biztributor

Trellix

Összekapcsolt egészségügy:

a kiberbiztonsági csatatér, ahol nyernünk kell

Az egészségügyi szolgáltatóknak életek megmentése a feladata, alapesetben, még ha nem is mindig közvetlenül. Az iparági szereplők és munkavállalók gyakran rendkívül stresszes környezetben végzik az igencsak stresszes munkájukat, miközben a betegadatokat is védeniük kell. Az online térben is. Az egészségügyi szektorra kiemelt célpontként tekintenek a kiberbűnözők, így ezt a csatát mindenképpen meg kell nyerni.

Az elmúlt években – az egészségügyi adatok értékessége és az egészségügyi folyamatok sajátosságai miatt – az adatokkal történő visszaélés egyre nagyobb jelentőséggel rendelkezik. Az egészségügyi ágazatot egyedülálló támadásveszély fenyegeti a számos olyan célzottan használt eszköz miatt, mint például az altatógépek, az infúziós pumpák, a point of care rendszerek, az MRI-készülékek és számos más eszköz. Ezen eszközök közül sok más iparágban vagy éppen a hétköznapi háztartásokban nem található meg. Ezért talán az átlagnál kevesebbet foglalkoznak velük és a biztonságukkal, ami akár egyfajta hamis biztonságérzetet is eredményezhet.

Azegészségügyi rendszerekben tárolt adatok egy része ráadásul annyira egyedi és specifikus (gondolhatunk itt egyes genetikai vagy akár biometrikus adatokra stb.), hogy azok az átlagnál talán még szenzitívebb adatoknak tekinthetők, legalábbis az ilyen adatok védelmi kiemelt feladat kell, hogy legyen. Hiszen ezen információk megismerésével egy adott személy egyértelműen beazonosíthatóvá válik, illetve az adatok elemzésével prognosztikus, prediktív értékek és tulajdonságok (esetleg várható megbetegedések) is jósolhatók. Mindezek mellett az egészségügyi szektorra globálisan jellemző, hogy előszeretettel használnak kereskedelmi céllal létrejött levelezőrendszereket (például Gmail), ami tovább növeli a kitettség lehetőségét (nem beszélve arról, ha egy vonatkozó hatóság vagy hivatal is hasonló csatornákon kommunikál). A személyzet leterheltsége pedig a legtöbbször nem teszi lehetővé, hogy részletes IT biztonsági oktatáson essenek át a munkavállalók. Ennek hiányában, és mindezek mellett is, az e-mail egy olyan veszélyforrás lehet, melyet a kiberbűnözők előszeretettel használnak támadási vektorként. Vagy akár csak bejutási eszközként.

A kockázatokat minden esetben és minden intézményben szükséges (lenne) idejében felmérni. Példának okáért egy intézkedési terv mentén jól kidolgozott kiberbiztonsági kockázatkezelési jelentés sokat tud dobni a biztonságon. Ugyanakkor a releváns kockázatok mérséklésének elmulasztása súlyos következményekkel járhat az egészségügyi szolgáltatók és a betegek számára egyaránt. Nem csak a routerek és a számítógépek lehetnek a fenyegetettségi szereplők célkeresztjében, hiszen az olyan, látszólag hétköznapi eszközök is felhasználhatók rosszindulatú célokra, mint például a nyomtatók.

Az orvosi eszközök lehetővé tehetik a támadók számára, hogy megvethessék a lábukat egy kritikus hálózaton, vagy oldalirányban mozogjanak az infrastruktúrán, ami a betegadatok ellopását vagy megsemmisítését eredményezheti. Az egészségügyi ágazatnak nem csak a hétköznapi eszközökkel kell foglalkoznia, hanem minden olyan eszközzel is, amelyet telepítenek, rákapcsolnak a hálózatra, és amelyek – ebből fakadóan – súlyosabb biztonsági réseket is tartalmazhatnak. Az információbiztonsági fenyegetések nem korlátozódnak csak egy bizonyos típusú és méretű intézményre, hanem minden intézmény ki van téve ennek a fenyegetésnek. Az orvosi csoportoknak és egészségügyi dolgozóknak pedig minden szinten erőfeszítéseket kell tenniük a biztonsági intézkedések megerősítése, a korszerűsített IT-infrastruktúra fenntartása, valamint a biztonsági és „hackelési" eseményekből szerzett ismeretek megosztása érdekében.

