biztributor

Trellix

A fenyegetettségi jelentés:

2022 nyara, és ami eddig történt

2022 első fele a kiberbiztonságban inkább az evolúcióról, mintsem a forradalomról szólt. A zsarolóvírus-támadások technikái és elterjedtsége tovább fejlődtek, míg az orosz kibertámadások lassú fejlődésnek indultak, amelyet az orosz-ukrán konfliktus eszkalálódása táplált.

A Trellix legújabb fenyegetettségi jelentése kitér 2022 első felére vonatkozó fontos kutatásokra és megállapításokra: többek között az orosz kiberbűnözés fejlődésére, a zsarolóvírus támadásokra, és e-mail biztonsági trendekre is. Mindezek mellett lehull a lepel a Trellix biztonsági kutató csoportjának legújabb kutatási eredményeiről is: példának okáért az épületek beléptető rendszereiben talált sebezhetőségekről, valamint az összekapcsolt egészségügyi ellátásban rejlő egyedi kockázatokról.

Az orosz kiberbűnözés fejlődése és az orosz-ukrán konfliktus

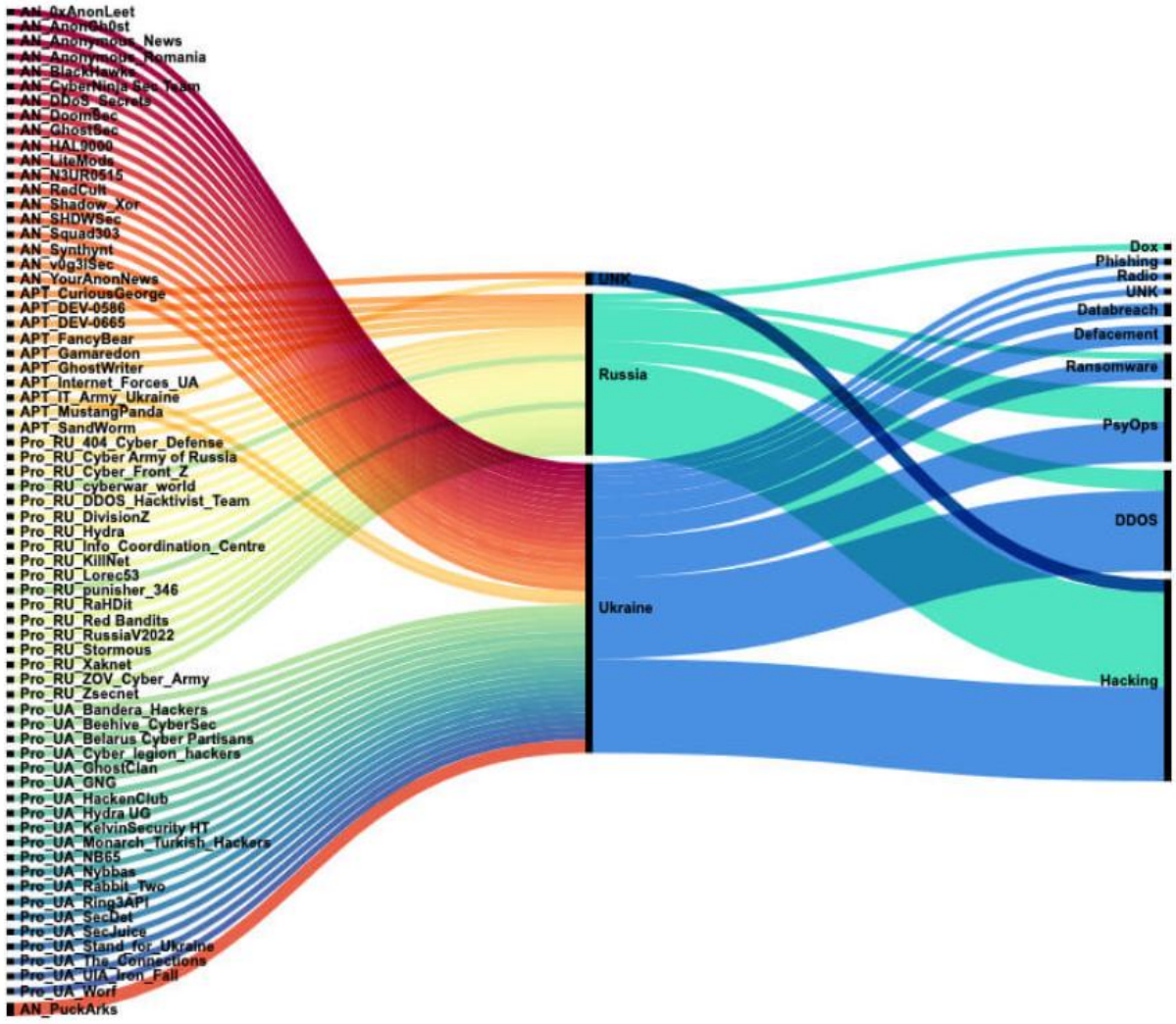
Az orosz kiberbűnözői csoportok - a közvélekedés szerint - mindig is aktívak voltak. Taktikáik, technikáik és eljárásaik (TTP-k) az idők során nem fejlődtek jelentősen, bár megfigyelhetőek bizonyos változások. Az utóbbi időben a fenyegetések színtere megváltozott, mivel több terület - részben - összeolvadt. Ez a tendencia már korábban is megfigyelhető volt, de a megnövekedett digitális aktivitás tovább gyorsította és feltárta az említett tendenciát.

