CTI Jelentés

APT csoportok

NEMZETI
KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Mik azok az APT csoportok? **4**

Az APT csoportok céljai **7**

A támadás folyamata **8**

Az APT csoportok által használt technológiák **10**

A leghírhedtebb APT csoportok **12**

Kína 13

- APT1 14
- APT41 15

Oroszország 18

- APT28 18
- APT29 21

Észak-Korea 23

- APT37 23
- APT38 24

Irán **26**

- APT33 26
- APT35 27
- APT39 28

Izrael 29

- UNIT 8200 29

USA 32

- Equation Group 32

Vietnám 34

- APT32 34

A CERT-EU és az ENISA által javasolt gyakorlatok **38**

Mik azok az APT csoportok?

Jelen dokumentum célja, hogy bemutassa az APT csoportok legfőbb jellemzőit, támadásaik, eszközkészleteik jellegzetességeit, valamint a céljaik és motivációjuk sajátosságait.

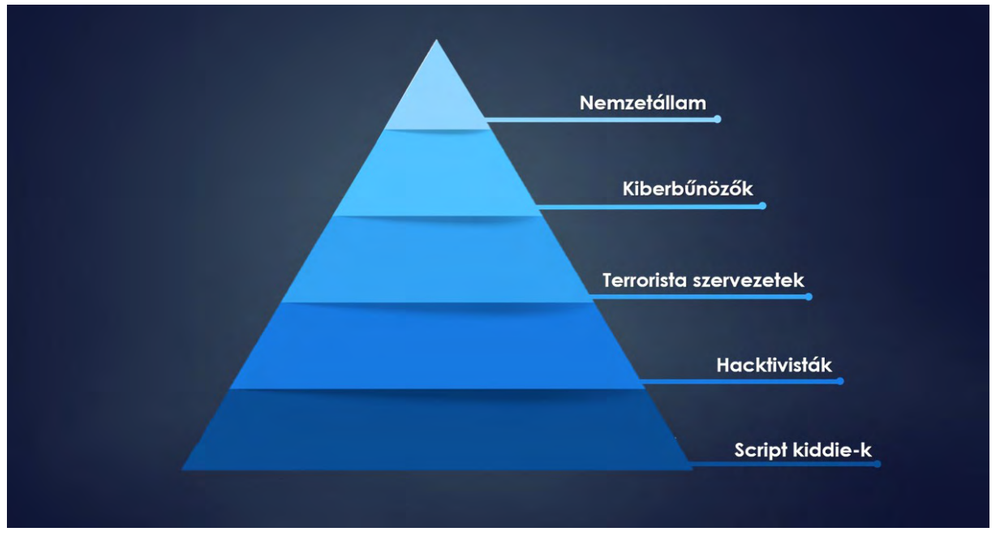
Az APT (Advanced Persistent Threat) csoportok olyan **kiberbűnözői szervezetek**, amelyek **hosszú távú, célzott támadásokat hajtanak végre** az áldozataik ellen, akik jellemzően **nagyobb gazdasági szervezetek** és **államok**.

Az APT elnevezés a **Mandiant/FireEye**-hoz köthető, de léteznek ettől eltérő névkonveciók is, mivel az egyes kiberbiztonsági cégek más-más elnevezési rendszert használnak.
Például a CrowdStrike állatneveket, a Symantec és a Kaspersky fantázianeveket, a Dell SecureWorks és a Cisco Talos egyszerű számokat rendel az egyes csoportokhoz.

TUDTAD?

Az APT csoportok célja általában olyan **adatok megszerzése**, amelyek titkosítottak, érzékenyek, személyes jellegűek vagy szellemi tulajdon részét képzik. Továbbá bármely olyan adat célponttá válhat, amely zsarolásra vagy a célszemély megkárosítására használható és komoly anyagi vagy politikai haszonnal járhat.

Az egyes **szereplők motivációi eltérhetnek egymástól**, és jelentős különbségek adódhatnak képességeik, kifinomultságuk, képzési szintjük és a tevékenységükhöz nyújtott támogatások tekintetében. Ezek közül a **nemzetállami szereplők számítanak a legkifinomultabb kártékony aktoroknak**, akik elkötelezettek valamint korszerű erőforrásokkal és eszközökkel rendelkeznek.



APT csoportok elhelyezkedése a fenyegetettségi szereplők hierarchiájában

Többnyire a lehető legnagyobb gondossággal végzik műveleteiket, annak érdekében hogy elkerüljék a lebukást. Ennek érdekében **alapos felderítést végeznek**, hogy információkat gyűjtsenek a célpont szervezeti és informatikai infrastruktúrájáról, a vállalati kultúráról, az alkalmazottakról, a biztonsági irányelvekről és eljárásokról.

Képesek alkalmazkodni a célpontnál bevezetett biztonsági ellenőrzések változásaihoz. Különleges jellemzőik mellett az APT-k általában **időt szánnak a nulladik napi sebezhetőségek felfedezésére** és olyan exploitok vagy rosszindulatú programok kifejlesztésére, amelyeket a célpontok nem tudnak időben észlelni.

Az elmúlt években egyre növekvő fenyegetést jelentenek különböző országokban és iparágakban. Ezek a csoportok általában **nagyon jól finanszírozott bűnözői szervezetek**, amelyek rendelkeznek minden olyan olyan eszközzel, amelyek szükségesek lehetnek az ilyen típusú támadások végrehajtásában: különféle kiberfegyverekkel és technológiákkal, amelyek lehetővé teszik számukra, hogy észrevétlenül behatoljanak a célpont hálózatába és a céljuknak megfelelően kárt tegyenek. A tevékenységüket általában nagyon nehéz detektálni, mert a magas szintű technikai tudásuknak köszönhetően képesek nagyon ügyesen elrejteni a nyomaikat.

A jelenlétük nem újdonság, az első ismert támadást az 1990-es évek végén dokumentálták.

TUDTAD?

Az APT csoportok elleni védekezésnek általában a kiberbiztonsági intézkedések megerősítését, a folyamatos figyelemmel kísérést és az átfogó kiberbiztonsági stratégiák kidolgozását kell magában foglalnia. Fontos azonosítani a legérzékenyebb adatokat, és szigorú védelmi intézkedéseket kell alkalmazni védelmük érdekében.