A biztonságos eszközök, szoftverek kiválasztása és hadrendbe állítása nehéz feladat, amit a hackerek és az államilag támogatott fenyegetettségi szereplők újra és újra bebizonyítanak. Ezért a fenyegetés megelőzésben verhetetlen, vezető kiberbiztonsági cég, a Trellix nyilvános adatok, például a CVE-adatbázisok[1] felhasználásával és elemzésével megvizsgálta az egészségügyi szektor támadási felületének jelenlegi állapotát, és értékelte az aktív fenyegetéseket, valamint a felfedezett sebezhetőségek elterjedését. A Trellix úgy véli, hogy az orvosi eszközök gyártói, az egészségügyi intézmények és a biztonsági kutatók között a jövőben szorosabb együttműködésre és partnerségre van szükség.

A dark webtől a zsarolásig

Régebben a rosszindulatú szereplők orvosi adatokat gyűjtöttek, és ezeket az adatokat tömegesen értékesítették a dark weben. Ennek nagy részét valószínűleg csalárd célokra, például személyazonosság-lopásra és biztosítási csalásokra használták fel. Ezek az idők azonban elmúltak, vagyis inkább átalakultak a módszerek. Miután a Trellix alaposan körülnézett a dark netes piactereken, azt tapasztalta, hogy nagyon kevés eladható adatot lehet manapság felfedezni a különféle fórumokon és piactereken. Lehetséges, hogy egyes adatok egyszerűen más platformokra kerültek, de a zsarolóvírus-kampányok is nagy szerepet játszanak a jelenlegi helyzet kialakulásában. A kórházakra és más egészségügyi létesítményekre például keményen és gyakran csapnak le olyan zsarolóvíruscsoportok, mint a Conti. Az utóbbi években egyre gyakoribbak a zsarolások, amelyek a kiberbűnözők által fizetni nem hajlandó egészségügyi intézmények bizalmas adatainak kiadásával fenyegetnek.

[1] A sérülékenységek azonosítására és visszakereshetőségének biztosítására szolgáló világszerte használt Common Vulnerabilities and Exposures (CVE) nevű rendszer. Minden azonosított biztonsági hiba egyedi azonosítóval rendelkezik.

Sok országban jogszabályok vonatkoznak a személyes egészségügyi információk védelmére, és egy kiszivárgás következményei katasztrofálisak lehetnek, a bírságoktól a büntetőjogi felelősségre vonásig terjedő hatásokkal. Ezek a kiszivárogtatások drasztikusan megnövelték az ellopott orvosi adatok kínálatát, és szinte teljesen felszámolták a korábban jól ismert piacot. Adatlopás és adatértékesítés mindig is lesz, de a vevők közül sokan most már ingyen is hozzájuthatnak ezekhez az adatokhoz. Az orvosi ágazat szempontjából ma egyértelműen a zsarolóprogramok jelentik a legnagyobb veszélyt.

Éppen ezért kiemelten fontos, hogy az orvosi eszközöket nem csak behatolási kísérletek elleni védelemmel kell felvértezni, hanem mindent meg kell tenni annak érdekében, hogy az adott intézmény ne váljon zsarolóvírus támadás áldozatává.