A Trellix jelentős ügyfélkörrel rendelkezett Ukrajnában, és amikor az országot célzó kibertámadások felerősödtek, szorosan együttműködött kormányzati és ipari partnereivel, hogy nagyobb rálátást biztosítsanak a fejlődő fenyegetési környezetre. Lelkesen támogatták a régiót a rosszindulatú kibertevékenységek elleni védekezés során, és a tudásmegosztáson túlmenően a biztonsági eszközök széles skáláját is ingyenesen tudta biztosítani az érintett régióban.

Az RSA-val együttműködve a Trellix Threat Labs csapata közzétette az orosz kiberbűnözők időbeli fejlődéséről, egy (kiber)háború hatásáról, valamint a megfigyelt szervezettségről és tevékenységről szóló kutatását is. A Growling Bears Make Thunderous Noise c. publikációban – többek között – leírták, hogy azután, hogy 2022 januárjában számos ukrán kormányzati webhelyet - vélhetően az orosz államhoz köthető fenyegetettségi szereplők – elérhetetlenné tettek, a Trellix Threat Labs számos érintett felet látott a kibertérben, a civil csoportoktól kezdve, a félig a kormány által támogatott csoportokon át (mint az "ukrán kiberhadsereg"), egészen a kommunikációt és infrastruktúrát megzavaró nemzetállami csoportokig. Mindegyikük nyílt forráskódú ellenséges eszközöket használ támadásaik során, ami megnehezíti a támadások egy vagy több konkrét csoporthoz rendelését. Az alábbi képen a Trellix Threat Labs által az idők során megfigyelt különböző csoportok és a legelterjedtebb megfigyelt támadási módszerek láthatók.

A csoportok kategorizálva vannak:

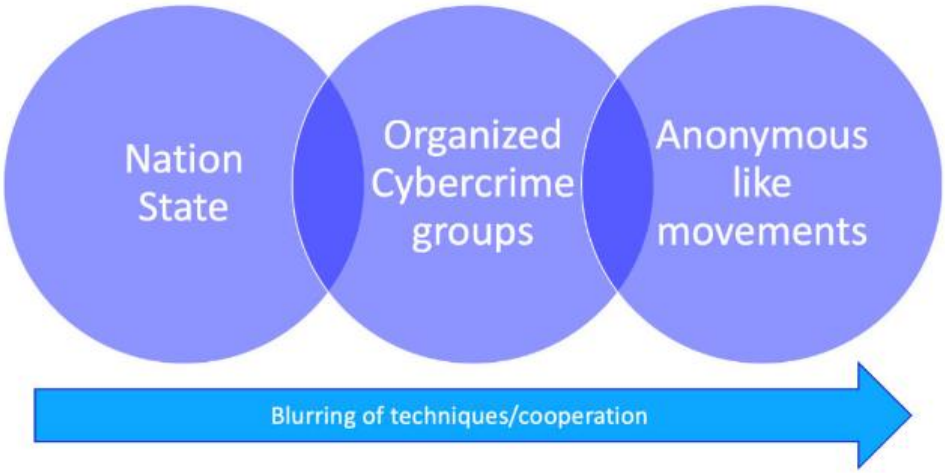
- "AN_" csoportok, az anonim mozgalomszerű csoportok;
- "Pro_" csoportok, amelyek a konfliktusban részt vevő országok valamelyike iránti hűségüket bizonyítva hajtanak végre támadásokat;
- és "APT_" csoportok, a nemzetállamok által támogatott csoportok.



A konfliktusban érintett csoportok és támadási módszereik

Amint azt sejteni lehetett: az ilyen csoportok által használt közösségi média platformokon folytatott tevékenységek nyomon követése kihívást jelent. A közzétett információkat mérlegelni kell: megbízhatóak-e, esetleg téves információk, vagy egyenesen propagandának szánták őket, manipuláltak-e képeket, videókat vagy adatokat stb.