APT csoportok céljai

Az APT csoportok céljai az alábbi kategóriába sorolhatók:

- **Kiberkémkedés** (szellemi tulajdon vagy államtitkok ellopása)
- **Pénzügyi vagy politikai haszonszerzés**
- **Károkozás**

Az APT csoportok céljai eltérőek és széleskörűek lehetnek, általában azonban a hosszú távú kémkedés jellemző rájuk, ami lehetővé teszi számukra az érzékeny információk megszerzését és felhasználását. Gyakran **célzottan támadnak állami szervezeteket, kormányokat, kritikus infrastruktúrákat, multinacionális és ipari vállalatokat**, azonban nem korlátozódnak kizárólag az állami és ipari szektorra, hanem egyre inkább **a hétköznapi felhasználókat is célpontjaiknak tekintik**, például identitáslopás vagy pénzügyi csalás céljából.

Amennyiben az APT aktorok állami szervezeteket, kormányokat és kritikus infrastruktúrákat céloznak, akkor a hosszú távú megfigyelés, befolyásolás és károkozás lehet a fő indítékuk. A multinacionális és ipari vállalatok az értékes ipari titkok ellopása és a tevékenységeik utáni kémkedések miatt kerülhetnek az APT csoportok célpontjai közé. Ilyenkor a károkozás és a versenyelőny megszerzése lehet a motiváló erő számukra.

A támadások folyamata

Az APT támadásokat általánosan a következő szakaszokra lehet bontani:

1. Beszivárgás

A támadók az első fázisban külső felderítést végeznek, hogy a lehető legjobban megismerjék a célpont sajátosságait. Ebbe beletartoznak a támadott személyek és az infrastruktúra egyaránt. Gyakran social engineering technikák segítségével jutnak be a célhálózatba, vagy használhatnak saját vagy ismert nulladik napi exploitokat és fejlett malware-eket a kezdeti hozzáférés megszerzésére. Sok esetben a támadás egyik indikátora egy olyan célzott adathalász e-mail, amely magas beosztású személyeket (spear phishing) céloz meg gyakran más, már kompromittálódott csapattagoktól szerzett információk felhasználásával.

Az ilyen e-mailek sok esetben még a rutinos felhasználókat is megtéveszthetik, ha néhány percre is, de figyelmetlenné válnak. Általában egy kolléga vagy partner nevében íródnak és pontos információkat tartalmaznak például egy éppen folyamatban lévő projektről. Ezekkel a közölt konkrétumokkal a munkatárs nem fogja egyből azt feltételezni, hogy egy támadás kellős közepébe csöppent, hanem sajnos jó eséllyel be fog dőlni a támadónak.

Javasoljuk megtekintésre egy korábbi CTI jelentésünket, amelyet az adathalász technikákról készítettünk és megtekinthet a honlapunkon.

2. Eszkaláció

A kezdeti hozzáférés megszerzése után a támadók rosszindulatú szoftvereket juttatnak be a szervezet hálózatába. Ilyenkor oldalirányú mozgást végeznek annak érdekében, hogy feltérképezzék a hálózatot, és hitelesítő adatokat, például fiókneveket és jelszavakat gyűjtsenek a kritikus üzleti információkhoz való hozzáférés reményében. Az igazán szofisztikált támadások egyik ismérve, hogy ilyenkor létrehoznak egy backdoort (hátsó ajtó), amely lehetővé teszi számukra, hogy a későbbiekben észrevétlenül tudjanak behatolni a hálózatba. Gyakran további belépési pontokat hoznak létre a perzisztencia, vagyis a folyamatos hozzáférés biztosításához, ha esetlegesen egy veszélyeztetett pontot felfedeznek és lezárnak a célpontok.

3. Kiszivárogtatás

Ebben a fázisban a kiberbűnözők a hálózaton belül egy biztonságosnak ítélt helyen addig tárolják az ellopott információkat, amíg elegendő adatot nem gyűjtenek a céljuk elérése érdekében. Ezt követően észrevétlenül kijuttatják a megszerzett adatokat, amelyre olyan módszereket alkalmazhatnak, mint például egy szolgáltatásmegtagadással járó támadás (DoS), hogy eltereljék a biztonsági csapat figyelmét.

Az APT csoportok által használt technológiák

A kiberbűnözők és a hatóságok, kutatók és biztonsági szakemberek folyamatosan macska-egér játékot játszanak egymással. A biztonsági cégek és high-tech vállalatok kutatói és szakemberei idővel képesek felismerni, alkalmazkodni ezekhez a támadásokhoz és ki tudják adni a megfelelő javításokat. Ekkorra már elképzelhető, hogy komoly károkat okozott az adott hacker csoport, éppen ezért az egyik legfontosabb tényező ebben a párharcban az idő.

Az alább felsorolt technikák csak **tájékoztató jellegűek**, ugyanis ahány csoport, annyiféle és fajta módszert, technológiát, sebezhetőséget, eszközt és eszközkészletet használnak.

- **Rosszindulatú szoftverek:** Saját fejlesztésű vagy álcázott rosszindulatú szoftvereket használnak, amelyek lehetővé teszik a rendszeren belüli tevékenységeiket. Ezek a szoftverek lehetnek kémprogramok, trójaiak, férgek vagy más típusú rosszindulatú kódok.
- **Keyloggerek:** A jelszavak és más érzékeny információk eltulajdonításához használhatják. Ezek a programok titokban rögzítik az összes billentyűleütést a rendszeren, majd az érzékeny adatokat eljuttatják a támadónak.
- **Remote Access Trojans:** a RAT-ek lehetővé teszik számukra a távoli hozzáférést a rendszerekhez, a rendszeren belüli terjeszkedést, az adatok lehallgatását és eltulajdonítását, valamint a rendszer irányítását.
- **Exploit kitek:** a rendszerek különféle sebezhetőségeinek kihasználásához használják. Ezek a szoftverek automatikusan feltérképezik a rendszert, és keresik a meglévő és foltozatlan sebezhetőségeket.
- **Rootkitek:** lehetővé teszik számukra a rendszerben való rejtőzködést. Ezek a szoftverek gyakran manipulálják a rendszer működését, hogy ne lehessen észrevenni az APT csoportok jelenlétét.
- **Social engineering:** gyakran használnak social engineering technikákat is, például a phishinget, hogy hozzáférést szerezzenek a rendszerekhez. Az ilyen támadások célja az áldozatok megtévesztése és rávezetése arra, hogy bizalmas információkat adjanak át az APT csoportoknak.

