FrostyNeighbor

Fenyegető csoport elemzése

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

A csoport bemutatása

Összesítés

Fenyegetettségi csoport típusa	Állami támogatású fejlett, tartós fenyegetés (APT)
Támadott iparágak	Állami, katonai, civil média
Megnevezés	FrostyNeighbor
Alternatív megnevezés	Ghostwriter, Storm-0257, TA445, UAC-0057, UNC1151
Eredet	Fehéroroszország
Motiváció	Politikai és katonai hírszerzés
Célzott szektorok és régiók	NATO, Kelet-Európa
Használt technikák	Spear phishing, Dezinformáció, Ismert sebezhetőség kihasználása, XSS, Pszichológiai manipuláció, Defacement
Használt eszközök	Cobalt Strike, PicassoLoader, WhisperGate
Felhasznált sebezhetőségek	CVE-2024-42009 - Roundcube, CVE-2023-38831 - WinRAR, CVE-2022-30190 - MS Windows

Háttér és eredet

A FrostyNeighbor, más néven GhostWriter, UNC1151, UAC-0057, TA445, vagy Storm-0257, egy feltehetően Fehéroroszországhoz köthető, legalább 2016 óta aktív APT-csoport. Műveletei elsősorban Fehéroroszország szomszédos országaira irányulnak, különösen Ukrajnára, Lengyelországra és Litvániára, ugyanakkor kisebb számban más európai uniós országok elleni aktivitást is tulajdonítottak neki. A csoportot a szakirodalom több különböző néven azonosítja, ami az eltérő kiberbiztonsági vállalatok és kutatócsoportok saját elnevezési gyakorlatából fakad. Tevékenysége hosszabb időszakon át követhető, és több kampányban kormányzati, katonai, politikai, valamint magánszektorbeli célpontok kompromittálásával hozták összefüggésbe. Ez alapján a FrostyNeighbor a kelet-európai térség egyik tartósan jelen lévő, Fehéroroszországhoz igazodó fenyegetési szereplőjeként definiálható.

Aktivitás kezdete és ismert aktív időszakok

A csoport első dokumentált tevékenységét 2016-ra datálják, ekkor indultak az első dezinformációs kampányok a balti államokban, amelyek a NATO jelenlétét igyekeztek hitelteleníteni. A kibereszközöket alkalmazó műveletek 2017-től váltak egyre kifinomultabbá, és 2022-től - az orosz invázióval párhuzamosan - jelentősen fokozódtak. A csoport 2026 közepéig folyamatosan aktív maradt.

Motiváció és célok

A FrostyNeighbor csoport tevékenységét feltehetően állami érdekek által meghatározott motivációk vezérlik, tevékenysége a politikai és katonai hírszerzés, mely három fő pillérre bontható:

- Kiberkémkedés: Érzékeny kormányzati, katonai és politikai kommunikáció megszerzése; hozzáférés kritikus infrastruktúrához. A csoport célzottan keresi az e-mail fiókok, webmail-rendszerek és közösségi média fiókok tartalmát.
- Befolyásolási műveletek / dezinformáció: NATO-ellenes narratívák terjesztése, az orosz-belarusz érdekeket sértő politikai szereplők hitelrontása, hamis dokumentumok gyártása és terjesztése (pl. állítólagos ukrán kapitulációs nyilatkozatok), valamint az orosz katonai jelenlét legitimizálása.
- Destruktív/zavaró mellékhatás: Bár a csoport elsősorban nem destruktív célokat követ, egyes kampányok (pl. 2022-es defacement műveletek, DDoS-akciók) zavarást és bizalomvesztést okoztak ukrán és lengyel intézményekkel szemben.

A csoport geopolitikai orientációja egyértelműen pro-orosz és pro-belarusz: minden dokumentált kampány konzisztensen a NATO-tagállamok (különösen Lengyelország és a balti államok), Ukrajna, valamint a belarusz ellenzék ellen irányul. Ez az irányvonal 10 évnyi megfigyelés alatt nem változott, ami erős indikátora a tartós állami megbízói kapcsolatnak.

Célzott szektorok és régiók

Elsődleges célterületek (régiók)

A források alapján állami, Fehéroroszországhoz köthető szereplőről van szó, amely egyes leírások szerint Belarusz katonai haderejéhez, más források szerint pedig orosz katonai hírszerzési érdekekhez is kapcsolódhat. Ez fontos, mert a csoport műveletei így nem elszigetelt, alkalomszerű

támadásoknak, hanem hosszabb távon összehangolt állami műveleti mintát követőnek tűnnek. A FrostyNeighbor célzási mintázata földrajzilag erősen koncentrált. A kampányok túlnyomó többsége Kelet-Európára, illetve a NATO keleti szárnyára összpontosul.

Célzott szektorok

A FrostyNeighbor célpontválasztása jól tükrözi a csoport stratégiai és geopolitikai célrendszerét. A célzott szervezetek többsége olyan területen működik, amely közvetlen kapcsolatban áll az állami döntéshozatallal, a katonai műveletekkel, a közvélemény formálásával vagy a kritikus információk kezelésével.

Szektor	**Célpont**
Kormányzati szektor	minisztériumok, külügyi szervek, helyi önkormányzatok, parlamenti intézmények, állami hivatalok
Védelmi és katonai szektor	védelmi minisztériumok, katonai személyzet, tartalékos állomány, védelmi beszállítók, NATO-partnerszervezetek
Média és kommunikáció	Facebook, Istagram, Twitter (azóta X), YouTube
Nem állami szervezetek	médiafelületek, civil társadalom és ellenzéki szervezetek
Kritikus infrastruktúra	energetikai szervezetek, közlekedési rendszerek, távközlési szolgáltatók, állami IT-szolgáltatók

Magyarországi relevancia

A csoport tevékenysége Magyarország szempontjából is releváns lehet, mivel Magyarország NATO- és EU-tagállamként ugyanazon geopolitikai és biztonságpolitikai környezet része, amelyet a csoport hagyományosan célba vesz. A korábbi célpontválasztás alapján különösen a védelmi, külügyi, kormányzati és kritikus infrastruktúrához kapcsolódó szervezetek tekinthetők potenciális célpontnak.
Bár a legutóbb dokumentált FrostyNeighbor-műveletek elsősorban ukrán katonai és kormányzati szervezetek, illetve belarusz ellenzéki szereplők ellen irányultak, a csoport által alkalmazott támadási módszerek és eszközök széles körben adaptálhatók más államok ellen is. A közelmúlt kampányaiban a szereplők adathalász e-maileket, rosszindulatú Excel-

dokumentumokat, VBA-makrókat, DLL-alapú letöltőket, PicassoLoader-variánsokat és Cobalt Strike keretrendszert alkalmaztak, továbbá rendszeresen kihasználták a felhasználói bizalomra építő social engineering technikákat. A NATO-tagállamokkal és Ukrajna támogatásával összefüggő korábbi célpontválasztás, valamint a Lengyelország és Ukrajna ellen még 2025–2026 során is megfigyelt aktivitás alapján nem zárható ki, hogy a csoport a jövőben magyarországi szervezeteket is célba vegyen hírszerzési vagy befolyásolási célból, különösen a regionális biztonságpolitikai feszültség fokozódása esetén.

TTP elemzés

A FrostyNeighbor tevékenysége alapján a csoport elsődlegesen social engineeringre és phishing alapú kezdeti hozzáférésre épít. A támadási láncban kiemelt szerepet kapnak a rosszindulatú csatolmányok, hivatkozások és adathordozók használata, majd a felhasználói interakciót követő kódfuttatás. A kompromittálást követően a szereplő parancs- és szkriptnyelveket, legitim Windows-binárisokat, távoli hozzáférési szoftvereket és HTTP/S-alapú C2-kommunikációt alkalmazhat. A perzisztencia és jogosultságszint-emelés jellemzően érvényes fiókok, automatikus indítási mechanizmusok, DLL hijacking vagy token-manipuláció útján történik. A későbbi fázisokban megjelenik a rendszer- és fájl-felderítés, hitelesítő adatok gyűjtése, lokális adatgyűjtés, e-mail gyűjtés, majd alternatív protokollon vagy C2-csatornán keresztüli adatkiszivárogtatás.

Kiemelt TTP-k

T1566.002 – Phishing: Spear phishing Link

A layer alapján ez az egyik legerősebben reprezentált kezdeti hozzáférési technika. A támadó célzott üzenetben küldött hivatkozással próbálhatja rávenni az áldozatot rosszindulatú tartalom megnyitására, hitelesítő adatok megadására vagy jogosultságok engedélyezésére egy rosszindulatú alkalmazás számára.

Védekezési lehetőségek:

- URL Reputation Analysis (D3-URA) – Bejövő e-mailekben található URL-ek reputáció alapú vizsgálata.
- URL Analysis (D3-UA) – Bejövő e-mailekben található URL-ek sandbox és viselkedéselemzésen alapuló vizsgálata.

