MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Júl 2021

Vypracoval: CSIRT.SK

TLP: White

V júli tohto roku svetom otriasol masívny kybernetický útok na dodávateľský reťazec Kaseya VSA. Kaseya VSA je cloudová MSP (managed service provider) platforma, ktorá umožňuje poskytovateľom vykonávať správu opráv a monitorovanie klientov pre svojich zákazníkov. Spoločnosť Kaseya bola zasiahnutá ransomvérom REvil, pričom postihnutých bolo viac ako tisíc jej zákazníkov. V súčasnej dobe je známych 8 MSP platforiem, ktoré boli zasiahnuté v rámci tohto útoku. Kaseya varovala všetkých zákazníkov VSA, aby počas vyšetrovania okamžite vypli svoj server VSA, pre zabránenie šíreniu útoku.

Zraniteľnosť typu zero-day, ktorú útočníci stojaci za ransomvérom REvil zneužili na prelomenie serverov Kaseya VSA, bola v čase útoku v štádiu opravy. Chybu objavil bezpečnostný výskumník Wietse Boonstra a bol jej priradený identifikátor CVE-2021-30116.

Prostredníctvom útoku na Kaseya VSA bola zasiahnutá sieť švédskych supermarketov Coop, pričom bola nútená zatvoriť približne 500 obchodov. Dôvodom bolo, že prestali fungovať pokladnice kvôli útoku na jedného z ich dodávateľov Visma Esscom. Softvér Kaseya VSA šifroval poskytovateľov internetových služieb po celom svete. Útok na Coop je len jedným z dlhého zoznamu obetí útoku na dodávateľský reťazec.

Kaseya tvrdí, že tento útok narušil systémy zhruba 60-tich jeho priamych zákazníkov, ktorí používajú produkt VSA. Cloudový poskytovateľ softvéru MSP dodal, že vie až o 1 500 následných obetiach, ktoré svoje siete spravovali pomocou nástrojov vzdialenej správy Kaseya. Útočníci stojaci za týmto ransomvérovým útokom tvrdia, že zašifrovali viac ako milión systémov a požadujú 50 miliónov dolárov za univerzálny dešifrovací kľúč.

Útočníci sa zamerali na potenciálne obete v spamovej kampani, kde v emailoch rozposielali Cobalt Strike maskovaný za bezpečnostné aktualizácie pre Kaseya VSA. Správa obsahovala odkaz, ktorý zdanlivo viedol na oficiálne stránky spoločnosti Kaseya. V skutočnosti však daný odkaz viedol ku spustiteľnému súboru (pload.exe), ktorý sa nachádzal na serveri tretej strany. Email taktiež obsahoval prílohu s názvom SecurityUpdates.exe. Oba tieto súbory schovávali Cobalt Strike. Cieľom takýchto útokov je zväčša zber a exfiltrácia citlivých údajov, prípadne nasadenie ďalšieho malvéru.

Po tom, ako sa spoločnosť o tejto kampani dozvedela, začala s varovaním svojich zákazníkov. Cieľom útočníkov bolo nasadiť zadné vrátka na zariadenia príjemcov a pomocou nich nasadiť ďalší malvér alebo exfiltrovať údaje. Akonáhle používateľ spustil škodlivú prílohu, alebo stiahol a spustil falošnú aktualizáciu, útočník získal trvalý vzdialený prístup ku kompromitovanému systému.

Po niekoľkých dňoch Kaseya vydala záplatu pre zneužívané zraniteľnosti v rámci ransomvérového útoku a tiež začala s obnovou SaaS služieb. Okrem opráv Kaseya vydala tiež nástroj pre zákazníkov, ktorý je možné použiť na „vyčistenie všetkých procedúr, ktoré sa nahromadili pred reštartovaním VSA“ a návod, ktorý má pomôcť zákazníkom pripraviť sa na zavedenie a obnovu služieb.

V ten istý deň infraštruktúra a stránky operátorov ransomvéru REvil boli záhadne uvedené do režimu offline. Zástupca ransomvéru LockBit zverejnil na ruskom hackerskom fóre správu, že útočníci stojaci

za ransomvérom REvil vymazali svoje servery po tom, čo sa dozvedeli o predvolaní vládou. Táto informácia však nie je potvrdená.

