ATTACK TRENDS AGAINST CRITICAL INFORMATION INFRASTRUCTURE SYSTEMS

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA RENDSZEREI ELLEN INTÉZETT TÁMADÁSI TRENDEK

DÉR AttilaTibor [1] BUSA Attila József[2]

Abstract

Based on the experience of the past few years, it is safe to say that attacks against critical infrastructures are an increasing percentage of the attackers' target. Attackers are increasingly focusing on developing and upgrading the toolkits used to prepare these attacks. Critical object defences need to be equipped with a similar intensity against external threats. As a consequence, one of the most important starting points is to provide critical infrastructure protection managers with an adequate picture of attack trends. This information can then be used to decide in which direction to organise and innovate individual defence systems and where to concentrate and divert resources. In this article, we briefly explain the background of cyber threats, some possible alternatives to supply chain attacks, and finally analyse the ENISA report and make suggestions for a more effective and modernised method of defence.

Keywords

Strategy, cybersecurity, Information security, legal regulation, critical infrastructure.

Absztrakt

Az elmúlt évek tapasztalatai alapján biztosan kimondható, hogy a támadók célkeresztjében egyre nagyobb százalékában vannak jelen a kritikus infrastruktúrák elleni támadások. A támadók egyre nagyobb figyelmet szentelnek, ezen támadások előkészítéséhez használt eszközparkok fejlesztésére és korszerűsítésére. A kritikus objektumok védelmeit is hasonló intenzitással kell felvértezni a külső fenyegetésekkel szemben. Ennek következtében az egyik leglényeges kiindulási pont, hogy a támadási trendekről megfelelő képet kapjanak a kritikus infrastruktúrák védelmi vezetői. Ezen információk alapján lehet, majd eldönteni melyik irányban kell szervezni, illetve fejleszteni az egyes védelmi rendszereket, hová kell csoportosítani, illetve elvonni erőforrásokat. Ebben a cikkben a röviden kifejtjük kiberfenyegetések hátterét, ellátási lánc ellen irányuló támadások néhány lehetséges alternatíváját. végül elemezzük az ENISA jelentését és javaslatot teszünk egy hatékonyabb és korszerűbb védekezési módszerekre.

Kulcsszavak

Stratégia, kiberbiztonság, információbiztonság, jogi szabályozás, kritikus infrastruktúra.

[1] der.attila@uni-obuda.hu | ORCID: 0009-0008-9547-102X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] busa.attila@phd.uni-obuda.hu | ORCID: 0009-0009-6167-2154 | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Napjainkban az információs rendszerek főként a kritikus infrastruktúrák védelme egyre jobban felértékelődik gazdasági és nemzetbiztonsági érdekek összefonódása következtében. Az egész világon fontos kiberbiztonsági stratégia a kritikus infrastruktúrák védelme és a már bekövetkezett támadások enyhítésének segítése. Erre a nemzetállamok külön figyelmet fordítanak jogszabályi szinteken és egyéb szabványosítások és iránymutatások terén. Európában a hálózati és információs rendszerek biztonsága NIS 2 (Network and Information Systems Directive) direktívában már jól tükröződnek ezek a törekvések, hogy egy egységes zászló alatt kell felvonultatni a kibervédelmet érintő főbb stratégiai kérdéseket, hogy majd később nemzetállamok szintjén ne legyenek nagy eltérések a különféle nézetek és elképzelések között. Több szervezetet is alapított erre az Unió, hogy a tagállamokat egy mederbe terelje és ez által egy egységes erős védelmet alakítson ki. Az egyik ilyen szervezet az Európai Unión belül az ENISA (European Network and Information Security Agency), amely az Unió egyik legfontosabb kiberbiztonsági szervezete. Tanácsadó szervezetként különféle ajánlásokkal, dokumentumokkal segíti a tagállamokat stratégiáik kialakításában.

KIBERTÁMADÁSOK ÁLTALÁNOSSÁGBAN

Ahhoz, hogy megértsük a kibertámadások trendjeit, fontos tisztázni néhány alapvető kibervédelmi fogalmi rendszert. A kiberfenyegetések hátterében rengeteg féle okot találhatunk a szakirodalomban. Az akarat lenne a legkézenfekvő közhelye ennek a gondolatkörnek, de nyilvánvaló nem elégséges feltétele egy támadás kivitelezéséhez. Így kell a szándékhoz megfelelő motiváció is, amely későbbiekben lesz kifejtve bővebben a tanulmányban, de annyit „elárulhatok", hogy nem mindegy, hogy megkora nyeresége, illetve haszna lesz ebből a támadónak, mint anyagi és mint szakmai téren. Tovább folytatva általánosságban a támadás feltételrendszerét, minél összetettebb egy kibertérben bekövetkezett behatolás, annál több szaktudásra és időre van szükség. A szaktudás külön nem ecsetelném, viszont az ehhez hozzácsapott évek alatt felhalmozott szakmaspecifikus gyakorlatot már igen, ahol az elkövetők akár tesztkörnyezetben vagy éles helyzetekben már bizonyították szakmai rátermettségüket. A szakmai fortélyok illetve trükkök elengedhetetlen feltételei, hogy valaki éles környezetben egy sikeres támadást hajtson végre egy kiszemelt létesítmény ellen. Meg kell még említeni az anyagi és a támadást segítő eszközök forrásait, amelyek nem az utolsó szempontok a fent nevesített szándék tettleges formába öntésére. Sőt az egyes szerzők által emlegetett különféle fenyegetési formákra is nagymértékben hatással vannak, mint kiberterrorizmus, kiberbűnözés, kiberkémkedés stb.