- Domain Reputation Analysis (D3-DRA) – Újonnan regisztrált, megtévesztő vagy obfuszkált domainek monitorozása.
- Homoglyph Detection (D3-HD) – Homoglyph és typosquatting domainek detektálása, különös tekintettel a szervezetek és szolgáltatók megszemélyesítésére.
- Sender Reputation Analysis (D3-SRA) – E-mail feladók reputációjának folyamatos értékelése.
- Sender MTA Reputation Analysis (D3-SMRA) – Feladó levelezőszerverek (MTA-k) reputációjának elemzése.
- User Behavior Analysis (D3-UBA) – Felhasználói kattintási események korrelációja böngésző-, proxy- és végponti aktivitással.
- Authentication Anomaly Detection (D3-AAD) – OAuth vagy SSO bejelentkezési anomáliák, illetve szokatlan tokenengedélyezések figyelése.

Forrás: MITRE D3FEND - Spearphishing Link - T1566.002

Detekciós stratégiák:

- AN0298: Rosszindulatú URL-t tartalmazó e-mail → felhasználói kattintás → böngészőből indított szokatlan folyamatok (pl. PowerShell, cmd) vagy letöltési aktivitás korrelációja.
- AN0299: Gyanús URL-t tartalmazó e-mail és a böngészőből indított shell vagy interpreter folyamatok összekapcsolása.
- AN0300: E-mailben érkező hivatkozás → Safari/Chrome hozzáférés újonnan regisztrált vagy megtévesztő domainhez → váratlan Terminal vagy osascript folyamatindítás.
- AN0301: OAuth consent phishing detektálása bejövő e-mail, OAuth URL meglátogatása és szokatlan identitáskezelő (IdP) tokenengedélyezések korrelációjával.

Mitigációs lehetőségek:

- M1054 - Software Configuration: SPF, DKIM és DMARC használata az e-mail hitelesítés és spoofing elleni védelem érdekében.
- M1017 - User Training: Felhasználók rendszeres phishing- és social engineering tudatossági képzése, figyelmeztető bannerek alkalmazása külső e-maileknél.
- M1021 - Restrict Web-Based Content: Magas kockázatú vagy üzletileg nem indokolt weboldalak elérésének korlátozása.
- M1018 - User Account Management: Az OAuth-hozzájárulások és harmadik fél alkalmazások engedélyezésének korlátozása.

- M1047 - Audit: Alkalmazásjogosultságok rendszeres felülvizsgálata a legkisebb jogosultság elvének megfelelően.

Forrás: MITRE ATT&CK – T1566.002 Spearphishing Link

T1204.002 – User Execution: Malicious File

A támadó a felhasználó interakciójára épít: az áldozat megnyit egy rosszindulatú fájlt, például Office/PDF dokumentumot, archívumot, LNK/ISO/EXE fájlt vagy telepítőt, amely kódvégrehajtást indít. A technika gyakran spearphishing melléklet, chat/web letöltés vagy megosztott tárhelyen elhelyezett csali fájl után jelenik meg. A MITRE szerint a technika Linux, Windows és macOS platformokon releváns.

Védekezési lehetőségek:

- File Analysis (D3-FA) - Rosszindulatú fájlok statikus és dinamikus elemzése ismert malware-jellemzők, exploitok vagy beágyazott payloadok azonosítása érdekében.
- File Integrity Monitoring (D3-FIM) - Fájlok változásainak folyamatos monitorozása. Segíthet a rosszindulatú állományok létrejöttének, módosításának vagy cseréjének észlelésében.
- Dynamic Analysis (D3-DA) - A fájl végrehajtásának sandbox vagy izolált környezetben történő megfigyelése a tényleges viselkedés feltárására.
- Emulated File Analysis (D3-EFA) - Emulációs környezetben végzett fájlelemzés, amely lehetővé teszi a rosszindulatú logika vagy rejtett funkcionalitás detektálását teljes végrehajtás nélkül.
- File Encryption (D3-FE) - Az állományok titkosítása csökkentheti a rosszindulatú fájlokhoz kapcsolódó adathozzáférési kockázatokat, valamint nehezítheti a támadó számára a kompromittált fájlok felhasználását.
- Restore File (D3-RF) - A fertőzött vagy módosított állományok helyreállítása megbízható forrásból vagy biztonsági mentésből.

Forrás: MITRE D3FEND - Malicious File - T1204.002

Detekciós stratégiák:

DET0294 - User Execution - Malicious File via download/open → spawn chain (T1204.002)

- AN0819 - A felhasználó e-mailből, webről, chatből vagy megosztásból származó fájlt nyit meg. A kezelőalkalmazás — például Word, PDF-olvasó vagy archívumkezelő — fájlt hoz létre felhasználó által írható útvonalon, például Downloads, Temp vagy Desktop könyvtárban, majd új vagy szokatlan gyermekfolyamatot indít, például

powershell.exe, wscript.exe, cmd.exe, regsvr32.exe, rundll32.exe vagy msiexec.exe. Opcionális előzményként figyelhető a FileStreamCreated esemény, URL/UNC eredet, illetve Office-folyamatok által létrehozott System32 batch fájlok.

- AN0820 - macOS környezetben a felhasználó letöltött dokumentumot vagy telepítőt nyit meg, amely EndpointSecurity fájllétrehozási eseményt eredményez a ~/Downloads vagy ~/Library útvonalakon, majd gyanús segédprogram végrehajtását indítja. Kiemelten figyelendő folyamatok: osascript, bash, zsh, curl, chmod, illetve open - a Terminal. A detekció a fájllétrehozási eseményeket későbbi process execution eseményekkel, opcionálisan quarantine vagy LSQuarantine eseményekkel korrelálja.
- AN0821 - Linux környezetben a felhasználó vagy egy desktop alkalmazás új fájlt ír a ~/Downloads, /tmp vagy csatolt eltávolítható adathordozó útvonalaira, majd ezt követően kockázatos interpreter vagy loader fut le. Példák: bash, sh, python, perl, php, node, curl|wget pipe-olva sh felé, ld.so, rdesktop, illetve xdg-open szokatlan argumentumokkal. A detekció auditd PATH és SYSCALL eseményeket — például open, creat, write, rename — kapcsol össze execve eseményekkel.

Mitigációs lehetőségek:

- M1040 - Behavior Prevention on Endpoint – Endpoint ASR/EDR szabályok alkalmazása Office, script interpreterek és e-mail kliensek által indított gyanús végrehajtások blokkolására.
- M1038 - Execution Prevention – Alkalmazáskontroll, allowlisting és végrehajtási korlátozások alkalmazása ál-dokumentumnak vagy legitim fájlnak álcázott futtatható állományok ellen.
- M1017 - User Training – Felhasználói tudatossági képzés phishing mellékletek, makróengedélyezés, jelszóval védett archívumok és megtévesztő fájlkiterjesztések felismerésére.

Forrás: MITRE ATT&CK – T1204.002 User Execution: Malicious File

T1059 – Command and Scripting Interpreter

A technika során a támadó parancsértelmezőket vagy szkriptnyelveket használ parancsok végrehajtására, további payloadok letöltésére, perzisztencia kialakítására vagy a fertőzés utáni tevékenységek végrehajtására.

Védekezési lehetőségek:

- File Analysis (D3-FA) - A szkriptállományok és parancsfájlok statikus vagy dinamikus elemzése rosszindulatú utasítások, obfuszkáció vagy ismert támadói minták azonosítása érdekében.
- File Integrity Monitoring (D3-FIM) - A szkriptek és konfigurációs állományok módosításainak monitorozása, különösen adminisztratív könyvtárakban vagy automatikus végrehajtási pontokon.
- Dynamic Analysis (D3-DA) - Parancsértelmezők és szkriptek futásidejű viselkedésének elemzése sandbox vagy monitorozott környezetben.
- Emulated File Analysis (D3-EFA) - A szkriptek emulációs környezetben történő vizsgálata a tényleges végrehajtás nélküli viselkedéselemzés érdekében.
- File Encryption (D3-FE) - A kritikus szkriptállományok és konfigurációk integritásának védelme, valamint az illetéktelen hozzáférés megnehezítése.
- Restore File (D3-RF) - A kompromittált vagy módosított szkriptek helyreállítása hiteles forrásból vagy biztonsági mentésből.

Forrás: MITRE D3FEND - Command and Scripting Interpreter - T1059

Detekciós stratégiák:

DET0516 – Behavioral Detection of Command and Scripting Interpreter Abuse

- AN1428 - Parancs- és szkriptértelmezők (pl. powershell.exe, cmd.exe, wscript.exe) végrehajtásának detektálása a megszokott adminisztrációs időablakokon kívül vagy rendellenes felhasználói kontextusból. Kiemelt indikátor az obfuszkált vagy Base64-kódolt argumentumok használata, illetve a másodlagos folyamatindítások megjelenése.
- AN1429 - Shell interpreterek (pl. bash, sh, python, perl) használatának észlelése olyan felhasználók vagy folyamatok által, amelyek normál működésük során nem futtatnak ilyen eszközöket. Különösen gyanús a netcat, curl, wget vagy ssh segédprogramokkal történő láncolt végrehajtás.
- AN1430 - Parancsértelmezők indításának detektálása Terminal, Automator vagy rejtett osascript folyamatokon keresztül, különösen akkor, ha a szülőfolyamat nem tipikus felhasználói alkalmazás.
- AN1431 - VMware ESXi környezetben az esxcli system parancsok vagy közvetlen interpreter-hívások (pl. BusyBox shell) váratlan használatának észlelése SSH vagy helyi konzol kapcsolatból.

