



2026 szeptember havi CTI riport



NEMZETI
KIBERBIZTONSÁGI
INTÉZET

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



Helyzetkép

A szeptember havi jelentésünkben a támadási technikák és a káros kódok elterjedtségének alakulását részletezzük, kitérünk a célzott támadó csoportok tevékenységére, a zsarolóvírusok aktivitására, valamint az ipari és peremhálózati rendszereket érintő biztonsági kockázatokra. Emellett áttekintjük a hazai megfigyelési adatok alapján azonosított trendeket és az egyes ágazatokat jellemző fenyegetési mintázatokat.

A dokumentum ezután a legfontosabb sérülékenységeket és azok kihasználásának lehetőségeit tárgyalja, különös tekintettel a hálózati infrastruktúrára gyakorolt

hatásokra. Bemutatja a honeypot-rendszerekkel észlelt támadási tevékenységet és a kapcsolódó kártevőelemzést, majd javaslatokat fogalmaz meg a kockázatok mérséklésére. A cél annak bemutatása, hogy a nemzetközi események és a hazai megfigyelések hogyan segíthetik a szervezetek védelmi felkészültségének erősítését.

APT csoportok

A 2026. szeptemberi időszakban több fejlett fenyegetési szereplő bővítette támadási eszköztárát és infrastruktúráját.

A feltételezetten kínai állami háttérű TAG-190, más néven Calypso APT vagy Red Lamassu, infrastruktúrájának nyilvánosságra kerülése után is új [Showboat vezérlőszervereket helyezett üzembe](#), majd célpontjai között távközlési szolgáltatók és kormányzati szervezetek szerepeltek.

A Pakisztánhoz köthető SideCopy [oktatási intézményeket célzott](#) megtevesztő ZIP-állományokkal és dokumentumnak álcázott Windows-parancsikonokkal, amelyek adatlopásra és távoli parancsvégrehajtásra alkalmas ReverseRAT kártevőt telepítettek.

A NightEagle megszerzett VPN-hitelesítő adatokkal [jutott vállalati hálózatokba](#), majd Microsoft Exchange szervereken alkalmazta a memóriában futó GhostContainer backdoor-t, tevékenysége egészen a tartományvezérlők kompromittálásáig terjedt.

A [Cisco Talos három támadói csoportnál azonosította](#) a Cisco Secure Firewall Management Center CVE-2026-20079 és CVE-2026-20316 sérülékenységeinek aktív kihasználását, amely hitelesítő adatok és konfigurációk eltulajdonításához, Cyclops Blink telepítéséhez, illetve Qilin zsarolóvírusos támadáshoz vezetett.

A Mirage Kitten hamis állásajánlatokkal és fejlesztői próbafeladatokkal [terjesztette](#) a NodeRabbit és PollCat távoli hozzáférést biztosító kártevőket, több operációs rendszeren is lehetővé téve a parancsvégrehajtást és a fájlműveleteket.

Általános káros kód trendek

A vizsgált időszak egyik legjelentősebb kiberbiztonsági eseménye a több mint két évtizede működő Sality P2P-botnet elleni, 2026. augusztus 31-én [végrehajtott nemzetközi művelet volt](#), amelyben az amerikai, bolgár, román és magyar hatóságok is részt vettek. A 2003 óta ismert kártevőhálózathoz működése során több mint 11 millió egyedi IP-címet kapcsoltak, csúcspontján pedig akár egymillió fertőzött számítógép felett biztosíthatott hozzáférést az üzemeltetőinek. A botnetet hitelesítő adatok eltulajdonítására, kéretlen levelek terjesztésére, proxyhálózatok kialakítására és DDoS-támadások végrehajtására is felhasználták. A nemzetközi együttműködés eredményeként több, a botnethez kapcsolódó domaint és infrastrukturelemet vontak hatósági ellenőrzés alá, jelentősen megzavarva a hálózat működését.

A [Group-IB kutatói azonosították](#) a RemControl nevű, szolgáltatásként kínált Android-kártevőplatformot (MaaS), amelynek segítségével a támadók elsősorban európai, kanadai és közel-keleti felhasználókat céloznak meg hamis alkalmazásletöltési oldalakon és rosszindulatú hirdetésekkel keresztül, banki hitelesítő adatok megszerzése érdekében.

