EGYÜTTES ERŐVEL

# Globális fenyegetettség ellen globális védelem

A kiberbűnözés nem ismer határokat, ezért csak úgy lehet hatékonyan felvenni ellene a harcot, ha a védekezés sem ismer határokat. A közös fenyegetettség elleni fellépésben az iparági és más szereplőknek félre kell tenniük a piaci és nemzeti rivalizálást, és meg kell osztaniuk egymással a tudásukat, mondja Tóth Árpád, a Kaspersky magyarországi igazgatója.

FORRÁS: KASPERSKY

TÓTH ÁRPÁD, KASPERSKY

**– Miért fontos a nemzetközi együttműködés a kiberbűnözés elleni harcban?**

– A kiberbűnözők nem állnak meg a határoknál, és az egyre kifinomultabb fenyegetések megjelenésével az ökoszisztémán belüli együttműködés és a szakértelem globális szintű megosztása minden eddiginél fontosabb az ellenük folytatott sikeres küzdelemhez. A Kasperskynél mi ezt pontosan tudjuk, ezért nyíltan megosztjuk szakértelmünket, tudásunkat és eredményeinket a világ biztonsági közösségével. Büszkék vagyunk arra, hogy a számítógépes bűnözés elleni küzdelemben világszerte együttműködünk a globális IT-biztonsági gyártókkal, nemzetközi szervezetekkel, mint például az INTERPOL-lal, az Orosz Föderáció Szövetségi Biztonsági Szolgálatával, az Orosz Föderáció Műszaki és Exportfelügyeletért Felelős Szövetségi Szolgálatával, a londoni

rendőrséggel, a holland rendőrség Nemzeti High Tech Crime Unitjával (NHT-CU), a Microsoft Digital Crimes Unitjával, más bűnüldöző szervekkel, valamint számítógépes vészhelyzeti reagáló csoportokkal (CERT-ekkel).

**– Milyen formákat ölthet ez az együttműködés?**

– Egyebek mellett technikai konzultációkat és rosszindulatú programok szakértői elemzését kínáljuk a kiberbűnözés kivizsgálásának támogatására. Elemezzük például a sérülékenységi vektorokat, a rosszindulatú programokat, az ellenőrző-irányító infrastruktúrákat és a kihasználás módszereit. A vizsgálatok során a támogatásunk a műszaki konzultációra és a rosszindulatú programok kutatására korlátozódik anélkül, hogy a felhasználói adatokat harmadik felek dolgoznák fel. A vállalat ezekben az esetekben ugyanazokat a módszereket és elveket alkalmazza a kivizsgálásra, mint a gazdasági előnyszerzésre irányuló rosszindulatú programok esetében.

A Kaspersky a kiberbiztonsági kezdeményezések és szabványok megvitatásában és fejlesztésében is részt vesz tanácsadói csoporttagságain keresztül, mint amilyen az Anti-Malware Testing Standards Organization. Mivel a modern világ kiberbiztonsági kihívásainak megoldására törekszünk, a Kaspersky olyan kezdeményezéseknek és szervezeteknek is tagja, mint például a Securing Smart Cities és az Industrial Internet Consortium.

## Hiszünk egy olyan jövőben, amelyben a technológia mindannyiunk életére pozitív hatással van

**– Csak a védekezésben vagy a megelőzésben is együtt tudnak működni a szereplők, például biztonságos szoftverfejlesztési irányelvek lefektetésével?**

– Természetesen a megelőzésben is részt veszünk, hiszen sokkal könnyebb elkerülni a fenyegetést, mint leküzdeni, ha már érintett a rendszer. Számos projekt célja kifejezetten a figyelem felhívása, illetve a felhasználók képzése, biztonságtudatosságuk növelése.

Tavaly elindított együttműködési programunk célja, hogy az intézmények jobban megértsék a legfrissebb és legelterjedtebb ipari kiberbiztonsági fenyegetéseket. A program keretében a kritériumoknak megfelelő oktatási intézmények, laboratóriumok, kutatási részlegek, biztonsági műveleti központok (SOC) és vészhelyzeti reagáló csoportok (CERT és CSIRT) a Kaspersky Industrial CyberSecurity megoldás használatával fejleszthetik kutatási módszereiket, illetve képezhetik kiberbiztonsági szakemberekeit.