- AN1432 - Hálózati eszközök CLI-interpretereihez (pl. Cisco IOS, Juniper JUNOS) történő hozzáférések azonosítása, különösen akkor, ha azokat szokatlan felhasználói fiókok vagy ismeretlen IP-címek használják.

Mitigációs lehetőségek:

- M1049 – Antivirus/Antimalware - Végpontvédelmi megoldások alkalmazása a rosszindulatú szkriptek, parancsfájlok és kapcsolódó állományok automatikus felismerésére és karanténba helyezésére.
- M1047 – Audit - A környezetben telepített parancsértelmezők és szkriptmotorok rendszeres felmérése az engedély nélküli vagy nem támogatott interpreterek azonosítása érdekében.
- M1040 – Behavior Prevention on Endpoint - Windows rendszereken Attack Surface Reduction (ASR) szabályok alkalmazása a Visual Basic, JavaScript és egyéb szkriptek által végrehajtott potenciálisan rosszindulatú műveletek blokkolására.
- M1045 – Code Signing - Csak digitálisan aláírt szkriptek és parancsfájlok futtatásának engedélyezése a jogosulatlan kódvégrehajtás csökkentése érdekében.
- M1042 – Disable or Remove Feature or Program - A nem használt vagy üzletileg nem indokolt parancsértelmezők és szkriptmotorok eltávolítása vagy letiltása.
- M1038 – Execution Prevention - Alkalmazásvezérlési megoldások alkalmazása. Például a PowerShell Constrained Language Mode használata korlátozhatja a veszélyes PowerShell-funkciók és API-hívások elérését.
- M1033 – Limit Software Installation - A felhasználók számára szükségtelen interpreterek és fejlesztői környezetek telepítésének korlátozása.
- M1026 – Privileged Account Management - A PowerShell használatának adminisztrátori jogosultsághoz kötése, valamint Just Enough Administration (JEA) alkalmazása a távoli PowerShell munkamenetekben végrehajtható parancsok korlátozására.
- M1021 – Restrict Web-Based Content - Scriptblokkoló böngésző-kiegészítők, HTA-blokkolás és reklámszűrők alkalmazása a webes környezetből érkező rosszindulatú szkriptek végrehajtásának megakadályozására.

Forrás: MITRE ATT&CK – T1059 Command and Scripting Interpreter

T1071.001 – Application Layer Protocol: Web Protocols

A technika során a támadó webes protokollokat, például HTTP-t, HTTPS-t vagy WebSocketet használ parancs- és vezérlési kommunikációra, adatszivárogtatásra vagy további payloadok letöltésére. A forgalom gyakran legitim böngésző- vagy alkalmazáskommunikációnak álcázódik, így nehezíti a hálózati detekciót.

Védekezési lehetőségek:

- Network Traffic Filtering (D3-NTF) – A kimenő HTTP/HTTPS forgalom szűrése és engedélyezési listák alkalmazása a nem jóváhagyott célállomások, domainek és IP-címek blokkolása érdekében.
- Outbound Traffic Filtering (D3-OTF) – Kritikus szerverek kimenő webes kapcsolatainak korlátozása kizárólag üzletileg indokolt célokra.
- Remote Terminal Session Detection (D3-RTSD) – Távoli terminálmunkamenetekből indított curl, wget vagy egyéb HTTP-kliens használat detektálása.
- Network Traffic Community Deviation (D3-NTCD) – A megszokott hálózati közösségi mintázatoktól eltérő HTTP/HTTPS kommunikáció azonosítása.
- Application Protocol Command Analysis (D3-APCA) – HTTP-fejlécek, URI-k, cookie mezők és WebSocket üzenetek elemzése C2-parancsokra vagy kódolt tartalomra utaló minták alapján.
- Network Traffic Signature Analysis (D3-NTSA) – Ismert rosszindulatú webes C2-minták, user-agentek, URI-struktúrák és TLS-jellemzők felismerése.
- Per Host Download-Upload Ratio Analysis (D3-PHDUA) – Rendellenes feltöltési-letöltési arányok vizsgálata, különösen POST-heavy vagy beacon jellegű kommunikáció esetén.
- Client-server Payload Profiling (D3-CSPP) – HTTP/HTTPS payloadok méretének, gyakoriságának és irányának profilozása szokatlan C2-csatornák felismerésére.
- Relay Pattern Analysis (D3-RPA) – Ismétlődő, közvetítő infrastruktúrán keresztül történő webes kommunikációs minták azonosítása.
- Protocol Metadata Anomaly Detection (D3-PMAD) – HTTP fejlécek, TLS handshake adatok, WebSocket upgrade kérések és egyéb protokoll-metaadatok anomáliáinak detektálása.
- User Geolocation Logon Pattern Analysis (D3-UGLPA) – Szokatlan földrajzi eredetű vagy rendellenes hozzáférések összekapcsolása webes C2-forgalommal.

Forrás: MITRE D3FEND – Web Protocols / Application Layer Protocol

Detekciós stratégiák:

DET0027 – Detection of Web Protocol-Based C2 Over HTTP, HTTPS, or WebSockets

- AN0075 – Váratlan vagy nagy volumenű HTTP/S/WebSocket kommunikáció detektálása gyanús folyamatokból, például PowerShellből vagy rundll32-ből, szokatlan user-agentekkel, illetve böngészőforgalmat utánzó kapcsolatokkal ritka domainek vagy IP-címek felé.
- AN0076 – curl, wget, Python requests vagy egyedi HTTP-kliensek azonosítása nem szabványos portokon, ismétlődő, beacon-szerű mintázatokkal vagy POST-domináns kommunikációval ritka domainek felé.
- AN0077 – Automator, AppleScript vagy LaunchDaemon komponensek által indított HTTP/S forgalom detektálása nem megszokott domainek felé, különösen gyanús fejlécek, Base64-kódolt URI-k vagy cookie mezők használata esetén.
- AN0078 – Shell alapú szkriptek vagy menedzsment démonok által kezdeményezett HTTP/HTTPS kommunikáció észlelése, különösen publikus IP-címek felé, 80/443-as portokon, beágyazott curl vagy wget használatával.
- AN0079 – Webes protokollokkal való visszaélés detektálása, például kódolt HTTP-fejlécek, rendellenes WebSocket upgrade kérések vagy TLS handshake anomáliák alapján, amelyek beágyazott C2-csatornára utalhatnak.

Mitigációs lehetőségek:

- M1037 – Filter Network Traffic – A kritikus szerverek kimenő HTTP/HTTPS forgalmának korlátozása és monitorozása kizárólag jóváhagyott célállomások felé. Ez csökkentheti annak lehetőségét, hogy a támadók curl, wget vagy más eszközök segítségével külső C2-szerverekkel kommunikáljanak vagy rosszindulatú payloadokat töltsenek le.
- M1031 – Network Intrusion Prevention – Hálózati behatolásdetektáló és -megelőző rendszerek alkalmazása, amelyek ismert rosszindulatú minták, hálózati szignatúrák, anomáliák és malware-specifikus webes kommunikáció alapján képesek a támadói aktivitás blokkolására vagy riasztására.

Forrás: MITRE ATT&CK – T1071.001 Application Layer Protocol: Web Protocols

T1078 – Valid Accounts

A technika során a támadó érvényes felhasználói hitelesítő adatokat használ fel kezdeti hozzáférés megszerzésére, perzisztencia fenntartására, jogosultság-emelésre vagy a védekezési mechanizmusok megkerülésére. A kompromittált helyi, tartományi, felhőalapú vagy alapértelmezett felhasználói fiókok lehetővé teszik a legitim felhasználói tevékenységnek álcázott hozzáférést, amely jelentősen megnehezíti a támadói jelenlét felismerését. A támadók gyakran VPN-, SSH-, RDP-, felhőszolgáltatások vagy identitáskezelő rendszerek (IdP) segítségével használják fel a megszerzett hitelesítő adatokat, illetve kihasználhatják az inaktív vagy elfelejtett felhasználói fiókokat is.