Zmiznutie útočníkov bránilo spoločnostiam zaplatiť za dešifrovací kľúč. Avšak Kaseya neskôr uviedla, že obdržala univerzálny dešifrátor od dôveryhodnej tretej strany a začala ho distribuovať medzi svojich zákazníkov. Spoločnosť sa rozhodla nezdieľať informácie o zdroji kľúča a tiež nepotvrdila ani nevyvrátila či zaň zaplatila výkupné.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti, CSIRT.SK v mesiaci jún riešil najmä phishingové kampane zasahujúce jeho konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov. Jednotka zaznamenala aj cielené, spear-phishingové útoky šíriace malvér.

CSIRT.SK prijal hlásenie informujúce o štyroch slovenských doménach, ktoré vykazovali znaky infraštruktúry útočníkov skupiny REvil z kampane Kaseya. Tento incident riešil s príslušnými správcami obsahu.

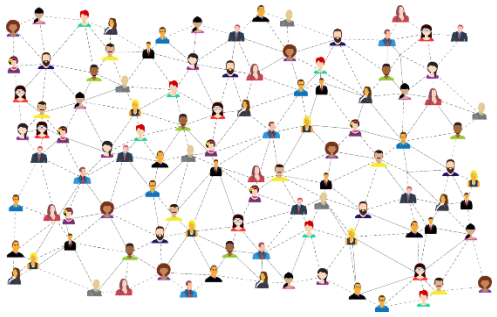
Okrem toho riešila jednotka prípad skenovania webovej služby a brute-force útoku na mailserver organizácie v jej konštituencii. Taktiež sa zaoberala medializovaným prípadom zraniteľnej aplikácie eHranica pod NCZI, odhalenej a reportovanej spoločnosťou Nethemba.

CSIRT.SK v rámci svojej proaktívnej činnosti kontaktoval organizácie ohľadom útokov APT skupiny Zirconium (APT 31) na malé routery, ktoré skupina používala ako platformu pre ďalšie útoky a ich anonymizáciu. Komunikácia medzi zariadením a jedným z C&C serverov bola identifikovaná v prípade jednej organizácie, pravdepodobne však bez spojitosti s popísaným útokom.

Varovanie rozposlala jednotka svojej konštituencii ohľadom zraniteľnosti služby Windows Print Spooler (CVE-2021-1675) a indikátorov kompromitácie kampane Kaseya, vedenou skupinou REvil, šíriacou ransomvér. Vybrané subjekty boli informované o nebezpečenstvách z internetu dostupnej služby RDP s odporúčaním takémuto prístupu zamedziť.

Významné útoky vo svete

Na hackerskom fóre boli zdieľané údaje o takmer 90-tisíc členoch sociálnej siete GETTR



Sociálna sieť GETTR (platforma podporujúca Trumpa, vytvorená jeho bývalým poradcom Jasonom Millerom ako alternatíva k Twitteru) utrpela únik údajov po tom, čo útočník použil nezabezpečené API na získanie rôznych informácií o takmer 90-tisíc členoch. Následne tieto získané údaje zdieľal na hackerskom fóre. Uniknuté údaje zahŕňajú emailové adresy členov, prezývky, mená, rok narodenia, polohu a ďalšie. Väčšina z údajov je priamo viditeľných v profiloch, avšak emailová adresa, poloha a rok narodenia nie sú verejne dostupné informácie. Tento typ informácií môžu útočníci použiť na cielené útoky typu phishing.

Spoločnosť Mint Mobile sa stala obeťou úniku údajov po tom, čo tretia strana pristúpila k údajom o predplatiteľoch

Spoločnosť Mint Mobile potvrdila únik údajov po tom, čo neoprávnená osoba získala prístup k informáciám o účtoch predplatiteľov a preniesla niekoľko telefónnych čísel k inému mobilnému operátorovi bez akejkoľvek autorizácie. Neoprávnená osoba mala potenciálne prístup aj k osobným informáciám osôb ako história hovorov, mená, adresy, emailové adresy a heslá. Spoločnosť Mint Mobile neuviedla spôsob, ako útočník získal prístup k údajom o predplatiteľoch. Útočníci mohli navyše použiť prenesené číslo na ďalšie útoky, ako napríklad phishing, alebo získať prístup k dvojfaktorovým autentifikačným kódom odosielaným prostredníctvom textových správ.

V dôsledku útoku ransomvéru módna značka Guess utrpela únik, ktorý sa dotkol približne 1300 zamestnancov a zmluvných partnerov

GUESS

Americká módna značka Guess sa stala obeťou útoku ransomvéru, ktorý viedol k odcudzeniu údajov. K údajom tejto spoločnosti mohla pristúpiť neoprávnená tretia strana. Únik sa týkal približne 1300 obetí. Medzi

dotknuté osoby patria zamestnanci a zmluvní partneri. Medzi uniknuté údaje patria napríklad čísla účtov, čísla debetných a kreditných kariet, no tiež bezpečnostné kódy, prístupové kódy a osobné identifikačné čísla. V čase útoku skupina DarkSide tvrdila, že získala prístup k viac ako 200 GB údajom.