Ha a szaktudást és a mögötte megbúvó erőforrásokat vesszem alapul, akkor a következő képpen osztályozhatok: A legalsó kategóriába vannak, akiknek nincs képességük, hogy saját támadási eljárást dolgozzanak ki és csak kész termékből dolgoznak, nyomot hagynak és csak egyszerűbb sérülékenységeket használnak ki. Középen helyezkednek el az úgymond erős szaktudással, de kevés erőforrással rendelkező támadók, akik elsősorban becsvágyból illetve szakmai tudásukból fakadó kíváncsiságból elégítik ki ezen hajlamukat. A tevékenységük irányulhat a rendszerek hiányosságainak felderítésére, a hiányosság javításának kikényszerítésére, de irányulhat a támadott rendszer kompromittálására is. Egy adott célcsoportra kiélezett informatikai támadások, ahol inkább ideológiai háttér a legfőbb

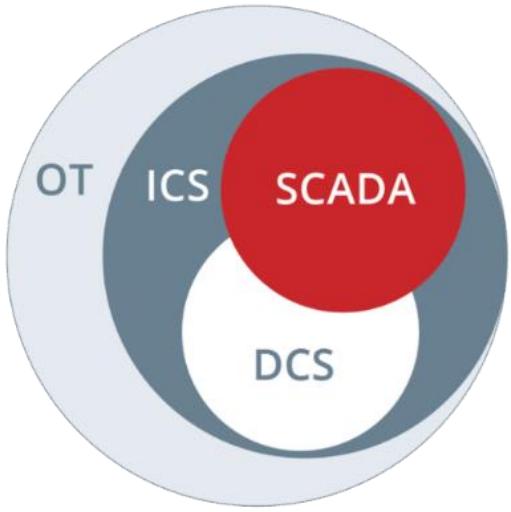
motiváció. A tagok szimpátia alapján alkotnak egy közösséget egy szervezet zászlója alatt, a legfőbb mozgatórugó nem a rombolás, hanem a figyelemfelhívás. A másik csoportosulás, ahol a tagok csak haszonszerzés reményében csatlakoznak egy bűnözői szervezethez. Itt van lehetőség drága eszközök használatára, káros programok elkészítésére, illetve megvételére. Így ezen a szinten már meg van a lehetősége az úgynevezett APT (Advanced Persistent Threat): jellegű támadási megoldásokra is. Az APT olyan informatikai adatszerzésre, illetve irányuló módszer, ahol távolról kiadott irányításnak megfelelően különféle kódok és parancsok folyamatosan és észrevétlenül fejtik ki hatásukat. Végül ennek a csoportosításnak a csúcsa, ahol az állam is valamilyen szinten közreműködik, illetve teljes mértékben szerepet vállal egy kibertámadási forgatókönyvben. Rengeteg anyagi és emberi erőforrás áll rendelkezésre, sok az ismert faktor főként saját ország határain belül.

Az elérni kívánt cél elérése szempontjából is megkülönbözhetünk támadásokat úgy, mint: Sérülés, szivárgás, megtagadás. Továbbá lehetséges még az információs rendszer működésének teljes vagy részleges működésének irányítása a fenyegető általi kompromittálása is.

Ezeknél a módszereknél jellemző veszélyeztetési formula, ahol az agresszor a rendszer vagy annak egyes elemeit a rendszer módosítása nélkül, külső úgynevezett szolgáltatásmegtagadással járó támadást (Denial of Service vagy DoS) vagy elosztott szolgáltatásmegtagadással járó támadást (Distributed Denial of Service vagy DDoS) hajt végre. Ezen támadások jellemzően rövid ideig tartanak, és intenzitásuk nagy mértékben függ a támadás végrehajtójától.[1]

OT SECURITY SZEREPE A KRITIKUS INFRASTRUKTÚRÁKNÁL

Az üzemeltetési technológia (OT) olyan hardver és szoftver, amely az ipari berendezések, eszközök, folyamatok és események közvetlen felügyelete és/vagy ellenőrzése révén változást észlel vagy okoz. Az OT-n belül megjelennek az ipari vezérlőrendszerek (ICS) és ezen belül a SCADA és DCS rendszerek (1. ábra: Az üzemeltetési technológiák felépítése1. ábra).



