2025 november havi CTI riport

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet havi rendszerességgel ad ki fenyegetéselemzést, mely összefoglalja a kibertér globális, valamint magyarországi helyzetét. A riport megismerése megfelelő támpontot adhat az olvasó számára, hogy szervezete milyen IT biztonsági kihívásokkal nézhet szembe a közeli jövőben.

Helyzetkép

2025 novemberében a globális kibertérben tovább erősödtek a geopolitikai motivációjú, célzott APT-támadások, különösen orosz, kínai és észak-koreai kötődéssel, miközben több új vagy továbbfejlesztett kártevő (pl. GamaWiper, módosított gh0st RAT, platformfüggetlen Konni-variáns) jelent meg. Fokozódott a banki trójai programok (Sturnus, Gootloader) szerepe, valamint az Android-ökoszisztéma elleni támadások súlya, amit a Landfall és a katonai Android-tilalmak is jeleznek.

A zsarolóvírus-ökoszisztéma tovább erősödött, a sikeres ransomware-incidensek száma nő, a támadók egyre inkább a kisebb, kevésbé felkészült szervezeteket célozzák, amelyek gyenge IT-infrastruktúrával és hiányos incidenskezeléssel rendelkeznek. Az Akira csoport kiemelkedő aktivitással, főként Cisco VPN-végpontokon keresztül támad, emelkedő trendet mutat több más csoport (CL0P, INC, InterLock, Kazu, NightSpire, WordLeaks) is.

Az ICS/SCADA- és kritikus infrastruktúra-környezetek célzott fenyegetettsége szintén növekedő tendenciát mutat. Rosszindulatú NuGet-csomagok (pl. Sharp7Extend) ipari PLC-ket és gyártási folyamatokat veszélyeztetnek, miközben a leggyakoribb sérülékenységtípusok (CWE-78, CWE-787) távoli kódfuttatást és teljes rendszerkompromittálást tehetnek lehetővé, különösen biztonsági és hozzáférés-kezelő rendszerekben.

Az egészségügy világszinten kiemelt célponttá vált: többek között a Qilin és más ransomware-csoportok nagy volumenű adatlopási és zsarolási kampányokat folytatnak, komoly adatvédelmi és betegbiztonsági kockázatot okozva – ami rávilágít az egészségügyi intézmények hozzáférésvédelemre, sérülékenység-menedzsmentre és incidenskezelésre fókuszáló védelmének sürgős megerősítésére.

Káros kódok és zsarolóvírusok

Káros kódok

2025 novemberében több APT-csoport támadása is ismertté vált, amelyek többsége a jelenlegi geopolitikai konfliktusok, valamint érdekellentétek kibertérben történő kiterjesztéseként értelmezhető. Az orosz–ukrán háborúhoz kapcsolódva az Oroszországhoz köthető Gamaredon csoport ukrán kormányzati szervezeteket támadott a GamaWiper káros kóddal[1], míg a Tomiris APT (Storm-0473) közép-ázsiai, orosz nyelvű – elsősorban kormányzati – intézményeket vett célba[2]. A kazahsztáni kötődésű Cavalry Werewolf (YoroTrooper) több orosz állami szervezet ellen folytatott támadásokat bizalmas adatok megszerzésére törekedve[3]. A Kínához kapcsolható Dragon Breath APT (APT-Q-27) egy módosított gh0st RAT változatát terjesztette[4], főként kínai nyelvterületen lévő célpontok ellen. Az észak-koreai Konni APT (APT37) dél-koreai szervezeteket támadott olyan káros kóddal, amely Android és Windows rendszereken egyaránt működik, a fenyegetés pedig spearphishing kampányok útján jutott be állami intézményekbe, ahol később adatlopást vagy adattörlést hajthattak végre.

A GlassWorm kártevő-kampány újabb hullámban tért vissza[5], ezúttal három frissen azonosított Visual Studio Code (VS Code) kiterjesztésen keresztül. A támadások az OpenVSX és a Visual Studio Code Marketplace platformokat érintik, és a múlt hónapban megfigyelt fertőzési lánc folytatásának tekinthetők.