A leghírhedtebb APT csoportok

Több száz ismert APT csoport létezik, és szinte lehetetlen felsorolni mindet, mivel rejtve végzik a tevékenységüket és nehéz róluk bármilyen információt szerezni. Ezen csoportok aktivitása kérdéses, ugyanis csak abból lehet következtetni, hogy folytatnak-e jelenleg bármilyen tevékenységet, hogy történt-e valamilyen esemény vagy incidens, amely egyértelműen hozzájuk köthető. Sok esetben hónapokra, akár évekre is eltűnnek, majd hirtelen felbukkannak. Ez nem azt jelenti, hogy ezidő alatt nem tevékenykedtek, csak elképzelhető, hogy addig teljesen rejtve munkálkodtak.

A lista rendkívüli mérete miatt a **legismertebb és a legaktívabb csoportokat részletezzük** egy rövid leírás, kapcsolódó malware-ek, alias nevek, főbb célországok, célágazatok és kihasznált sérülékenységek formájában.

Az alábbi linkekre kattintva az egyes csoportok tevékenységeiről és használt technikáikról további hasznos információk olvashatók:

https://attack.mitre.org/groups/

https://apt.etda.or.th/cgi-bin/listgroups.cgi

https://www.mandiant.com/resources/blog/demonstrating-hustle

Kína

A legtöbb APT csoport rendelkezésre álló információk alapján Kínában folytat vagy folytatott tevékenységet.

A csoportok, amelyek közül nem mindegyik aktív: **APT1**, APT2, APT3, APT4, APT5, APT6, APT7, APT8, APT9, APT10, APT12, APT14, APT15, APT16, APT17, APT19, APT20, APT21, APT22, APT23, APT24, APT25, APT26, APT27, APT30, APT30, APT31, APT40, **APT41**, Antlion, Allanite, Aoqin, AVIVORE, Axiom, Group 72, Barium, Blackgear, BlackTech, Blue Termite, Bookworm, Bronze Butler, Bronze Highland, Bronze Starlight, Calypso, CardinalLizard, Chimera, Curious Gorge, Dalbit, Dragon, DragonBridge, DragonOK, DragonSpark, Dust Storm, Earth Berberoka, Earth Lusca, Earth Wendigo, FunnyDream, Gallium, Gelsemium, GhostEmperor, GhostNet, Goblin Panda, Hafnium, Hidden Lynx, Hurricane Panda, Icefog, IndigoZebra, IronHusky, Lead, LightBasin, Lotus Blossom, Lucky Cat, LuminousMoth, Mikroceen, Moafee, Mustang Panda, Naikon, Night Dragon, NineBlog, Nitro, Operation Dragon Castling, Operation EmailThief, Operation Harvest, Operation LiberalFace, Operation Poisoned News, Operation PseudoManuscrypt, Operation Red Signature, Operation Shady RAT, Operation Titan Rain, PassCV, PittyTiger, PKPLUG, Platinum, Poison Carp, Rancor, RedAlpha, RedDelta, RedEcho, RedFoxtrot, RedGolf, Roaming Tiger, Safe, Samurai Panda, Scarab, Scarlet Mimic, Shadow Network, ShaggyPanther, SharpPanda, Siesta, Snake Wine, Space Pirates, Suckfly, TA413, TA428, TA459, TAG-22, TAG-28, TAG-38, Taidoor, TaskMasters, Temper Panda, Tropic Trooper, Tonto Team, Twisted Panda, UNC215, UNC4191, Vicious Panda, Wicked Panda, Worok.

APT1

Az APT1 egy kínai csoport, amelyet a Népi Felszabadító Hadsereg (PLA) Főparancsnokságának (GSD) 3. osztálya 2. irodájához kötnek, és amelyet a katonai egység fedőneve (MUCD) alapján 61398-as egységként is ismernek.

Bevetéseik közé tartozott a GhostNet, Shady RAT és az Aurora hadművelet. Utóbbi több tucat más szervezetet is célzott, mint például az Adobe Systems Akamai Technologies-t, Juniper Networks-t, Rackspace-t, Yahoot, Symantec-et, Northrop Grumman-t, Morgan Stanley-t, Dow Chemical-t és a BlackBerry-t.

Kapcsolódó malware-ek: TROJAN.ECLTYS, BACKDOOR.BARKIOFORK, BACKDOOR.WAKEMINAP, TROJAN.DOWNBOT, BACKDOOR.DALBOT, BACKDOOR.REVIRD, TROJAN.BADNAME, BACKDOOR.WUALESS.

Alias nevek: Comment Panda, Comment Group, Operation "Oceansalt", Operation "Seasalt", PLA Unit 61398, Comment Crew, Byzantine Candor, ShadyRAT, Byzantine Hades, TG-8223, Brown Fox, GIF89a.

Főbb célországok: Szingapúr, Kanada, Dél-Afrika, USA, Svájc, Norvégia, Tajvan, Izrael, Luxemburg, Egyesült Arab Emírségek, Egyesült Királyság, Belgium, Franciaország, India, Japán.

Főbb célágazatok: építőipar, energiaszektor, élelmiszeripar és mezőgazdaság, IT, oktatás, média, nonprofit szervezetek, kormányzat, műholdak, szórakoztató ipar, közlekedés, távközlés, egészségügy, légiközlekedés, pénzügyi szektor, vegyipar.

Kihasznált sérülékenységek: CVE-2020-11023, CVE-2019-11358, CVE-2020-11022, CVE-2015-9251.

További információk a csoport által használt technikákról az alábbi linken érhetők el.

APT41

Az APT41 egy olyan kínai csoport, amely pénzügyileg motivált és államilag támogatott kémtevékenységet is folytat. Az APT41 már 2012 óta aktív és legkevesebb 14 országban figyelték meg az egészségügyi, távközlési, technológiai és videojáték iparág ellen irányuló támadásaikat. 2020 szeptemberében az amerikai igazságügyi minisztérium vádat emelt az 5 kínai és 2 malajziai állampolgár ellen, akik több mint 100 vállalatot veszélyeztettek világszerte. Az APT41 megfigyelt célpontjai összhangban vannak Kína nemzeti stratégiáival, amelyek célja, hogy a termelési kapacitásokat a kutatás-fejlesztés (K+F) súlyponti területeire helyezze át.

A 2015-ben bejelentett “Made in China 2025” terv célja, hogy a kínai gazdaságot a magasabb értékű termékek és szolgáltatások (gyógyszeripar, félvezetők és más csúcstechnológiai iparágak) felé terelje.

Kapcsolódó malware-ek: Legalább 46 különböző kódcsaládot és módszert használtak a küldetéseik teljesítésére.

Alias nevek: Double Dragon, WinNTI, Wicked Panda, Deputy Dog, Wicked Spider, Winnti Umbrella, Barium, Blackfly, Winnti Group.

