MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

August 2021

Vypracoval: CSIRT.SK

TLP: White

Posledný júlový deň a začiatkom augusta sa konalo v poradí už 24. podujatie s názvom Black Hat USA. Jedná sa o podujatie, kde sa stretávajú odborníci z oblasti kybernetickej a informačnej bezpečnosti z celého sveta a posúvajú svoje poznatky ofenzívnym a defenzívnym hackerom na všetkých úrovniach. Tento rok sa odborníci podelili o svoje skúsenosti nie len v rámci prednášok (tentoraz naživo v Las Vegas), ale tiež prostredníctvom virtuálnych školení.

Bezpečnostnú konferenciu odštartoval výskumník Matt Tait, ktorý zastával pozíciu v tíme Google Project Zero a v britskej spravodajskej agentúre GCHQ. Vyzval dodávateľov platforiem, aby urobili zásadné technologické zmeny, vďaka ktorým by bolo možné zvládnuť nárast zero-day zraniteľností na mobilných zariadeniach a tiež nárast útokov na dodávateľské reťazce. Hovoril napríklad o tom, že jednou z chýbajúcich funkcií mobilných zariadení je možnosť skenovania aplikácií. V Google Obchode Play je to do istej miery povolené, avšak v obchode v systémoch iOS to urobiť nevieme.

V rámci podujatia bezpečnostní výskumníci tiež ukázali ako je možné obísť biometrickú autentifikáciu Windows Hello pomocou falošnej USB kamery. Zraniteľnosť CVE-2021-34466 spoločnosť Microsoft opravila v júli tohto roku. Avšak podľa výskumu v rámci Black Hat USA chyba stále umožňuje útočníkom obísť Windows Hello a Windows Hello for Business. Výskumník Omer Tsarfati uviedol, že všetko čo je potrebné, je infračervený rámec cieľa. Následne môže útočník tieto údaje vložiť do klonovanej kamery na báze USB a zapojiť ju do systému Windows 10. Ukázalo sa teda, že v júlová oprava zraniteľnosť neodstránila, len zmiernila.

Edmund Brumaghin, výskumný inžinier, priniesol zaujímavú prednášku na tému ransomvérových útokov. Rozprával o vývine taktík používaných operátormi ransomvéru. Tzv. trend „lov veľkých hier“ spočíva v tom, že útočníci nenasadzujú ransomvér okamžite do cieľového systému. Namiesto toho najprv získajú počiatočný prístup prostredníctvom koncového bodu, a potom sa pohybujú laterálne po sieti, aby získali prístup k čo najväčšiemu počtu systémov. Následne útočníci nasadia ransomvér. Potom, čo obeť stratí kontrolu nad svojimi systémami, sa objavuje trend dvojitého vydierania (tzv. „one-two-punch“ vydieranie). Nie len že obeť má len obmedzený čas na zaplatenie výkupného pre opätovné získanie prístupu na zašifrovaný server, no útočníci sa tiež vyhrážajú zverejnením ukradnutých údajov.

Na konferencii Black Hat 2021 sa taktiež predstavila nová vedúca agentúry americkej vlády pre kybernetickú bezpečnosť Jen Easterly. Riaditeľka CISO vo videonahrávke oznámila novú spoluprácu (Joint Cyber Defense Collaborative – JCDC), ktorá má spojiť federálne agentúry s veľkými spoločnosťami ako Microsoft, Amazon Web Services, Google Cloud a ďalšími, za účelom zvládania ransomvérových útokov a útokov na dodávateľské reťazce. JCDC sa spočiatku zameria na zdieľanie informácií a nástrojov, ktoré obrancom pomôžu vyrovnať sa s ransomvérom, vrátane vytvorenia plánovacieho rámca na koordináciu incidentov zasahujúcich poskytovateľov cloudových služieb.

V rámci podujatí akým je Black Hat sa nie len obrancovia, ale aj potenciálni útočníci dozvedia mnoho zaujímavých informácií, ktoré vedia využiť vo svoj prospech – my uvádzame len niekoľko z nich. Je už

na spoločnostiach a jednotlivcoch, ako sa k takýmto informáciám postavia. Či ich využijú pre zvýšenie svojej obranyschopnosti, alebo ponechajú útočníkom otvorené možnosti zneužiť ich.

Riešené incidenty na Slovensku a z našej činnosti

Mesiac august sa vzhľadom na počet a závažnosť prijatých hlásení o kybernetických bezpečnostných incidentoch v rámci konštituencie CSIRT.SK niesol v pokojnom duchu.