1. ábra: Az üzemeltetési technológiák felépítése

Az "OT security" az "Operational Technology security" rövidítése, és olyan intézkedéseket és technológiákat foglal magában, amelyeket az ipari technológiák védelmére terveztek. Az üzemeltetési technológia biztonság tehát a fizikai eszközök, folyamatok és események megfigyelésében és/vagy ellenőrzésében részt vevő személyek, eszközök és információk védelmére használt gyakorlatok és technológiák összessége. Ez a terület különösen fontos a kritikus infrastruktúrákban, ahol az ilyen típusú technológiák irányítják és felügyelik az energiahálózatokat, vízkezelő rendszereket, közlekedési rendszereket és egyéb kulcsfontosságú infrastruktúrákat.

Az OT security tehát azokat a védelmi intézkedéseket jelenti, amelyek a kritikus infrastruktúrákat üzemeltető rendszerek, eszközök és folyamatok biztonságát szolgálják. Ez magában foglalhatja a következőket:

Fizikai biztonság: Az OT rendszerek és eszközök fizikai hozzáférésének korlátozása és védelme.

Hálózatbiztonság: A hálózatok védelme, beleértve az adatforgalom titkosítását, tűzfalak alkalmazását és más hálózati biztonsági intézkedéseket.

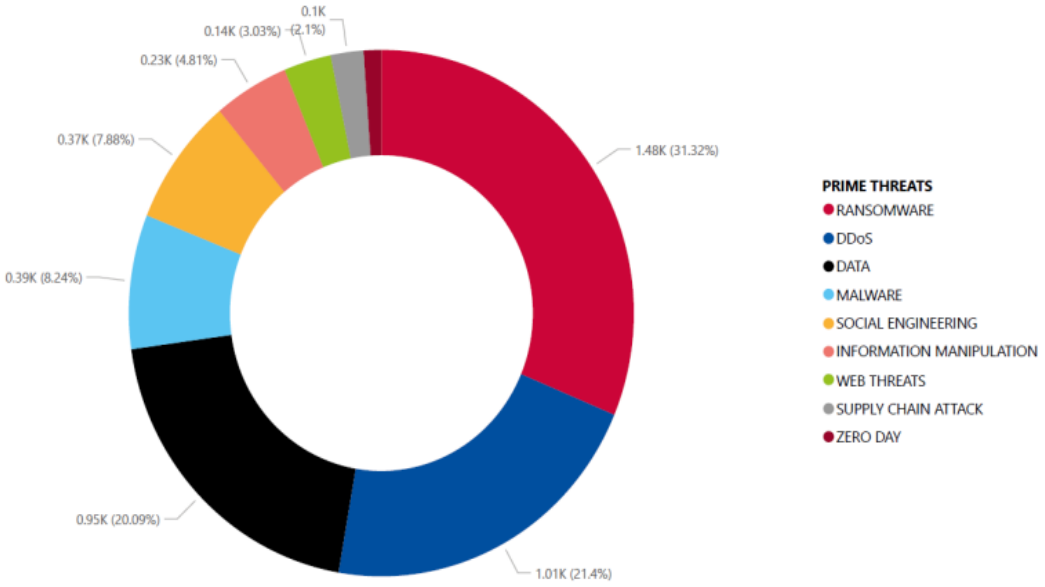
Rendszerbiztonság: A számítógépes rendszerek védelme, beleértve a frissítések rendszeres telepítését, a jogosultságkezelést és a sebezhetőségek elleni védelmi intézkedéseket.

Adatbiztonság: Az adatok védelme, különös tekintettel az érzékeny információkra, például az üzemeltetési adatokra és vezérlőrendszer-információkra.

Incidenskezelés: Az esetleges biztonsági incidensek és támadások kezelése, beleértve az azonnali választ és a rendszer helyreállítását.

A kritikus infrastruktúrák terén az OT security kiemelten fontos, mivel az ilyen típusú rendszerek sérülése vagy megbénulása jelentős károkat okozhat az egész társadalomban. Az energiaellátás, vízellátás, közlekedés és más kritikus szolgáltatások fenntartása érdekében elengedhetetlen a megfelelő OT security intézkedések alkalmazása.

Az OT rendszerek sérülékenysége igen magasnak mondható, hiszen egy gyártósort csupán 10-20 évente cserélnek le és a működtető szoftverek, operációs rendszerek is rengeteg sérülékenységet hordoznak magukban életkoruknál fogva.[4] Így a fent kifejtett okok miatt a kritikus infrastruktúrák és az OT rendszerek kiemelkedő célpontnak számítanak a kibertámadások terén.



2. ábra: 2022 június és 2023 július között véghez vitt kibertámadások csoportosítása a kritikus infrastruktúrák ellen [4]

ELLÁTÁSI LÁNC ELLEN IRÁNYULÓ TÁMADÁSOK

Az ellátási lánc közvetlenül nem jelenik meg a kritikus infrastruktúrák felsorolásánál, ha szigorúan értelmezzük a 2012. évi CLXVI. törvényt. Azonban mindenhol megjelenhet, mint kritikus infrastruktúrát kiszolgáló rendszerelem, hiszen a rendelkezésre állás kiemelkedően fontos ezeknél a szervezeteknél, mivel számos gazdasági, társadalmi és egyéb terület működését meghatározó elemeket foglal magában.