A jelenlegi helyzet megértése

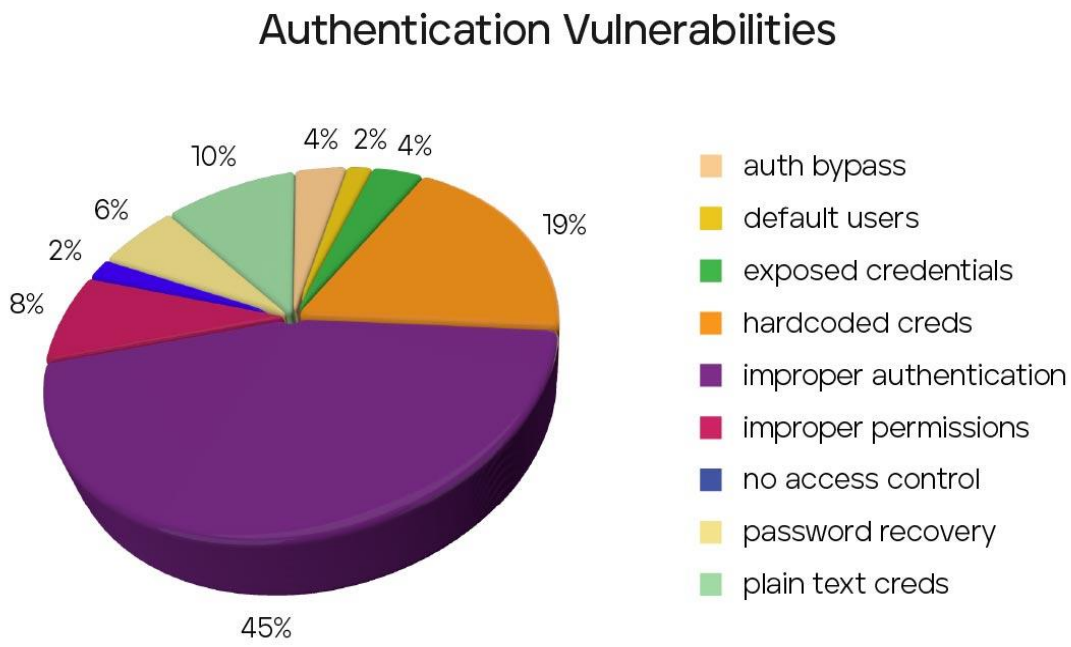
Ahhoz, hogy a Trellix felmérje a sebezhetőségek jelenlegi helyzetét az egészségügyi szektorban, megvizsgálta a 2019-2022 közötti időszakban globálisan bejelentett 270 sebezhetőséget, amelyek kifejezetten az orvosi eszközökre és szoftverekre vonatkoznak. A meglévő sebezhetőségek számbavételére három módszert alkalmaztak:

- Szabványos internetes keresőmotorok használata;
- Nemzeti sebezhetőségi adatbázisban (NVD) való kutatás;
- Ipari vezérlőrendszer (ICS) Medical Advisories információk a CISA-tól.

Az internetes keresőmotorok (például a Google) használata általában jó kiindulópont bármely projekthez. Ez az alapvető keresési módszer lehetővé tette a Trellix számára, hogy megtalálja az elérhető kutatásokat és jelentéseket. Ezen adatok összegyűjtése nagyszerű betekintést nyújt a kutatás jelenlegi állásába; ami azonban hiányzik belőle, az pl. a kevésbé ismert sebezhetőségek leírása. Ezeket sokkal nehezebb feltárni. Ebben segíthet azonban Nemzeti Sebezhetőségi Adatbázis (NVD). A CVE-hez rendelt összes nyilvános sebezhetőség megtalálható az NVD-ben. Az NVD segítségével részletes adatokat gyűjtöttek az egyes sebezhetőségekről és azok hatásáról. Ezen adatok kiegészítésére az ICS Medical Advisories-t használták. Az ICS Medical Advisories az ICS által az egészségügyi szektor számára kiemelten fontosnak ítélt esetekről tesznek közzé közleményeket. Az egyes tanácsok tartalmazhatnak az orvosi területre vonatkozó CVE-ket, cégneveket és terméknéveket. A terméknevek és a vállalatok leágazásával a Trellix tovább gazdagította az NVD-kereséseinket és a webes kereséseket, és kombinálta ezeket a módszereket.