Főbb célországok: Belgium, Finnország, Franciaország, Németország, Olaszország, Katar, Svédország, Törökország, Egyesült Arab Emírségek, Egyesült Királyság, USA.

Célágazatok: Építőipar, energiaipar, online videojáték cégek, olaj- és gázipari vállalatok, petrolkémia, oktatás, hajózás és logisztika, média, gyógyszeripar, high-tech, kormányzat, technológia, kiskereskedelem, közlekedés, telekommunikáció, egészségügy, magánszektor, pénzügyi ipar, légiközlekedés.

Kihasznált sérülékenységek: CVE-2018-0802, CVE-2017-11151, CVE-2019-19781, CVE-2019-16920, CVE-2019-11510, CVE-2019-1652, CVE-2019-1653, CVE-2019-16278, CVE-2020-10189.

További információk a csoport által használt technikákról az alábbi linken érhetők el.

Oroszország

Ismert orosz csoportok: **APT 28**, **APT 29**, Berserk Bear, Buhtrap, Cobalt Group, Cold River, Corkow, Cyber Berkut, Doppel Spider, DustSquad, Energetic Bear, FIN7, Gamaredon Group, GCMAN, Hades, IAmTheKing, Inception Framework, Indrik Spider, InvisiMole, Lurk, MoneyTaker, OldGremlin, Operation BugDrop, Operation Domino, Pinchy Spider, RTM, SaintBear, Sandworm Team, TA505, TeamSpy Crew, TeleBots, TEMP.Veles, Turla, UNC3524, Venom Spider, Wizard Spider.

APT28

Az APT28-at az amerikai igazságügyi minisztérium 2018. júliusi vádiratában az orosz vezérkar fő hírszerzési igazgatóságához köti. Ez a csoport állítólag 2016-ban kompromittálta Hillary Clinton kampányát, a Demokratikus Nemzeti Bizottságot (Democratic National Committee) és a Demokratikus Kongresszusi Kampánybizottságot (Democratic Congressional Campaign Committee), hogy megpróbáljon beavatkozni az amerikai elnökválasztásba. Az APT28 legalább 2004 óta aktív.

Tevékenységek, támadások, események:

- Támadások neves újságírók ellen Oroszországban, az Egyesült Államokban, Ukrajnában, Moldovában és a Baltikumban
- A francia televízió feltörése
- root9B jelentés
- EFF Spoof, Fehér Ház és NATO támadás
- Holland Biztonsági Tanács és a Bellingcat
- Demokratikus Nemzeti Bizottság hackelése
- Ukrán tüzérség elleni támadás
- Holland minisztériumok elleni támadás
- Nemzetközi Atlétikai Szövetség (IAAF) hackelése
- Nemzetközi Olimpiai Bizottság elleni támadás
- Svéd Sportszövetség elleni támadás
- Egyesült Államok konzervatív csoportjai elleni támadás
- Az Ökumenikus Patriarchátus és más egyházi személyek elleni támadás
- 2019 Think Tank támadások
- 2019 Strategic Czech Institution
- 2020 A német hatóságok elfogatóparancsa
- 2016 első negyedévében a Fancy Bear spear phishing támadásokat hajtott végre a DNC e-mail címei ellen. A Hillaryclinton.com címeket is megtámadták és 50 000 e-mailt loptak el.

Kapcsolódó malware: CHOPSTICK, SOURFACE.

Főbb támadási módszerek: Spear phishing, Mimikatz, Coreshell.

Alias nevek: Yttrium, Fancy Bear, SIG40, TsarTeam, ATK 5, Operation "Russian Doll", PawnStorm, Tsar Team, The Dukes, Operation "Ghost", Swallowtail, ATK 7, Operation "DealersChoice", STRONTIUM, Operation "Komplex", ITG05, IRON TWILIGHT, Operation "Office monkeys", ITG11, TAG_0700, Grizzly Steppe, Group 74, Iron Hemlock, Iron Twilight, Operation "Pawn Storm", Sednit, Operation "Dear Joohn", T-APT-12, apt_sofacy, Pawn Storm, Strontium, Group-4127, Group 100, CloudLook, Minidionis, TG-4127, SNAKEMACKEREL, Sofacy.

Főbb célországok: Ausztrália, Belgium, Kanada, Kína, Franciaország, Németország, India, Irán, Izrael, Japán, NATO, Hollandia, Új-Zéland, Norvégia, Dél-Afrika, Spanyolország, Svédország, Svájc, Törökország, Egyesült Arab Emírségek, Egyesült Királyság, Ukrajna, USA.

Főbb célszektorok: repülőipar, autóipar, védelmi intézmények és katonaság, pénzügyi szektor, egészségügyi szektor, energia ipar, IT, olaj- és gázipari vállalatok, távközlési szektor.

Kihasznált sérülékenységek: CVE-2017–0213, CVE-2019–1458, CVE-2015–1701, CVE-2020–0796, CVE-2019–11510, CVE-2019–18935.

További információk a csoport által használt technikákról az alábbi linken érhetők el.

APT29

Az APT29 egy olyan fenyeget csoport, amelyről azt feltételezik, hogy az orosz kormány támogatását élvezi. Legalább 2008 óta működik és állítólag 2015 nyarától kezdve veszélyeztette a Demokratikus Nemzeti Bizottságot (Democratic National Committee).

Tevékenységek, támadások, események:

- Office Monkeys
- Pentagon elleni támadás
- Demokratikus Nemzeti Bizottság elleni támadás
- US Think Tanks és NGO-k elleni támadások
- Norvég kormány elleni támadás
- Holland minisztériumok elleni támadás
- Ghost hadművelet
- COVID-19 oltási adatok

A Cozy Bear kapcsolatban állt a Pentagon e-mail rendszere elleni látványos kibertámadással, amely következtében 2015 augusztusában leállt az összes vezérkari egység.

Kapcsolódó malware-ek: HAMMERTOSS, TDISCOVER, UPLOADER.