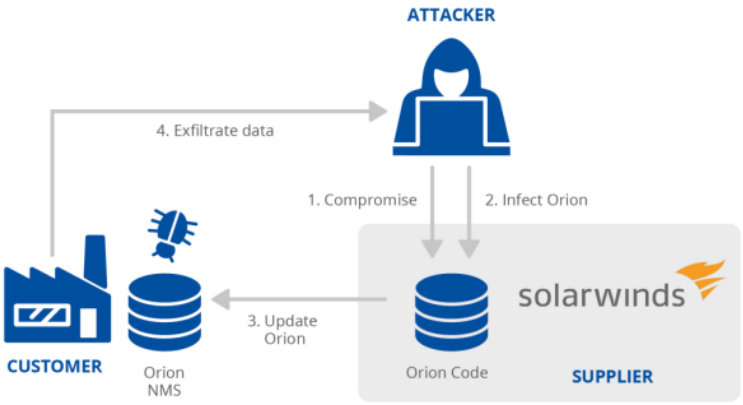
Az ellátási lánc elleni támadás a szervezetek és beszállítóik közötti kapcsolatot veszi célba. Egy támadás akkor tekinthető ellátási lánc komponenssel rendelkezőnek, ha legalább két támadás kombinációjából áll. Ahhoz, hogy egy támadás ellátási láncot érintő támadásnak minősüljön, a szállítónak és a vevőnek egyaránt célpontnak kell lennie. A SolarWinds volt az egyik első ilyen jellegű támadás, amely megmutatta az ellátási láncot érintő támadások potenciális hatását.

SolarWinds

SolarWinds Orion Platform ellen irányult támadás, egy sikeres kiberbiztonsági incidens volr 2020 decemberében. Ezt a támadást "SolarWinds-hack" vagy "Sunburst" néven ismerik.

A támadók a SolarWinds Orion Platformba bejutva manipulálták az egyik szoftverfrissítést, amelyet a SolarWinds ügyfelek automatikus frissítési rendszere használt.

Az ártalmas szoftver egy backdoor-t nyitott meg a rendszereken, amelyen keresztül a támadók további tevékenységeket folytathattak a célpontok munkaállomásán (3. ábra).



3. ábra: A SolarWinds támadási mechanizmusa

A támadók és információkat gyűjtöttek, illetve hozzáférést szereztek a célcsoportok hálózati rendszereihez.

A SolarWinds-hack jelentőségét az adja, hogy a támadók képesek voltak olyan rendszerekbe és hálózatokba bejutni, amelyek kulcsszerepet játszanak az államigazgatásban és a vállalati szektorban. A kibertámadás súlyossága és összetettsége miatt jelentős figyelmet kapott a kiberbiztonsági szakértők, a kormányok és a vállalatok részéről. A támadás forrása hivatalosan Oroszországot hozta összefüggésbe a csoporttal, amelyet kiberbiztonsági közösségek APT29 vagy Cozy Bear néven ismernek. [6]

Az eset megmutatta, hogy mennyire fontos az informatikai rendszerek és szoftverek biztonsága, és kihangsúlyozta a kritikus infrastruktúrák és az üzleti szektor védelmének jelentőségét a kibertámadások ellen.

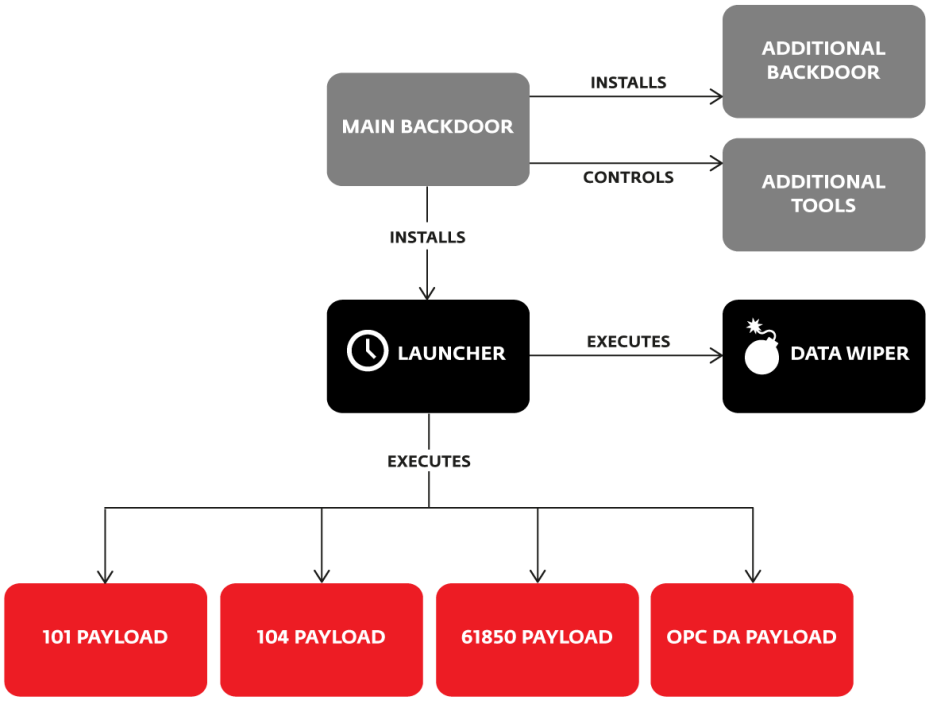
Industroyer

A vírus képes közvetlenül irányítani az elektromos alállomások kapcsolóit és megszakítóit. Ezek a kapcsolók és megszakítók az analóg kapcsolók digitális megfelelői. Így a potenciális hatás az áramelosztás egyszerű kikapcsolásától kezdve a tényleges meghibásodásokon át a berendezések súlyosabb károsodásáig terjedhet.