Novemberben a banki trójai programok is tovább fejlődtek. Új variánsként azonosították a Sturnust, emellett hét hónap szünet után ismét aktivizálódott a Gootloader kártevőterjesztő platform[6], amely a korábbiaknál kifinomultabb módszerekkel igyekszik kikerülni a védelmi rendszereket. A Gootloader egy JavaScript-alapú malware loader,

[1] https://x.com/ClearskySec/status/1995061537183011084
[2] https://securelist.com/tomiris-new-tools/118143/
[3] https://hackread.com/cavalry-werewolf-russia-government-shellnet-backdoor/
[4] https://www.elastic.co/security-labs/roningloader
[5] https://nki.gov.hu/it-biztonsag/hirek/ujabb-fertozesi-hullamban-ter-vissza-a-glassworm-kartevo/
[6] https://nki.gov.hu/it-biztonsag/hirek/uj-modszerekkel-tamad-a-gootloader-malware/

amely kompromittált vagy támadók által kontrollált weboldalakon keresztül fertőz, gyakran keresőoptimalizálási manipuláció (SEO poisoning) alkalmazásával.

Az Android operációs rendszereket célzó kártevők száma továbbra is növekszik. Új szereplőként jelent meg a Landfall[7], amely a Palo Alto Networks jelentése szerint egy nulladik napi sérülékenységet kihasználva kerül fel Samsung készülékekre. Közben az Androidos fenyegetések terjedése miatt az izraeli hadseregben alezredesi rendfokozattól felfelé megtiltották az Android operációs rendszerű eszközök használatát[8].

Magyarországi trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzöttségi információk elemzését. November hónapban emelkedés mutatható ki a banki trójai fertőzések, valamint az információ lopást végző kártevők számában, továbbá a nemzetközi trendeknek megfelelően hazánkban is igen elterjedtek az Android kártevők is.

Káros kód	Trend
Vextrio	↔
BADBOX 2.0	↔
Ranbyus	↑
Vo1d(2)	↓
Nymaim	↑
Tiny Banker	↑
Ngioweb	↔
Mirai	↓
SmokeLoader	↔
Matsnu	↑

1. ábra: Káros kód trendek Magyarországon

A beérkezett adatok elemzése alapján megállapítható, hogy az elmúlt hónapban növekvő tendenciát mutattak a .hu TLD-vel rendelkező weboldalakon az adathalász és egyéb malware-terjesztésre használt fertőzések, ugyanakkor a vezérlőszerverként működő webszerverek száma csökkenést mutatott.

[7] https://nki.gov.hu/it-biztonsag/hirek/a-landfall-android-spyware-samsung-telefonok-nulladik-napi-serulekenyseget-hasznalja-ki/
[8] https://nki.gov.hu/it-biztonsag/hirek/az-izraeli-hadsereg-korlatozza-az-android-hasznalatat/

Zsarolóvírusok

2025 novemberében az NBSZ–NKI információi alapján az előző hónaphoz képest emelkedett a sikeres zsarolóvírus-támadások száma. Ez arra utal, hogy a ransomware-ökoszisztéma az eddigi trendeknek megfelelően tovább fejlődhetett. Az előző hónapban a Coveware jelentése[9] szerint a harmadik negyedéves időszakban átlagos és a medián zsarolódíj is csökkent, ami arra enged következtetni, hogy a támadók – tanulva az előző év tapasztalataiból – a nagyvállalatok (úgynevezett „nagyhalak") helyett egyre inkább a kisebb cégeket veszik célba. Visszatekintve: a tavalyi évben több nagyvállalatot is támadás ért, ám ezek nem fizettek, mivel a tudatosítási tevékenységeknek, illetve az eddigi tapasztalatoknak köszönhetően felismerték, hogy a váltságdíj kifizetése után sem biztos, hogy visszakapják adataikat. A kisebb vállalatokhoz azonban ezek az információk nehezebben jutnak el, IT-infrastruktúrájuk kevésbé felkészült, így könnyebben válnak célponttá, és – akár biztonsági mentés hiányában – fizetési hajlandóságuk is magasabb lehet.