Az ilyen jellegű és volumenű információs hadviselés miatt a különböző szereplők között hagyományosan fennálló határok elmosódnak. Ahogy a határok eltorzulnak, a hasonló eszközök, technikák és célpontok miatt egyre bonyolultabbá válik a különböző érintett szereplőkre vonatkozó behatolás gyémántmodelljének kitöltése.

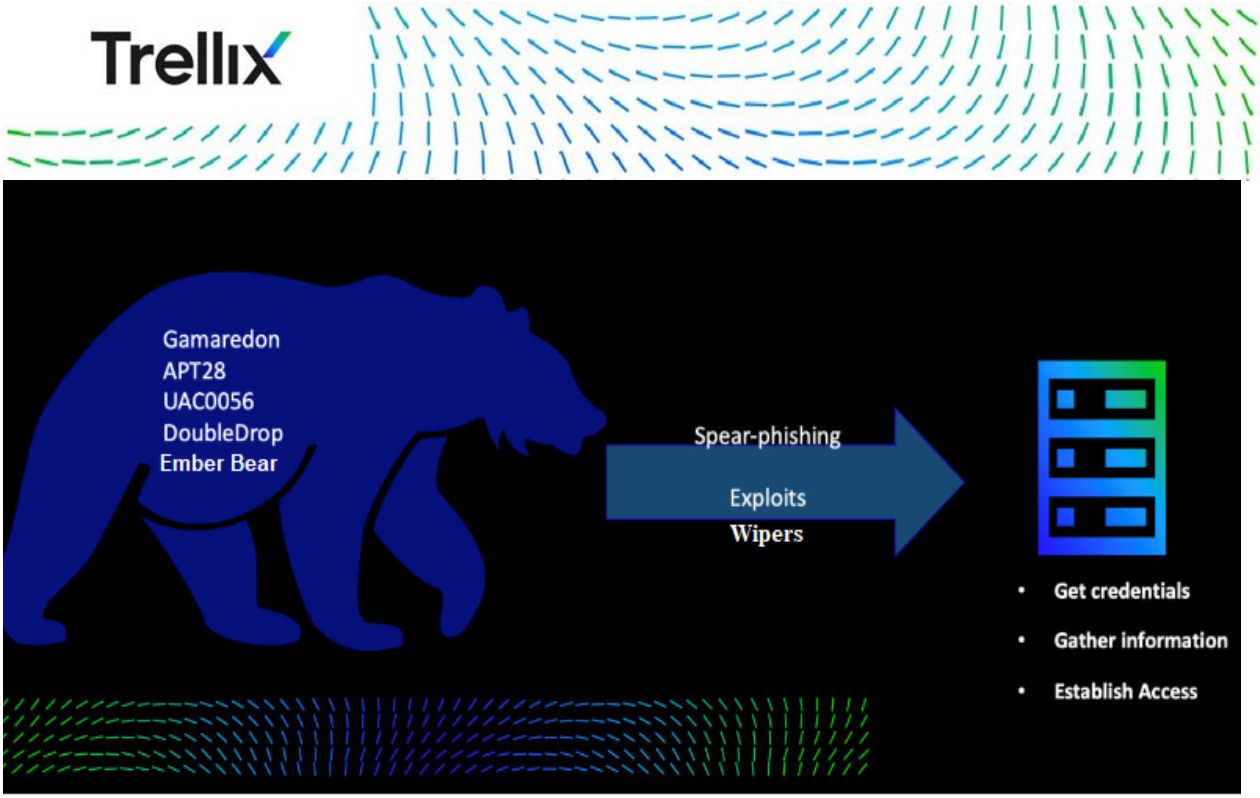


Elmosódó határok

Az egyik legfontosabb fejlemény, hogy a Conti zsarolóvírus csoport nyílt és egyértelmű állásfoglalása az orosz-ukrán konfliktus kapcsán elég sokba került a kollektívának. Miután lépten-nyomon hangoztatták oroszbarát álláspontjukat, nem csak az adataik szivárogtak ki, hanem komplett csevegéseik, üzenetváltásaik és levelezéseik is, amelyekkel kapcsolatosan – többek között – a Trellix is komplett tanulmányt készített a Conti működéséről. Ez óriási presztízs és hitelesség vesztés egy ilyen csoport számára, amely ezt követően gyakorlatilag fel is oszlott. Mindezek mellett a legértékesebb adat az általuk használt zsarolóvírus forráskódjának másolata volt. Ezt a forráskódot aztán egy NB65-nek nevezett ukránbarát csoport átvette és módosította, majd oroszországi célpontokat kezdett támadni. A kocka elvolt vetve, aztán megfordult.