V rámci svojej bežnej činnosti, CSIRT.SK v mesiaci august riešila štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Jednotka zaznamenala aj cielené, spear-phishingové útoky šíriace malvér. V tejto súvislosti došlo aj ku kompromitácii mailového účtu zamestnanca orgánu v konštituencii CSIRT.SK, odkiaľ útočníci hromadne rozposielali e-maily so škodlivým odkazom na ďalšie organizácie jej konštituencie.

Jednotka prijala hlásenie od zahraničného partnera, ohľadom infikovaných zariadení v SR v rámci kampane šíriacej malvér SystemBC RAT. Tento škodlivý kód zneužívajú útočníci pri ransomvérových útokoch (Ryuk, Sodinokibi, Egregor). Podľa verejne dostupných zdrojov zvyknú útočníci niektoré útoky kombinovať s nástrojom Cobalt Strike. Jednotka poskytla zasiahnutým subjektom indikátory kompromitácie, ktoré prijala od zahraničného partnera. Ku škodám podľa informácií jednotky v rámci jej konštituencie však nedošlo.

Významné útoky vo svete

Nový variant malvéru AdLoad je hrozbou pre zariadenia Apple

Nový variant malvéru AdLoad pre zariadenia Apple prechádza vstavaným antivírusovým riešením XProtect, ktoré je založené na YARA pravidlách, pričom infikuje zariadenia Mac. Jedná sa o trójskeho koňa, ktorý sa zameriava na macOS už od roku 2017. AdLoad nainštaluje webové proxy, ktoré ukradne výsledky vyhľadávačov a za účelom finančného zisku vkladá reklamy na webové stránky. Inštaláciou LaunchAgents získava perzistenciu na infikovaných zariadeniach. Napriek tomu, že AdLoad aktuálne využíva len advér a bundlevér, tvorcovia môžu rýchlo prejsť na nebezpečnejší malvér.

Na internetovom trhu s názvom AllWorld Cards sa objavil 1 milión platobných kariet ukradnutých v rokoch 2018 až 2019

Na internete vznikol nový trh s názvom AllWorld Cards s ponukou 1 milióna platobných kariet ukradnutých v rokoch 2018 až 2019. Útočník uvádza, že náhodný výber 98 kariet ukázal, že približne 27% z nich je stále aktívnych. Zo správy talianskej spoločnosti D3Labs však vyplýva, že až 50% zo všetkých kariet je stále funkčných a aktívne používaných. Podľa spoločnosti Cybersecurity Cyble únik zahŕňa čísla kariet, dátumy vypršania platnosti, CVV bezpečnostné kódy, mená, krajiny, štáty a ďalšie. Pre dotknuté osoby je dôrazne odporúčané požiadať o vystavenie novej karty. Ceny kariet na tomto novom trhu sa pohybujú od 0,30 do 14,40 dolárov.

Malvér FlyTrap odcudzuje cookies relácie a následne kradne facebookové účty

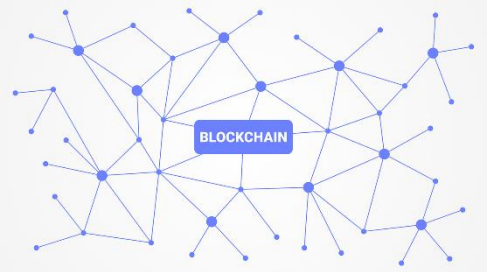
Nový malvér pre Android s názvom FlyTrap kradne účty na Facebooku odcudzovaním cookies relácií. Krádež sa týka rôznych účtov z viac ako 140tich krajín. V kampaniach sa malvér spolieha na taktiky sociálneho inžinierstva. K odcudzeným údajom mal prístup každý, komu sa podarilo objaviť riadiaci server malvéru.

Útočníci používali škodlivé aplikácie distribuované prostredníctvom obchodu Google Play alebo obchodov tretích strán pre Android. Jednalo sa konkrétne o ponuky na bezplatné kupóny napríklad pre Netflix a ďalšie. Obeťami je viac ako 10-tisíc používateľov operačného systému Android.