Szektoranalízis

A novemberben megismert információk szerint a zsarolóvírus-csoportok elsősorban az építőipari, gyártási, ipari gépgyártó, állami és egészségügyi szektort vették célba. A legtöbb incidens az Amerikai Egyesült Államokban történt, ugyanakkor Európa továbbra is érintett: Ausztriából, Németországból, Spanyolországból és Olaszországból is jelentettek ilyen eseményeket.

[9] https://www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet

Zsarolóvírus-csoportok havi aktivitási trendje

Novemberben az Akira bizonyult a legaktívabb zsarolóvírus-csoportnak, amely elsősorban Cisco eszközök VPN végpontjait támadja, ezen a módon szerezve hozzáférést az érintett rendszerekhez. Az Akira térnyerése összhangban áll a szeptemberben nyilvánosságra került Cisco ASA VPN sérülékenységekkel, amelyekről az NBSZ–NKI riasztást[10] is közzétett. Ismételten felhívjuk a figyelmet az érintett eszközök mielőbbi frissítésére. Második helyen pedig a Qilin csoport található mely aktivitását saját észlelőrendszerünk adatai alapján is érzékeltük.

Típus	Trend
Akira	↑
Qilin	↓
CL0P	↑
INC	↑
InterLock	↑
Kazu	↑
NightSpire	↑
Play	↔
Dragon	↔
WordLeaks	↑

2. ábra: Top 10 zsarolóvírus trendadatai

[10] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-cisco-termekeket-erinto-serulekenysegekrol-2025-szeptember/

Kihasznált sérülékenységek

A sikeres zsarolóvírus-támadások során a támadók több ismert sérülékenységet is kihasználnak, elsősorban azért, mert ezek frissítése sok szervezetnél rendszeresen elmarad, így a kihasználásuk különösen egyszerű. A leggyakrabban felismert sebezhetőség a CVE-2020-1472 (Zerologon)[11], amely a Netlogon Remote Protocol (MS-NRPC) hibáit használja ki, jogosultságkiterjesztést lehetővé téve az érintett rendszereken. A CVSS metrika szerinti 10.0 pontos értékelése azt jelzi, hogy távolról, autentikáció nélkül, könnyen támadható.

A támadók emellett továbbra is előszeretettel élnek a CVE-2021-44228 (Log4Shell), a CVE-2023-27532, a CVE-2023-48788, a CVE-2024-55956, a CVE-2021-35211 és a CVE-2024-50623 által kínált lehetőségekkel. Az NBSZ-NKI javasolja a frissítési előírások következetes betartását, valamint a szervezet weboldalán rendszeresen megjelenő sérülékenységi közlemények folyamatos figyelemmel kísérését.

[11] https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2020-1472/

ICS/SCADA

2024 eleje óta öt kibertámadás érte[12] Nagy-Britannia ivóvíz-szolgáltatóit, amelyek jellemzően a szervezeti/IT-környezetet érintették és nem okoztak az ivóvízellátás biztonságát veszélyeztető szolgáltatáskimaradást. A Drinking Water Inspectorate (DWI) 2024. január 1. és 2025. október 20. között összesen 15, a NIS-szabályozáshoz kapcsolódó bejelentést fogadott, amelyekből öt minősült kiberbiztonsági incidensnek, több esetben a hivatalosan NIS-hatókörön kívüli rendszerekben.

2025 novemberében a CISA ICS Advisoryhoz 8 db kritikus OT/ICS sérülékenységeket összegző riasztás került publikálásra:

- Survision License Plate Recognition Camera[13]
- Radiometrics VizAir[14]
- General Industrial Controls Lynx+ Gateway[15]
- Siemens COMOS[16]
- METZ CONNECT EWIO2[17]
- Emerson Appleton UPSMON-PRO[18]
- Zenitel TCIV-3+[19]
- Festo Compact Vision System, Control Block, Controller, and Operator Unit products[20]

A CVE-2021-26829[21] egy olyan biztonsági hiba az OpenPLC ScadaBR-ben, amely lehetővé teheti, hogy egy támadó rosszindulatú tartalmat helyezzen el a rendszer egyik