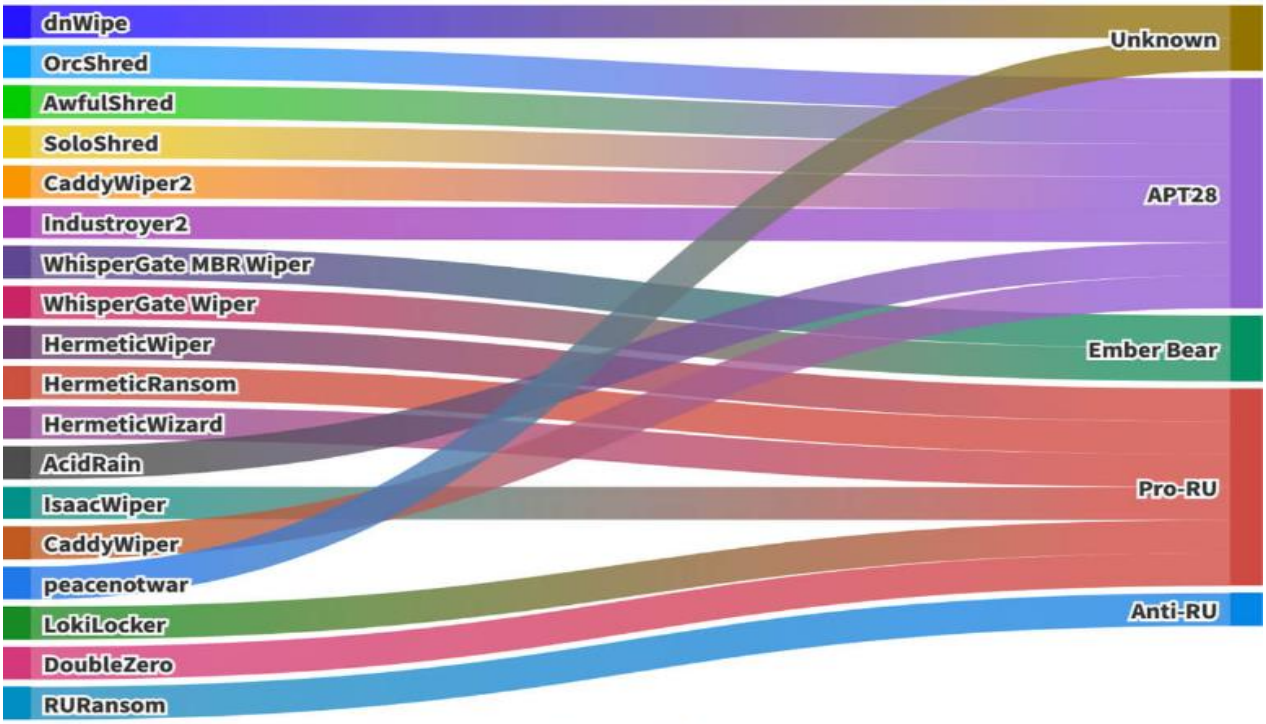
Az egész orosz-ukrán konfliktus során megállapítható, hogy számos összefüggés van a fizikai harctéren történtek és a kibertér eseményei között. Ahogyan a fizikai hadviselésben is számos katonai taktikát és eszközt használnak, a Trellix Threat Labs hasonló tevékenységet figyelt meg a kiberfronton is. Az elmúlt időszakban láthattunk: adattörlő káros kódokat, spear-phishing kampányokat, civileket célzó phishing kampányokat, back doorokat, sebezhetőségeket, DDoS támadásokat és számos más technikát is.

A következő ábrán az egyes fenyegetettségi szereplők konkrét támadási módszerei figyelhetők meg.



A megfigyelt csoportok által alkalmazott leggyakoribb támadási technikák

Mindezek közül mégis az ún. adattörlő (wiper) kártevőket kell kiemelni, hiszen az elmúlt hónapokban soha nem látott koncentráltságban jelentek meg a kibertérben. Az ilyen jellegű támadások azért különösen veszélyesek, mert a wiperek, ha bejutnak az adott hálózatra, képesek törölni az informatikai eszköz, rendszer tartalmát, és használhatatlanná tenni őket. A támadók bevett módszere, hogy ezeket az adattörlő kártevőket zsarolóvírusnak álcázzák, pedig a valódi céljuk nem a haszonszerzés, hanem a puszta rombolás és zavarkeltés.