Riasztó eredmények

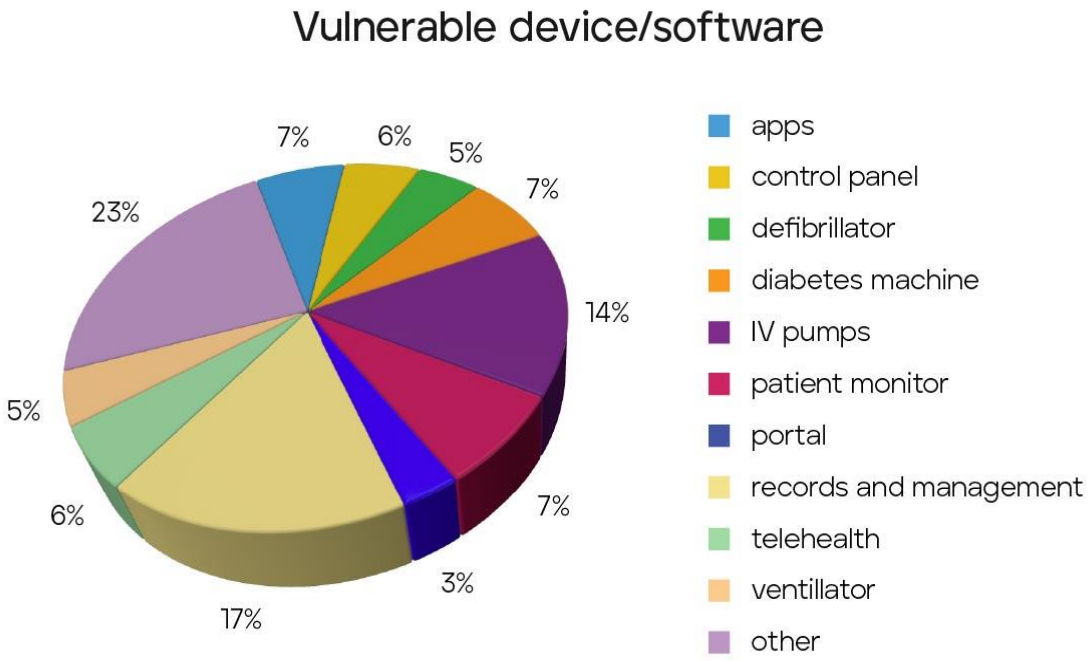
Az eszközök és szoftverek értékelésekor azt találta a Trellix, hogy a leggyakoribb hatás az iratokhoz és a felügyeleti szoftverekhez kapcsolódik. Ez a kategória a minták mintegy 17%-át teszi ki. Ez nem is olyan meglepő, mivel a szoftvereket jellemzően sokkal könnyebb megszerezni és tesztelni a biztonsági 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 MRI-készülékek, 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.

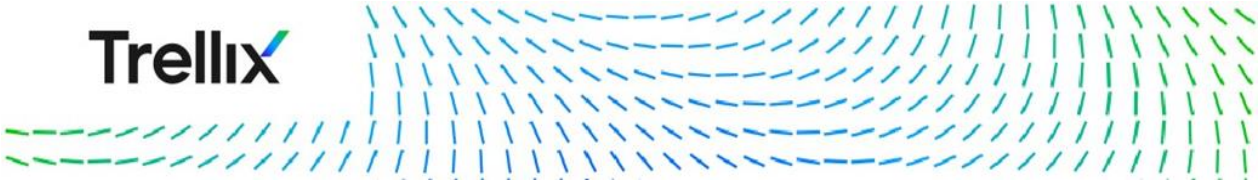
Ezek a hitelesítő adatok felfedésétől, a tiszta szöveges tárolástól vagy akár a hitelesítés teljes hiányától is terjedhetnek. A mintában szereplő CVE-k valamivel több mint 33%-a szenved ilyen típusú problémáktól. Tekintettel arra, hogy a hitelesítés a nem kívánt hozzáférés elleni védelem egyik első formája, ez riasztó, és mélyebb biztonsági problémára utal.



