelkezik annak biztosítása érdekében, hogy ne legyenek rések vagy hasonlók a kiberpáncélzatban. A helyszíni Kaspersky Security Console szolgáltatásból való áttelepítés egyszerűen megoldható egy áttelepítési varázsló segítségével, amely szakaszos és átállásos áttelepítési opciókat kínál (az utóbbit a beállítások exportálása révén).

A mennyiség és a költségek fejjel lefelé fordított jéghegye

Az egyszerűbb rosszindulatú programok kavalkádja nem mutatja a csökkenés jeleit; a kiberbűnözők továbbra is adathalász támadásokkal, vírusokkal, trójai programokkal, valamint alapvető kémprogramokkal és rosszindulatú programokkal bombázzák a vállalkozásokat szerte a világon. Valójában ezek a támadások még mindig az összes kibertámadás 90%-át teszik ki.

Az egyszerűbb rosszindulatú programokból álló egyre nagyobb kavalkád elfedi ezt a nagyon fontos, de gyakran elhanyagolt tényt: a támadások fennmaradó 10%-a, amely APT-kből áll, támadásonként csaknem százszor nagyobb költséget jelentenek, mint az egyszerűbb rosszindulatú programok által okozott támadások. Egy egyszerűbb rosszindulatú program által okozott átlagos költség 10 000 dollár, míg egy APT-incidens 926 000 dollár költséggel jár.

A helyzet egy fejjel lefelé fordított jéghegyhez hasonlítható: a 90%-a teljesen látható a víz felett, míg a halálos 10%-a a mélyben van, és nem látható. A jó hír az, hogy nem kell elhanyagolni a 90%-ot, hogy figyelmünket a halálos 10%-ra fordítsuk. Az **AV-Test** (2019 októberében) elvégzett tesztjén a Kaspersky Endpoint Protection for Business tökéletesen észlelte a fájl nélküli fenyegetések 100%-át, és 14 forgalmazó közül a legmagasabb prevenciós arányt (94,12%) biztosította.

A rejtett 10% elhanyagolása nem opció, és az APT-támadások utáni incidensre adott válasz és helyreállítás költségei nem csupán rombolóan hatnak pénzügyi szempontból, hanem a későn való cselekvés egyértelmű esetét is jelképezik.

A fenyegető jéghegynek két (jóllehet egyenlőtlen) részre bontása szintén szükségtelen. Valójában, amikor bármilyen vállalat napi biztonsági műveleteiről van szó, nem szükséges ketté választani ezeket. A fenyegetés mindkét kategóriája ugyanazt a végső célt tartja szem előtt; csak a technikák (illetve a költség és a kár szintjének) ördögiessége változik.

Ha egy vállalat nem gondoskodik a víz feletti 90%-ot kitevő egyszerűbb fenyegetésekkel szembeni megfelelő védelemről, azzal végül a vesztébe rohan. Még a legalapvetőbb támadások is kimerültséget okozhatnak, és úgy érezhetjük magunkat, mintha állóháborúban lennénk, különösen akkor, ha az informatikai költségvetés szűk, és a biztonsági szakértőket nehéz felvenni és megtartani. A Kaspersky Endpoint Security for Business megszünteti a sokféle fenyegetés elleni küzdelem terhét, így a vállalkozások szabadon összpontosíthatnak az APT-kre és más kiszámíthatatlanabb támadásokra. Eközben a Kaspersky Sandbox zökkenőmentesen együttműködik a Kaspersky Endpoint Security for Business szolgáltatással úgy, hogy automatikusan blokkolja a modern, lopakodó fenyegetéseket.

A vízfelszín alatt rejlő támadások 10%-ában elengedhetetlen az Endpoint Detection and Response (EDR) alkalmazása. Néhány vállalkozásnak nehéz elképzelni, hogy pontosan miért olyan fontos az EDR a mai fenyegetések környezetében. Ha azonban egy olyan vállalkozást kérdezünk meg, amely áldozatává vált APT-támadásnak, az EDR fontossága üzleti szempontból kristálytisztán látszik: támogassa vállalkozása kibervédelmét ma a biztonságos és jövedelmező holnap garantálása érdekében.

„Az integrált csomag lehetőséget ad arra, hogy megfelelően telepítse és működtesse az EDR-t, illetve hogy kihasználja a benne rejlő értéket.”

Kuppinger Cole

Szoros integráció = helytálló kibervédelem

Az egész jéghegy holisztikus kezelése egyszerű: a Kaspersky Endpoint Detection and Response és a Kaspersky Sandbox tökéletesen integrálódik a Kaspersky Endpoint Protection for Business szolgáltatásba, és mindent egyetlen központi felület – a Kaspersky Security Console Cloud – kezel, ahogyan annak lennie kell. Nem kell váltani a divergens rendszerek között, és nem kell megismerni új szoftverkezelési folyamatokat – ez az új lopakodó fenyegetések horizontját tekintve kimerítő lenne.

Az iparágunk és az ügyfelek által elismert kiberbiztonsági technológiák –amelyek középpontjában az EDR áll – lehetővé teszik, hogy villámsebességgel észlelje és megakadályozza a kiszámíthatatlan támadásokat, és ez nem kerül extra erőfeszítésekbe csapata számára.

Mivel a kiberbiztonsági tehetséghiány nem mutatja a csökkenés jeleit, szorosan integrált proaktív kibervédelmi rendszerünk megkönnyíti a borotvaéles elemzést. A végpont láthatósága és az automatizált osztályozás felszabadítja kapacitását, hogy csak a legfenyegetőbb célzott támadásokra kelljen összpontosítania figyelmét.

Díjnyertes végpontvédelem, automatizált Sandbox és egységesített felhőkonzol támogatja az EDR működését az Ön IT-parkjának agresszív megvédéséhez.

Minimalizálja a jövőbeli üzleti növekedés kockázatait ma!

Kiberfenyegetésekkel kapcsolatos hírek:
www.securelist.com
IT-biztonsági hírek:business.kaspersky.com

www.kaspersky.com

kaspersky MŰKÖDÉSBE HOZZUK A JÖVŐT