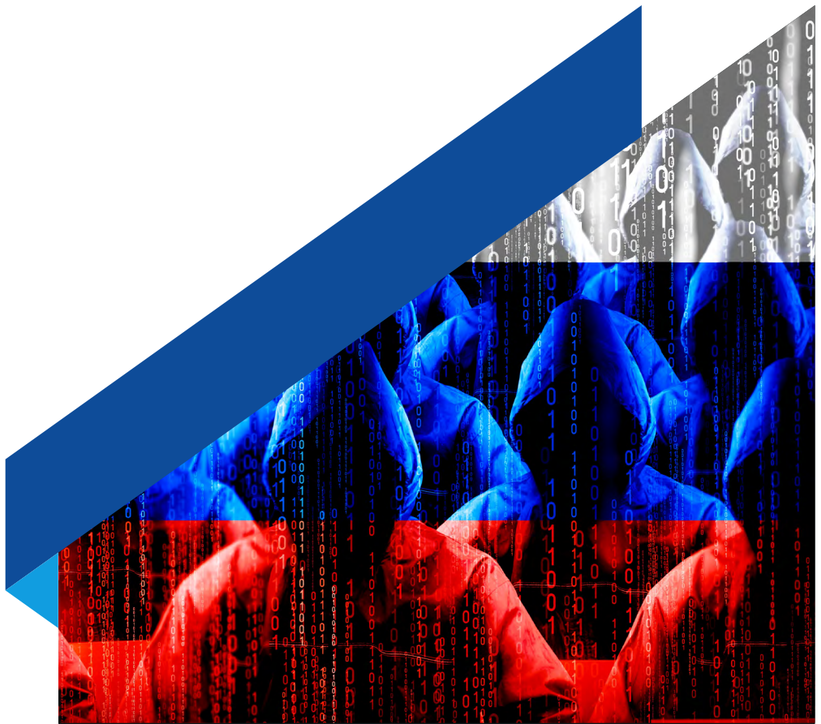
Alias nevek: Dukes, Group 100, Cozy Duke, CozyDuke, EuroAPT, CozyBear, CozyCar, Cozer, Office Monkeys, OfficeMonkeys, Cozy Bear, The Dukes, Minidionis, SeaDuke, Hammer Toss, YTTRIUM, Iron Hemlock, Grizzly Steppe.

Főbb célországok: Belgium, Brazília, Kína, Grúzia, India, Japán, Kazahsztán, Mexikó, Új-Zéland, Portugália, Románia, Dél-Korea, Törökország, Ukrajna, USA.

Főbb célágazatok: kormányzati és magánszektor.

Kihasznált sérülékenységek: CVE-2019-17026, CVE-2020-0674, CVE-2019-9670, CVE-2018-13379, CVE-2019-19781, CVE-2019-11510.

További információk a csoport által használt technikákról az alábbi linken érhetők el.



Észak-Korea

Ismert észak-koreai csoportok: **APT37**, **APT38**, Covellite, Kimsuky, Operation Earth Kitsune, Operation WizardOpium, Wassonite.

APT37

Az APT37 egy feltételezett észak-koreai kiberkémkedő csoport, amelyet a kormánya támagott. Legalább 2012 óta aktív és jellemzően pénzügyi intézmények elleni műveletekben vesz részt, hogy Észak-Korea számára vagyont generáljon, de egyes országok ipari ágazatai ellen is végez támadásokat. A CrowdStrike szerint a csoport főként különböző dél-koreai szervezeteket és magánszemélyeket támad, köztük akadémikusokat, újságírókat és észak-koreai disszidenseket. A csoport kijelentette, hogy Japán, Vietnam, Hongkong, a Közel-Kelet, Oroszország és az Egyesült Államok ellen is indított támadásokat.

Tevékenységek, támadások, események:

- Daybreak hadművelet
- Erebus hadművelet
- Golden Time
- Evil New Year
- Are you Happy?
- FreeMilk
- Észak-koreai emberi jogok
- Evil New Year 2018

Alias nevek: Ricochet Chollima, Reaper, ScarCruft

Főbb célországok: Kína, Thaiföld, Ecuador, Fülöp-szigetek, Izrael, Franciaország, Németország, Lengyelország, Hongkong, Oroszország, Tajvan, Mexikó, Egyesült Királyság, USA, Chile, Guatemala, Japán, Banglades, Kanada, Ausztrália, Dél-Korea, Vietnam, Brazília, India.

További információk a csoport által használt technikákról az alábbi linken érhetők el.

APT38

Az APT38 egy pénzügyileg motivált fenyegetettségi csoport, amelyet az észak-koreai rezsim támogat. A csoport főként bankokat és pénzügyi intézményeket vesz célba, és 2014 óta több, mint 16 szervezetet vett célba legalább 13 országban.

Tevékenységek, támadások, események:

- Troy hadművelet
- 2013-as dél-koreai kibertámadás
- Sony Pictures Hack
- Blockbuster művelet
- WannaCry támadás
- 2017 kriptovaluta támadások
- 2019 szeptemberi támadások

A csoport megtámadta a Sony Pictures-t és nagy mennyiségű adatot szivárogtattak ki. A hackerek azt akarták, hogy a Sony ne dobja piacra "Az interjú" című 2014-es című amerikai vígjátékot, amelyben a főhősök az észak-koreai vezető Kim Jong-un-t akarták meggyilkolni. A hackereknek sikerült hozzáférni a film megjelenése előtt, az e-mailekhez és mintegy 4000 alkalmazott érzékeny adataihoz.

Kapcsolódó malware-ek: különféle egyéni kártevőcsaládok

Főbb támadási módszer: ransomware (WannaCry, MimiKatz)

Aliasnevek: Lazarus Group, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team, Hidden Cobra

Főbb célországok: Kína, Thaiföld, Ecuador, Fülöp-szigetek, Izrael, Franciaország, Németország, Lengyelország, Hongkong, Oroszország, Tajvan, Mexikó, Egyesült Királyság, USA, Chile, Guatemala, Japán, Banglades, Kanada, Ausztrália, Dél-Korea, Vietnam, Brazília, India.

Főbb célágazatok: média, kormányzat, technológia, pénzügyi szektor, repülőgépipar.

További információk a csoport által használt technikákról az alábbi linken érhetők el.

Irán

Ismert iráni csoportok: Agrius, **APT33**, APT34, **APT35**, **APT39**, APT42, Boss Spider, Cadelle, Clever Kitten, CopyKittens, Cutting Kitten, DarkHydrus, DNSpionage, Domestic Kitten, Ferocious Kitten, Flying Kitten, Group5, Hexane, Infy, Iridium, ITG18, Leafminer, Mabna Institute, Madi, Magic Kitten, MalKamak, MuddyWater, Seedworm, Nazar, Parisite, Rampant Kitten, Rocket Kitten, Sima, Tortoiseshell, Tracer Kitten, xHunt.

APT33

Az APT33 egy feltételezhetően iráni csoport, amely kormányszintű támogatásban részesül. A legfrissebb információk szerint 2013 óta folytat műveleteket több iparágban is. Légiközlekedési és energiaágazati szervezeteket támadnak leginkább az Egyesült Államokban, Szaúd-Arábiában és Dél-Koreában.