Védekezési lehetőségek:

- Local Account Monitoring (D3-LAM) – A helyi felhasználói fiókok folyamatos monitorozása rendellenes bejelentkezések, jogosultságváltozások és újonnan létrehozott fiókok azonosítása érdekében.
- Domain Account Monitoring (D3-DAM) – Tartományi felhasználói fiókok hitelesítési eseményeinek és jogosultságmódosításainak elemzése a kompromittált hitelesítő adatok felismerésére.
- Account Locking (D3-AL) – Fiókzárolási szabályok alkalmazása ismétlődő sikertelen hitelesítési kísérletek esetén a brute force és jelszópróbálgatási támadások megakadályozására.
- Agent Authentication (D3-AA) – Eszközök és szolgáltatások kölcsönös hitelesítésének alkalmazása annak biztosítására, hogy kizárólag megbízható rendszerek használhassanak érvényes felhasználói fiókokat.
- Change Default Password (D3-CDP) – Az alapértelmezett felhasználói fiókok jelszavainak azonnali módosítása és erős hitelesítő adatok alkalmazása a kezdeti kompromittálás megelőzése érdekében.

Forrás: MITRE D3FEND – Valid Accounts

Detekciós stratégiák:

DET0560 – Detection of Valid Account Abuse Across Platforms

- AN1543 – Kompromittált vagy jogosulatlanul használt felhasználói fiókok detektálása rendellenes bejelentkezési minták, szokatlan hitelesítési típusok, illetve földrajzi vagy időalapú anomáliák alapján Windows végpontokon.

- AN1544 – Érvényes hitelesítő adatokkal végrehajtott SSH-bejelentkezések, sudo/su jogosultság-emelések és szolgáltatásfiókok rendellenes használatának felismerése a megszokott működési mintáktól eltérő esetekben.
- AN1545 – Szolgáltatásfiókok vagy felhasználói fiókok interaktív, illetve távoli bejelentkezéseinek detektálása szokatlan időpontokban, különösen akkor, ha ezt váratlan gyermekfolyamatok indítása követi.
- AN1546 – Identitásszolgáltatók (IdP) naplóiban megjelenő rendellenességek észlelése, például lehetetlen utazás (Impossible Travel), földrajzi anomáliák, kockázatos bejelentkezések, illetve ismétlődő MFA-kérések vagy sikertelen hitelesítések alapján.
- AN1547 – Kubernetes szolgáltatásfiókok vagy kompromittált kubeconfig állományok használatának detektálása váratlan csomópontokról vagy IP-címekről történő klaszterhozzáférések során.

Mitigációs lehetőségek:

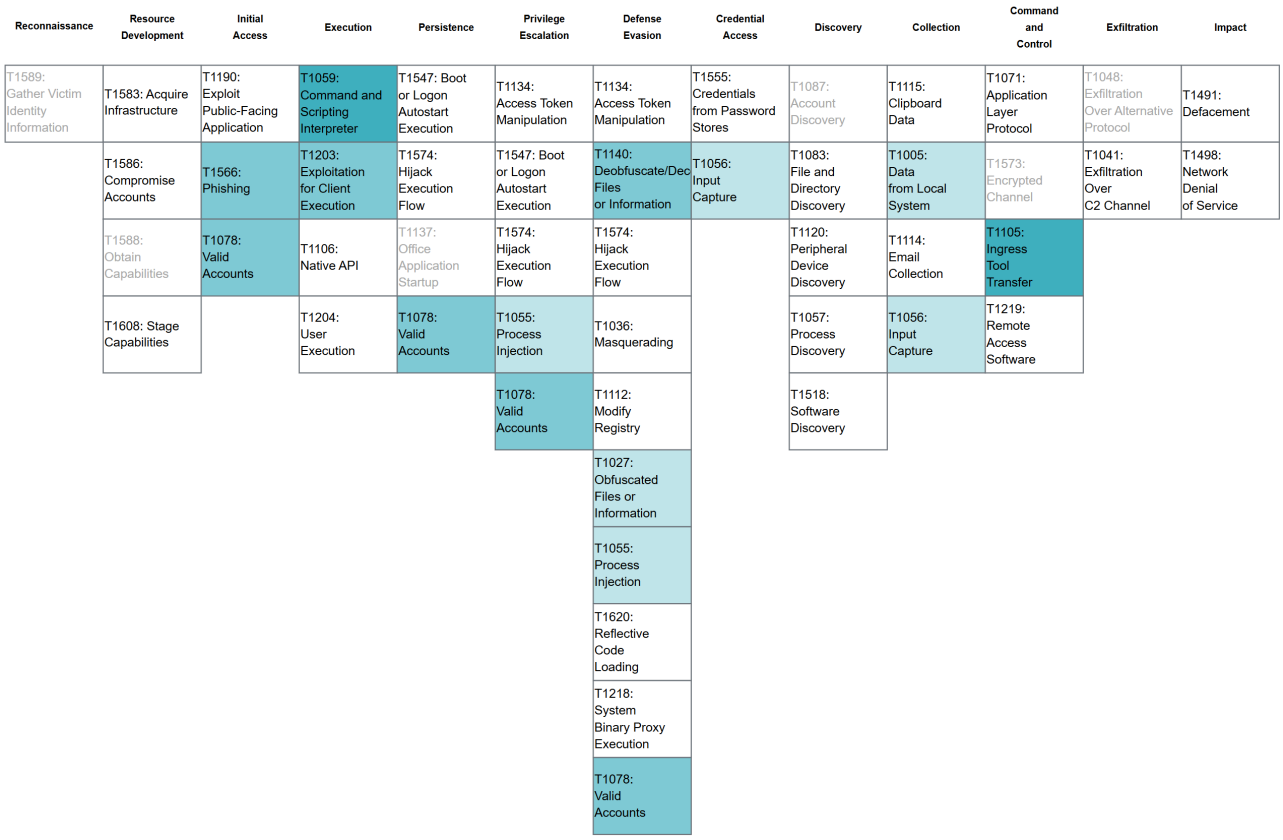
- M1036 – Account Use Policies – Feltételes hozzáférési (Conditional Access) szabályok alkalmazása a nem megfelelő állapotú eszközökről vagy nem engedélyezett IP-tartományokból érkező bejelentkezések blokkolására.
- M1015 – Active Directory Configuration – A régi hitelesítési protokollok letiltása és a modern, többtényezős hitelesítést támogató mechanizmusok használatának kikényszerítése.
- M1013 – Application Developer Guidance – Gondoskodni kell arról, hogy az alkalmazások ne tároljanak hitelesítő adatokat nem biztonságos módon (például forráskódban, publikus repositorykban vagy felhőtárolókban).
- M1032 – Multi-factor Authentication – Többtényezős hitelesítés (MFA) alkalmazása valamennyi fióktípus esetében (helyi, tartományi, alapértelmezett és felhőalapú), amely jelentősen csökkenti a kompromittált hitelesítő adatokkal végrehajtható jogosulatlan hozzáférések kockázatát.
- M1027 – Password Policies – Erős jelszóházirendek bevezetése, az alapértelmezett jelszavak azonnali lecserélése, a jelszó-újrafelhasználás tiltása, valamint az SSH-kulcsok rendszeres cseréje és megfelelő védelme.
- M1026 – Privileged Account Management – A privilegizált helyi és tartományi fiókok rendszeres felülvizsgálata, jogosultságaik

minimalizálása, valamint a jogosulatlanul létrehozott vagy engedélyezett fiókok azonosítása.

- M1018 – User Account Management – A felhasználói fiókok rendszeres auditálása, valamint a már nem használt vagy inaktív fiókok letiltása vagy eltávolítása.
- M1017 – User Training – A felhasználók oktatása az MFA push értesítések biztonságos kezelésére, a gyanús hitelesítési kérelmek felismerésére és jelentésére.

Forrás: MITRE ATT&CK – T1078 Valid Accounts

MITRE ATT&CK mapping / ábra



1. kép:

A vizsgált csoport támadási technikái aggregált formában láthatók: A sötétebb szín magasabb előfordulási gyakoriságot vagy több csoport általi alkalmazást jelez. Forrás: MITRE ATT&CK® Navigator.

Megjegyzés: A FrostyNeighbor TTP-profilja alapján a legfontosabb védelmi fókuszterületek: phishing ellenállóképesség, végponti script- és LOLBin-monitorozás, identitásalapú detekció, HTTP/S C2 anomáliák felismerése, valamint exfiltrációs viselkedés korai azonosítása. A technikák alapján a

csoport képes legitim felhasználói tevékenységnek álcázott műveletekre, ezért a detekciót nem kizárólag indikátorokra, hanem viselkedésalapú korrelációra érdemes építeni.

Jelentősebb támadások és kampányok

A FrostyNeighbor csoport közel egy évtized alatt számos, jól dokumentált kampányt hajtott végre. Az alábbiakban a hét legjelentősebb kampányt mutatjuk be időrendben, hangsúlyozva az alkalmazott módszereket, célpontokat és az adott kampány geopolitikai kontextusát.

Dezinformációs kampánysorozat (2016-2022)

A kampány elsődlegesen NATO-ellenes narratívák terjesztését célozta a balti államokban (Észtország, Lettország, Litvánia) és Lengyelországban, kihasználva az oroszajkú kisebbségek kulturális kötődését. A csoport hamis híreket tett közzé a kompromittált médiaszerverek weboldalain, mintha azok eredeti szerkesztőségi tartalomkent jelennének meg.