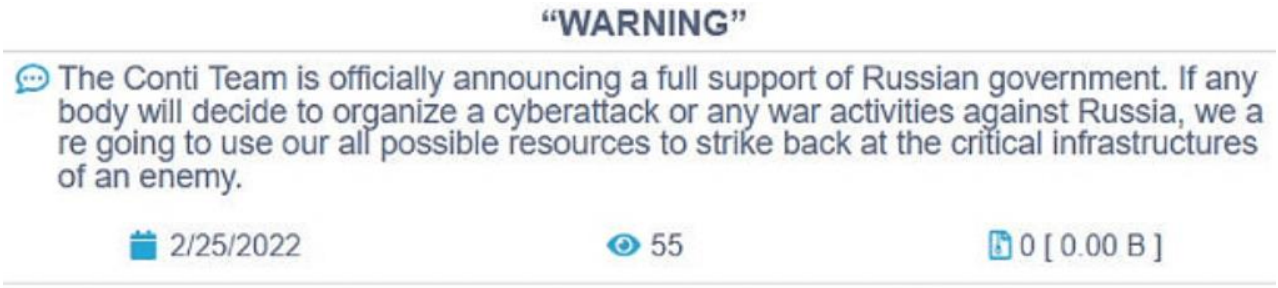
Wiperek és az azokat leggyakrabban használó csoportok

Zsarolóvírus trendek

2022 elején optimisták voltunk, amikor megjelent a hír, hogy az orosz FSZB letartóztatta a REvil zsarolóvírus-banda több tagját Oroszországban. A Trellix elemzései alapján a letartóztatott tagok kisebb szerepet játszottak a bűncsoporton belül, ennek ellenére bíztunk abban, hogy ez az akció további letartóztatásokhoz vezethet majd Oroszországban.

Ukrajna 2022. február végi orosz inváziójával ma már tudjuk, hogy ez csak vágyálom volt. A háború katalizátor lett a kiberbűnözők szétszakadásához. Korábban soha nem látott mértékben történt az meg, amire már volt korábban is példa, de ennyire egyértelműen nem: a kiberbűnözők félretették a politikai nézetüket, és láthattuk, hogy az orosz és az amerikai zsarolóvírus-kollektívák pénzügyi haszonszerzés céljából együttműködnek. A cél érdekében mindent.

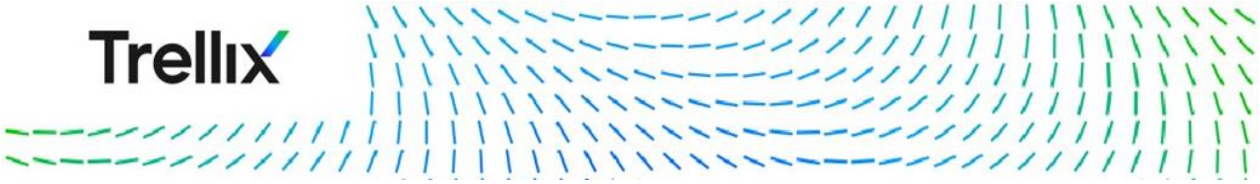
Mindezek mellett azt is láthattuk, ahogy korábban is írtuk, hogy egyes csoportok letették voksukat egyik vagy másik fél irányába. Az oldalválasztás a Conti zsarolóvírus esetében vált a legnyilvánvalóbbá, amikor nyilvánosan kifejezték támogatásukat az orosz kormányzat és annak akciói iránt.



A Conti ezzel az üzenettel fejezte ki az orosz kormány támogatását

A Trellix információi szerint a CONTI csapat legalább egy jó nagy része oroszországi székhelyű, és az onnan tevékenykedő bűnözők egy része már dokumentáltan is kapcsolatban áll az orosz hírszerző apparátussal, leginkább az FSZB-vel (Szövetségi Biztonsági Szolgálat). A Conti fenti kijelentésre egy ukrán biztonsági kutató, akihez a @contileaks nevű Twitter fiók is kapcsolódik, úgy döntött, hogy közzéteszi a Conti nevű kollektíva több éves belső Jabber beszélgetéseit az interneten. A konverzációk több évet ölelnek fel, és több ezer üzenetből állnak, így gyakorlatilag ez lett a zsarolóvírus kollektívák / zsarolóprogramok „Panama papírja"[1].

[1] Az úgynevezett Panama-akták vagy Panama-papírok az elnevezése annak a mintegy 11,5 millió kiszivárogtatott bizalmas dokumentumnak (összesen 2.6 terabájtnyi), melyet egy panamai ügyvédi iroda, az offshore cégek alapításával foglalkozó Mossack Fonseca (MF) szivárogtatott ki. Ezek a dokumentumok több mint 210 ezer, az MF közreműködésével alapított offshore cégről, illetve több száz érintett vállalatról (többek között bankokról és ügyvédi irodákról) és ismert emberekről (politikusokról, sportolókról, híresség ekről) tartalmaznak bizalmas adatokat.