12 therecord.media
13 cisa.gov
14 cisa.gov
15 cisa.gov
16 cisa.gov
17 cisa.gov
18 cisa.gov
19 cisa.gov
20 cisa.gov
21 nki.gov.hu

beállítási felületén. Ez a tartalom később automatikusan lefuthat azoknak a felhasználóknak a böngészőjében, akik megnyitják az érintett oldalt. A probléma a Linuxos kiadásoknál 0.9.1-ig, Windows alatt pedig 1.12.4-ig lehet jelen. A sebezhetőség kockázatot jelenthet a felhasználói munkamenetek biztonságára és akár arra is lehetőséget adhat, hogy valaki visszaéljen a webes kezelőfelületen elérhető jogosultságokkal. A CISA 2025. november 28-án felvette a sérülékenységet a Known Exploited Vulnerabilities (KEV) katalógusba[22], ami arra utal, hogy valós környezetben is észleltek aktív kihasználást.

A CISA ipari vezérlőrendszerekről (ICS) szóló figyelmeztetéseket[23] adott ki, amelyek sérülékenységeket részleteznek az Ashlar-Vellum, a Rockwell Automation, a Zenitel, az Opto 22, a Festo, a SiRcom és a Mitsubishi Electric termékeiben. A gyártók az érintett termékeik legfrissebb verzióiban javították ezeket a sérülékenységeket.

A Socket Threat Research Team kilenc rosszindulatú NuGet-csomagot azonosított[24], amelyeket a shanhai666 alias alatt 2023 és 2024 között tettek közzé. A csomagok időben késleltetett payloadokat juttatnak be adatbázisokba, valamint ipari vezérlőrendszereket is célba vesznek. A legveszélyesebbnek a Sharp7Extend tűnik, amely ipari PLC-ket támad, azonnali véletlenszerű folyamatleállítással és a telepítés után 30–90 perccel induló, csendes írási hibákkal veszélyeztetve gyártási környezetek biztonságkritikus rendszereit. A kilenc csomag összesen 9 488 letöltést ért el; a kutatók 2025. november 5-én jelentették őket a NuGetnek.

[22] cisa.gov

[23] cisa.gov

[24] socket.dev

Sérülékenységek

A hónap során leggyakrabban megfigyelt gyengeségek a CWE-78[25] (operációs rendszer parancs injektálás) és a CWE-787[26] (határon kívüli értékek írása) voltak.

Sérülékenység publikálások az NKI weboldalán november hónapban (kritikus)	Sérülékenység publikálások a CISA KEV katalógusában november hónapban
CVE-2025-5397	CVE-2025-48703
CVE-2025-11533	CVE-2025-11371
CVE-2025-5947	CVE-2025-21042
CVE-2025-48703	CVE-2025-12480
CVE-2025-20358	CVE-2025-62215
CVE-2025-20354	CVE-2025-9242
CVE-2025-64459	CVE-2025-64446
CVE-2025-21042	CVE-2025-58034
CVE-2025-12480	CVE-2025-13223
CVE-2025-64446	CVE-2025-61757
CVE-2025-59367	CVE-2021-26829
CVE-2022-40684	
CVE-2025-25256	
CVE-2025-24893	
CVE-2025-61757	
CVE-2025-4581	

3. ábra: Novemberi összegző táblázat az NKI által publikált kritikus sérülékenységekből, illetve a CISA KEV katalógusából

A hónap kritikus hibáinak közös jellemzője, hogy jelentős részük hálózatról elérhető és több esetben hitelesítés nélkül vagy minimális előfeltétellel kihasználható. Ez a kitettség különösen magas kockázatot jelent olyan környezetekben, ahol az érintett rendszerek az internet felől közvetlenül elérhetők, mivel a támadók gyorsan automatizálhatják a felderítést és a kihasználást. A sérülékenységek között több olyan is szerepel, amely távoli kódfuttatáshoz (RCE), adminisztrátori jogosultság megszerzéséhez vagy teljes rendszerkompromittáláshoz vezethet.

[25] cwe.mitre.org

[26] cwe.mitre.org

A legnagyobb üzleti kockázatot a biztonsági infrastruktúrát érintő hibák jelentik, mivel ezek kompromittálása közvetlen belépési pontot adhat a belső hálózatok irányába. Hasonlóan kiemelt figyelmet érdemelnek a hozzáférés-kezelési rendszereket érintő sérülékenységek, amelyek sikeres kihasználása esetén a támadók felhasználói és adminisztrátori fiókok felett is kontrollt szerezhetnek.