Jelentős fenyegetést jelenthet a [PoisonedRefresh](#) nevű, memóriában működő backdoor, amely az F5 BIG-IP Access Policy Manager rendszerek kritikus, CVE-2025-53521 azonosítójú sérülékenységének kihasználásához kapcsolódik, és fájl nélküli működésével megnehezíti a támadás észlelését.

Hazai káros kód trendek

Az NBSZ-NKI hónapról hónapra elvégzi a Magyarországhoz köthető fertőzőttiségi információk elemzését. A jelenlegi trendek alapján az első hat kártevő stagnálást mutat, emelkedő tendenciát látunk az LA02, Andromeda és Avalanche káros kódok elterjedtségében.

Káros kód	Trend
BADBOX 2.0	↔
IPIDEA	↔
Vo1d(2)	↔
NetNut	↔
Popcorn Time	↔
Socks Escort	↔
LA02	↑
Andromeda	↑
Ranbyus	↔
Avalanche	↑

1. ábra: Káros kód trendek Magyarországon

Zsarolóvírusok

Zsarolóvírus-csoportok havi aktivitási trendje

A 2026. szeptemberi adatok alapján az INC, Akira, Safepay, Lockbit csoport mutatta a legnagyobb trendelemkedést, míg a Quilin és Gentlemen tartja a két legnépszerűbb zsarolóvírus csoport pozíciót.

Típus	Trend
Quilin	↔
Gentlemen	↔
INC	↑
Akira	↑
Storm	↔
Krybit	↔
Safepay	↑
Lockbit	↑
Emperador	↑
Vexy	↑

2. ábra: Top 10 zsarolóvírus trendadatai

ICS/SCADA

Szeptemberi hónapban az ipari vezérlőrendszereket (ICS/OT) és a hozzájuk kapcsolódó informatikai infrastruktúrát érintő sebezhetőségi jelentések száma továbbra is magas maradt. A CISA több tucat gyártótól származó ICS-tanácsadást adott ki, amelyek között olyan széles körben használt megoldások szerepeltek, mint a Siemens ipari és felügyeleti platformjai, a Hitachi Energy hálózati irányítási rendszerei, a MikroTik RouterOS, valamint különböző videómegfigyelési, hálózati és beágyazott eszközök. A bejelentett hibák jellemzően hitelesítés-kerülést, távoli kód futtatást, parancsinjektálást, érzékeny adatokhoz való jogosulatlan hozzáférést vagy a rendszerek működésének zavarát tették lehetővé; több esetben fizikai biztonsági kockázat is felmerülhetett. Különösen figyelemre méltó, hogy a MikroTik RouterOS hitelesítés-megkerülési hibáját aktívan kihasználták.

Kiber-fizikai peremeszközök és IIoT rendszerek

A vizsgált időszakban a [Tycon Systems TPDIN-Monitor-WEB2](#), az [Eufy Omni C20](#) és [Omni X10 Pro](#), valamint a [Viidure Dashcam Android](#) alkalmazás került a figyelem középpontjába. A felsorolt termékek különböző felhasználási területeket képviselnek: a Tycon Systems eszköze hálózati felügyeleti és monitorozási funkciókat lát el, az Eufy modelljei automatizált háztartási készülékek, míg a Viidure alkalmazás fedélzeti kamerák kezelését támogatja. Hálózati kapcsolataik és beágyazott szoftverkomponenseik révén az ilyen eszközök sérülékenységei illetéktelen hozzáférést, adatvédelmi problémákat vagy működési zavarokat eredményezhetnek, az egyes kockázatok tényleges mértéke azonban az érintett hibák jellegétől és súlyosságától függ.