Alkalmazott módszerek

- Hírportálok CMS-rendszereinek feltörése, hamis cikkek közzététele eredeti újságírók nevében
- Hamis dokumentumok gyártása: pl. állítólagos NATO-dokumentumok a csapatkivonásról a balti régióból
- Személyazonosság-hamisítás: kormánytisztviselők, katonai személyek nevével küldött e-mailek
- Hamis levelezés orosz-belarusz újraegyesítési megállapodásról
- Ukrán weboldalak megrongálása (defacement) hamis ukrán kapitulációt hirdető üzenetekkel

Koordinált kibertámadások Ukrajna ellen (2022 január- február)

Azonosított akciók

- **Webmail-célzás:** 2022. január - február: Tömeges spear phishing kampány ukrán katonai személyzet webmail fiókjai ellen.
- **Facebook befolyásoló műveletek:** 2022. február 27.: A Meta (Facebook) nyilvánosságra hozta, hogy a FrostyNeighbor ukrán katonai személyek és közszereplők Facebook-fiókjait próbálta feltörni,

majd ezekről dezinformációs YouTube-videókat terjesztett, amelyeken ukrán csapatok megadását ábrázolták hamisan.

- **MicroBackdoor terjesztés:** 2022. március 4-7.: A CERT-UA MicroBackdoor-mintákat azonosított, amelyeket egy .zip fájlban terjesztettek. A zip tartalma az SBU, az Elnöki Hivatal és a Minisztertanács logóival ellátott hamis ukrán kormányzati értesítés volt, bombázásokra hivatkozva.
- **Dworczyk-ügy (Lengyelország):** Michał Dworczyk lengyel miniszterelnöki kancellária vezetőjének postafiókját kb. 60 000 e-maillel kompromittálták.

Browser-in-the-Browser phishing kampány- lengyel webmail célzás (2022)

2022 márciusától a FrostyNeighbor egy új, kifinomult adathalász technikát alkalmazott: a Browser-in-the-Browser (BitB) módszert. Ez a technika egy megtévesztően valósnak látszó, a böngészőablakon belül megjelenő hamis bejelentkezési popup-ot jelenít meg, amely legitim OAuth-bejelentkezési folyamatot utánoz. A megszerzett hitelesítő adatokat közösségi média fiókok kompromittálására használták.

PicassoLoader többfázisú kampányok - Ukrajna és Lengyelország (2022-2024)

2022 áprilisától a PicassoLoader kampányt a FrostyNeighbor csoporthoz kötötték. A kampány legalább 2024 közepéig aktív maradt, és az egyik legkomplexebb, több fázisból álló fertőzési láncot alkalmazta a csoport eddigi tevékenységei közül.

Kiemelt incidensek

- **2023. aug.:** PPT-dokumentum ('daewdfq342r.ppt') makróval - PicassoLoader - Cobalt Strike Beacon.
- **2024. jul. 12-18.:** PicassoLoader + Cobalt Strike kampány ukrán helyi önkormányzatok és USAID-kapcsolt szervek ellen.
- **2024. apr.:** az Ukrán védelmi Minisztériumot célozta kiberkémkedési művelet keretében.

Fertőzött Excel-kampány - belarusz ellenzék és ukrán hadsereg (2024-2025)

A csoport 2024-től párhuzamosan célozta a Lukasenko-rezsim ellenzékét és az ukrán kormányzatot is. A terjesztési vektor egy Google Drive link volt egy 'Vladimir Nikiforech' (vladimir.nikiforeach@gmail[.]com) névvel küldött phishing e-mailben, amelyen keresztül RAR archívum tölthető le a fertőzött Excel-fájlokkal. A PicassoDownloader variáns, a bruhdll32.dll, a Macropack-obfuszkáció és a célzási mintázat alapján köthető a kampány a FrostyNeighbor csoporthoz.

Roundcube CVE-2024-42009 kihasználás - lengyel szervezetek (2025. június)

2025. június 5-én a CERT Polska spear phishing kampányt azonosított lengyel szervezetek ellen, amely nagy bizonyossággal a FrostyNeighbor csoporthoz köthető. A kampány a CVE-2024-42009 azonosítójú Roundcube webmail sebezhetőséget használta ki, amely rosszindulatú JavaScript kód böngészőben történő futtatását teszi lehetővé.

OYSTERFRESH és OYSTERBLUES kampány (2026. március-)

2026 márciusától dokumentálták a csoport legfrissebb kampányát. A célpontok ukrán helyi önkormányzatok. A kampány több szempontból is technikai evolúciót mutat a korábbi kampányokhoz képest.

Gmail phishing kampány (2026. március-)
2026. márciusától a csoport intenzív spearphishing kampányt folytat lengyel Gmail-felhasználók ellen. A kampány célja a lengyel politikusok, újságírók, kutatók és hivatalnokok Gmail fiókjának átvétele, ahol a támadók a jelszavak mellett a kétfaktoros azonosítás (2FA) kódokat is ellopják. A rosszindulatú üzenetek Google biztonsági figyelmeztetéseknek mutatják magukat, és a link megnyitásakor egy a Gmail bejelentkező felületét utánzó hamis oldalon kérnek be a felhasználóadatokat.

Belarusz célpontok, Gmail phishing kampány (2026)
2026 júniusában egy belarusz politikust és más kapcsolódó célpontokat céloztak hamis Google bejelentkezési oldalakkal. A támadás célja elsősorban a Gmail fiókokhoz tartozó felhasználónév, jelszó és 2FA-kód megszerzése

volt, amiket valós időben továbbítottak egy websocketen keresztül. A támadók nem egyetlen, elszigetelt oldalt használtak, hanem több, egymással összefüggő phishing-infrastruktúrát építettek ki kompromittált weboldalakra, CDN-ek mögé rejtve.

Új technikai elemek

- **PDF-alapú csali** dokumentumok, amelyek Prometheus online tanulási platformhoz kapcsolódó tartalomként jelennek meg.
- **Victim validation, szerveroldali geofencing:** a C2 ellenőrzi az áldozat IP-címének földrajzi helyzetét, és csak ukrán IP-tartományokból érkező kérésekre küldi a rosszindulatú payloadot. Ez megnehezíti a sandbox elemzést.
- **OYSTERFRESH loader:** JavaScript-alapú loader; a neve egy GitHub repo-ban jelent meg 2026. május 25-i dátummal.
- **OYSTERBLUES (registry-persisted):** Registry perzisztenciával rendelkező komponens (T1547.001 – Registry Run Keys / Startup Folder).
- **Végső payload** ebben a kampányban is Cobalt Strike Beacon, amelyet a PicassoLoader installál.

Megjegyzés: Az OYSTERFRESH és OYSTERBLUES elnevezések a GitHub általános tárolóból (repository) származnak.

Védekezési ajánlások

A FrostyNeighbor elleni védekezés során nem elegendő kizárólag technikai kontrollokra támaszkodni. A csoport elsődleges erőssége a célzott adathalászat, a hitelesítő adatok megszerzése, valamint az információs műveletekkel kombinált kompromittálás. A csoport által fenyegetett szektorok alapján különösen javasolt a kormányzati, védelmi és kritikus infrastruktúrákat üzemeltető szervezetek felkészítése a csoport támadásaival szemben, melyek ellen a sérülékeny, távolról kihasználható sebezhetőségek mielőbbi javításával, a felhasználói tudatosság növelésével, valamint szigorú hitelesítési és jelszóházirendek alkalmazásával védekezhetnek a szervezetek.

A csoport által rendszeresen alkalmazott spear phishing kampányok miatt kiemelten fontos a többtényezős hitelesítés (MFA) alkalmazása valamennyi internet felől elérhető szolgáltatás esetében, különös tekintettel a webmail-rendszerekre, felhőalapú szolgáltatásokra és közösségi médiafiókokra. Az MFA bevezetése mellett javasolt a feltételes hozzáférési szabályok

(Conditional Access) alkalmazása, az ismeretlen eszközökről vagy földrajzi helyekről történő bejelentkezések korlátozása, valamint az anomáliaalapú identitásfigyelés bevezetése.

Mivel a FrostyNeighbor rendszeresen használ legitim felhasználói fiókokat a kompromittálást követő műveletek végrehajtására, különös hangsúlyt kell fektetni az identitásalapú fenyegetésfelderítésre. Javasolt az új eszközről történő bejelentkezések, a rendellenes munkarenden kívüli hitelesítések, valamint az adminisztratív jogosultságok szokatlan használatának monitorozása és automatikus riasztása.