Főbb támadási módszerek: Phishing, Shamoon, Mimikatz, PowerSploit, Spyware.

További információk a csoport által használt technikákról az alábbi linken érhetők el.

APT35

Az APT35 egy 2010 óta aktív csoport, amely feltehetően Iránból tevékenykedik. 2014-től a fő profiljuk a rosszindulatú szoftvereken alapuló kiberkémkedési kampányok, amelyek az amerikai védelmi ipari szekort és a cenzúraellenes technológiák iráni felhasználóit célozta meg.

Főbb tevékenységek:

- 2013-ban Monica Witt, aki az amerikai légierő őrmestere volt és részt vett katonai hírszerzésben, Iránba disszidált. A kormánynak adott hírszerzési információi alapján később az amerikai katonai vállalkozókat célozták meg (kiképzéssel, tanácsadással, műszaki javítással stb. foglalkozó, magas katonai tapasztalattal rendelkező személyek). 2019-ben az amerikai kormány vádat emelt Witt és társai ellen összeesküvés, számítógépes behatolás kísérletével és személyazonosság lopás vádjával.
- Hozzájuk fűződik az HBO elleni 2017-es támadás, amikor 1,5 TB-nyi adatot szivárogtattak ki, köztük például a **Trónok harca** című sorozat epizódjainak forgatókönyveit is.
- Bár az iráni kormány tagadja a közreműködését, az APT35-t vádolják a 2015-os iráni nukleáris megállapodásban érintett amerikai tisztviselők célbevételével

- A Microsoft szerint a 2019 augusztusa és szeptembere között 2700 kísérletet tettek arra, hogy információkat szerezzenek a megcélzott e-mail fiókokkal kapcsolatban. A támadás 4 kompromittált fiókot eredményezett. Bár a kezdeményezésről úgy vélték, hogy az Egyesült Államok egyik elnökválasztási kampánya ellen irányult, a kompromittált fiókok egyike sem kapcsolódott a választásokhoz. Irán tagadta a választásokba való beavatkozást, azonban a ClearSky Cyber Security kiberbiztonsági szakemberei is azt állították, hogy az APT35 áll a támadások mögött.

Alias nevek: Phosphorus, Ajax Security, Charming Kitten, NewsBeef, CopyKittens

További információk a csoport által használt technikákról az alábbi linken érhetők el.

APT39

Az APT39 legalább 2014 óta folytatja tevékenységét, amelyet az iráni hírszerzési és biztonsági minisztériuma (MOIS) a Rana Intelligence Computing fedőcégen keresztül üzemeltet. Elsősorban utazási, vendéglátási, tudományos és telekommunikációs iparágakat vesz célba Iránban, Ázsiában, Afrikában, Európában és Észak-Amerikában, hogy a MOIS által fenyegetésnek tekintett személyeket és szervezeteket kövesse.

Kapcsolódó malware-ek: SEAWEED, CACHEMONEY, POWBAT

Alias nevek: ITG07, Chafer, Remix Kitten, Group G0087

Főbb célországok: az APT39 célpontjai globálisak, de tevékenységei a Közel-Keletre koncentrálódnak

Főbb célágazatok: távközlési, utazási ágazatok és az azt támogató IT-cégek, valamint a csúcstechnológiai ipar

További információk a csoport által használt technikákról az alábbi linken érhetők el.

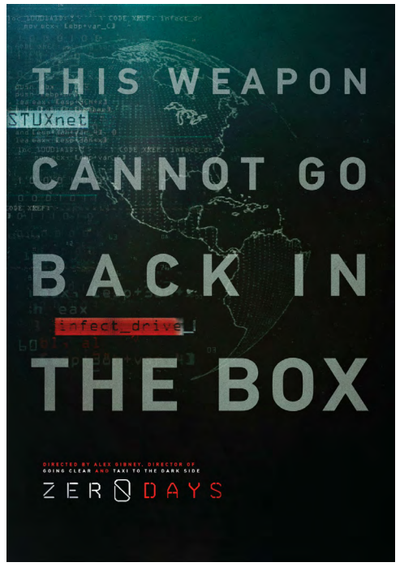
Izrael

Unit 8200

A Unit 8200 hivatalosan az Israeli Defense Forces (IDF) hírszerző csoportja, és a legtöbb kiberbiztonsági intézmény nem ismeri el APT csoportként. A 8200-as egység az izraeli hadsereg legnagyobb egysége, amely legfőbb tevékenysége a SIGINT, kiberműveletek és kódfejtés. Az egységet 1952-ben hozták létre, és elsődleges feladata, hogy hírszerzési információkat gyűjtsön Izrael ellenségeiről világszerte.

A Unit 8200-hoz is köthető, egyik legismertebb művelet a Stuxnet, egy kifinomult számítógépes féreg kifejlesztése, amely az iráni nukleáris programban használt ipari vezérlőrendszereket célozta meg. A Stuxnetet úgy tervezték, hogy beszivárogjon Irán urándúsító létesítményébe, és megzavarja az ország nukleáris programját azáltal, hogy kárt okoz az urándúsításhoz használt centrifugákban.

A Stuxnet úttörő módon **számos fejlett technikát alkalmazott**, többek között a Microsoft Windows és a PLC-k korábban **ismeretlen sebezhetőségeit használta ki**. Ez volt az első ismert példa arra, hogy egy kiberfegyver fizikai kárt okozott egy célpontban. A támadás jelentős csapást mért az iráni atomprogramra, és több évvel visszavetette az országot a nukleáris fegyverek kifejlesztése felé vezető úton.



Zero Days, a Stuxnet-ről készült dokumentumfilm
Forrás IMDb:

Az izraeli kormány nem erősítette meg, de a Unit 8200-höz kötik a rendkívül kifinomult, Flame névre keresztelt hírszerzési kiberfegyvert, amelyet iráni, szíriai és más közel-keleti országok ellen használtak.

Szintén nem erősítette meg az izraeli kormány, de a Duqu malware kifejlesztésében és a WhatsApp sebezhetőségének felfedezésében is részt vett a csoport, amelyet emberi jogi aktivisták és újságírók ellen használtak fel.

Főbb célágazatok: ipari vezérlőrendszerek, nukleáris dúsító létesítmények

Főbb támadási módszerek: social engineering, malware-k, nulladik napi sebezhetőségek

Támadások: Stuxnet, Duqu, Flame, Operation Orchard, Operation Full Disclosure, Ogero incidens

USA

Ismert amerikai csoportok: **Equation Group**, Strider, Operation Olympic Games (amerikai-izraeli).