Ipari kommunikációs csatornák és hálózatfelügyelet

Az [IXON VPN Client](#), a [Pyramid Solutions NetStaX EtherNet/IP Stack](#), az [lwIP TCP/IP Stack MQTT Client Application](#) és a [MikroTik RouterOS](#) kapcsán merültek fel biztonsági szempontból releváns kérdések. Az érintett megoldások ipari távoli hozzáférést, protokollkommunikációt, TCP/IP-alapú adatátvitelt, illetve hálózati forgalomirányítást biztosítanak. Az ezekben található sérülékenységek megfelelő körülmények között lehetőséget teremthetnek illetéktelen hozzáférésre, a kommunikáció megzavarására vagy a hálózati eszközök működésének befolyásolására. A MikroTik RouterOS esetében külön figyelmet érdemelnek az aktívan kihasznált sérülékenységekről szóló közlemények, míg a többi terméknel a konkrét kockázatok megítéléséhez az egyes gyártói biztonsági tájékoztatók részleteinek figyelembevétele szükséges.

Folyamatvezérlési és gyártásirányítási környezetek

Több, ipari folyamatok felügyeletéhez, villamosenergia-rendszerek védelméhez és ipari alkalmazások kezeléséhez kapcsolódó termék is érintett volt biztonsági közleményekben. A [mySCADA myPRO Manager](#) SCADA-környezetek felügyeletét támogatja, a [Siemens Reyrolle 7SR5](#) digitális védelmi relé az elektromos hálózatok védelmében játszik szerepet, míg a [Hitachi Energy FACTS Control Platform \(FCP\)](#)

a villamosenergia-átviteli rendszerek szabályozásához kapcsolódik. A [Siemens Industrial Edge Management](#) az ipari peremeszközök és alkalmazások központi kezelését teszi lehetővé, a [Siemens Mendix Runtime](#) alkalmazások futtatási környezetét biztosítja, a [Toptech TMS7](#) és [TopHAT](#) pedig az üzemanyag-kezelési és terminálirányítási folyamatokhoz kapcsolódik. Az ilyen rendszereket érintő sérülékenységek a hozzáférés-vezérlést, az alkalmazások biztonságos működését vagy az ipari folyamatok rendelkezésre állását veszélyeztethetik; a konkrét hatás az érintett termékverziótól és a sérülékenység jellegétől függ.

Mérnöki munkaállomások és fizikai biztonsági zónák

A fizikai biztonsági rendszerekhez és videómegfigyelési megoldásokhoz kapcsolódóan a [Digital Watchdog VMAX DVR és NVR](#) termékei, a [Siemens Siveillance Control](#), a [VIVOTEK](#) kamerák firmware-e, valamint az [Anjvision YSSD-RTMP-H5](#) került az érintett termékek közé. A felsorolt megoldások videófelvételek rögzítését, hálózati kamerák működtetését, illetve biztonsági rendszerek központi felügyeletét támogatják. Az ilyen eszközök sérülékenységei illetéktelen hozzáférést tehetnek lehetővé a kameraképekhez és a rögzített felvételekhez, veszélyeztethetik a megfigyelési funkciók rendelkezésre állását, vagy gyengíthetik a fizikai biztonsági rendszerek megbízhatóságát. Az egyes termékeket érintő konkrét kockázatok megítéléséhez a gyártói közleményekben meghatározott sérülékenységek és az érintett verziók vizsgálata szükséges.

Kiemelt fenyegetési esemény

A MikroTik RouterOS sérülékenységeinek aktív [kihasználása veszélyezteti](#) az érintett hálózati eszközök biztonságát veszélyeztetik, és megfelelő körülmények között lehetővé tehetik a hitelesítés megkerülését, illetve az eszközök feletti jogosulatlan hozzáférés megszerzését. A sérülékenységek különösen azoknál a rendszereknél jelentenek kockázatot, amelyek távoli elérése nincsen megfelelően korlátozva.

A támadási tevékenységről szóló beszámolók szerint a sérülékenységek kihasználása már szeptember elején megkezdődött. A RouterOS-t futtató eszközök hálózati forgalomirányítási és távoli hozzáférési feladatokat láthatnak el, ezért kompromittálásuk az érintett hálózatok biztonságára és rendelkezésre állására is

hatással lehet. Amennyiben ilyen eszközök ipari környezetben, ICS/SCADA-hálózatokhoz kapcsolódva működnek, a támadás az ipari kommunikációs infrastruktúrát is veszélyeztetheti. Az ipari rendszerek tényleges érintettségére azonban a rendelkezésre álló információk nem szolgáltatnak közvetlen bizonyítékot.