A Trellix alaposan megvizsgálta a kiszivárgott csevegéseket, és egy nagyon terjedelmes blogot tett közzé, amelyet érdemes elolvasni. A csevegésekben találtunk olyan kiemelkedő pontokat, mint az orosz kormányzatot támogató nyilvános nyilatkozatuk, valamint a Conti vezetése és az orosz hírszerző szolgálatok közötti lehetséges szoros kapcsolat.

Ezek a kapcsolatok alátámasztják a “In the Crosshairs: Organizations and Nation-State Cyber Threats” című tanulmányt, amelyet korábban a CSIS-szel együttműködve tettünk közzé. A jelentés egyik legfontosabb megállapítása az volt, hogy az állami és nem állami szereplők közötti határvonal továbbra is elmosódik.

Kezdetben arra lehetett számítani, hogy ez a kommunikációs rés komoly hatással lesz a zsarolóvírus-banda működésére. Úgy tűnt azonban, hogy megduplázták a tempót, és folytatták a támadásaikat, olyannyira, hogy elérték, hogy egy ország, nevezetesen Costa Rica, szükségállapotot hirdessen az államot ért kibertámadások miatt.

2022. második negyedévének végén azonban megfigyelhettük, hogy a Contihoz kapcsolódó infrastruktúrát felszámolták. De ez sajnos még nem ad okot az ünneplésre. Tekintettel arra, hogy e bűnözői csoport egyetlen magas rangú tagját sem tartóztatták még le, és az orosz titkosszolgálatokkal való kapcsolataikra, figyelembe kell venni, hogy talán egy hibrid csoport kialakulásának lehetünk tanúi, amely képes a kormány által kiválasztott célpontokat megtámadni, de fenntartja egy bűnözői csoport hihető tagadhatóságát az anyagi haszonszerzés után. A zsarolóprogramnak kettős célja lehet, egyrészt zavaró jellegű, másrészt pedig figyelemelterelésként szolgálhat egy adatszivárgási művelethez.

Jöjjenek a konkrét adatok. 2022 első negyedévében a top 10 szektor közül az üzleti szolgáltatások tették ki az összes zsarolóvírus észlelés 64%-át. A nonprofit szervezetek a második helyen álltak a zsarolóvírus észlelések között. Az amerikai zsarolóvírus-kampányokban használt eszközökről az alábbiakat lehet elmondani:

- a Cobalt Strike volt nevű káros kódot az esetek 32%-ában használták;
- az RCLONE nevű káros kódot 12%-ban;
- a BloodHound és a Bazar Loader 10-10%-ban vetették be.

2022 első negyedévében a Lockbit volt a legelterjedtebb zsarolóprogram-család, amelyet az Egyesült Államokban a top 10 lekérdezések 26%-ában használtak, megelőzve a Conti (13%), a BlackCat (11%) és a Ryuk (10%) típusokat.

A legnépszerűbb zsarolóvírus-családok

Ha a szektorális előfordulást nézzük, akkor a telekommunikációs ágazat a második egymást követő negyedévben, az észlelések 53%-ával vezeti a globális ügyfélszektort ért zsarolóvírus támadások kategóriáját.

A globális ügyfélszektort ért zsarolóvírus támadások összesítése

Sérülékenységek

A kritikus infrastruktúra továbbra is az egyik legcsábítóbb célpontot jelenti a bűnözők számára világszerte. A kritikus infrastruktúrákat jellemzően – tisztelet a kivételnek - triviális hardver- és szoftverhibák, konfigurációs problémák és rendkívül lassú frissítési ciklusok jellemzik. Ez azért kulcsfontosságú, mert számos olyan rendszer sorolható ide, amire az élet mindennapjai során szüksége van az embereknek: az üzemanyag-csővezetékektől a vízkezelésig, az energiahálózatoktól az épületautomatizálásig, a védelmi rendszerektől az egészségügyi szektorig még sok minden mást is ide lehet hozni példának.

Az ipari vezérlőrendszerek egyik gyakran figyelmen kívül hagyott területe az épületautomatizálási keretrendszer részét képező beléptető rendszer. A beléptető rendszerek olyan általános, de facto megoldások, amelyek automatizálást és távmenedzsmentet biztosítanak a kártyaolvasók és a biztonságos helyekre való be- és kilépési pontok számára.

Az IBM 2021-ben készített tanulmánya szerint a fizikai biztonság sérülésének átlagos költsége 3,54 millió dollár, és átlagosan 223 napot vesz igénybe a sérülés felderítése.