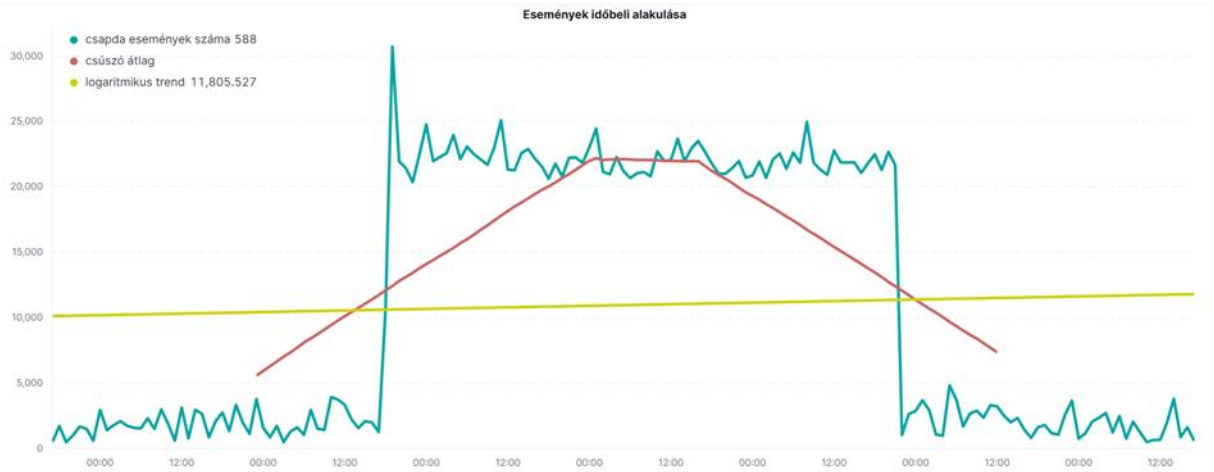
A webes platformok és fejlesztői keretrendszerek is érintettek. Vállalati tudásbázis- és portálrendszerek, valamint adminisztrációs panelek esetében a támadási felület jellemzően a publikus webes funkciókon keresztül nyílik meg. Emellett a széles körben használt tartalomkezelő rendszerek bővítményei és sablonjai között több kritikus, fiókátvételre alkalmas hiba jelent meg.

Az internet felől elérhető rendszerek esetében azonnali hibajavítás javasolt a sérülékenységek kezelése érdekében. Szükséges a patch-szintek és verziók haladéktalan ellenőrzése, az érintett komponensek frissítése vagy verzióváltása, valamint ahol indokolt, az érintett funkciók ideiglenes korlátozása. Ezzel párhuzamosan javasolt az adminisztrátori és felhasználói fiókok célzott felülvizsgálata, különös tekintettel a jogosultsági szintekre, a közelmúltban létrehozott vagy módosított fiókokra, illetve a gyanús belépésekre és szerepkör változásokra.

Honeypot forgalom elemzése

Az Elosztott Kormányzati Csapdarendszer – avagy GovProbe Honeypot – a hazai kritikus infrastruktúrákkal bíró ágazatok között kiemelt figyelmet biztosít az egészségügyi intézményekre. Több kórház hálózataiban megtalálható a Honeypot szonda, amely különböző forrásokból érkező eseményeket kezel. Az itt feltárt információk elősegítik a védelem fokozását és egyes trendek előre jelzését. Ahogyan az előző fejezetekben kifejtésre került, sajnos az egészségügyi szervezetek magasan kitettek a különböző főleg zsarolóvírusos támadásoknak.