A kockázatok mérséklése érdekében indokolt az érintett RouterOS-verziók felülvizsgálata, a gyártó által kiadott javítások telepítése, valamint az internet felől elérhető adminisztrációs és SSH-szolgáltatások korlátozása. Emellett javasolt a hálózati eszközök naplójának és hozzáférési eseményeinek ellenőrzése az esetleges kompromittálás jeleinek azonosítására. Az esemény kiemelt jelentőségét az aktív kihasználás ténye és a hálózati infrastruktúrára gyakorolt lehetséges hatás indokolja.

Saját hálózati monitoringon (EWS) alapuló CTI helyzetkép

A nemzetközi ICS/SCADA fenyegetési környezet mellett a saját hálózati monitoring rendszer július–szeptember közötti adatai alapján megállapítható, hogy a vizsgált ágazatok magasabb súlyosságú fenyegetési képét továbbra is elsősorban az internet felől elérhető webalkalmazások, webszerverek és hálózati szolgáltatások sérülékenységeinek felderítésére, valamint azok kihasználására irányuló kísérletek határozták meg. A MITRE ATT&CK szerinti besorolásokban az Exploit Public-Facing Application technika továbbra is meghatározó maradt, miközben a júliusban kiugró File and Directory Discovery aktivitás szeptemberre jelentősen visszaszorult. A malware-family besorolású események továbbra is csak kisebb részét képezték a megfigyelt aktivitásnak, így a helyzetkép összességében változatlanul elsősorban sérülékenységvezérelt, jelentős részben automatizált webes felderítési és exploitációs mintázatot mutat.

Szeptemberben a teljes jelzési volumen az előző hónapokhoz képest tovább csökkent, ugyanakkor a magasabb besorolású webes exploitáció továbbra is a fenyegetési kép meghatározó eleme maradt. Az augusztusban kiugró Vite [CVE-2025-30208](#) aktivitása mérséklődött, azonban továbbra is a legjelentősebb sérülékenységi fókuszok között szerepelt. A Log4Shell szintén csökkenő tendenciát mutatott, ugyanakkor változatlanul tartós háttéraktivitásként jelent meg, hasonlóan a PHPUnit

[CVE-2017-9841](#) sérülékenységhoz. Ezzel szemben a korábban nagy volumenű általános directory traversal, valamint a Cisco ASA/Firepower [CVE-2020-3452](#) sérülékenységhoz kapcsolódó aktivitás szeptemberre nagymértékben visszaesett. Ennek következtében a június óta folyamatosan jelen lévő Cisco ASA/Firepower-fókusz gyakorlatilag eltűnt a meghatározó aktivitási minták közül.

A csökkenő összvolumen mellett szeptemberben új, illetve korábban már megfigyelt technológiai fókuszok erősödése is azonosítható volt. A Drupal [CVE-2014-3704](#) SQL injection, valamint a Grafana [CVE-2021-43798](#) path traversal sérülékenységekhez kapcsolódó aktivitás az augusztusi alacsony szintet követően jelentősen megerősödött, különösen a közigazgatási környezetben. Új elemként a Langflow sérülékenységeihez kapcsolódó jelzések is érdemi szintet értek el, elsősorban a pénzügyi szektorban. A kritikus besorolású Apache Struts, F5 TMUI és VMware NSX kihasználási kísérletei az augusztusi visszaesést követően ismét emelkedést mutattak, azonban nem érték el a júliusi kiugró aktivitási szintet.

Ágazati helyzetkép

Egészségügy

Az egészségügyi ágazatban a nyár folyamán megfigyelt csökkenő összaktivitás szeptemberben is folytatódott, miközben a fenyegetési profil alapvetően változatlan maradt. A Vite sérülékenységhoz kapcsolódó aktivitás az augusztusi szinten maradt, míg a PHPUnit továbbra is tartósan jelen volt, bár csökkenő tendenciát mutatott. A directory traversal és az általános fájlfelderítési aktivitás további mérséklődése volt megfigyelhető.