Equation Group

Az Equation Group egy hírhedt és kifinomult támadócsoport, amelyet az Egyesült Államok Nemzetbiztonsági Ügynöksége (NSA) állítólagos szponzorálásával és az izraeli Unit 8200-zal hoztak összefüggésbe. Tevékenységük valódi mélységét nehéz felmérni, mivel a támadásaik leginkább államok és kormányzati szervek ellen irányulnak. A csoport hosszú ideig működött rejtve, és főként speciális támadási eszközök, kifinomult malware-ek és adathalász technikák alkalmazásával érte el céljait. Egyes információk szerint a csoportot az NSA elleni belső kiszivárogtatásoknak köszönhetően fedték fel, amelyek során a csoport titkos eszközei és dokumentumai nyilvánosságra kerültek. Ezek az események hozzájárultak a nagyobb tudatossághoz a kibertérben folyó állami szintű támadásokkal kapcsolatban.

A Kaspersky kutatói 500 Equation Group által okozott fertőzést dokumentáltak legalább 42 országban. Főként Irán, Oroszország, Pakisztán, Afganisztán, India, Szíria és Mali ellen irányultak a támadások.

A rosszindulatú szoftverbe épített önmegsemmisítő mechanizmus miatt a kutatók gyanítják, hogy ez csak egy kis százalékos arány; az áldozatok tényleges száma valószínűleg több tízezerre tehető. A vizsgált incidensekből az derül ki, hogy az Equation Group magasszintű tudással és korlátlan erőforrásokkal rendelkezik.

Főbb tevékenységek:

- Stuxnet kártevő létrehozását az Equation csoporthoz, illetve az izraeli Unit8200-hoz kötik.
- A virtuális fájlrendszerek használata, ami a rendkívül kifinomult Regin malware-ben is megtalálható. Az Edward Snowden által közzétett dokumentumok szerint az NSA a Regint a részben állami tulajdonban lévő belga Belgacom cég megfertőzésére használta.

A hírhedt adatszivárogtató, Edward Snowden könyve.
Forrás moly.hu:

- Rosszindulatú fájlok elrejtése a fertőzött számítógépek registryjében. Azáltal, hogy a kártékony fájlokat titkosították és a számítógép Windows registry-ben tárolták, a fertőzést lehetetlen volt vírusirtó szoftverekkel felismerni.
- Átirányítások, amelyek az iPhone felhasználókat egyedi exploit weboldalakra küldték. Sikerült egyaránt iOS és OS X eszközöket is megfertőzni.
- Több mint 300 domaint és 100 szervert használtak egy kiterjedt C&C infrastruktúra létrehozására.
- USB pendrive alapú felderítő rosszindulatú szoftverek az air-gapped hálózatok feltérképezésére. A Stuxnet és a Flame is képes volt kijátszani az air-gap megvalósításokat.
- A Windows újabb verzióiban alkalmazott kódaláírási korlátozások megkerülésének egy módja megköveteli, hogy az operációs rendszer kernelével kapcsolatot létesítő minden harmadik féltől származó szoftvert elismert tanúsító hatósággal digitálisan aláírjanak. E korlátozás megkerülése érdekében az Equation Group rosszindulatú programja egy ismert sebezhetőséget használt ki a CloneCD már aláírt illesztőprogramjában, hogy kernel szintű kódfuttatást érjen el. Az elért eredmények összességében arra engedték következtetni a Kaspersky kutatóit, hogy az Equation Group valószínűleg a világ legfejlettebb hackercsoportja, amelynek technikai képességei és erőforrásai a legmagasabb szinten áll. További tevékenységeik közé tartozik a PRISM és a GCHQ-val együtt az INCENSER programokkal folytatott világméretű kémkedés, amelynek során különböző nemzetközi internetes csatornákat hallgattak le.

Kapcsolódó malware-ek, toolok: Stuxnet, Flame, EternalBlue, EquationDrug, EquationLaser, DoubleFantasy, TripleFantasy, Fanny, GrayFish

Főbb támadási módszer: nulladik napi exploitok, kémprogramok, RAT-ok.

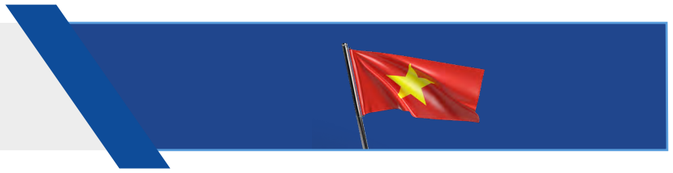
Alias nevek: Tilded Team, EQGRP, G0020, Shadow Brokers.

Főbb célországok: Afganisztán, Banglades, Belgium, Brazília, Ecuador, Franciaország, Németország, Hongkong, India, Irán, Irak, Izrael, Kazahsztán, Libanon, Líbia, Malajzia, Mali, Mexikó, Nigéria, Pakisztán, Palesztina, Fülöp-szigetek, Katar, Oroszország, Szingapúr, Szomália, Dél-Afrika, Szudán, Svájc, Szíria, Egyesült Arab Emírségek, Egyesült Királyság, USA, Jemen.

Főbb célágazatok: energia, kormányzat, média, olaj és gáz, távközlés, közlekedés.

További információk a csoport által használt technikákról az alábbi linken érhetők el.

Vietnám



APT32

A csoport komoly fenyegetést jelent az országban üzleti tevékenységet folytató, gyártó vagy beruházásra készülő vállalatokra. A tevékenység konkrét motivációja nem ismert, azonban az elemzők arra asszociálnak, hogy a célszervezetek versenyelőnyét áshatja alá a hazai vállalatokkal szemben.

Tevékenységek, támadások, események:

- 2020-ban a kínai katasztrófavédelmi minisztériumot és a wuhani önkormányzatot vette célba, hogy információkat szerezzen a COVID-19 világjárványról. A vietnámi külügyminisztérium alaptalannak nevezte a vádakat.
- 2020-ban a csoport a Google Play Store-t, létrehozott hamis híroldalakat és Facebook oldalakat használtak rosszindulatú programok terjesztésére.
- 2021 februárjában számos kémprogram támadást indított vietnami emberi jogi aktivisták, köztük Bui Thanh Hieu ellen.
- 2021 márciusában a csoport működését befolyásolta egy tűzvész az OVH egyik franciaországi adatközpontjában.

Főbb célágazatok: A vietnami gyártási, fogyasztási cikkek és vendéglátási ágazatába befektető külföldi vállalatok.