**– Hogyan lehet ezekben az együttműködésekben feloldani a piaci szereplők közötti üzleti érdekellentéteket? Mindenki számára komoly értéket jelentenek a saját globális hálózatából származó sérülékenységi, támadási adatok – ezeket is megosztják?**

– Több mint két évtizede az a küldetésünk, hogy mindenki számára biztonságosabbá tegyük a világot. Hiszünk egy olyan jövőben, amelyben a technológia mindannyiunk életére pozitív hatással van. E célok elérése során nemigen látunk teret a partikularizmus vagy az ellentétes egyéni érdekek számára. Mindig örömmel osztjuk meg tudásunkat, tapasztalatainkat és meglátásainkat. Azt is elmondhatom, hogy a kiberbiztonsági szakértők és szakemberek nagy része ugyanígy gondolkozik.

Mint az egyik vezető kiberbiztonsági vállalat, mindig a tágabb perspektívát nézzük. Mindannyian egy ellen küzdünk - az egyre elterjedtebbé és kifinomultabbá váló számítógépes bűnözés ellen, amelynek célja a számítógépek károsítása, valamint a rendszerek normális működésének megzavarása, leggyakrabban nyereségvágyból, de előfordul, hogy politikai vagy személyes okok miatt.

**– Nem egy támadás gyaníthatóan (vagy biztosan) nemzetállami hátterű. Ezekkel mit tudnak kezdeni a piaci szereplők, meddig tudnak elmenni a feltárásban?**

– A Kaspersky alapelve a rosszindulatú programok minden formájának felderítése és semlegesítése, függetlenül azok eredetétől vagy céljától. Arra összpontosítunk, hogy mindenkit megvédjünk a kiberbiztonsági fenyegetésektől, és a bűncselekményt mindig bűncselekményként kezeljük. A GReAT csapatunk jelenleg több mint száz szereplő tevékenységét és kifinomult, rosszindulatú műveleteit követi nyomon, amelyek a világ több mint 80 országának kereskedelmi és kormányzati szervezeteit célozzák meg. Ezekről rendszeresen beszámolunk az APT logbookban, amely mindenki számára elérhető az interneten.

**– Tudna egy-két példát mondani a sikeres együttműködésre, amikor közös fellépéssel sikerült lefülelni csoportokat?**

– Az egyik legismertebb példa egyértelműen a Carbanak. Ez egy nagyon összetett kártevő, amely lehetővé teszi a bűnözők számára, hogy hozzáférjenek a vállalatok online banki rendszereihez. 2013 és 2014 során több mint 100 banki szervezetet érintett Oroszország, az USA, Németország, Kína és Ukrajna területén. Ezeknek a szervezeteknek legalább a fele szenvedett 2,5-10 millió dollár közötti pénzügyi veszteségeket. Amióta elkezdtük kivizsgálni ezeket a támadásokat, nagyon szorosan együtt dolgoztunk a bűnüldöző szervekkel a Carbanak csoport nyomon követésében. Az együttműködés eredményeként megismertük a támadások mértékét, és minden pénzügyi szervezetet sürgetni próbálunk, hogy gondosan vizsgálják át hálózatukat a Carbanak jelenlétének kiszűrésére.

A közelmúltból az A41APT kampány jó példa még arra, hogy a különböző kiberbiztonsági szolgáltatók közös erőfeszítéssel miként derítettek fényt egy komoly fenyegetésre. 2019-ben egy több iparágat, például a japán gyártóipart célzó APT támadási kampányt figyeltünk meg, amelynek célja információk ellopása volt. 2020 novemberében és decemberében a Symantec és a LAC tett közzé blogbejegyzéseket erről a kampányról, egy hónappal később pedig mi fedeztünk fel új tevékenységeket az A41APT-től.

Kiemelnék egy másik fontos példát is. Ez a „No More Ransom” weboldal, a holland NHT-CU, az Europol Európai Kiberbűnözési Központ, a Kaspersky és a McAfee közös kezdeményezése, amelylyel a zsarolóvírusok áldozatainak nyújtanak segítséget a titkosított fájljaik visszanyerésében anélkül, hogy fizetniük kellene a bűnözőknek. Jelenleg több mint 100 támogató partnere van a köz- és magánszférából, és az oldalt rendszeresen frissítik új leírásokkal, tanácsokkal és útmutatókkal, amelyek hasznos forrásai mindazoknak, akinek szüksége van rá. ■