Ezzel párhuzamosan a magasabb besorolású Apache Struts, F5 és VMware jelzések az augusztusi alacsony szintről ismét emelkedtek. A kompromittált vagy alacsony reputációjú külső IP-címekhez kapcsolódó forgalom továbbra is stabil háttérjelenségként volt azonosítható, szeptemberben enyhe erősödéssel.

A malware-jelzések továbbra is kis volumenű webshell-aktivitásra, valamint elszórt Mirai-detektálásokra korlátozódtak. Önálló, tartós malware-trend nem alakult ki.

Közigazgatás

A közigazgatási szektor szeptemberben az augusztusi visszaesést követően ismét jelentős aktivitásnövekedést mutatott. Az ágazat továbbra is a legszélesebb technológiai és sérülékenységi spektrummal rendelkező vizsgált környezetnek tekinthető.

Kiemelkedő növekedés volt tapasztalható a PHP local file inclusion, a Drupal SQL injection, valamint a Grafana path traversal jelzések esetében. A Drupalhoz kapcsolódó aktivitás az augusztusi visszaesést követően a korábbi hónapoknál is hangsúlyosabban tért vissza, míg a Grafana esetében hasonló visszatérő aktivitási minta volt megfigyelhető. A Vite és a PHPUnit szintén erősödést mutatott.

Ezzel párhuzamosan ismét növekedett a fájl és könyvtárfelderítési aktivitás. Ezt többek között az /etc/passwd, a phpinfo, valamint egyéb felderítési minták emelkedése is alátámasztotta. A kompromittált vagy alacsony reputációjú külső IP-címekhez kapcsolódó jelzések szintén jelentősen emelkedtek a korábbi hónapokhoz képest.

A közigazgatási szektor szeptemberi fenyegetési profilját így nem egyetlen domináns sérülékenység határozta meg, hanem több, egymással párhuzamosan erősödő webes támadási és felderítési minta együttes jelenléte.

Pénzügy

A pénzügyi szektor szeptemberben az augusztusi kiugró időszakhoz képest jelentős aktivitásmérséklődést mutatott, ugyanakkor a fenyegetési profil továbbra is erősen koncentrált és szinte teljes egészében magasabb besorolású exploitációs, illetve webes aktivitásból állt.

A Vite sérülékenységhez kapcsolódó aktivitás számottevően csökkent, azonban továbbra is az ágazat elsődleges sérülékenységi fókusza maradt. A Log4Shell szintén mérséklődött, de továbbra is tartósan jelentős aktivitást képviselt.

A legnagyobb változást a directory traversal, valamint a Cisco ASA/Firepower aktivitásának visszaesése jelentette. Az előző hónapokban meghatározó Cisco-sérülékenységi minta szeptemberre gyakorlatilag megszűnt. Ezzel

párhuzamosan új fókuszként jelentek meg a Langflow sérülékenységei, továbbá erősödött

a React/Next.js környezethez kapcsolódó exploitáció.

A WordPress-felderítés továbbra is tartósan magas szinten maradt, így az alacsonyabb besorolású szkennelési aktivitás továbbra is releváns CTI-kontextust biztosított az ágazat esetében.

A pénzügyi szektor adatai alapján továbbra is sajátos, immár több hónapon keresztül fennálló jellemző, hogy kompromittált vagy alacsony reputációjú IP-címekhez kapcsolódó összesített találatok nem jelentek meg.

Turizmus

A turisztikai szektor szeptemberben mérsékelt aktivitásnövekedést mutatott, miközben alapvetően megőrizte viszonylag keskeny, webalkalmazás-központú fenyegetési profilját.

A Vite aktivitása tovább emelkedett, miközben a PHPUnit fokozatosan csökkent, ugyanakkor továbbra is visszatérő elemként volt jelen. Az Apache HTTP Server request smuggling aktivitása stabil szinten maradt, míg a Grafana path traversal aktivitása is érzékelhetőbbé vált.

A kompromittált vagy alacsony reputációjú IP-címekhez kapcsolódó találatok az augusztusi kiugráshoz képest kismértékben mérséklődtek, ugyanakkor továbbra is a nyár elején megfigyelt szint felett maradtak.

A malware-family besorolású aktivitás továbbra sem képviselt érdemi, önálló fenyegetési trendet.

A szeptemberi helyzetkép az augusztusban megfigyelt, koncentrált sérülékenységi hullám részleges lecsengését mutatja. Ezzel párhuzamosan a publikus webes szolgáltatások exploitációja továbbra is a saját hálózati monitoringban megfigyelt fenyegetési kép stabil alapját képezte.

A Vite és a Log4Shell továbbra is meghatározó, ugyanakkor csökkenő aktivitása mellett több korábbi, illetve új technológiai fókusz – különösen a Drupal, a Grafana és a Langflow – erősödött meg. Ágazati szinten a közigazgatás ismét szélesebb és növekvő aktivitást mutatott, míg a pénzügyi szektorban az augusztusi kiugró

aktivitás jelentősen mérséklődött. Az egészségügy és a turizmus esetében az alapvető webes exploitációs profil lényegében stabil maradt.

A gördülő háromhavi adatok alapján továbbra is az a tendencia rajzolódik ki, hogy az egyes konkrét sérülékenységi fókuszok rövid idő alatt jelentősen változhatnak, miközben az automatizált felderítés, valamint az internet felől elérhető szolgáltatások ismert sérülékenységeinek kihasználására irányuló kísérletek tartósan jelen vannak a megfigyelt környezetben.

Sérülékenységek

A hónap fenyegetési képét a peremhálózati eszközök sebezhetőségei határozták meg. Többek között a Citrix [NetScaler](#) (CVE-2026-88771), Check Point (CVE-2026-85102), F5 BIG-IP (CVE-2026-94127), Cisco (CVE-2026-20079, CVE-2026-76460, CVE-2026-76504), Fortinet (CVE-2025-25249), SonicWall (CVE-2026-0257), MikroTik (CVE-2026-86060), Zyxel (CVE-2026-0257) és Arista (CVE-2026-0257) gyártók termékeiben is aktívan kihasznált sebezhetőségeket javítottak. Ezek közül a [NetScaler](#), Check Point VPN és az [F5 BIG-IP APM](#) esetében autentikálatlan támadók tetszőleges kódot futtathatnak az érintett eszközökön.

Szeptemberben közel 15 000 új sebezhetőség vált ismertté, ami 21%-os növekedést jelent az augusztusi adatokhoz képest. Ez az eddigi legmagasabb havi érték, amely a sebezhetőségek publikálásának történetében új rekordot jelent.

A legfontosabb új sebezhetőségek között az említett peremhálózati eszközökön kívül felsorolható még a WordPress ([CVE-2026-87902](#)), a Gitlab ([CVE-2026-85706](#)), illetve a Chrome V8 ([CVE-2026-85046](#)) hibái. Szeptember hónapban továbbra is látható volt aktivitás több régebbi sebezhetőség kihasználására is, mint az Apache Log4j2 ([CVE-2021-44228](#)), WebPros cPanel & WHM ([CVE-2026-41940](#)), végül a Linux Kernel ([CVE-2026-43499](#)). Ezen szoftverek esetén javasolt a lehető legfrissebb verzióra való frissítés.

Honeypot forgalom elemzése

A hónap egyik kiemelt eseménye egy korábban nem észlelt, összetett Linux malware-eszközkészlet azonosítása volt. A GovProbe Honeypot kihelyezett szondák által rögzített dropper URL egy tömörített állományhoz vezetett, amelynek részletes statikus elemzése során Tsunami/Kaiten-alapú kártevőkomponenseket sikerült azonosítani.

A Tsunami (más néven Kaiten) egy régóta ismert, elsősorban Linux-alapú rendszereket célzó botnet-kártevőcsalád, amelynek fő rendeltetése az elosztott szolgáltatásmegtagadással járó (DDoS) támadások végrehajtása. A kártevő IRC-protokollon keresztül kommunikál a támadók által üzemeltetett vezérlőszerverekkel (C2), amelyek segítségével a kompromittált eszközök távolról irányíthatók. A Tsunami különböző változatai többféle támadási módszert támogatnak, köztük TCP SYN-, TCP PUSH/ACK- és UDP-alapú túlterheléses támadásokat. A DDoS-funkciók mellett távoli rendszerparancsok végrehajtására és további kártékony állományok letöltésére is alkalmas lehet. A kártevő különösen veszélyes tulajdonsága, hogy a megfertőzött rendszereket a támadók egy nagyobb botnet részévé tehetik, így azok tulajdonosaik tudta nélkül használhatók fel összehangolt kibertámadásokhoz.

Habár a globális trendek között 2024-ben regisztráltak utoljára nagyobb Tsunami kampány folyamatokat, a különböző kódverziók folyamatos jelenlétet mutatnak az utóbbi két évben is.

Az elemzett archívum 13 db, egymást kiegészítő állományt tartalmazott, amelyek egy összetett támadási és perzisztenciamechanizmust alkotnak. Az install végzi a kártevő telepítését, míg a crond.c, monitor.c és where.c lényegében ugyanazon IRC-vezérelt bot különböző rendszerfolyamatoknak álcázott változatai. Az execute a kártevő működésének fenntartásáért, az authorized_keys és a flush az SSH-alapú hozzáférés biztosításáért felel. A módosított netstat, top, crontab és whereis rendszereszközök a kártékony tevékenység elrejtését és a komponensek újraindítását támogatják. A cleaner.c naplóállományok manipulálásával anti-forenzikus funkciókat lát el, míg a decode.c obfuszkált adatok dekódolására szolgál.

```

1  /*****
2  * This is a IRC based distributed denial of service client. It connects to *
3  * the server specified below and accepts commands via the channel specified. *
4  * The syntax is:
5  *   !<nick> <command>
6  * You send this message to the channel that is defined later in this code. *
7  * Where <nick> is the nickname of the client (which can include wildcards) *
8  * and the command is the command that should be sent. For example, if you *
9  * want to tell all the clients with the nickname starting with N, to send you *
10 * the help message, you type in the channel:
11 *   !N* HELP
12 * That will send you a list of all the commands. You can also specify an *
13 * astrick alone to make all client do a specific command:
14 *   !* SH uname -a
15 * There are a number of commands that can be sent to the client:
16 *   TSUNAMI <target> <secs>      = A PUSH+ACK flood
17 *   PAN <target> <port> <secs>    = A SYN flood
18 *   UDP <target> <port> <secs>    = An UDP flood
19 *   UNKNOWN <target> <secs>      = Another non-spoof udp flood
20 *   NICK <nick>                  = Changes the nick of the client
21 *   SERVER <server>              = Changes servers
22 *   GETSPOOFS                    = Gets the current spoofing
23 *   SPOOFS <subnet>              = Changes spoofing to a subnet
24 *   DISABLE                      = Disables all packeting from this bot
25 *   ENABLE                      = Enables all packeting from this bot
26 *   KILL                         = Kills the knight
27 *   GET <http address> <save as> = Downloads a file off the web
28 *   VERSION                     = Requests version of knight
29 *   KILLALL                      = Kills all current packeting
30 *   HELP                        = Displays this
31 *   IRC <command>                = Sends this command to the server
32 *   SH <command>                 = Executes a command
33 * Remember, all these commands must be prefixed by a ! and the nickname that *
34 * you want the command to be sent to (can include wildcards). There are no *
35 * spaces in between the ! and the nickname, and there are no spaces before *
36 * the !
37 *
38 *   - contem on efnet
39 *****/
40 ///////////////////////////////////////////////////
41 //                                EDIT THESE                                //
42 ///////////////////////////////////////////////////
43 #define STARTUP                  // Start on startup?
44 #undef IDENT                    // Only enable this if you absolutely have to
45 #define FUCKNAME "crond"         // Fake process
46 #define CHAN "#"                // Channel to join
47 #define KEY "changethekey"       // The key of the channel if encirc = 0 (without encrypt)
48 #define enc_passwd "$7$73|tFE"  // The key of the channel if encirc = 1 (using encrypt)
49 #define encirc 1                 // Enable or Disable encrypt.
50 int numservers=2;               // Must change this to equal number of servers down there
51 char *servers[] = {             // List the servers in that format, always end in (void*)0
52     "3qC?nys7ooqv\y3ryqn",
53     "3qC?nyAq*7y3ryqn",
54     (void*)0
55 };
56
57 ///////////////////////////////////////////////////
58 //                                STOP HERE!                                //
59 ///////////////////////////////////////////////////

```

3. ábra: Képernyőkép a malware állomány "crond.c" fájlban megtalálható működési leírásról.

Az elemzés során két obfuscált IRC C2 cím is azonosításra került, amelyekkel a botok a szokatlan TCP/20-as porton kommunikálnak. A kártevő több párhuzamos tartós jelenlétet biztosító mechanizmust alkalmaz, beleértve az SSH-kulcsok elhelyezését, a cronfeladatok módosítását, a rendszereszközök lecserélését, valamint az állományok időbélyegeinek és jogosultságainak manipulálását.

Az azonosított Tsunami/Kaiten malware-csomag egyik legérdekesebb sajátossága az összetett felépítése, valamint a legitim rendszerfolyamatokkal és rendszereszközökkel történő álcázása. Különösen figyelemre méltó, hogy a kártevő olyan legitim Linux-rendszereszközöket is lecserél, mint a netstat, a top, a crontab és a whereis. A módosított változatok egyes hálózati kapcsolatok elrejtése mellett a kártékony komponensek automatikus újraindítását is biztosíthatják, akár egy hétköznapi rendszergazdai művelet során.

Az észlelés jelentőségét elsősorban nem egy új kártevőcsalád megjelenése, hanem egy többfunkciós, rejtőzködésre és tartós hozzáférésre optimalizált támadói eszközkészlet azonosítása adja. A feltárt működés alapján a kompromittált Linux-rendszerek nemcsak DDoS-támadások végrehajtására használhatók fel, hanem további kártékony tevékenységek kiindulópontjaivá is válhatnak.

Fájl	Azonosított funkció
install	Fő telepítőszkript, amely létrehozza az SSH-backdoort, lefordítja és telepíti a kártékony komponenseket, lecseréli a rendszereszközöket, valamint kialakítja a cron-alapú perzisztenciát.
crond.c	IRC-alapú Kaiten/Tsunami DDoS-bot, amely crond rendszerfolyamatnak álcázza magát. Távoli parancsvégrehajtást és további állományok letöltését is támogatja.
monitor.c	A Kaiten/Tsunami bot második példánya, amely spamd child folyamatnak álcázva biztosít párhuzamos támadói hozzáférést.
where.c	A Kaiten/Tsunami bot harmadik példánya, amely sshd: [accepted] folyamatnak álcázva működik.
execute	A monitor komponens működését ellenőrzi, szükség esetén újraindítja, valamint gondoskodik a cron szolgáltatás elindításáról.
authorized_keys	Két támadói SSH-nyilvános kulcsot tartalmaz, amelyek illetéktelen, kulcsalapú hozzáférés kialakítására szolgálnak.
flush	Az SSH-backdoor helyreállítását végzi, módosítja a daemon felhasználó bejelentkezési környezetét, és újratelepíti a támadói SSH-kulcsokat.
netstat	Módosított hálózati diagnosztikai eszköz, amely többek között a TCP/20, TCP/43 és 3389-es portokhoz kapcsolódó bejegyzések kiszűrésére szolgál.
top	Módosított rendszerfelügyeleti eszköz, amely meghívja az execute és flush komponenseket, támogatva a kártevő működésének fenntartását.
crontab	Módosított rendszerparancs, amely a legitim működés mellett root jogosultság esetén ellenőrzi és szükség esetén elindítja a crond botot.
whereis	Módosított rendszerparancs, amely root jogosultság esetén ellenőrzi és szükség esetén elindítja a where botkomponenst.
cleaner.c	Anti-forenzikus eszköz, amely rendszer- és bejelentkezési naplók manipulálására, meghatározott bejegyzések eltávolítására, valamint a naplózási folyamat ideiglenes leállítására alkalmas.
decode.c	Egyszerű, bitenkénti negáláson alapuló dekódoló segédprogram, amely a /usr/share/boot.sync állomány tartalmát dolgozza fel.



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



NEMZETI
KIBERBIZTONSÁGI
INTÉZET