Hitelesítéssel kapcsolatos biztonsági rések terjesztése

Aktív kihasználás

Az orvosi vonatkozású CVE-k aktív kihasználása után kutatva a Trellix három aktívan kihasználható CVE-re bukkant, amelyek potenciálisan hatással lehetnek az orvosi eszközökre és szoftverekre: CVE-2017-1043, CVE-2019-0708, CVE-2020-1938. Ezek az exploitok nem specifikusan az orvosi eszközökre és szoftverekre vonatkoznak, de mégis hatással lehetnek rájuk. Ha a CVE-2019-0708 ismerősen hangzik, az azért van, mert ez egy széles körben elterjedt 9.8-as, BlueKeep nevű távoli kódfuttatási sebezhetőség az RDP-ben. Ugyanez a sebezhetőség a sebezhető kód használata miatt egy betegmegfigyelő vevőegységben is megtalálható. A másik két CVE abban hasonlít egymáshoz, hogy a sebezhetőségek nem specifikusan az orvosi területre vonatkoznak, de a beépítésük veszélyezteti azt.



A CVE-2020-1938 egy másik 9.8-as sebezhetőség, amely az Apache tomcat JServ protokolljára jellemző. Sajnos ezt számos orvosi képalkotó szoftvermegoldás használja. A CVE-2017-0143 egy 8.1-es SMB távoli kódfuttatási hiba, amelyet szintén egy IV Mixture megoldásban találtak. Fontos azonban, hogy a fentieket senki se tekintse mindent átfogó listának!

Egészségügyi kockázatok

A kibertámadások általános hatásain (egészségügyi ellátási vagy más, üzleti támogatófolyamatok megszakadása, bizonytalan időre történő felfüggesztése, a folyamatok helyreállítási szükségessége, reputációcsökkenés, közvetlen pénzügyi hatások) kívül vannak az egészségügyre jellemző speciális hatások is. A legfontosabb funkciózavarok között az alábbiakat lehet megemlíteni:

- sürgősségi szolgáltatást felfüggesztése;
- a betegek egészségügyi adatai elérhetetlenné válnak, vagy módosításra kerülnek;
- végleges adatvesztés;
- egyéb szolgáltatások felfüggesztése (pl. képalkotó eljárások szüneteltetése), beavatkozások elhalasztása;
- közvetett anyagi károk.

Felhívás cselekvésre

Az egészségügyi ágazatot már évek óta érik zsarolóvírus támadások. Ezek elég jelentősek ahhoz, hogy még az egészségügyi piacra és a vonatkozó értékesítési piacra is hatással legyenek. A trendetek elemezve nem látható az, hogy a közeljövőben ez a jelenség meg fog változni. Az orvosi eszközök és szoftverek hiányosságokat mutatnak az alapvető biztonsági gyakorlatokban, például a hitelesítő adatok kezelésében, és tele vannak RCE sebezhetőségekkel. Ez csábító lehet a kiberbűnözők számára, és óvatosnak, valamint figyelmesnek kell lenni a további támadások megelőzése érdekében. Minden érdekelt félnek el kell ismernie, hogy a hitelesítési sebezhetőségek nagy választéka azt jelzi, hogy az orvosi területen több belső és külső kutatásra van szükség ezen eszközök megvédése érdekében. Nem egyszerűen a kezelőrendszerekre és más webalapú alkalmazásokra kell összpontosítani, hanem minden hálózatra csatlakoztatott orvosi eszközhöz hozzá kell férni és meg kell vizsgálni.

Mindazonáltal fontos kiemelni, hogy jelenleg nem tűnik úgy, hogy ezeket az eszközöket rosszindulatú szereplők aktívan és rendszeresen kezdték volna célba venni, de ez nem jelenti azt, hogy megnyugodhatunk. Rengeteg RCE sebezhetőséget lehet találni, és nyilvános exploit kódot lehet újra felhasználni.

Amíg a támadók más módszerekkel támadják a kórházakat és klinikákat, addig talán időt nyerhetünk és felkészülhetünk a védekezésre, amellett, hogy felvesszük a kesztyűt a szektort érintő és veszélyeztető zsarolóvírusok ellen.

Az eredeti tanulmány itt érhető el.

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.**