A csoport által alkalmazott malware-ek (PicassoLoader, OYSTERFRESH, OYSTERBLUES, Cobalt Strike Beacon) és scriptalapú fertőzési láncok miatt indokolt a korszerű EDR/XDR-megoldások alkalmazása. A védelemnek különösen fókuszálnia kell a PowerShell, wscript.exe, cscript.exe, mshta.exe, rundll32.exe és regsvr32.exe folyamatok monitorozására, valamint a szokatlan szülő-gyermek folyamatkapcsolatok detektálására. Javasolt az Office-alkalmazásokból indított végrehajtható állományok és szkriptek blokkolása, illetve az Office-makrók alapértelmezett tiltása.
A dokumentált kampányok alapján a csoport gyakran használ sérülékeny webmail- és kliensoldali alkalmazásokat kezdeti hozzáférés megszerzésére. Ennek megfelelően kiemelt prioritású a sebezhetőségkezelési folyamatok megerősítése, különösen a különböző webmail alkalmazások, illetve Microsoft Windows, Office és egyéb Microsoft-termékek esetében. Javasolt a magas kockázatú, internet felől elérhető rendszerek rendszeres sérülékenységvizsgálata és a kritikus javítások gyors telepítése.

A FrostyNeighbor által alkalmazott HTTP/HTTPS-alapú parancs- és vezérlőkommunikáció miatt célszerű hálózati szinten is viselkedésalapú detekciós képességeket kialakítani. A ritkán használt külső domainek, az alacsony reputációjú infrastruktúrák, valamint a rendellenes TLS-paraméterek és User-Agent értékek monitorozása hozzájárulhat a kompromittáció korai felismeréséhez.

A csoport műveleteinek jelentős része információs és befolyásolási komponenseket is tartalmaz, ezért a technikai védelem mellett fontos a szervezeti kommunikációs és incidenskezelési felkészültség fejlesztése. A kormányzati és védelmi szervezetek számára javasolt olyan eljárásrendek kialakítása, amelyek lehetővé teszik a kompromittált kommunikációs

csatornák, hamis dokumentumok vagy manipulált médiatartalmak gyors hitelesítését és cáfolatát.

Források

https://malpedia.caad.fkie.fraunhofer.de/actor/frostyneighbor
https://brandefense.io/blog/ghostwriter-apt-2025/
https://csirt.csi.cip.gov.ua/en/posts/uac-0057-ghostwriter
https://www.sentinelone.com/labs/ghostwriter-new-campaign-targets-ukrainian-government-and-belarusian-opposition/
https://www.eset.com/us/about/newsroom/research/belarus-frostyneighbor-attacks-ukrainian-government-eset-research/
https://cloud.google.com/blog/topics/threat-intelligence/unc1151-linked-to-belarus-government/
https://cloud.google.com/blog/topics/threat-intelligence/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity/
https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/
https://blog.talosintelligence.com/malicious-campaigns-target-entities-in-ukraine-poland/
https://www.gov.pl/web/special-services/russian-cyberattacks
https://mitre-attack.github.io/
https://cybernews.com/news/meta-bans-ghostwriter-hacker-group/
https://cloud.google.com/blog/topics/threat-intelligence/ghostwriter-influence-campaign
https://www.nytimes.com/2022/04/07/world/europe/russia-hackers-facebook-disinformation.html
https://therecord.media/ghostwriter-targets-personal-gmail-accounts-in-poland

Függelék

Kihasznált sebezhetőségek

Azonosító	Sűlyosság	Termék	Ismerten kihasznált
CVE-2022-30190 (Follina)	Magas	MS Windows 7 (Service Pack 1), 8.1, 10 (Version 1507, Version 1607, Version 1809, Version 20H2, Version 21H1, Version 21H2); MS Windows Server 2008 R2, 2012 (R2), 2016, 2019, 2022 Microsoft Support Diagnostic Tool (MSDT) in Windows	Igen: 2022-06-14
CVE-2023-38831	Magas	RARLAB WinRAR < 6.23	Igen: 2023-08-24
CVE-2024-42009	Kritikus	Roundcube 1.5.7, 1.6.0 – 1.6.7	Igen: 2025-06-09

Indicators of Compromise

Domain

poczta.kontrola-bezpieczenstwa.website
net-verify.website
interia-pl.website
jorgava.com
authorization-inbox.site
wp-pl-potwierdz-dostep.site
interia.walidacja-konta.space
groups-signal.site
group-teneta.online
mirrohost.space
login-microsoftonline.site
signal-security.online
interia.kontrola-bezpieczenstwa.space
walidacja-uzytkownika.site
verify-email.space
login-inbox.online
weryfikacja-uzytkownika.site
hatdfg-rhgreh684.frge.io
teneta.join-group.online
ron-mil.space
group.kropyva.site
i-ua.site
empoweringparents.shop
op-pl.site
ukroboronprom.online
aplikacje.ron-mil.space
mirohost.online
walidacja-konta.space
post-mil-gov.com-verify.site
command-email.online
secure-firewall.website
sciencealert.shop
com-validate.site
signin-inbox.online
ua-passport.online
group-signal.com
verify-check.digital
consumerspanel.frge.io

secure-firewall.site
kontrola-poczty.space
ua-consumerpanel.frge.io
net-support.site
com-verify.site
konto.weryfikacja-poczty.space
creditals-mirohost.space
account-logins.online
com-firewall.online
book-happy.needbinding.icu
weryfikacja-uzytkownika.website
sprawdzanie-konta.space
telekom-dienste.online
frge.io
poczta.walidacja-konta.space
meta-ua.online
sprawdzanie-poczty.space
sign-in-inbox.site
interia-firewall.site
helperanalytics.ru
domtern.com
service.walidacja-konta.space
add-signal-groups.com
nama-belakang.nebao.icu
signal-protect.host
mirohost.site
accounts.verify-email.space
accounts.secure-ua.website
net-firewall.online
ua-agreements.online
interia.sprawdzanie-konta.space
post.verify-mail.space
login.walidacja-poczty.space
www.walidacja-poczty.space
konta-24weryfikacja.netlify.app
mickeymousegamesdealer.alexavegas.icu
konto-verify.space
signin-telekom.online
signal-security.site
anabapress.com
kontrola-bezpieczenstwa.online
ru-mailbox.site
mail-validation.online
net-account.space
signal-group.tech
verify-ua.online
signal-group.site
kontrola-bezpieczenstwa.space
goudieelectric.shop
a.mpk-krakow.pl
mail.mirrohost.space
passport.command-email.online
ron-mil-pl.space
secure-ua.site
service.kontrola-poczty.space
teneta.group
signals-group.com
login-verify.online
login.creditals-email.space
bigmir.space
check-mail-verify.biz
net-verify.site
signalgroup.site
mod-mil.online
net-account.online
shinesafar.sardk.icu
meta-ua.space
interii.konto-verify.space
confirm-signal.site
wp-agreements.online
weryfikacja-uzytkownika.space
onet-pl.online
safe-onet.online
id-unconfirmeduser.frge.io
thevegan8.shop
mirohost-creditals.space
weryfikacja-konta.space
inbox-admin.site
backstagemerch.shop
walidacja-uzytkownika.online
wp-firewall.website
safe-onet.space
login-mail.online
login-yahoo.site
kontrola-poczty.site
accounts-login.online
account-inbox.online
walidacja-uzytkownika.space
pis.kontrola-bezpieczenstwa.site
i.ua-passport.space
logowanie-pl.site
service.verify-mail.space
login-telekom.online
everythingandthedog.shop
kontrola-bezpieczenstwa.site
credentials-telekom.online

akademia-mil.space
poczta.kontrola-bezpieczenstwa.site
wirtualna-polska.online
login-inbox.site
signal-groups.tech
mil-gov.space
post.mil-gov.space
login.verify-mail.space
service-auth.netlify.app
cache-pdf.com
golgba.com
mailverify.digital
signal-device-off.online
i.ua-passport.top
kontrola-bezpieczenstwa.website
creditals-email.space
verify-ua.site
mil-secure.site
poczta.walidacja-uzytkownika.space
verify-ua.space
best-seller.lavanille.buzz
potwierdzenie.site
teneta.add-group.site
pigglywigglystores.shop
pis.kontrola-bezpieczenstwa.website
easiestnewsfromourpointofview.algsat.icu
accounts-telekom.online
ua-passport.site
signal-groups-add.com
dd-signal-group.com
ru-passport.online
hinesafar.sardk.icu
americandeliriumsociety.shop
everything-everywhere.at.ply.gg
com-account.website
mod-mil.site
monitoring-google-konta.netlify.app
signal-confirm.site
safe-control.space
xbeta.online
signal-groups.site
walidacja-uzytkownika.website
cookingwithbooks.shop
weryfikacja-poczty.space
id.bigmir.space
verify-mail.space
konto.weryfikacja-uzytkownika.space
ua-login.site
walidacja-poczty.space
signal-group-add.com
wp-potwierdzac.site
secure-ua.website
attachment-storage-asset-static.needbinding.icu
verify.rambler-profile.site
net-verification.online
lauramcinerney.shop
is-lt.online