Ransomvér eCh0raix je schopný šifrovať NAS zariadenia spoločností QNAP a Synology v rámci jednej kampane

Novoobjavený variant ransomvéru eCh0raix pridal funkcionalitu na šifrovanie NAS zariadení spoločností QNAP a Synology. Tento kmeň ransomvéru bol prvýkrát objavený v roku 2016. Nová verzia malvéru eCh0raix zneužíva kritickú zraniteľnosť CVE-2021-28799 súvisiacu s nesprávnou autorizáciou. V minulosti sa malvér zameriaval zvlášť na zariadenia spoločnosti QNAP a zvlášť na zariadenia spoločnosti Synology, avšak od septembra roku 2020 je schopný zameriavať sa na zariadenia oboch spoločností v rámci jednej kampane. Útočníci sa hrubou silou snažia doručiť ransomvér – snažia sa uhádnuť bežne používané administrátorské prihlasovacie údaje. Podľa spoločnosti Palo Alto Networks existuje viac ako 250-tisíc zariadení vystavených do internetu.

V rámci útoku na kryptomeny bolo údajne ukradnutých viac ako 611 miliónov dolárov



Pri jednom z najväčších útokov na kryptomeny bolo údajne ukradnutých viac ako 611 miliónov dolárov. Spoločnosť Poly Network oznámila, že bola zasiahnutá veľkým útokom, kde sa útočníkom podarilo previesť jednotky Binance Chain, Ethereum a Polygon Assets do svojich peňaženiek. Spoločnosť SlowMist zaoberajúca sa bezpečnosťou blockchainu tvrdí, že sa im podarilo vypátrať ID útočníka a identifikovať útočníkovu emailovú adresu, IP adresu a odtlačok prsta. Útočník sa však na druhý deň rozhodol ukradnuté financie vrátiť. Motiváciu pre kradnutie vysvetlil vkladaním správ do transakcií, avšak motivácia na vrátenie ostáva záhadou. Je možné, že sa útočník bál odhalenia svojej totožnosti a prípadných postihov za takéto konanie.

Spoločnosť Gigabyte utrpela útok ransomvérom. Odcudzených bolo 112 GB údajov

Výrobca matičných dosiek Gigabyte bol napadnutý skupinou stojacou za ransomvérom RansomEXX. Skupina tvrdí, že sa jej podarilo odcudziť 112 GB údajov. Spoločnosť v dôsledku tohto útoku bola nútená uviesť svoje systémy na Taiwane do režimu offline. Zasiahnutý bol malý počet serverov, pričom o útoku informovali tiež orgány činné v trestnom konaní. Operátori ransomvéru RansomEXX po zašifrovaní údajov vytvárajú poznámky obsahujúce informácie o výkupnom na každom šifrovanom zariadení. Útočníci zdieľali na stránke informáciu, že sa im podarilo ukradnúť tiež mnoho dokumentov, ktoré sú pod zmluvou o mlčanlivosti (Intel, AMD, American Megatrends).

Spoločnosť Accenture sa stala obeťou úniku údajov o veľkosti 6 TB

Spoločnosť Accenture bola zasiahnutá útokom ransomvéru. Za ransomvérom údajne stojí ransomvérový gang LockBit. Skupina hrozí zverejnením údajov, ak nebude zaplatené výkupné. Spoločnosť Accenture uviedla, že postihnuté systémy obnovila zo zálohy, pričom po identifikovaní podozrivej aktivity izolovala dotknuté servery. Skupina útočníkov tvrdí, že ukradla 6 TB údajov a vyžaduje výkupné o výške 50 miliónov dolárov. Napadnutých bolo 2500 počítačov patriacich zamestnancom a partnerom. Útočníci zverejnili na ich webových stránkach viac ako 2000 súborov údajne patriacich spoločnosti Accenture. Spoločnosť sa zatiaľ nevyjadrila k uniknutým súborom, avšak analytici uvádzajú, že súbory zrejme neobsahujú informácie o zákazníkoch.

T-Mobile utrpel únik údajov, ktorý údajne obsahoval záznamy o približne 100 miliónoch zákazníkov

T-Mobile sa stal obeťou úniku údajov, pričom útočník tvrdil, že ukradol údaje približne o 100 miliónoch zákazníkov. Databázu plnú údajov o 30tich miliónoch zákazníkov predával na hackerskom fóre za 6 Bitcoinov. Uniknuté údaje môžu zahŕňať dátumy narodenia, čísla

vodičských preukazov, čísla sociálneho zabezpečenia, telefónne čísla a ďalšie údajne od roku 2004. Útočníci tvrdia, že sa nabúrali na produkčné, pracovné, ale aj vývojové servery vrátane databázového Oracle servera. Uviedli, že útok bol vykonaný ako pomsta voči USA za únos a mučenie Johna Erina Binnsa v Nemecku agentmi CIA a tureckými spravodajskými službami v roku 2019.