Kapcsolódó malware-ek: BEACON, KOMPROGO, PHOREAL, SOUNDBITE, WINDSHIELD

Főbb támadási módszer: ActiveMime fájlokat használnak, amelyek social engineering módszereket alkalmaznak, hogy az áldozatokat makrók engedélyezésére csábítsák. Végrehajtáskor az inicializált fájl jellemzően több rosszindulatú payload-ot tölt le egy távoli szerverről. A rosszindulatú mellékleteket spear phishing e-maileken keresztül juttatják el a célszemélyekhez. Egyes bizonyítékok alapján néhányat a Gmailen keresztül is küldtek.

Alias nevek: OceanLotus Group, SeaLotus, Group G0050, APT-C-00

További információk a csoport által használt technikákról az alábbi linken érhetők el.

Forrás: rewterz.com

A CERT-EU és az ENISA által javasolt gyakorlatok

Megelőzés

- **Kövessük a gyártók által javasolt bevett biztonsági gyakorlatokat (best practices)** a termékeik hardeningjéhez és a magasan privilegizált fiókok és kulcsfontosságú eszközök kezelésére!
- **Törekedjünk az eszközleltárak folyamatos aktualizálására** (fizikai és virtuális eszközök), így a sebezhetővé vált rendszerek időben azonosíthatóvá válnak!
- **Blokkoljuk vagy szigorúan korlátozzuk** a ritkán újraindított szerverek vagy más eszközök internet hozzáférését!

  Minden fiókra vonatkozóan **alkalmazzunk szigorú jelszópolitikát** és amennyiben lehetséges, használjunk többfaktoros hitelesítést!
- **Készítsünk biztonsági mentési stratégiát**, és alkalmazzuk a 3-2-1 szabály megközelítését, amely szerint a szervezeteknek három teljes másolatot kell készíteniük adataikról, amelyek közül kettőt helyben, különböző típusú adathordozókon, és legalább egy másolatot pedig külső helyszínen kell tárolnunk!
- **Szegmentáljuk a hálózatunkat** a kritikus rendszerek és erőforrások elkülönítése érdekében - különösen az internettel és harmadik felekkel való összeköttetések tekintetében hajtsuk végre az elkülönítést!
- **Biztosítsuk a felhőkörnyezeteket**, mielőtt kritikus eszközöket helyeznénk át oda! Használjuk a felhőplatformokon rendelkezésre álló erős biztonsági ellenőrzéseket, és megfelelően szegmentáljuk a felhőalapú és lokális rendszereket annak biztosítása érdekében, hogy a támadók egy esetleges sikeres betörés után ne tudjanak tovább terjeszkedni!
- **Vezessünk be rugalmas e-mail szabályzatot**, amely megfelelő mechanizmusokat tartalmaz a rosszindulatú tartalmak szűrésére és vizsgálatára! Egy biztonságos e-mail átjáró tovább fokozhatja a címzettek védelmét.
- Fontoljuk meg az úgynevezett **Pass-the-Ticket technikán alapuló támadások** megelőzését Active Directory környezetekben!
- **Fektessünk hangsúlyt a különféle kiberbiztonsági oktatásokba**, például ösztönözzük a kiberbiztonsági szakembereket arra, hogy a saját területükre vonatkozó speciális szakmai képzésekre iratkozzanak be, valamint a végfelhasználók számára tömör tudatosságnövelő kampányokat végezzenek!

Észlelés

- **Végezzünk robosztus naplógyűjtést**, és rendszeresen vizsgáljuk felül a kiváltott riasztásokat!
- **Figyeljük a hálózatunkban lévő eszközök tevékenységét** megfelelő eszközökkel, például a végpontok észlelésével és reagálásával (EDR) és a felhasználói viselkedésének elemzésével (UEBA), mivel a hálózati forgalom jelentős része manapság titkosított. Ez a szerverekre és a végpontokra egyaránt vonatkozik!

- **Végezzünk robosztus naplógyűjtést**, és rendszeresen vizsgáljuk felül a kiváltott riasztásokat!
- **Figyeljük a hálózatunkban lévő eszközök tevékenységét** megfelelő eszközökkel, például a végpontok észlelésével és reagálásával (EDR) és a felhasználói viselkedésének elemzésével (UEBA), mivel a hálózati forgalom jelentős része manapság titkosított. Ez a szerverekre és a végpontokra egyaránt vonatkozik!
- **Használjuk a gondosan összeállított CTI-t**, hogy meg tudjuk találni a kompromittálódás lehetséges jeleit!
- **Használjunk behatolásérzékelő szignatúrákat és NetFlow-t** a gyanús forgalom kiszűrésére!
- Fektessünk energiát a **PowerShell alapú támadások** megelőzésére és észlelésére!
- Fektessünk energiát az **NTLM és Kerberos** protokollokat Windows környezetben kihasználó oldalirányú mozgások felderítésére!
- Erőteljesen **tudatosítsuk munkatársainkat és felhasználóinkat**, hogy minden gyanús tevékenységet azonnal jelentsenek a helyi kiberbiztonsági csoportoknak!

Reagálás

- **Hozzunk létre és tartsunk fenn egy incidensreagálási tervet!**
- **Mérjük fel az incidens súlyosságát!** A fejlettebb támadások kezelése külső biztonsági szolgáltatók bevonását teheti szükségessé, akik szakmai tanácsadást és személyzetet biztosíthatnak. A megfelelő szolgáltatónak komoly tapasztalattal és szakértelemmel kell rendelkeznie az APT támadások kezelésében.
- **Kerüljük el az incidenskezelés során elkövetett gyakori hibákat:**
  - egy biztonsági esemény figyelmen kívül hagyása anélkül, hogy felmérnénk, mi váltotta ki azt, és milyen lehetséges hatásai vannak,
  - a fenyegetési aktor által használt infrastruktúra (pingelés, DNS lekérdezések, böngészés stb.) megelőző blokkolása vagy szondázása,
  - az érintett rendszerek migrációja, mielőtt a bizonyítékokat begyűjtenénk,
  - a telemetriaforrások (hálózati, rendszer- és hozzáférési naplók) figyelmen kívül hagyása,
  - a kiváltó okok figyelmen kívül hagyása,
  - a megtett intézkedések és az események részletes nyilvántartásának vezetésének elmulasztása.
- Az incidensek elhárítása számos belső érdekelt fél közötti kommunikációt igényel, és erősen ajánlott, hogy **világos, tömör kommunikációs irányelveket készítsün**k és teszteljünk előre.
- Ha az incidens személyes adatokra is kiterjed, **kérjük ki az adatvédelmi tisztviselő és a jogi csoport tanácsát!**

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2023