IP

2001:67c:e60:c0c:192:42:116:216
150.107.31.194
185.170.144.158
185.156.177.92
136.144.41.177
185.175.158.27
194.110.248.92
162.241.216.236
84.32.188.96
185.244.180.13
31.41.45.112
64.190.113.51
185.143.223.29
94.131.108.109
5.199.174.219
5.199.173.152
185.170.144.159
157.230.104.79
87.251.64.5

Hash

a97a28276e4f88134561d938f60db495
00ae9c36c0ebce87efcd63852716ed88599d0ba8bf117ad1771a35b9c67e3402
eaf3fd4dd5f6ea621ddc1bbccd5626cfa47bd3f8370c254866d9540dfda24374
a7b7691baa21ad118348661a035b69605a6efd1cd1fa0fd52e5645c64f5f61e6
1c118d8fb0be904b129e4552f86cd0b3e239ecd25f4d599c54cc96c1096747af
22af576e3c9ff82d2ddf45701e9f0db5ec6320ab9837d39d5d9d76d15a084f16
dd61887d5cdf361a335fec917cd6d1bb186aad56b1f9f5d09b66355ff7f41751
651e551854a4d949c4168efd6ae374f20e7951ad09fbea0e7d03456072644a99
e41b3bdbfb816d5cfd4b235d2b985894153c41da6726ebfa83e45f3b5b4a1945
51f6b8dfcbe757f5df935203369da894c45727028d972b1207e449d0a592f7e2
ce5481496b58ef0bdf43d650bc8b70db5a2e03b1f8f42e30002bc95d9be8fe03
d90f6e12a917ba42f7604362fafc4e74ed3ce3ffca41ed5d3456de28b2d144bf
bc6932a0479045b2e60896567a37a36c
af8104e567c6d614547acb36322ad2ed6469537cd1d78ae1be65fbde1d578abc
72721f96599ab1191d2588e1a8001cc76f9bd8968fa4708dff153b1383b37aeb
6fded427a16d5314ba3e1eb9afd120dc84449769
2e1de7b61ed25579e796ec4c0df2e25d2b98a1f8d4fdb077e2b52ee06c768fca
2c06c01f9261fe80b627695a0ed746aa8f1f3744
27fa11f6a1d653779974b6fb54de4af47f211232
a7694687ac179a48f07d306ed1b08cd60e9aa7063ee91ab64b0a50ddd7371378
18bcc91ad3eed529d44926f4ae65acf44480f39d
5969180b072703709764d1ca40be3eeb40f2eb0090859b3743cc21b884fa2106
3670115fa5fac918ad0dafe399568788690f0f205dd0bebe4f55180fd70d36e9
15fd138a169cae80fecf4c797b33a257d587ed446f02ecf3ef913e307a22f96d
976b7b17f2663fee38d4c4b1c251269f862785b17343f34479732bf9ddd29657
9a5a37b16350da20f86553df67eb7edf2142e1d36da1fcf99cacc6a74cc03730
d10fbef2fe8aa983fc6950772c6bec4dc4f909f24ab64732c14b3e5f3318700c
02b77a482120b7997f06da67f33cdb286ab06b7ef1bd9dfb2ad77a634595abfe
343afa62f69c7c140fbbf02b4ba2f7b2f711b6201bb6671c67a3744394084269
e5ebc7deca1ff1f0a4b1462d37ef813dad8413a6
b1997a5bb5da44e05e05935ebe79d44f11358b8d8da7d4a99ad3e0367b5c567e
6e6f5bebd6bf0fd0b626d6521cdb4faa06275f558bacd419c76702e2728f734c
27a061daee3ec9cff928b8152159a472797821834a3aa7639749489b90f703c3
4e52c92709a918383e90534052aaa257ace2780c
a3cf45b6206bedee45c45b6ccdc8be98
6837c16dce562abf4c55949cfc8d00b019f7fcc6db6a2e9a71d268312fba813e
8a7fbafe9f3395272548e5aadeb1af07baeb65d7859e7a1560f580455d7b1fac
0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32
ad8e3ebd496fb4d97e5075adb4f2f1b91195cca059800d0acd182a07698c13b6
00fdb03518c238dc649a39e94f0bcc95dacf3b832979d14d0ed5194b9b482b87
745e8c90a8e76f81021ff491cbc275bc134cdd7d23826b8dd23e58297fd0dd33
f063766d0481194829be3c5db209bfcf
4a00b428a6513ea69a7185903f773bf8008e862ac295be86ef26536001ba17ef
3694f63e5093183972ed46c6bef5c63e0548f743a8fa6bb6983dcf107cab9044
d7edb2ef6e95cbd77368ba5f5644d67c4de23feea9336bd324146b8abd63eab1
a9dcaf1c709f96bc125c8d1262bac4b6

f97f26f9cb210c0fcf2b50b7b9c8c93192b420cdbd946226ec2848fd19a9af2c
027e50b96e1683f22c448f9c7157f518d7d8f887c22862df3837fcfee558a6f2
4cedec3e1a2f72a917ad9a59ebe116ed50c3268567946d1e493c8163486b888b
924d3589d642e8fd65746dc156ff9f104d43114a04ea9509f51ee6a439d1915b
00030b0db567afa524eb68faf6f194f25bc5361c380599668a82dbae12af088e
2318ae5d7c23bf186b88abecf892e23ce199381b22c8eb216ad1616ee8877933
20180a8012970453daef6db45b2978fd962d2168fb3b2b1580da3af6465fe2f6
853da593d2a489c2bd72a284a362d7c68c3a4d4c
67e282aeadd040e14519a3755e526228a0e91472520728d258568cf61e68097f
991a19fb00cda372dd1ce4a42580dc40872da5c5bfbb34301615f3870ea3fb58
df33b1187c20582560ffaa1c3e86b92003c4a7c8a61acbbe886ab195531c5c89
a032348d09c21894b14e9accee0bfd4a14b9dfda6f113cfc1476f45bec500135
a3f3402656fc5be4439899b2a5f25eb6
7bf33b494c70bd0a0a865b5fbcee0c58fa9274b8741b03695b45998bcd459328
ab6c70af19f7d41a443feb8ccb57d264
5f590fbd8307c7568737b62379a1fc0559308c7f29cb31920aa64097ffc0ca56
3fa7d1b13542f1a9eb054111f9b69c250af68643
41f050f3d003edd67ec02710c60a7b4022685465cb61ae37fc0b3193c1dab5cb
88c97af92688d03601e4687b290d4d7f9f29492612e29f714f26a9278c6eda5b
7f29c3ea5b8fbd8b8ab6f7b508b6f8b6fa68fdebfec928f57f203bdef63b1c08
d3bddb5de864afd7e4f5e56027f4e5ea
b2434817428c6e38e435343db0d758498ba73952703c9d835f8ba62cbd36763d
7b95747eeea196c1485d089fa47a06bacb07d06399603d3a4fa153c21ce0a9ba
4ae6b8adc980ba8a212b838f3ca6a9718d9a3757
269526c11dbb25b1b4b13eec4e7577e15de33ca18afa70a2be5f373b771bd1ab
a5fb6b9417e50bd2260afdcdb5a9eed33e48a283a51408344a4caa2b1025b9a7
7a9a5317a88afb53b44f6cfed59c48907f63aaa7ef63b1587f990951c423c211
6f4642a203541426d504608eed7927718207f29be2922a4c9aa7e022f22e0deb
23cf0517359c014a8d25085eceb2cb25
08fa6aaf064470dbfac7894469457b2d78541adccba3f1bb278dd4c3f936131a
52f371a4f06f3398a5a361335920618c
3c62b24594ec3cacc14bdca068a0277e855967210e92c2c17bcf7c7d0d6b782a
37c7b934661f31e526ffb31f7c935d5a
bc92a5b1c4205ea1fbfec9144b8aab485e095142c7105c9d616b089ec668f198
7261ad5d4e760aa88df94b734bc44598a090852a
e9bbe7c6705a6f5a78c2a9b8060a7e32374b81058f7c2f24851c4d1ea38d7411
eca4273d922a66eb943a4bd1fd73ee4bd196289e32fe629cfe4ecf99e4cfadd3
e89612f017334f1bea536095abda92ded478a56ea4dce5e293222ce99a3e0c91
b1864aed85c114354b04fbe9b3f41c5ebc4df6d129e08ef65a0c413d0daabd29
f11310f075171f8502bcd32dcb2fe5894808b17a37f6fd960fb26653871e7b7d
501d4741a0aa8784e9feeb9f960f259c09cbceccb206f355209c851b7f094eff
70cea07c972a30597cda7a1d3cd4cd8f75acad75940ca311a5a2033e6a1dd149
fb418bb5bd3e592651d0a4f9ae668962
9d110879d101bcaec7accc3001295a53dc33371f
2b3617ae3fb743eaf604d0d3d36b68cf249dbeb180f06c8d0f3d60ccc3cc4b43
14ae02c521b85e60b11393ffc0da5e25946c4775a84995800b73398df4bceffb
bd65d0d59f6127b28f0af8a7f2619588
30d46a740e2677c8fee383c2a4762561a10c66c5b99215262e42bfabf6bfb1aa
ce96fe99ebe30ae44e74c22c0b2a055005d0da131e0082a1c290ddeb79dd1114