Spoločnosť SAC Wireless sa stala obeťou útoku ransomvérom Conti – uniklo 250 GB údajov

SAC Wireless, dcérska spoločnosť spoločnosti Nokia, utrpela útok ransomvérom Conti. Útočníkom sa podarilo úspešne kompromitovať jej sieť, ukradnúť údaje a tiež šifrovať systémy. Spoločnosť zistila, že jej sieť bola narušená už 16. júna 2021. Útočníci ukradli osobné údaje súčasných, ale aj bývalých zamestnancov. Ukradnuté údaje zahŕňajú meno, dátum narodenia, kontaktné údaje, číslo sociálneho poistenia, informácie o zamestnaní a ďalšie. Skupina útočníkov tvrdí, že ukradla 250 GB údajov a ak spoločnosť nezaplatí výkupné, plánujú tieto údaje zverejniť.

Skupina útočníkov FIN8 nasadzuje zadné vrátka s názvom Sardonic do siete americkej finančnej organizácie

Skupina útočníkov s názvom FIN8 narušila sieť americkej finančnej organizácie a nasadila do nej zadné vrátka Sardonic. Skupina využíva množstvo rôznych nástrojov a taktík ako napríklad malvér POS alebo spearphishingové kampane. Sardonic je malvér napísaný v jazyku C++ a je nasadzovaný prostredníctvom techník sociálneho inžinierstva. Funkcie malvéru zahŕňajú zber systémových informácií, vykonávanie príkazov na kompromitovaných zariadeniach a tiež načítanie DLL knižníc a vykonávanie ich funkcií.

Zoskupenie pod názvom „DeadRinger“ útočí na siete telekomunikačných spoločností v juhovýchodnej Ázii

Bezpečnostní výskumníci odhalili 3 kyberšpionážne kampane, ktoré sa zameriavajú na kompromitáciu sietí veľkých telekomunikačných spoločností v juhovýchodnej Ázii už od roku 2017. Útočníci údajne pracujú pre záujmy čínskeho štátu a sú zoskupení pod názvom „DeadRinger“. Skupiny stojace za útokmi sú Soft Cell, Naikon a pravdepodobne Emissary Panda (APT27). Skupina Soft Cell získavala prístup zneužívaním zraniteľností serverov Exchange a následne inštalovala webový shell China Chopper. Tiež využívala zadné vrátka PcShare, Cobalt Strike, WMI a modifikovaný Mimikatz. Naikon vo svojich útokoch využíval zadné vrátka Nebulae, PAExec, WMI, modifikovaný Mimikatz a ďalšie. Posledná skupina použila exploity servera Exchange na nasadenie vlastných zadných vrátok.

- **Malvér Solarmaker, ktorý sa zameriava na krádež údajov, je opäť aktívny.**
- **Nová APT skupina Praying Mantis sa zameriava na servery Microsoft IIS.**
- **Emailový marketingový účet spoločnosti Chipotle bol kompromitovaný na šírenie malvéru.**
- **Bezpečnostní výskumníci navrhli spôsob, ako zablokovať vektor útoku PetitPotam, ktorý umožňuje útočníkom ľahko prevziať kontrolu nad radičom domény Windows.**
- **Útok ransomvéru zasiahol taliansky región Lazio a tiež web určený pre registráciu na očkovanie proti COVID-19.**
- **Skupina stojaca za ransomvérom LockBit najíma insiderov na pomoc s kompromitáciou podnikových sietí.**
- **Talianska energetická skupina ERG hlási menšie poruchy po útoku ransomvéru.**

- **Nespokojný spolupracovník gangu za ransomvérom Conti zverejnil výcvikový materiál skupiny, vrátane informácií o jednom z operátorov ransomvéru.**
- **Linuxová verzia ransomvéru BlackMatter sa zameriava na servery VMware ESXi.**
- **Najmenej 30-tisíc Exchange serverov vystavených na internete je stále zraniteľných voči útokom ProxyShell.**
- **Útočníci zneužívajú zraniteľnosť na obídenie autentifikácie, ktorá ovplyvňuje milióny smerovačov.**
- **Útoky zamerané na iránske ministerstvo dopravy a národný vlakový systém, koordinoval útočník prezývaný Indra.**
- **Spoločnosť Crytek potvrdila, že za únik údajov spoločnosti je zodpovedný ransomvér Egregor.**
- **Dešifrovací kľúč z útokov ransomvéru REvil na zákazníkov spoločnosti Kaseya unikol na hackerskom fóre.**
- **Ransomvérová skupina zneužíva zraniteľnosť PrintNightmare na prelomenie Windows serverov.**
- **Útočníci využívajú vo svojich phishingových útokoch morzeovku na zabránenie detekcii.**
- **Skupina stojaca za ransomvérom SynAck uverejnila hlavné dešifrovacie kľúče.**
- **Údajné emaily z litovského ministerstva zahraničných vecí sú na predaj na fóre, ktoré slúži na obchodovanie s údajmi.**
- **Útočníci využívajú systém CAPTCHA na ukrytie phishingu alebo malvéru.**
- **Colonial Pipeline potvrdil únik údajov po májovom útoku ransomvéru DarkSide.**
- **Banka Chase sa priznala k technickej chybe na svojom webe a v aplikácii, ktorá umožňovala náhodný prístup k informáciám o bankovníctve iným zákazníkom.**
- **Brazílske ministerstvo hospodárstva odhalilo útok ransomvéru na Národnú pokladnicu.**