A Trellix Labs nemrégiben mutatta be az egyik ilyen rendszerrel, a HID Mercury által készített mindenütt elérhető beléptetőpanellel kapcsolatos betöréskutatását. Számos OEM-gyártó támaszkodik a Mercury táblákra és firmware-re a beléptető megoldások megvalósításában. A Trellix négy nulladik napi sebezhetőséget és négy korábban befoltozott, de CVE-ként soha nem publikált sebezhetőséget emeltek ki, amelyek közül a két legfőbb távoli kódfuttatáshoz és tetszőleges újraindításhoz vezet. Ez azt jelenti, hogy a támadók egy épület hálózatán távolról zárhatják és nyithatják ki az ajtókat, és elkerülhetik az észlelést a kezelőszoftveren keresztül.

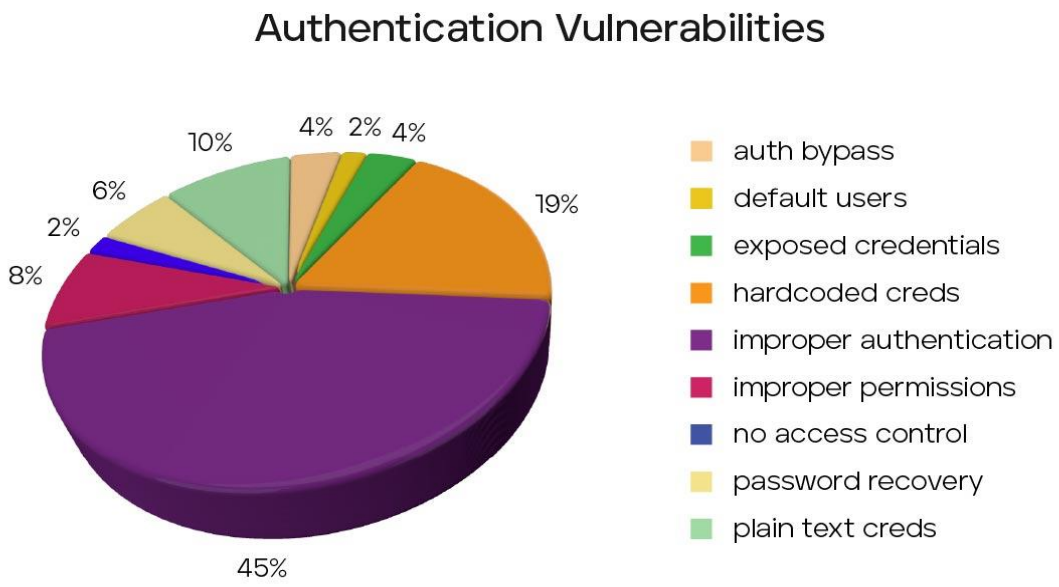
2022 első felében a Trellix kutatói az alábbi kritikus hibákat fedeztek fel épületek beléptető rendszereiben.

CVE	Detail Summary	Mercury Firmware Version	CVSS Score
CVE-2022-31479	Unauthenticated command injection	<=1.291	Base 9.0, Overall 8.1
CVE-2022-31480	Unauthenticated denial-of-service	<=1.291	Base 7.5, Overall 6.7
CVE-2022-31481	Unauthenticated remote code execution	<=1.291	Base 10.0, Overall 9.0
CVE-2022-31486	Authenticated command injection	<=1.291 (no patch)	Base 8.8, Overall 8.2
CVE-2022-31482	Unauthenticated denial-of-service	<=1.265	Base 7.5, Overall 6.7
CVE-2022-31483	Authenticated arbitrary file write	<=1.265	Base 9.1, Overall 8.2
CVE-2022-31484	Unauthenticated user modification	<=1.265	Base 7.5, Overall 6.7
CVE-2022-31485	Unauthenticated information spoofing	<=1.265	Base 5.3, Overall 4.8

Felfedezett sérülékenységek

Az egészségügyi ágazatot egyedülállóan nagy támadási kockázatnak teszi ki a számos célzottan használt eszköz, például altatógépek, infúziós pumpák, ellátórendszerek, MRI-készülékek és számos más eszköz. Ezen eszközök és szoftverek alapvető biztonsági gyakorlatokban, például a hitelesítő adatok kezelésében, elmaradnak, és tele vannak RCE sebezhetőségekkel. Ez csábító a kiberbűnözők számára, és résen kell lennünk a további támadások megelőzése érdekében, mivel ez nem lesz örökké figyelmen kívül hagyott támadási felület.

Az egészségügyi eszközök és szoftverek értékelésekor azt találta a Trellix, hogy a leggyakoribb hatás az iratokhoz és a felügyeleti szoftverekhez kapcsolódik. Ez a kategória a minták mintegy 17%-át teszi ki. Ez nem is olyan meglepő, mivel a szoftvereket jellemzően sokkal könnyebb megszerezni és tesztelni a biztonsági kutatóknak. Az intravénás pumpák szorosan követik a kezelőszoftvereket a minták 14%-ával, a betegmonitorok pedig a minták 7%-ával. Meg kell említeni az ultrahang készülékek, a lélegeztetőgépek, az MRIkészülékek, a defibrillátorok, a cukorbetegséggel foglalkozó gépek és az altatógépek sérülékenységeit is



Az eszközök sebezhetőségeinek megoszlása termékkategóriák és érintett szoftverek szerint

Mint minden biztonsági kockázatot, a sebezhetőségeket is súlyosságuk alapján kell rangsorolni. Sajnos az elemzett CVE-k jelentős százaléka súlyos. A mintában szereplő CVE-k alig 30%-a vezethet távoli kódvégrehajtáshoz (RCE), ami a támadók számára a koronaékszer, mivel a támadók kevés vagy semmilyen felhasználói beavatkozással megvethetik a lábukat a hálózaton. Ezeket minden szervezetnek kiemelt prioritásként kell nyomon követnie és javítania.

A problémák meglepően nagy százaléka a hitelesítési sebezhetőségeket érinti. Minderről az „Összekapcsolt egészségügy: a kiberbiztonsági csatatér, ahol nyernünk kell” címen már a biztributor is írt egy összefoglalót.

Nemzetállomokat értinő statisztikák és e-mail biztonsági trendek

A Trellix folyamatosan nyomon követi és monitorozza a nemzetállami kampányokat és a kapcsolódó mutatókat, technikákat. Kutatásuk a 2022. első negyedévének fenyegetettségi szereplőit, eszközeit, ügyfélországait, ügyfélszektorait és MITRE ATT&CK technikáit tükrözi. A legaktívabb APT csoportnak az APT36 nevű kollektíva tekinthető, amely a támadások 15%-ért felel.

Top 5 legaktívabb APT csoport

A 2022 első negyedévében az e-mailekhez köthető telemetria elemzések feltárták, hogy az adathalászat még mindig a legkedveltebb, és ezáltal a legveszélyesebb, támadási forma. Az elemzések során a Trellix számos adathalász URL-t és rosszindulatú dokumentumot fedezett fel és vizsgált meg.

Az észlelt rosszindulatú e-mailek többsége adathalász URL-t tartalmazott, amelyet vagy hitelesítő adatok ellopására, vagy rosszindulatú szoftverek letöltésére csábították az áldozatokat. A népszerűségi listán a következő helyen olyan e-maileket azonosítottak, amelyekhez rosszindulatú dokumentumokat, például Microsoft Office-fájlokat vagy PDF-eket csatoltak. Ezek a dokumentumok olyan makrókat tartalmaznak, amelyek letöltőprogramként vagy exploitként működnek.

Ha az áldozat telepíti, futtatja ezeket a saját eszközén, akkor a támadó átveszi az áldozat rendszere felett az irányítást. Végül pedig számos olyan e-mailt is detektáltak, amelyekhez rosszindulatú futtatható fájlokat, például információlopó vírusokat vagy trójaiakat csatoltak.

Ha a felhasznált exploitokra összpontosítunk, jól látható, hogy a legtöbbjük rosszindulatú RTF fájlokat, MS Office dokumentumokat fegyverként használt OLE objektumokkal, vagy Adobe Reader exploitokkal vagy rosszindulatú JS szkriptekkel fertőzött PDF-eket tartalmaz. A következő ábrán láthatjuk, hogy a három legnépszerűbb fájlformátum a windows rtf, ezt követi a legújabb office formátum, végül pedig az office formátum.

RTF	50.76%	Office	31.25%	OLE	17.99%
CVE-2017-11882	15.7%	CVE-2017-11882	23.84%	CVE-2017-11882	12.74%
CVE-2012-0158	12.84%	CVE-2017-0199	3.05%	CVE-0201-20158	4.16%
CVE-2017-0199	17.94%	CVE-2017-8570	1.7%		
CVE-2014-1761	5.8%				
CVE-2017-8759	4.41%				

A **biztributor** vezető IT-biztonsági, hálózati és üzemeltetés-támogató disztribútor cég. Az általa képviselt gyártók közé tartozik többek között az APT-támadások elleni védelem szakértője, a **Trellix**, a kiberhírszerzés etalonja, a **Mandiant**, a vezetékes és Wi-Fi hálózatokban jeleskedő **Ruckus**, a sokszoros végpontvédelmi tesztgyőztes **Bitdefender**, valamint a kis- és középvállalati biztonságban stabil pontnak tekintett **GFI.**