Helyi proxyval hitelesíti magát a belső hálózaton keresztül a backdoor telepítése előtt. A hitelesítés után HTTP-csatornát nyit a külső a C2 szerver felé.

A későbbi kommunikáció ezt követően a belső proxyn zajlik. Létrehoz egy fertőzött fájlt a helyi rendszeren (melyen keresztül életben tartja a kapcsolatot), amely egy futó szerviz szolgáltatáshoz kapcsolódik. A megfertőzött szolgáltatás folyamatosan nyitva tartja a backdoor-t, úgy, hogy előre meghatározott időközönként újranyitja a kapcsolatot a támadó szerver felé, így a rosszindulatú program továbbra is fut az újraindítások után is. [6]

Az Industroyer rendkívül testreszabható malware. Bár univerzális, mivel bármely ipari vezérlőrendszer megtámadására használható, amely a célzott kommunikációs protokollok némelyikét használja, az elemzett minták egyes összetevőit úgy tervezték, hogy bizonyos hardvereket célozzanak meg.



4. ábra: Az Industroyer támadási mechanizmusa [6]

Industroyer 2

A beavatkozást 2022.04.08-ra tervezték, de a jelek arra utalnak, hogy a támadást legalább két héttel előtte előkészítették.

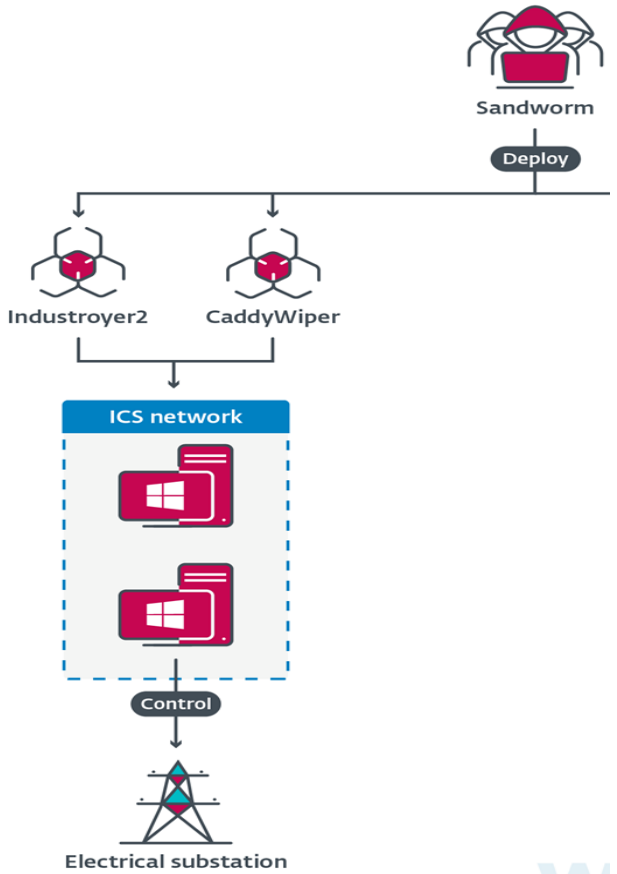
A támadásban ICS-képes rosszindulatú szoftvereket és Windows, Linux és Solaris operációs rendszerekhez alkalmazható lemeztörlőket használtak. Nagy valószínűséggel a támadók az Industroyer rosszindulatú szoftver új verzióját használták, amelyet 2016-ban az ukrajnai áramkimaradáshoz használtak.

Az Industroyer2 mellett a Sandworm több pusztító kártevő családot is használt, köztük a CaddyWiper-t. A CaddyWiper-t először 2022.03.14-én fedezték fel, amikor egy ukrán bank ellen használták. A CaddyWiper egy változatát 2022.04.08 14:58-án ismét felhasználták a korábban említett ukrán energiaszolgáltató ellen.

Az Industroyer2-t egyetlen Windows futtatható fájlként telepítették, amelynek neve 108_100.exe, és egy ütemezett feladat segítségével 2022.04.08-án 16:10:00 UTC-kor futtatta le. A PE időbélyege szerint 2022.03.23-án állították össze, ami arra utal, hogy a támadók több mint két hétig tervezték a támadást.