- **Malvér ShadowPad sa stáva obľúbenou voľbou čínskych špionážnych skupín.**

- **Cloudflare zmiernil jeden z najväčších DDoS útokov zahŕňajúci 17,2 miliónov požiadaviek za sekundu.**

Závažné zraniteľnosti bežných softvérových produktov

Kritické zraniteľnosti Cisco

Spoločnosť Cisco opravila viacero závažných a 4 kritické zraniteľnosti.
CVE-2021-1609: Zraniteľnosť vo webovom rozhraní správy Cisco Small Business RV340, RV340W, RV345 a RV345P Dual WAN Gigabit VPN smerovačov môže umožniť neautentifikovanému útočníkovi vzdialene vykonať ľubovoľný kód alebo spôsobiť narušenie dostupnosti služby (DoS).
CVE-2021-34730: Zraniteľnosť v službe Universal Plug-and-Play (UPnP) Cisco Small Business RV110W, RV130, RV130W a RV215W smerovačov by mohla umožniť neoverenému vzdialenému útočníkovi vykonať ľubovoľný kód alebo spôsobiť narušenie dostupnosti služby (DoS).
CVE-2021-22156: Zraniteľnosť súvisiaca s pretečením premennej typu integer sa nachádza v nasledujúcich vydaniach softvéru BlackBerry: QNX Software Development Platform (SDP) - 6.5.0SP1 a staršie, QNX OS for Medical - 1.1 a staršie a QNX OS for Safety - 1.0.1 a staršie. Úspešným zneužitím by mohlo dôjsť k vykonaniu ľubovoľného kódu alebo narušeniu dostupnosti služby (DoS).
CVE-2021-1577: Zraniteľnosť v koncovom bode API Cisco Application Policy Infrastructure Controller (APIC) a Cisco Cloud Application Policy Infrastructure Controller (Cloud APIC) by mohla umožniť neoverenému vzdialenému útočníkovi čítať alebo zapisovať ľubovoľné súbory v dotknutom systéme.

Zraniteľnosti Intel

V produktoch Intel boli opravené dve závažné zraniteľnosti.
Prvá zraniteľnosť *CVE-2021-0084* súvisí s nesprávnym overením vstupu v ovládači Intel® Ethernet Controllers X722 a 800 Series Linux RMDA pred verziou 1.3.19.
Druhá zraniteľnosť *CVE-2021-0196* súvisí s nesprávnym riadením prístupu v ovládači režimu jadra niektorých súprav Intel® NUC 9 Extreme Laptop Kits pred verziou 2.2.0.20.
Obe tieto zraniteľnosti môžu umožniť autentifikovanému útočníkovi povoliť eskaláciu privilégií prostredníctvom lokálneho prístupu.

Zraniteľnosť Atlassian Confluence

Produkty Confluence Server a Confluence Data Center obsahujú chybu s označením CVE-2021-26084, ktorá umožňuje autentifikovanému útočníkovi vykonávať ľubovoľný kód. V istých prípadoch nie je autentifikácia pre zneužitie zraniteľnosti potrebná. Spoločnosť Atlassian vydala opravené verzie zraniteľných produktov (6.13.23, 7.4.11, 7.11.6, 7.12.5, and 7.13.0).

Zraniteľnosť F5 BIG-IP

Spoločnosť F5 opravila v auguste v produkte BIG-IP 13 zraniteľností vysokej závažnosti. Zraniteľnosť CVE-2021-23031 v moduloch Advanced WAF a Application Security Manager umožňuje autentifikovaným útočníkom eskaláciu privilégií, pričom v niektorých konfiguráciách dosahuje hodnotenie kritická. Môže viesť k úplnej kompromitácii systému.

Mesačník zraniteľností August 2021

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java

https://www.csirt.gov.sk/posts/2549.html?csrt=5049432114705709451