**Új APT-csoportot fedeztek fel az ESET kutatói**

Afrikai és közel-keleti diplomatákat támad a BackdoorDiplomacy

Az **Advanced Persistent Threat (APT) olyan magas szintre fejlesztett és tartós kiberbiztonsági fenyegetettséget jelent, amely során szervezett bűnözői csopo**rtok indítanak támadást a kiszemelt célpontok ellen, amelyek jellemzően diplomáciai testületek.

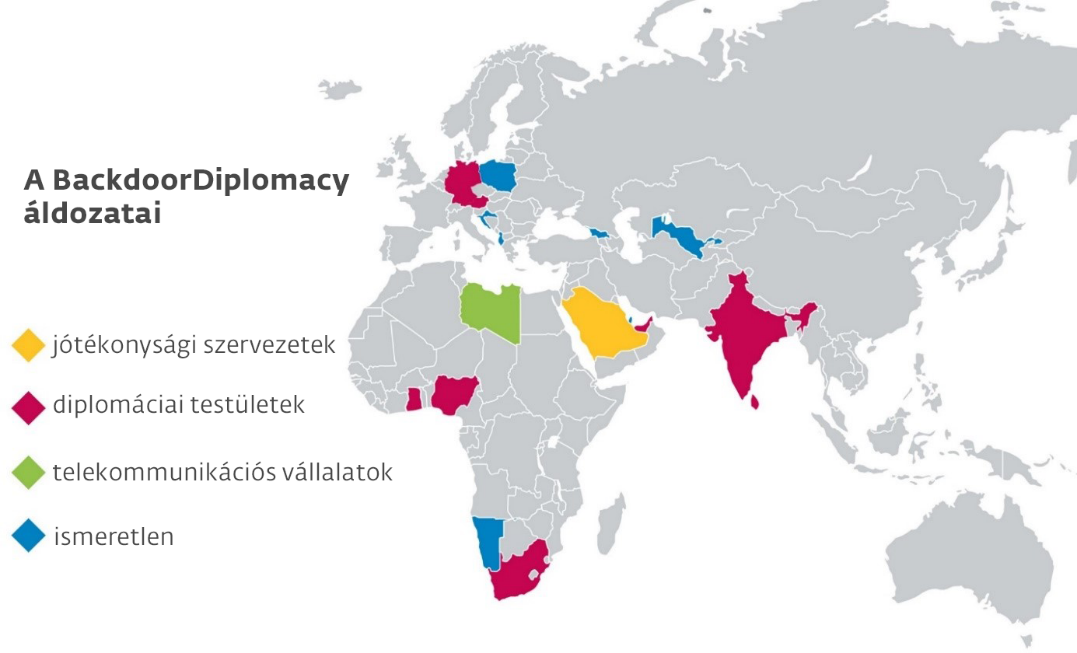
Sajtóközlemény – 2021.06.18./PResston PR

**Az ESET Research által felfedezett új APT-csoport, a BackdoorDiplomacy elsősorban közel-keleti és afrikai külügyminisztériumok hálózatába próbál bejutni, de az is előfordul, hogy telekommunikációs vállalatok kerülnek a támadások célkeresztjébe. A folyamat során a kiberbűnözők a szervereken futó programok sebezhetőségeit kutatják fel és használják ki annak érdekében, hogy hátsó ajtót telepíthessenek ezekre. Az újonnan beazonosított csoportról szóló kutatást az idei ESET World konferencián mutatták be először a kutatók.**

A BackdoorDiplomacy esetében a támadást az ESET által Turian névre keresztelt hátsó ajtón (backdoor) keresztül indították. A hátsó ajtó szoftver lehetővé teszi a hackerek számára, hogy a titkosítási módszereket megkerülve távolról belépjenek a rendszerbe, ahol titokban érzékeny adatokat, jelszavakat és más fontos bizalmas információkat gyűjthetnek és lophatnak el a felhasználóktól. A BackdoorDiplomacy képes felismerni a cserélhető adathordozókat, főleg az USB flash meghajtókat, melyek tartalmát a fő meghajtó lomtárába másolja át.

„*A BackdoorDiplomacy ugyanolyan taktikákat, technikákat és eljárásokat használ, mint más hasonló ázsiai székhelyű kémkedő csoportok. A Turian valószínűleg egy fejlettebb verziója a Quarian nevű hátsó ajtónak, mely utoljára 2013-ban mutatott aktivitást szír és amerikai diplomáciai célpontok ellen.*” – mondja Jean-Ian Boutin, az ESET fenyegetéskutatási vezetője.

A Turian hálózati titkosítási protokollja szinte teljesen megegyezik más ázsiai központú bűnszervezetek által használt, Calypso, illetve Whitebird nevű hátsó ajtó program titkosítási protokolljával. Érdekesség, hogy a Whitebird-öt a BackdoorDiplomacy-val egyidőben (2017-2020) alkalmazták diplomáciai szervezetek elleni támadások során Kazahsztánban és Kirgizisztánban egyaránt.