A novemberi Honeypot adatok között felfedeztünk egy kórházi infrastruktúrát célzó feltehetően Qilin típusú Ransomware támadás előjeleit. A vizsgált szervezetnél drasztikus forgalmat tapasztalhattunk egy 3 napos periódus során:



4.ábra: A vizsgált egészségügyi szervezetet Honeypot eseményeinek novemberi változása

A brute force jellegű eseménysorozat mögött több bolgár IP címről származó szkennelés bújt meg amely során a nyitott portok és a mögötte található eszközökről próbáltak meg hasznos információkat gyűjteni. Ezek közül kiemelkedő érdeklődés fedezhető fel a 3389-es TCP port iránt. Alapértelmezetten ezen keresztül érhetőek el az RDP avagy távoli asztal protokoll szolgáltatások. Az adott Honeypot szenzoron ugyanis fut egy speciális sandbox jellegű RDP szolgáltatás is amely mélyebb interakciót képes nyújtani a támadóval szemben. Az RDP naplók megtekintésével azonosítható voltak a következő események:

- Jogosultságnövelés „superuser" szintre (uid=0)
- Rendszerinformáció gyűjtés/Szkennelés
- Nyomok eltüntetése (log fájlok módosítása/törlése)
- Script élesítése a feladatütemezőben
- Perzisztencia megerősítése

A Qilin ransomware esetében ugyanis TTP-ként azonosítható az RDP szolgáltatások kihasználása az oldalirányú mozgás és a fertőzés elterjesztése érdekében. Magyarul az RDP egy ugródeszkaként szolgál a káros kódok telepítéséhez és a támadás további fázisainak megvalósításához.

A védelem megerősítéséhez mindenképpen ajánlott az nyílt RDP szolgáltatások tiltása, hozzáférést felügyelete és az ahhoz tartozó azonosítók rendszeres cseréje.

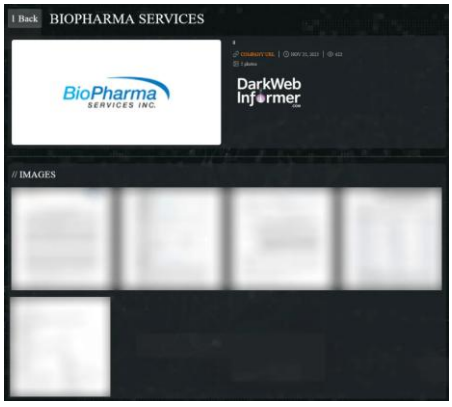
Havi vendégszektor elemzés: fókuszban az egészségügy

2025 év vége felé jelentősen fokozódtak a kibertámadások az egészségügyi szektorban, amely továbbra is kiemelt célpontjai a különböző ransomware-csoportoknak: a Quilin havonta több tucat szervezetet támad, az INC Ransom kifejezetten egészségügyi intézményeket céloz, míg a RansomHub, a Medusa és a korábban BlackCat/ALPHV néven ismert csoportok szintén aktívak maradtak. A támadók egyre gyakrabban alkalmaznak titkosítás helyett adatlopáson alapuló zsarolást, mivel az orvosi és biztosítási adatok magas értéket képviselnek a feketepiacon, ami több jelentős adatvédelmi incidenst eredményezett: a Vibra Hospital, a Fleet Landing, a Delta Dental of Virginia, a Western Wayne és az American Associated Pharmacies (AAP) is érzékeny személyes és egészségügyi adatok, többek között név, SSN, PHI és biztosítási adatok kiszivárgását jelentette, miután ismeretlen támadók dolgozói e-mail fiókokhoz és belső hálózatokhoz fértek hozzá, illetve zsarolóvírust vetettek be. Ezzel párhuzamosan a hozzáférések kereskedelme is erősödött: Kiberbűnözői körökben aktív fenyegető szereplők (köztük a FASTPRISONER nevű aktor) domain-szintű, hálózati és nagyméretű RDP-hozzáférést kínáltak eladásra egészségügyi hálózatokhoz, elsősorban zsarolóvírus-kampányok és adatlopás céljából, miközben az Acronis egy TamperedChef néven azonosított globális malvertising- és SEO-kampányra hívta fel a figyelmet, amely digitálisan aláírt, hamis telepítők révén obfuszkált JavaScript-alapú kártékony kódot terjeszt, és perzisztenciát, C2-kommunikációt, valamint távoli kódfuttatást tesz lehetővé. Az American Associated Pharmacies ellen külön sikeres ransomware-támadás történt, amely a rendszerek titkosításával és adatszivárgással járt, és amelyhez az Embargo Ransomware Group később zsarolási célú adatszivárogtatási igényt társított; mindez együttesen komoly biztonsági aggályokat vet fel, és megmutatja, miszerint az egészségügyi ágazat informatikai védelmének megerősítése sürgető.