394cbab9eb87ef8ee795d184137ac2634b22a0a3e642534a55c1623a813c8a59
720df41451f9de8d863fce8c90310cd9f14dabe2519f98580c963784628eea55
18151b3801bd716b5a33cfc85dbdc4ba84a00314
d2a795af12e937eb8a89d470a96f15a5
df4724e21d9dea9b3e7f38b1ad905ad1922d30b6142da01c0218ed80644ca22a
83545b07d74087acd8408d7810cafdb6c2200a72ae7dd990af40b082ad533368
7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152
c0c455cd3e18be14d2e34cf4e3fb98e7ab0a75ef04b6049ff9f7b306d62704b8
776a43e46c36a539c916ed426745ee96e2392b39
301ffdf0c7b67e01fd2119c321e7ae09b7835afc
b7ef3c08cea0c50a43a7e3904f386189bd92f5da2920f026febc9f42c4de109d
e15abee1cfde8be7d87c7c0b510450bad6bc0906
85851e09b368ebba90f5d922cd77f348
0397c586fa56e672db7f14afa8c19992b6e08ab0c1d282c960df1af26371bd72
4da99f963c26bcc4537ba0437c9cc1445be8bea64067d34308dda6c2e49c8c65
b65551d339aece718ea1465bf3542c794c445efc
5b317f27ad1e2c641f85bef601740b65e93f28df06ed03daa1f98d0aa5e69cf0
43e30be82d82b24a6496f6943ecb6877e83f88ab
c40e6b176ad3fd7332cd217191e557352ef4b82bf91f29939121267598737990
e32f016fe347dd29e263c026c680b9044dcf75340b6fa72b43f1a73a4d7605cf
7e537d8e91668580a482bd77a5a4caba26d6bdac
eafa11070f213f16efc030f625a423d1
d0dccd3a46392875b480c3666e2da62d12fdb0b4e5557185d4116344ed73110d
e078778b62796bab2d7ab2b04d6b01bf
a7a7c4062ced46275638719c100ea2397c673148e8473e56a3ec4313ca7dc5f9
169b38e089926371592a5ef66ae5c52b
65237e705e842da0a891c222e57fe095
4f2c1856325372b9b7769d00141dbc1a23bddd14
ea5a8f1052e40cb6bcebf384fe67a6920b3651fbd8f3a34a844f39789ebc4d5f
5039d76e697f242c36c5a0ebf7dec127757bc34ddaf33c58251c2798da3ce03e
f4a434dd2ac33ffe67575a61c1048d8c9c7f75363727dae9af578a943e9e512a
b27ff24870d93d651ee1d8e06276fa98
4ad367cd1089a68c4e709194d2aae6a01e14de6d
303e004364b1beda0338eb10a845e6b0965ca9fa8ee16fa9f3a3c6ef03c6939f
e390d3d9004124616a18d10dc5b9f6eeab6b01bd167fac4d783036af574a4278
c7ec4570524ad59d5bd7a3e8f0d23c8cf05cc0e8a98dcdbec00c9dc075084558
ebb30fd99c2e6cbae392c337df5876759e53730d
5a4bd78a4d3d1a772e9e9b14983646a4c1c6a25cc983b804e4522774ebfa1c14
478c650401b6ea7d68f649fab17a8eb9581b81607b49e1cff0f61d65df29d1da
fbbe7ee073d0290ac13c98b92a8405ea04dcc6837b4144889885dd70679e933f
d89e5524e49199b1c3b66c524e7a63c3f0a0c199
44fd895174a7c1c0019fc95bb04201106dc165704c70e902e3de58db98f03c7e
737f08702f00e78dbe78acbeda63b73d04c1f8e741c5282a9aa1409369b6efa8
2ed48e578a522a4e718510572056c5cd86d11bdf7e71a52c68a55ebb823771da
3f29f5c1733b3ea1c1cfe36826e33a2a
40b87c5444e03b6b4f3d38315c1525cedfafc20355fff84502cc594799dc41df
31d765deae26fb5cb506635754c700c57f9bd0fc643a622dc0911c42bf93d18f
fa6882672ad3654800987613310d7c3fbade027e
9fa00a4ee4e95bc50a3919d2d3c0be2a567d8845

1561ece482c78a2d587b66c8eaf211e806ff438e506fcef8f14ae367db82d9b3
7e35ce60d80c85e050133de142a3b261160259846c9c967c7b2bb84923328f8c
7f0511b09b1ab3a64c8827dd8af017acbf7d2688db31a5d98fea8a5029a89d56
9479ff59794cbf5f26996eb702f027e700bdbb13858463b7d2537a3fdff4af64
f3f43f3f4d55c0382f9045fd8093eef66074ca7d97dad066746ace47cc47319a
042de780112ef6d50b37a3f57e5a8f1e9910ad986fbba984be8fea3a18f39d59
35d1e819d2ac2535f0aa9e2294570135f37519386872c415e326146e931b8fb9
f00939201f7e77221e94e917a8e34c3d2143324e02fdf35058526d870a0023a0
2cde8de330a874020340f2110bd1fd013fab7e93ef884c9006a646b49b567a75
6cac251512ecd9f0627cf0da5d0a0ff7
02d15669996853594424e5e7f957e12b2042b7775535bd2160953b4e84bb61cd
9aa3ca96a84eb5606694adb58776c9e926020ef184828b6f7e6f9b50498f7071
2556a9e1d5e9874171f51620e5c5e09a
73a21c1492996794688d9751edd1e5c287da645fa7a960e945bb4ea69855424a
2c5ba56a41f40bac2f21065fb9883545ef8d359883cb7bc351c481cb9542e104
ecafe10f0f7d6a9ae94d9735b45f88492b6ea11ff58f37e62fbf7070778af20a
71c0881d35f769fe58c084883d2aaee9ec284fcdc04500e5e5272973dfc78944
9ac5fa37f5cf3d0201f0e70a3e6527e58250ddcff77370262b8cb377e8c5995f
0f189246247c51a701d5a88a06e1fc4932f333d24d7ff40dc8152ad6224f6ca4
a8fd0a5de66fa39056c0ddf2ec74ccd38b2ede147afa602aba00a3f0b55a88e0
4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829
1a0e930fbdab2266e14dc501abdbb5623b5762d687df3670d86bb05f252509ac
bec98a8a5e6786ef415a7a7bf7e60cbd384d43ede4e882aa560fdcb24865ac55
c73d42d7546fe049f63115635c092288
8d1f2a6df51c7783f2eaf1a0fc0ff8d032e5b57f
a58da0e6a20fed03364a0cbae18008eb4f8d6bee7c9f5e8ffcdac34fb823d363
6b310bd23806272f6c69b84a0381915f16d705e79ce423f19de940247543c76a
b379d8f583112cad3cf60f95ab3a67fd
daaa271cee97853bf4e235b55cb34c1f03ea6f8d3c958f86728d41f418b0bf01
7d53782fab972b8b70c6c7134598da25fd125c58c88a6d468464cee6c9dbe764
de1bceb00c23e468f4f49a79ec69ec8ad3ed622a3ffc08f84c0481ad0f6f592b
815c1571356cf328a18e0b1f3779d52e5ba11e5e4aac2d216b79bb387963c2be
73e1f2762ffe8e674f08d83c1308362bd96ccd4f64c307ee0a568bc66faf45bb
aea76f905b0169e4289895a8d85980896f802fd18fe246a27d601310bfa5905e
e34d6387d3ab063b0d926ac1fca8c4c4
bc6898f0e66582ab92307809a409797749b49948fc265767579b224755b0a17b
d3f012662c44293ae07d8c763914db18fc9795673da7c1cdc4d862b1a7c887b9
2feb0bc8dec293ac19246cc0ecc05a1bc606ddac9aa57e677ade4cfac4e94d20
9649d58a220ed2b4474a37d6eac5f055e696769f87baf58b1d3d0b5da69cbce5
bea3df5f788e60d324f1623a4328dafd9eaa6bb01d0a93343176def708bc002f
22ba7234715ec7d99656fc6e16c2d75cbb5465c0fb2e5063c6d02baa4837a602
8932a95c10b088874bfb3471c352d2a7d64757ce77b226f19133301c481d9d03
e9167e0da842a0b856cbe6a2cf576f2d11bcedb5985e8e4c8c71a73486f6fa5a
d8aba4e6904e03daac2c154a1b6b6a9ebe351e4af9b59b44a8ed442f4e67abcf
64fca582cb69d9dc2afb1b432df58fb32ac18ca1
912e8f6d71d556c6def42cb01e8c17e7bd6e46bd3f90eba0c8e8f83937d362f0

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:
cyberthreat@nki.gov.hu

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI
KIBERBIZTONSÁGI
INTÉZET