A BackdoorDiplomacy korábban több afrikai ország külügyminisztériumában, valamint Európában, a Közel-Keleten és Ázsiában is indított támadásokat. Továbbá célpont volt számos afrikai telekommunikációs társaság és legalább egy közel-keleti jótékonysági szervezet is. Az elkövetők minden esetben hasonló támadási taktikákat, technikákat és eljárásokat (TTP) használtak, de még a közeli földrajzi régiókban is rendszeresen módosították az alkalmazott eszközöket, ami nagyban megnehezítheti a csoport nyomon követését.

A bűnözői csoport Windows és Linux alapú szervereket egyaránt támad, leginkább olyan internetes portokon keresztül, ahol valószínűsíthetően gyenge a fájlfeltöltési biztonság, illetve javítatlan biztonsági rések találhatóak a rendszerben. Az áldozatok egy részét olyan adatgyűjtő fájlokon keresztül célozták meg, amelyeket cserélhető adathordozók (valószínűleg USB flash meghajtók) keresésére terveztek. A beépülő modul rendszeresen megvizsgálja az ilyen meghajtókat, és a cserélhető adathordozók behelyezésének észlelésekor megkísérli az összes rajta található fájl jelszóval védett archívumba való másolását. A BackdoorDiplomacy képes továbbá az áldozat rendszerinformációinak ellopására, titokban képernyőképek készítésére, illetve tetszőleges fájlok írására, áthelyezésére vagy törlésére is.

A BackdoorDiplomacy csoport kártékony tevékenységéről további részletek az ESET [„BackdoorDiplomacy: Upgrading from Quarian to Turian”](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) című angol nyelvű blogcikkében olvashatók bővebben.

**A Sicontact Kft.-ről röviden:**

A Sicontact Kft. hazánkban az egyik legjelentősebb **IT biztonsággal foglalkozó** cég, az ESET termékek kizárólagos magyarországi forgalmazója. Mottója és küldetése, ami köré termékportfolióját kialakította: „**biztonság a digitális világban**”.

A Sicontact Kft. Magyarországon az **ESET NOD32** technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő. A cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact Kft. több ízben elny erte a kitüntető **Business Superbrands** díjat. Az ESET Smart Security programcsomagot többször is **az év antivírus megoldásának** választották.

A független tesztelő szervezet több díjjal is elismerte az otthoni ESET termékeket a 2019-es eredményeket összefoglaló riportjában:

- Arany díjat nyert a fejlett, célzott és fájlnélküli kártevő támadások kivédésében, amely új kategóriaként jelent meg 2019-ben. Az ESET volt azon két gyártó egyike, akik mind a 15 célzott támadást sikeresen blokkolták a tesztelés során.

- 2018-ban ezüst, majd 2019-ben arany díjat szerzett a rendszer gyorsaságára és teljesítményére gyakorolt hatást vizsgáló kategóriában, az ESET szoftverek alacsony erőforrásigényének köszönhetően.

- Bronz díjat nyertek el a téves riasztások kategóriájában, amelyek ugyanúgy gondot okozhatnak, mint egy valós fertőzés, ezért az elkerülésük kulcsfontosságú a biztonsági szoftvereknél.

A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban, magyar nyelvű terméktámogatással kínálja. Az ESET már több mint 25 éve biztosít védelmet a digitális világ fenyegetéseivel szemben. Egy kicsi és dinamikus vállalatból mára egy több mint 100 millió felhasználót számláló és 202 országot és területet lefedő globális márkává nőtte ki magát.

Rengeteg minden változott, de az alapvető törekvéseik és a hozzáállásuk változatlan maradt, továbbra is céljuk egy biztonságosabb digitális világ felépítése, amelyben mindenki élvezheti a biztonságos technológia előnyeit.

**További információ és interjúegyeztetés:**

**Terdik Adrienne| Ügyvezető igazgató | PResston PR | Rózsadomb Center |   
1025 Budapest | Törökvész u. 87-91. | T + 36 1 325 94 88 | F +36 1 325 94 89 |   
M +36 30 257 60 08 |** [adrienne.terdik@presstonpr.hu](mailto:adrienne.terdik@presstonpr.hu) **|www.presstonpr.hu**

**Szekeres Nikoletta | PR vezető | PResston PR | Rózsadomb Center |  
1025 Budapest | Törökvész u. 87-91. | T + 36 1 325 94 88 | F +36 1 325 94 89 |   
M +36 30 831 64 56 |** [nikoletta.szekeres@presstonpr.hu](mailto:nikoletta.szekeres@presstonpr.hu) **|** [www.presstonpr.hu](http://www.presstonpr.hu)