MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

September 2021

Vypracoval: CSIRT.SK

TLP: White

V septembri zverejnila spoločnosť McAffee správu ohľadom ransomvéru BlackMatter, ktorý je aktívny už od júla 2021. Malvér začal svoje „pôsobenie“ veľkým počtom útokov, pričom jeho vývojári tvrdia, že prebrali najlepšie časti z ransomvérov ako GandCrab, LockBit a DarkSide. Útočníci tvrdia, že sú novou skupinou, avšak McAfee Enterprise Advanced Threat Research o tom má veľké pochybnosti. Malvér má totižto veľmi veľa spoločných znakov s ransomvérom DarkSide, ktorý je spájaný s útokom na Colonial Pipeline.

Ransomvérom BlackMatter bola zasiahnutá spoločnosť v oblasti medicínskych technológií Olympus. Po zistení podozrivej aktivity spoločnosť pozastavila prenosy údajov v dotknutých systémoch a informovala príslušných externých partnerov. Bezpečnosť a služby pre zákazníkov neboli týmto incidentom ovplyvnené. Aj keď spoločnosť Olympus nezdieľala žiadne podrobnosti o identite útočníkov, poznámky o výkupnom zanechané na systémoch zasiahnutých počas útoku poukazujú na útok ransomvéru BlackMatter.

Obeťou ransomvéru BlackMatter sa stal tiež Marketron, poskytovateľ podnikových softvérových riešení. Zákazníci sa o incidente dozvedeli prostredníctvom emailu, v ktorom bolo uvedené, že za útok je zodpovedná ruská zločinecká skupina BlackMatter. Incident sa vyskytol aj napriek nedávnej investícii do implementácie kybernetickej bezpečnosti na ochranu pred útočníkmi. Po zistení, že sa spoločnosť stala obeťou incidentu, bolo nutné, aby uviedla svoje služby do režimu offline.

Za posledných niekoľko dní sa obeťou stalo aj americké farmárske družstvo NEW Cooperative, pričom skupina útočníkov žiadala výkupné o výške 5,9 milióna dolárov. Vyhrážali sa, že ak výkupné nebude zaplatené do piatich dní, sumu navýšia na dvojnásobok. Keď sa BlackMatter prvýkrát objavil, útočníci uviedli, že sa nebudú zameriavať na „zariadenia kritickej infraštruktúry (jadrové elektrárne, elektrárne, zariadenia na úpravu vody).“ Preto nie je celkom jasné, prečo sa útočníci zamerali práve na tento cieľ, keďže útok povedie k prerušeniu dodávky potravín.

Zaujímavosťou je, že útočníci sa zamerali aj na ďalšie poľnohospodárske družstvo Crystal Valley sídliace v Minnesote. Útok, ktorý infikoval počítačové systémy, viedol k vypnutiu systémov, čím zabránil platbám kreditnými kartami Visa, Mastercard a Discover. Nie je však stopercentne jasné, či sa jednalo o útok skupiny stojacej za ransomvérom BlackkMatter.

BlackMatter sa zvyčajne vyskytuje ako spustiteľný EXE súbor a v špeciálnych prípadoch ako DLL knižnica (pre Windows). Počítače s operačným systémom Linux môžu byť zasiahnuté špeciálnymi verziami. Hlavným cieľom ransomvéru BlackMatter je zašifrovať súbory v infikovanom počítači a následne požadovať výkupné. Útočníci kradnú súbory a citlivé údaje z napadnutých serverov a požadujú výkupné, aby tieto údaje nezverejnili na internete. Štýl kódu je nápadne podobný ransomvéru DarkSide. Vývojári sa však dopustili niekoľkých chýb, ktoré umožnili vytvorenie „vakcíny“, ktorá však môže ovplyvniť iné programy.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci september riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytol sa tiež prípad kompromitovanej schránky zamestnanca štátnej inštitúcie, odkiaľ útočníci rozposlali veľké množstvo phishingových e-mailov. Po zablokovaní konta a zmene hesla sa incident neopakoval.

Jednotka prijala informáciu o spearphishingovej kampani na niekoľko inštitúcií vo sovjej konštituencii. Incident vyšetrovala na základe indikátorov kompromitácie. Komunikácia na servery útočníkov sa nepreukázala.

Zaujímavým prípadom nahláseným jednotke v septembri bol únik informácií vo forme e-mailu, ktorého plné znenie mala s dispozícii strana, ktorá nepatrila k jeho adresátom. E-mail použila v rámci súdneho sporu. CSIRT.SK poskytol poškodenému subjektu pomoc pri identifikovaní vektora úniku a odporúčania pre ďalšie kroky.

CSIRT.SK informoval niekoľko subjektov o zraniteľnostiach ich mailserverov, ktoré našiel v rámci svojich proaktívnych činností.

V septembri spustila vládna jednotka CSIRT kampaň skenovania zraniteľností v IT infraštruktúrach organizácií vo svojej konštituencii. V pravidelných intervaloch bude neinvazívne skenovať zariadenia a zdroje viditeľné z internetu a upozorňovať zraniteľné organizácie na nálezy. Opravami známych zraniteľností IT systémov a produktov bude možné predchádzať mnohým útokom, ktoré ich zneužívajú ako vektor pre prienik. Jednotka pre tento účel vyvinula vlastnú platformu spájajúcu viacero open source riešení, ktorú nazvala Achilles.

V rámci svojej proaktívnej činnosti jednotka preškolila od leta 2021 niekoľko stoviek štátnych zamestnancov. Témou boli základy informačnej bezpečnosti a bežné hrozby, s ktorými sa účastníci môžu stretnúť v pracovnom aj súkromnom živote. Účastníci získali informácie, ako tieto hrozby rozpoznávať a ako sa pred nimi brániť. Prezentácia ku školeniu je dostupná na našej webstránke.

Významné útoky vo svete

Únik údajov týkajúci sa spoločnosti MyRepublic Singapore odhalil informácie o približne 80-tisíc zákazníkoch

Spoločnosť MyRepublic Singapore sa stala obeťou úniku údajov, ktorý odhalil informácie o približne 80-tisíc mobilných predplatiteľoch. Dátové úložisko bolo podľa oficiálneho stanoviska po útoku zabezpečené. Uniknuté údaje zahŕňajú dokumenty na overenie totožnosti, ako naskenované kópie oboch strán NRIC (národná registračná identifikačná karta), doklady o adrese bydliska, meno a mobilné číslo. MyRepublic tvrdí, že incident nahlásila singapurskému úradu Infocomm Media Development Authority a komisii pre ochranu osobných údajov a bude s nimi spolupracovať pri vyšetrovaní bezpečnostného incidentu.

Ruský internet sa stal obeťou najväčšieho útoku v histórii

Ruský internetový gigant Yandex sa stal obeťou DDoS útoku (distribuované narušenie dostupnosti služby). Za útokom stojí nový botnet s názvom Mēris. Rusko tento útok označilo za najväčší v histórii ruského internetu nazývaného RuNet. Spoločnosť Qrator Labs uviedla, že sa podarilo nahliadnuť na vnútornú štruktúru botnetu. Tunely L2TP sa používajú na komunikáciu v sieti, pričom počet infikovaných zariadení dosahuje 250-tisíc. Útočníci stojaci za botnetom Mēris však nechcú predvádzať plnú silu botnetu – zaznamenaná bola úderná sila viac ako 30-tisíc zariadení. DDoS útok botnetu Mēris dosiahol 21,8 miliónov požiadaviek za sekundu.

Na internete sa objavil zoznam takmer 500-tisíc prihlasovacích mien a hesiel pre Fortinet VPN

Útočníci uverejnili zoznam takmer 500-tisíc prihlasovacích mien a hesiel pre Fortinet VPN, ktoré boli údajne zozbierané ešte minulé leto. Tieto prihlasovacie

údaje môžu útočníkom slúžiť na získanie prístupu k sieti, vykonanie exfiltrácie údajov, inštaláciu malvéru alebo vykonanie ransomvérových útokov. Zneužívaná zraniteľnosť bola opravená, avšak mnohé prihlasovacie údaje do VPN ostali nezmenené. Zoznam týchto prihlasovacích údajov unikol skupine útočníkov s názvom Orange, ktorá je správcom hackerského fóra RAMP. Prihlasovacie mená a heslá sa týkajú viac ako 12-tisíc zariadení, pričom približne 3-tisíc sa nachádza v USA.

Trójsky kôň ZLoader využíva deaktiváciu Windows Defendera

Aktuálne útoky bankového trójskeho koňa ZLoader využívajú nový reťazec infekcií na deaktiváciu antivírusového riešenia Windows Defender. Útočníci tiež zmenili spôsob doručovania škodlivého softvéru – namiesto phishingových emailov využívajú TeamViewer Google reklamy publikované prostredníctvom služby Google Adwords. Obete si stiahnu škodlivé inštalačné súbory MSI, ktoré následne nainštalujú malvér ZLoader na počítače. Útočníci sa zamerali na banky po celom svete, od Austrálie a Brazílie až po Severnú Ameriku, pričom trójskeho koňa využívali pre získavanie finančných údajov.

Nový malvér Capoae sa zameriava na WordPress a Linux

Voči systému WordPress a operačnému systému Linux bol zaznamenaný nový malvér Capoae napísaný v programovacom jazyku Go. Stal sa obľúbeným vďaka schopnostiam naprieč platformám. Malvér sa šíri prostredníctvom zraniteľností ako CVE-2020-14882 (RCE na serveroch Oracle WebLogic) a CVE-2018-20062 (RCE v ThinkPHP). Malvér bol spozorovaný pomocou honeypotu Akamai. Vzorka PHP malvéru prišla cez zadné vrátka prepojené s doplnkom vo WordPress-e s názvom Download-monitor, ktorý bol nainštalovaný po získaní jednoduchých prihlasovacích údajov honeypotu pomocou útoku hrubou silou. Malvér nasadzuje XMRih na ťažbu kryptomeny Monero a rôzne webové shelly.

Útočníci využívajú nové metódy útokov a WSL

Bezpečnostní výskumníci objavili škodlivé linuxové binárne súbory vytvorené pre Windows subsystém pre Linux (WSL). Útočníci skúmajú nové metódy útokov a WSL využívajú, aby sa vyhli detekcii. Škodlivé súbory buď priamo obsahujú nástroje, alebo ich útočníci získavajú zo vzdialeného servera. Škodlivé súbory sa pri vykonávaní svojich úloh spoliehajú hlavne na Python verzie 3 a sú zabalené ako spustiteľný ELF súbor pre Debian pomocou PyInstaller. Najväčší problém spôsobuje, že väčšina antivírusových riešení pre Windows nemá vytvorené podpisy na analýzu súborov ELF.

Zraniteľnosti Azure OMIGOD sa stali terčom rôznych útokov

Útočníci aktívne zneužívali kritické zraniteľnosti Azure OMIGOD dva dni po tom, čo ich spoločnosť Microsoft odhalila. Celkovo tieto chyby ovplyvnili tisíce zákazníkov Azure a milióny koncových staníc. Botnet Mirai stojí za niektorými z pokusov o zneužitie týchto zraniteľností. Spoločnosť Cado Security analyzovala tento malvér a zistila, že uzatvára porty, ktoré zneužíva, aby tak zabránil iným botnetom prevziať kontrolu nad systémom. Iní útočníci sa zas snažia nasadiť škodlivý kód, ktorý by bol schopný ťažiť kryptomeny.

APT skupina Turla využívala malvér TinyTurla na zachovanie perzistencie v systémoch

Ruskí útočníci známi ako APT skupina Turla používali počas minulého roka malvér, ktorý slúžil na zachovanie perzistencie na kompromitovaných systémoch v USA, Nemecku a Afganistane. Malvér TinyTurla sa vďaka svojej obmedzenej funkcionalite dá použiť ako zavádzač škodlivého softvéru v druhej fáze. Tieto zadné vrátka sa používajú minimálne od roku 2020, pričom sa vyhli detekcii najmä vďaka svojej jednoduchosti. Forenzné dôkazy naznačujú, že sa útočníci zameriavali na predchádzajúcu afganskú vládu práve pomocou tohto malvéru. Útočníci použili rovnakú infraštruktúru, aká

bola zaznamenaná pri iných útokoch pripisovaných APT skupine Turla. Funkcionalita malvéru TinyTurla zahŕňa sťahovanie, nahrávanie a spúšťanie súborov.

Nový trójsky kôň BloodyStealer sa zameriava na herné platformy

Bezpečnostní výskumníci spoločnosti Kaspersky objavili nového trójskeho koňa, ktorý sa zameriava na herné platformy ako sú Steam, Epic Games, EA Origin, GOG Galaxy a ďalšie. Malvér nazvaný BloodyStealer je schopný zbierať a kradnúť rôzne citlivé údaje vrátane cookies, hesiel, bankových kariet, ako aj relácie z rôznych aplikácií. Používa sa pri útokoch zameraných na obete z Európy, Latinskej Ameriky a ázijsko-pacifického regiónu. Výskumníci zo spoločnosti Kaspersky tvrdia, že vďaka svojim antidetekčným technikám a atraktívnym cenám ho v budúcnosti určite uvidíme v kombinácii s inými rodinami malvéru.

Výskumníci zo spoločnosti Kaspersky objavili nové zadné vrátka Tomiris

Bezpečnostní výskumníci spoločnosti Kaspersky objavili nové zadné vrátka s názvom Tomiris, ktoré pravdepodobne vyvinula skupina Nobelium stojaca za útokom na SolarWinds. Tieto zadné vrátka využívajú útočníci na vzdialené získavanie citlivých informácií z AD FS serverov. Tomiris bol prvýkrát zaznamenaný v júni tohto roku. Objavený bol pri vyšetrovaní série útokov, ktoré súviseli s únosom DNS relácií. Tieto boli zamerané na niekoľko vládnych zón členských štátov CIS (Commonwealth of Independent States). Obete boli presmerované na falošné prihlasovacie stránky, ktoré útočníkom umožnili ukradnúť prihlasovacie údaje. V niektorých prípadoch ich donútili nainštalovať aktualizáciu škodlivého softvéru, ktorá namiesto toho stiahla predtým neznáme zadné vrátka Tomiris.

Malvér GriftHorse infikoval viac ako 10 miliónov Android zariadení

Malvér GriftHorse infikoval viac ako 10 miliónov zariadení so systémom Android, pričom ukradol pravdepodobne stovky miliónov dolárov od svojich obetí, ktoré mali predplatené služby bez ich vedomia. Objavili ho výskumníci zo Zimperium zLabs. Malvér bol doručený pomocou viac ako 200 infikovaných aplikácií, ktoré boli do mobilných zariadení stiahnuté prostredníctvom oficiálneho obchodu Play Store a obchodov tretích strán. Podľa odhadov výskumníkov by útočníci mohli ukradnúť milióny v opakujúcich sa platbách každý mesiac od obetí na celom svete. Aj napriek tomu, že spoločnosť Google odstránila aplikácie po upozornení na ich škodlivý charakter, stále sú k dispozícii na stiahnutie v úložiskách tretích strán.

- **Skupina LockBit zverejnila uniknuté údaje zákazníkov leteckej spoločnosti Bangkok Airways.**
- **Autodesk potvrdil, že bol tiež terčom ruských štátnych hackerov, ktorí stáli za rozsiahlym útokom na dodávateľský reťazec SolarWinds.**
- **FBI varuje pred ransomvérovými skupinami zameranými na potravinové a poľnohospodárske organizácie.**
- **Útočníci, pravdepodobne zo skupiny FIN7, spustili malvérovú kampaň s využitím aktuálne horúcej témy - Windows 11.**
- **Conti ransomvér sa zameriava na Exchange servery pomocou exploitov ProxyShell.**
- **Zdrojový kód ransomvéru Babuk unikol na hackerskom fóre.**
- **Únik údajov verejného školského systému v Dallase zahŕňal informácie o študentoch, rodičoch, zamestnancov a učiteľoch z roku 2010.**
- **Na juhokórejskom letisku bol zatknutý člen skupiny TrickBot.**
- **Univerzita Howard vo Washingtone bola nútená uviesť svoje siete do režimu offline po útoku ransomvéru.**

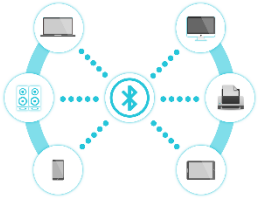
- **Ransomvér Pysa sa zameriava na operačný systém Linux.**
- **Skupina GrayFly využíva nový malvér proti podnikom na Taiwane, vo Vietname, v USA a v Mexiku. Zameriava sa na Exchange servery a MySQL.**
- **Malvér pre operačný systém Android používa tému Covid-19 na kradnutie finančných údajov.**
- **V rámci útokov bolo zaznamenané použitie neoficiálnej verzie Cobalt Strike Beacon Linux, ktorú vytvorili neznámi útočníci.**
- **Ransomvérový útok spôsobil zašifrovanie siete ministerstva spravodlivosti v Južnej Afrike.**
- **Útočníci ukradli osobné údaje približne 1,4 milióna ľudí, ktorí v polovici roka 2020 absolvovali testy na Covid-19 v parížskom regióne.**
- **Bankový trójsky kôň zneužíva YouTube, Pastebin a ďalšie verejné platformy na šírenie a kontrolu napadnutých počítačov.**
- **Spoločnosť EventBuilder odhalila súbory obsahujúce osobné informácie minimálne 100-tisíc používateľov, ktorí sa zaregistrovali na udalosti na jej platforme.**
- **Telefónne služby VoIP.ms boli narušené vydieračským útokom DDoS.**
- **Poskytovateľ webových služieb Epik potvrdil útok na svoje systémy.**
- **FBI, CISA a NSA varujú pred zvýšeným počtom útokov ransomvéru Conti.**
- **Nová APT skupina FamousSparrow stojí za sériou útokov na hotely, vládne organizácie, medzinárodné organizácie a ďalšie po celom svete.**
- **JVCKenwood zasiahol ransomvér Conti, pričom bolo ukradnutých 1,7TB údajov. Útočníci vyžadovali výkupné v hodnote 7 miliónov dolárov.**
- **Spoločnosť Forward Air potvrdila útok ransomvéru, ktorý umožnil útočníkom prístup k údajom o zamestnancoch.**

Závažné zraniteľnosti bežných softvérových produktov

Kritické zraniteľnosti Cisco

Spoločnosť Cisco opravila viacero závažných a 4 kritické zraniteľnosti.
CVE-2021-34746: Zraniteľnosť v TACACS+ funkcii autentifikácie, autorizácie a účtovania (AAA) softvéru Cisco Enterprise NFV Infrastracture môže neoverenému útočníkovi umožniť obídenie autentifikácie a prihlásenie sa s administrátorskými oprávneniami.
CVE-2021-34727: Zraniteľnosť v procese vDaemon v softvéri Cisco IOS XE SD-WAN by mohla umožniť neoverenému vzdialenému útočníkovi spôsobiť pretečenie vyrovnávacej pamäte na postihnutom zariadení.
CVE-2021-34770: Zraniteľnosť pri spracovaní protokolu riadenia a poskytovania bezdrôtových prístupových bodov (CAPWAP) softvéru Cisco IOS XE pre bezdrôtové ovládače rodiny Cisco Catalyst 9000 by mohla umožniť neoverenému vzdialenému útočníkovi vykonať ľubovoľný kód s oprávneniami administrátora alebo spôsobiť narušenie dostupnosti služby (DoS) na postihnutom zariadení.
CVE-2021-1619: Zraniteľnosť vo funkcii autentifikácie, autorizácie a účtovania (AAA) softvéru Cisco IOS XE by mohla umožniť neoverenému vzdialenému útočníkovi obísť autentifikáciu NETCONF alebo RESTCONF a následne inštalovať, manipulovať alebo vymazať konfiguráciu postihnutého zariadenia alebo spôsobiť poškodenie pamäte, ktoré môže vyústiť v narušenie dostupnosti služby (DoS).

Zraniteľnosti označené ako BrakTooth ovplyvňujú miliardy rôznych zariadení



Zraniteľnosti spoločne označené ako BrakTooth ovplyvňujú Bluetooth zásobníky implementované na obvodoch systému na čipe (SoC) od viac ako dvanástich predajcov. Výskumníci zo Singapurskej univerzity technológie a dizajnu zistili, že BrakTooth ovplyvňuje viac ako 1400 produktov ako napríklad smartfóny, klávesnice, reproduktory, slúchadlá a ďalšie.

Spoločnosť Netgear opravuje 3 závažné zraniteľnosti

Spoločnosť Netgear vydala aktualizácie firmvéru pre 20 svojich produktov, väčšinou inteligentných prepínačov. Ovplyvnené boli troma zraniteľnosťami označenými ako PSV-2021-0140, PSV-2021-0144 a PSV-2021-0145. CVSS skóre týchto zraniteľností sa pohybuje v rozpätí od 7.4 až 8.8 a umožňujú eskaláciu oprávnení, či falšovanie identity.

Spoločnosť Apple vydala bezpečnostné záplaty na opravu 2 zero-day zraniteľností

Obe zraniteľnosti v produktoch Apple umožňujú škodlivo vytvoreným dokumentom vykonávať rôzne príkazy pri otvorení na zraniteľných zariadeniach. Zraniteľnosť CVE-2021-30860 sa vyskytuje v CoreGraphics a súvisí s pretečením celočíselnej premennej. CVE-2021-30858 súvisí s použitím odalokovaného miesta v pamäti a vyskytuje sa v nástroji WebKit.

V smerovačoch spoločnosti Netgear sa vyskytuje závažná zraniteľnosť

Spoločnosť Netgear opravila závažnú zraniteľnosť CVE-2021-40847, ktorá môže viesť k vzdialenému vykonaniu kódu. Chyba sa vyskytuje v službe rodičovskej kontroly Circle, ktorá beží s administrátorskými oprávneniami na rôznych moderných SOHO (Small Offices / Home Offices) smerovačoch.

Mesačník zraniteľností September 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/2571.html?csrt=11131976137354343151