Spoločnosť CNA Financial Corporation utrpela únik údajov, ktorý sa týkal viac ako 75-tisíc osôb

Poisťovacia spoločnosť CNA Financial Corporation utrpela únik údajov po marcovom útoku ransomvéru Phoenix CryptoLocker. Útočníci pristupovali k systémom CNA, pričom pred nasadením samotného ransomvéru odcudzili obmedzené množstvo informácií. Zašifrovaných bolo viac ako 15-tisíc zariadení. Únik údajov sa týka viac ako 75-tisíc osôb, pričom sa jedná zväčša o súčasných alebo bývalých zamestnancov, zmluvných pracovníkov a ich závislých osôb. Odcudzené dáta zahŕňajú osobné údaje vrátane mena, čísla sociálneho poistenia a v niektorých prípadoch informácií súvisiacich so zdravotnými výhodami pre niektorých jednotlivcov.

Spoločnosti LimeVPN uniklo viac ako 69-tisíc záznamov o používateľoch

Spoločnosť LimeVPN potvrdila bezpečnostný incident, ktorý ovplyvnil viac ako 69-tisíc používateľských záznamov. Útočník tvrdil, že ukradol celú databázu zákazníkov spoločnosti a potom uviedol jej webovú stránku do offline režimu. Ukradnuté údaje zahŕňajú používateľské mená, heslá v plaintexte, IP adresy a fakturačné údaje. Útočník tiež informoval, že ukradol súkromné kľúče každého používateľa, čo znamená, že môže dešifrovať každú aktivitu používateľa LimeVPN. Údaje o platobných kartách alebo bankové údaje sa medzi uniknutými údajmi nenachádzajú.

Kompromitácia účtov zamestnancov akademického zdravotného systému Kalifornskej univerzity viedla k úniku údajov

Akademický zdravotný systém Kalifornskej univerzity v San Diegu sa stal obeťou úniku údajov po kompromitácii účtov niektorých zamestnancov v dôsledku phishingového útoku. Útočníci získali prístup k osobným informáciám pacientov, zamestnancov aj študentov v období od 2. decembra 2020 do 8. apríla 2021. Neexistuje však dôkaz o tom, že by tieto údaje boli zneužité. Uniknuté údaje potenciálne môžu zahŕňať meno, adresu, dátum narodenia, email, lekársku diagnostiku, informácie o vyšetreniach, identifikačné čísla študentov, používateľské mená, heslá a ďalšie. Systémy neboli nijako ovplyvnené.

Nový malvér Meteor je určený na ničenie súborov. Zasiahol iránske ministerstvo dopravy a vlakový systém

Pri nedávnych útokoch na iránsky železničný systém bol objavený nový malvér Meteor, ktorého cieľom je mazanie súborov. Začiatkom mesiaca júl došlo ku kybernetickému útoku na iránske ministerstvo dopravy a vnútroštátny vlakový systém, v dôsledku čoho došlo k uvedeniu webových stránok agentúry do režimu offline a k narušeniu vlakovej dopravy. Útočníci tiež na nástenkách železnice uvádzali správy o tom, že vlaky meškali alebo boli zrušené práve kvôli kybernetickému útoku. Tiež uzamkli zariadenia v sieti s operačným systémom Windows, čím znemožnili prístup k zariadeniam. Cieľom takýchto útokov je spôsobiť chaos v organizácii alebo rozptýliť správcov počas prebiehajúceho útoku.

Falošný softvér Zoom sa šíri za účelom sledovania osôb v juhovýchodnej Ázii

Čínska APT skupina LuminousMoth šíri falošný softvér Zoom za účelom sledovania osôb v juhovýchodnej Ázii. Skupina začína odosielaním spear-phishingových emailov, ktoré obsahujú odkazy na stiahnutie .rar archívu s názvom s politickou alebo COVID-19 tematikou. Archív obsahuje 2 škodlivé súbory .dll, ktoré

sú následne schopné stiahnuť a nasadiť škodlivé spustiteľné súbory do infikovaného systému. Následne si skupina zaistí pomocou nástroja Cobalt Strike perzistenciu a nakopíruje malvér na úložné jednotky pripojené k systému obete. LuminousMoth tiež hľadá súbory cookie a prihlasovacie údaje, vrátane tých, ktoré sa používajú pre účty Gmail.

Spyware Pegasus útočníci používali zväčša na sledovanie novinárov a politikov

Mimovládna organizácia pre ľudské práva Amnesty International a neziskový projekt Forbidden Stories zistili, že spyware Pegasus vyrobený spoločnosťou NSO Group bol nasadený na zariadeniach iPhone s najnovšou verziou iOS. Pegasus je nástroj s možnosťami vzdialeného prístupu, ktorý je schopný extrahovať informácie o telefóne, zbierať konverzácie prebiehajúce prostredníctvom aplikácií, vrátane WhatsApp a Facebook, monitorovať emailových klientov a aktivitu prehliadača, nahrávať hovory a sledovať obete prostredníctvom mikrofónu a kamery. Softvér bol používaný na sledovanie novinárov, aktivistov, politikov a ďalších. Infikovaných bolo viac ako 50-tisíc telefónov. Voči týmto útokom je takmer nemožné sa chrániť.

Spoločnosť Saudi Aramco utrpela únik údajov o veľkosti 1 TB

Útočníci ukradli saudskoarabskej ropnej spoločnosti Saudi Aramco údaje o veľkosti 1 TB. Tieto údaje ponúkajú na predaj za 5 miliónov dolárov, pričom útočníci sú ochotní cenu zjednávať. Spoločnosť ZeroX tvrdí, že údaje boli odcudzené napadnutím siete a serverov spoločnosti Aramco niekedy v roku 2020. Skupina uvádza, že ukradnuté údaje zahŕňajú dokumenty týkajúce sa rafinérií Saudi Aramco nachádzajúcich sa vo viacerých saudskoarabských mestách, napríklad Yanbu, Jazan alebo Jeddah. Únik sa dotkol viac ako 14-tisíc zamestnancov, pričom údaje zahŕňali mená, fotografie, kópie pasu, emaily a ďalšie osobné informácie. Súčasťou úniku sú aj špecifikácia projektu pre systémy súvisiace s elektrickou energiou,

interné analytické správy alebo rozloženie siete mapujúce IP adresy.

Právnická firma Campbell sa stala obeťou útoku ransomvéru

Americká právnická firma Campbell odhalila únik údajov po útoku ransomvéru z februára tohto roku. Medzi súčasných aj bývalých klientov patria Exxon, Apple, Mercedes Benz a ďalšie. Útočníci mali prístup k údajom ako mená osôb, dátum narodenia, čísla vodičských preukazov, čísla pasov, informácie o platobných kartách a ďalšie. Firma neodhalila identitu skupiny stojacej za týmto ransomvérom. Útok ransomvéru znemožnil prístup k určitým súborom v systéme.

- **Botnet TrickBot nasadzuje nový ransomvér s názvom Diavol.**
- **Spoločnosť Brenntag poskytla ďalšie informácie o tom, aké údaje boli ukradnuté z jej siete počas útoku ransomvéru DarkSide.**
- **Spoločnosť Google odstránila 9 aplikácií pre Android, ktoré kradli prihlasovacie údaje používateľov.**
- **Oficiálna webová stránka mongolskej certifikačnej autority obsahovala malvér.**
- **Útočníci podviedli najmenej 93-tisíc ľudí, aby si kúpili falošné aplikácie na ťažbu kryptomeny pre Android.**
- **Bezpečnostní výskumníci odhalili malvér Bandidos, ktorý sa zameriava na korporátne siete v Latinskej Amerike.**
- **Ministerstvo zdravotníctva Severného Írska dočasne pozastavilo online službu certifikácie vakcíny proti COVID-19 (COVIDCert). Obmedzený počet používateľov bol potenciálne vystavený údajom iných používateľov.**
- **UBEL je nový malvér, ktorý kradne prihlasovacie údaje z Android zariadení.**
- **Mobilný malvér Vultur využíva vo svojich útokoch VNC na získanie úplnej kontroly.**

- **Iránskej vláde zrejme unikli utajované súbory, ktoré vypovedajú o tom, že sa Irán snaží zlepšiť svoje útočné kybernetické schopnosti.**
- **Odborníci odhalili niekoľko riadiacich serverov prepojených s malvérom WellMess.**
- **Nová čínska skupina GhostEmperor sa zameriava na vládne organizácie a telekomunikačné firmy.**
- **Malvér XLoader kradne prihlasovacie údaje z operačných systémov Windows a macOS.**
- **Francúzska národná kyberbezpečnostná agentúra varuje pred útokmi skupiny APT31 na francúzske organizácie.**
- **Spoločnosť Microsoft varuje pred malvérom LemonDuck, ktorý sa zameriava na operačné systémy Windows a Linux.**
- **CISA zverejnila detaily o malvéri použitom v útokoch na zariadenia spoločnosti Pulse Secure.**
- **Bezpečnostní výskumníci zverejnili podrobnosti o metóde, ktorú malvér XCSSET používa na odcudzenie prihlasovacích údajov z viacerých aplikácií.**
- **Nový útok nazývaný PetitPotam umožňuje útočníkom prevziať radič domény, a teda celú doménu operačného systému Windows.**
- **Gitlab uviedol open-source nástroj na hľadanie škodlivého kódu v závislostiach projektov.**
- **Signal opravil chybu v aplikácii pre Android, ktorá rozposielala obrázky zlým kontaktom.**
- **Nový malvér MosaicLoader sa zameriava na softvérových „pirátov“ cez online reklamy.**
- **V obchode Google Play boli objavené aplikácie obsahujúce malvér Joker.**
- **Skupina stojaca za útokom na CD Projekt Red sa zameriava na virtuálne prostredia VMware ESXi.**

- **Moldavský „účtovný dvor“ (Court of Accounts) utrpel útok, ktorý viedol k zničeniu verejných databáz a auditov agentúry.**

Závažné zraniteľnosti bežných softvérových produktov

Kritická zraniteľnosť služby Print Spooler vo všetkých verziách Windows

V operačných systémoch Windows bola nájdená zraniteľnosť služby, ktorá sa využíva na komunikáciu s lokálnymi a sieťovými tlačiarňami. Chyba umožňuje vzdialené vykonávanie kódu s eskalovanými oprávneniami na úroveň System. Spoločnosť Microsoft vydala opravnú aktualizáciu všetkých podporovaných systémov, avšak zraniteľnosť nebola odstránená. Pre zabezpečenie infraštruktúry odporúčame administrátorom vypnúť službu Print Spooler ak je to možné, alebo postupovať podľa odporúčaní Microsoft.

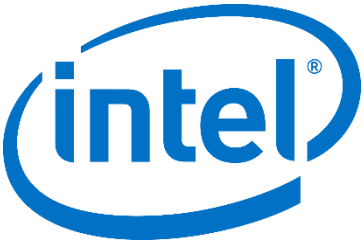
V smerovačoch Netgear série DGN-2200v1 sa vyskytujú 3 zraniteľnosti

Výskumníci spoločnosti Microsoft odhalili 3 zraniteľnosti v smerovačoch Netgear série DGN-2200v1, ktorých zneužitím môže dôjsť k obídeniu autentifikácie a následne k úplnej kompromitácii zariadenia. Útočníci tiež môžu získať prístup k uloženým prihlasovacím údajom. Zraniteľnosti sa týkajú smerovačov, na ktorých beží firmvér verzie v1.0.0.60. CVSS skóre týchto zraniteľností sa pohybuje v rozpätí od 7.1 do 9.4. Spoločnosť odporúča bezodkladne aktualizovať firmvér na najnovšiu dostupnú verziu na postihnutých zariadeniach.

Závažné zraniteľnosti Cisco

V produktoch Cisco bolo opravených viacero závažných zraniteľností. Zraniteľnosti ovplyvňujú Cisco Web Security Appliance, Cisco Intersight Virtual Appliance, softvér Adaptive Security Appliance (ASA), softvér Firepower Threat Defense (FTD), prepínače Cisco Catalyst série 4500 a 4500-X a ďalšie. Úspešným zneužitím týchto zraniteľností môže dôjsť napríklad k injektovaniu príkazov, eskalácii privilégií, umožneniu prístupu k citlivým interným službám, narušeniu dostupnosti služby alebo prezeraniu a modifikácii informácií zdieľaných cez Cisco Webex.

Zraniteľnosti Intel



V produktoch Intel bola opravená jedna závažná zraniteľnosť. Nájdená zraniteľnosť ovplyvňuje Intel BSSA DFT. Inicializácia nezabezpečenej predvolenej premennej pre funkciu Intel BSSA DFT môže privilegovanému používateľovi umožniť potenciálne zvýšenie privilégií prostredníctvom lokálneho prístupu.

Mesačník zraniteľností Júl 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 Flash Player, Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
    - Kritická zraniteľnosť služby Print Spooler vo všetkých verziách Windows

https://www.csirt.gov.sk/posts/2522.html?csrt=734397574759825234