Az Industroyer2 nagymértékben konfigurálható. Részletes konfigurációt tartalmaz a testében, amely a rosszindulatú programok műveleteit vezérli. Ez eltér az Industroyer-től, amely a konfigurációt egy különálló .INI fájlban tárolja. A rosszindulatú szoftver megszüntet egy legitim folyamatot, amelyet a szokásos napi műveletek során használnak. Ráadásul átnevezi ezt az alkalmazást úgy, hogy a fájlnévhez .MZ-t ad hozzá. Ezt azért teszi, hogy megakadályozza a valódi folyamat automatikus újraindulását. Ez a komponens képes bizonyos ICS-rendszereket vezérelni az áramellátás leállítása érdekében. [8]

A CaddyWiper egy loader segítségével a Hex-Rays IDA Pro szoftver egyik legális komponensének, konkrétan a távoli IDA debugger szerver win32_remote.exe fájljának javított változatának álcázták. A patch-elt bináris kód egy fájlból tölti be a titkosított shellcode-ot, amely a CaddyWiper kissé módosított változata. Ez törli a meghajtó partícióinak kiterjesztett információit: a Master boot record (MBR) vagy a GUID Partition Table (GPT). Ezáltal a gép indíthatatlanná válik. A megtámadott energiavállalat hálózatán további, Linux és Solaris rendszert futtató, pusztító hatású kártevőket is találtak. A támadásnak két fő összetevője van: egy féreg és egy wiper.



5. ábra: Az Industroyer 2 és a CaddyWiper közös használata [8]

HATÁSVIZSGÁLAT

Az ENISA fenyegetettségi térképében szerepelnek a kritikus infrastruktúrák ellen intézett kibertámadások hatása. Mivel a kibertámadások hatásával kapcsolatos információk gyakran nem állnak rendelkezésre vagy nem hozzák nyilvánosságra, az eseményt követő hatás meghatározása és értékelése olyan szintű feltételezéssel jár, amelyben bizonyos fokú szubjektivitás nem kerülhető el. Ez önmagában is érvként szolgál az EU-ban az incidensek jelentési folyamatának javítása mellett, amely szempont a NIS2-irányelvben is megjelenik, és az ENISA az elkövetkező években is folytatja erőfeszítéseit.

Az ETL-jelentés keretében az alábbi hatástípusok figyelhetők meg:

- A digitális hatás a sérült vagy nem elérhető rendszerekre, sérült adatfájlokra vagy adatok kiszivárgására, vagy valamilyen bejelentett rosszindulatú behatolásra vonatkozik.
- A gazdasági hatás a közvetlen pénzügyi veszteségre, a nemzetbiztonságot érő károkra utal, amelyek fontos anyagok elvesztését vagy váltságdíj követelését eredményezheti.
- A társadalmi hatás a közvéleményre gyakorolt bármilyen hatásra vagy olyan széles körű zavarra utal, amelynek a társadalomra lehet következménye (pl. egy ország nemzeti egészségügyi rendszerét megzavaró események, bármely adat kiszivárgása a lakosság személyi azonosítóira, társadalombiztosítási azonosítókra vonatkozó adatok kiszivárgása stb.).
- A hírnévre gyakorolt hatás a negatív nyilvánosság vagy a közvélemény negatív megítélésének lehetőségére utal.
- A fizikai hatás az alkalmazottak, ügyfelek vagy betegek sérülésére vagy károsodására utal.
- A pszichológiai hatás okozhat megtévesztést, kellemetlenséget, frusztrációt, aggodalmat vagy szorongást. [3]

MOTIVÁCIÓ

Az ellenség és a kiberbiztonsági incidens vagy célzott támadás mögött álló motiváció megértése azért fontos, mert így meghatározható, hogy az ellenfél mire törekszik. Az indítékok ismerete segíthet a szervezeteknek meghatározni és prioritásként kezelni, hogy mit és hogyan kell védeni. Emellett képet ad a támadók szándékairól, és segít a szervezeteknek abban, hogy védelmi erőfeszítéseiket az adott eszközzel kapcsolatos legvalószínűbb támadási forgatókönyvre összpontosítsák.

A motiváció öt különböző fajtáját határozták meg:

- Pénzügyi haszon: bármilyen pénzügyekkel kapcsolatos csalás (amelyet többnyire kiberbűnözői csoportok hajtanak végre).
- Kémkedés: információk megszerzése érzékeny adatokról, minősített adatokról (többnyire államilag támogatott csoportok hajtják végre).
- Megzavarás: bármilyen geopolitikai céllal végrehajtott bomlasztó akció (többnyire államilag támogatott csoportok hajtják végre).
- Rombolás: minden olyan romboló akció, amelynek visszafordíthatatlan következményei lehetnek.
- Ideológiai: minden olyan akció, amely mögött ideológia áll (például hacktivizmus).[3]

TÁMADÁSOK ELEMZÉSE

Fontos felismerés, hogy egyes kibertámadó csoportok némi állami segítséggel törvényes eszközöket vetnek be, hogy meghosszabbítsák a kiberkémkedési műveleteiket. Céljuk, hogy minél tovább elkerüljék a felderítést, és elfedjék tevékenységüket azáltal, hogy a

legtöbb rendszerből széles körben elérhető szoftvereket használnak, ami megnehezíti a védők számára az azonosításukat. A geopolitika továbbra is nagy hatással van a kiberműveletekre. Számos fenyegető szereplő tovább fejlesztette az úgynevezett As-a-Service programjait. Nemcsak a új taktikákat és módszereket használnak a célpontokhoz való behatoláshoz, hanem a nyomásgyakorlás alternatív megközelítéseit is egyre jobban finomítják, amellyel zsarolják az áldozatokat, mindezt tiltott vállalkozásaik előmozdítása mellett.

Az egyik legnagyobb malware fenyegetés még mindig az információlopók, mint például az Agent Tesla, a Redline Stealer és a FormoBook. Folyamatosan csökken a klaszszikus mobil kártevők száma, viszont az adware-ek továbbra is megmaradtak ebben az évben is, mint a mobil eszközökre leselkedő legelterjedtebb fenyegetés. Sajnos a kémprogramok előretörése folytatódni fog a következő években is egyre jobban felhasználva a mesterséges intelligenciát.

Az adathalászat ismét a reneszánszát éli a legújabb elemzések szerint, ahol a social engineering új modellje adja az alapot. Ennek a modellnek a lényege áldozatokat nem csak a fizikai világban hanem a virtuális térben is megtéveszthetik. Az üzleti e-mailek kompromittálása (BEC, VEC) továbbra is a támadók egyik kedvenc eszköze a megszerzésre, amely valószínűsíthető a közeljövőben is hasonlóképpen lesz.

A Microsoft makróktól az ISO , Onenote és LNK fájlok felé való elmozdulás folytatódik, az ISO , Onenote és LNK fájlok használata felé. Az adatok kompromittáltsága 2023-ban nőtt. 2021-ig növekedett az adatveszélyeztetések száma, és bár ez a tendencia 2022-ben viszonylag stabil maradt, 2023-ban ismét növekedni kezdett.Megugrott a kiberbiztonsági fenyegetettségre hatást gyakorló AI Chatbotok száma. A bomlasztó hatás és a generatív mesterséges intelligencia chatbotok, például az OpenAI ChatGPT exponenciális elterjedése,

A DDoS-támadások egyre nagyobbak és összetettebbek, a mobilhálózatok és az IoT felé mozdulnak el, és kontextusban használják, hogy egy konfliktus keretében további eszközök támogatására használják őket. Az internet leállása minden idők legmagasabb szintjén van. Az internet elérhetőségét fenyegető fenyegetések lendületben maradnak, különösen a covid utáni korszakban, mivel az emberi tevékenységek és a társadalom egyre inkább az internetre támaszkodik. Az "olcsó hamisítványok" és a mesterséges intelligenciával támogatott információmanipuláció továbbra is aggodalomra ad okot. Az elmúlt hónapokban a mesterséges intelligencia információmanipulációra való felhasználásáról szóló vita felerősödött mind az Unión belül, mind azon kívül. A fenyegető csoportok egyre nagyobb érdeklődést mutatnak az ellátási láncot érő támadások iránt, és egyre nagyobb képességet mutatnak az alábbiakra azáltal, hogy az alkalmazottakat használják fel belépési pontként.

Nagy kihatással járó események ebben az évben is csak kis mértékben emelkedtek. A minősített bizalmi szolgáltatások bejelentése is növekedett az elmúlt évek statisztikájához képest az összes incidens 75%-ra volt hatással. A nem minősített bizalmi szolgáltatások viszont közel sem ennyire egyértelműek számadatok tekintetében, mivel az adatot szolgáltatóknál általában, olyan automatizmusok vannak beépítve a rendszerben amelyek torzítják a kevésbé fontos adatok megérkezését a központi elemző rendszerek felé. A jelentett incidensekkel kapcsolatos pontos és teljes információ biztosítása elengedhetetlen a megfelelő elemzéshez és nyomon követési intézkedésekhez. Sajnos az ENISA jelentése szerint legalább 10% a bejelentett incidenseknek nem tartalmaz további feldolgozható információs

adattartalmat, amelyet adatelemzés céljára fel lehetne használni. A rosszindulatú tevékenységek kezelésére vonatkozó korai figyelmeztetések nagymértékben segíthetnek a különböző piaci szegmenseknek, amellyel csökkenteni lehet az incidensek hatását. Itt lehetne megemlíteni a kritikus infrastruktúrák közötti, egymástól való kölcsönös tanulást is, amelynek során jelentősen lehetne mérsékelni a potenciális kibertámadási veszélyeket. [3] a webhelytanúsítványok (TLS), amelyek az online/internetes biztonság alapvető elemei. Világszerte a webhelyek körülbelül 80%-a használ webtanúsítványt.

VÉDELMI INTÉZKEDÉSEK

Egy általános szervezet infokommunikációs felépítése általában minimum két, jól elkülöníthető szektorra bontható. Ezen szektorokhoz javaslok néhány egyszerű védelmi megoldást az alábbiakban.

1. szektor: Azok a szerverek, amik az internetről láthatóak.

Az egyes szerverek egy alhálózatban vannak és kommunikálnak egymással. A bejutás többnyire egy létező rendszersérülékenység segítségével történik.

Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- hálózati szegmentálás (nincs új a nap alatt);
- hardveres illetve szoftveres biztonsági megoldások (IDS, IPS, Firewall);
- ellenőrzött operációs rendszer frissítések alkalmazása;
- képzett személyzet (ahol nem üzemeltetés a cél!!!).

2. szektor: Felhasználói szféra vagy üzemi terület

Általában külön alhálózatot képeznek a szerver szekcióval. A bejutás többnyire phising kampánnyal kezdődik. Ebben az esetben a támadónak mindenképpen el kell érnie, hogy a felhasználó hibázzon.

Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- „erős jelszó” használata;
- kiberbiztonsági tudatosító oktatások megtartása (védekezni kell a social engineering ellen).

A felhasználókkal szemben elkövetett csalások jelentős kockázatot jelentenek az egyének személyes adataira és pénzügyi biztonságára, és az ilyen incidensek megelőzése és kezelése kulcsfontosságú a kiberbiztonsági stratégiákban.

ÖSSZEFOGLALÁS

A kibervédelem kritikus infrastruktúrák esetében kiemelkedően fontos, mivel ezek az intézmények és rendszerek olyan alapvető szolgáltatásokat nyújtanak, amelyek elengedhetetlenek a társadalom és a gazdaság működéséhez. Ilyen infrastruktúrákhoz tartoznak például az energiaszolgáltatások, víz- és csatornahálózatok, közlekedési rendszerek, egészségügyi intézmények, pénzügyi szervezetek, és más olyan létesítmények, amelyek kulcsfontosságúak a mindennapi életünkben.

A kibertámadások súlyos következményekkel járhatnak, nem csak az adott intézményre vagy szolgáltatásra, hanem az egész társadalomra nézve. A támadók célja lehet a szolgáltatások megbénítása, az adatok manipulálása, vagy akár a fizikai rendszerek károsítása is. Ezért a kibervédelem célja a biztonsági rések folyamatos monitorozása, az azokból adódó veszélyek azonosítása és azok elleni hatékony védekezés.

Az Industroyer típusú támadások tanulságos példák lehetnek a kritikus infrastruktúrák védelmének szempontjából. Az Industroyer egy kifinomult kártevő, amely képes irányítani és manipulálni az ipari vezérlőrendszereket, például az elektromos hálózatokat. Ezek a támadások rávilágítottak arra, hogy az ipari rendszerek sebezhetőségei jelentős veszélyt jelenthetnek, és hogy a támadók milyen mértékben tudnak kihasználni az ellátási láncokban rejlő gyenge pontokat. Az ilyen típusú támadásokból levonható tanulságok segíthetnek az ipari szektor és más kritikus infrastruktúrák védelmi stratégiáinak fejlesztésében, a biztonsági intézkedések javításában és az esetleges támadások elleni hatékony védekezés kidolgozásában.

A legfontosabb javaslat, hogy az üzemi területen is fel kellene váltania a „safety" nézőpontot, az informatikában alkalmazott „security" gondolkodásmódra. Ez azt jelenti, hogy be kell látni, hogy nem csupán a bitonságos rendelkezésreállásra van szükség az ipari területeken, hanem a tényleges információbiztonsága.

FELHASZNÁLT IRODALOM

[1] Sági G., „Informatikai rendszerek támadási folyamata." *Műszaki Katonai Közlöny,* 27 évfolyam, 3. szám, pp. 212-223., 2017.

[2] Almási L., Balog P., Berkecz G., Busa A., Drót L., dr. Eleki Z., Fekete A., dr. Kállai A., Kalmár I., Mihályi L., Nyulászi T., Szűcs P., dr. Tálas P. H., Tóth G., Zentai K., *Honvédelmi alapismeretek tankönyv*. Zrínyi Kiadó, Budapest, 2023.

[3] ENISA Threat Landscape 2023 [online]. Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (letöltve: 2023.11.20.)

[4] Kiberbűnözők célpontja lett az energiaszektor [online]. Elérhető: https://greendex.hu/kiberbunozok-celpontja-lett-az-energiaszektor/ (letöltve: 2023.11.18.)

[5] ENISA Threat Landscape for Supply Chain Attacks [online]. Elérhető: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (letöltve: 2023.11.18.)

[6] CyberArk Blog Team: The Anatomy of the SolarWinds Attack Chain [online]. Elérhető: https://www.cyberark.com/resources/blog/the-anatomy-of-the-solarwinds-attack-chain (letöltve: 2023.11.20.)

[7] Industroyer: Biggest threat to industrial control systems since Stuxnet [online]. Elérhető: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (letöltve: 2023.11.18.)

[8] MalPedia for win.industroyer [online]. Elérhető: https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer (letöltve: 2023.10.18.)

[9] How Kaspersky Industrial CyberSecurity deals with an APT based on Industroyer malware [online]. Elérhető: https://www.kaspersky.com/enterprise-security/mitre/industroyer (letöltve: 2023.11.07.)