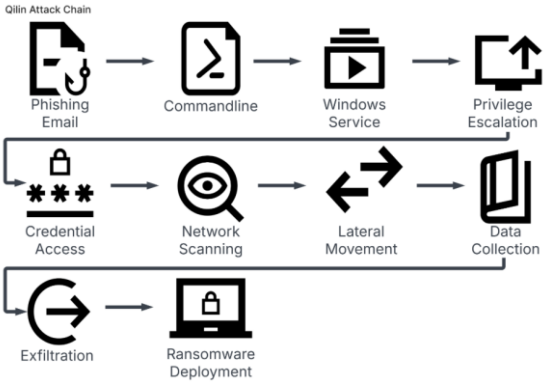
1.kép: A Shamir Orvosi Központ közleménye a Qilin DLS-éről.

Az utóbbi hónapokban az egyik kimagasló incidens egy amerikai, a Cottage Hospital-t ért támadása volt, amit a Qilin zsarolóvírus-csoport vállalt magára. Azt állítják, hogy betörtek kórház rendszerébe, és nagy mennyiségű belső dokumentumot, betegadatot, adminisztratív és működési anyagot loptak el és szivárogtattak ki, ami súlyos adatvédelmi incidenst jelent.

A kórház – mint Egészségügyi Adathordozhatósági és Számonkérhetőségi Törvény (HIPAA) hatálya alá tartozó egészségügyi szolgáltató – érzékeny egészségügyi információkat kezel, így a kompromittálódás jelentős kockázatot hordoz betegek és dolgozók tekintetében: személyazonosság-lopás, biztosítási és orvosi csalás, célzott adathalászat és hosszú távú magánszférasérelem lehet a következmény.



2. kép: A Qilin zsarolóvírus a BioPharma Services Inc.-et áldozataként tüntette fel



2. ábra: Az ábra a Qilin támadási láncot mutatja be

A támadás lehetséges technikái többek között adathalászat, sebezhető RDP/VPN, elavult rendszereken, melynek eredményeképpen kórelőzmény adatok, diagnózisok, laboreredmények, és biztosítási, valamint pénzügyi adatok sérülhettek a dolgozói nyilvántartások mellett. Fontos megemlíteni, hogy az ilyen esetek HIPAA-bejelentési kötelezettséget, hatósági vizsgálatot és akár bírságokat is maguk után vonhatnak, miközben a betegeknek fokozottan figyelniük kell számláikra, biztosítási kivonataikra és hitelaktivitásukra.

Lezárás, védelmi javaslatok

Javasoljuk ügyfeleink részére az NBSZ-NKI weboldalán megjelenő tartalmak rendszeres megismerését, különösképpen a riasztásokban foglaltakat. A novemberi hónapban nagy aktivitással rendelkező Qilin zsarolóvírus elleni felkészülést javasoljuk különösen az Egészségügyi intézmények számára:

Nyitott RDP szolgáltatások felülvizsgálata (javasolt az azonnali megszüntetésük)

Rendszeres biztonsági mentések készítése

Rendszeres felhasználói tudatosítás, különösképpen a beérkező gyanús levelekre, illetve nem biztonságos weboldalak felismerésére vonatkozóan.

Illetve általánosságban javasoljuk a szoftversebezhetőségek javítását célzó, rendszeres biztonsági frissítések telepítését. Az Ön Intézményére vonatkozó sebezhetőségekkel kapcsolatosan tájékozódhat a CTI Intézményi riportunkban (amennyiben jogosult) illetve az Automatikus Sebezhetőségdetektáló Rendszer eredményeiből (amennyiben csatlakozott).

Kérdés esetén keressen minket az alábbi elérhetőségeink egyikén!

Általános kérdések esetén:
titkarsag@nki.gov.hu

Hatósági kérdések esetén:
hatosag@nki.gov.hu

Incidensbejelentéssel kapcsolatos kérdések esetén:
csirt@nki.gov.hu

A riporttal kapcsolatos kérdések esetén:
edt@nki.gov.hu

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET