ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Marec 2020

Vypracoval: CSIRT.SK

TLP: White

Mesiac marec 2020 si pravdepodobne mnohí z nás zapamätajú ako mesiac pandémie. Koncom roka 2019 bol v Číne identifikovaný vírus SARS CoV-2, čiže takzvaný koronavírus, spôsobujúci ochorenie COVID-19. Tento vírus patrí do rovnakej skupiny ako vírusy SARS (ťažký akútny respiračný syndróm) a MERS (stredovýchodný respiračný syndróm). Kybernetické útoky sa neustále snažili využiť online trendy a COVID-19 samozrejme nie je výnimkou.

Útočníci využívajú rôzne spôsoby na zneužitie koronavírusu. Jedným zo spôsobov je šírenie malvéru a to napríklad prostredníctvom aplikácií Google Play. V názvoch alebo popisoch týchto aplikácií vývojári používajú kľúčové slová súvisiace s koronavírusom, pretože vedia, že tieto pojmy sú v súčasnej dobe často vyhľadávané. V marci, oproti predošlým dvom mesiacom, narástlo vyhľadávanie aplikácií súvisiacich s COVID-19 o viac ako 200%. Prostredníctvom aplikácií týkajúcich sa lokalizácie ochorenia či základných informácií o tomto ochorení, útočníci šíria adware, bankové trójske kone (napríklad Anubis, Cerberus) a získavajú citlivé údaje obetí. Spoločnosť Check Point Research odhalila 16 rôznych škodlivých aplikácií, ktoré sa maskovali ako legitímne aplikácie zamerané na tematiku boja proti koronavírusu. Všetky tieto aplikácie obsahovali škodlivý softvér zameraný primárne na odcudzenie citlivých informácií používateľov. Útočníci sa okrem odcudzenia osobných údajov zameriavajú aj na zarábanie na strachu z COVID-19. Ako na svojej stránke informuje Interpol, na rôznych webových stránkach sa rozbehol obchod so zdravotníckym materiálom, ako sú tvárové masky, rúška, respirátory, dezinfekčné gély či mydlá. Na predaj môžete nájsť dokonca aj „sprej proti koronavírusu“, falošné lieky, špeciálne medicínske balíčky na boj s COVID-19 či nefunkčné vakcíny a liečivá, ktoré majú chorobu vyliečiť.

Rob Lefferts, firemný viceprezident spoločnosti Microsoft 365 Security uvádza, že z miliónov cielených správ, ktoré sledujú každý deň, približne 60 000 obsahuje škodlivé prílohy alebo škodlivé URL adresy súvisiace s COVID-19, a že každá krajina na svete bola zasiahnutá aspoň jedným útokom súvisiacim s COVID-19. Z nedávnej analýzy tímu CERT-GIB vyplýva, že väčšina phishingových e-mailových správ súvisiacich s COVID-19 obsahovala ako prílohu malvér Agent Tesla (45%), NetWire (30%) a LokiBot (8%). Zaznamenané boli tiež phishingové e-maily, ktorých odosielateľ sa tvári ako miestna nemocnica a informuje prijímateľa správy, že bol vystavený koronavírusu, a že je potrebné ho otestovať. Správa obsahuje tiež výzvu na vytlačenie priloženej prílohy EmergencyContact.xlsm, ktorú má príjemca vyplniť a odniesť do najbližšieho zdravotníckeho zariadenia. Tento súbor však obsahuje škodlivé makrá, pomocou ktorých útočník získa informácie o existujúcich bitcoin peňaženkách a tiež o prihlasovacích údajoch zo súborov cookie z prehliadača. Vo phishigových e-mailoch sa tiež objavujú podvodné stránky s výzvou na vyplnenie osobných údajov s prísľubom balíka jedla ako formy pomoci v obrane proti koronavírusu.

Iným príkladom šírenia škodlivého kódu je napadnutie DNS smerovača. Obeti sa v prehliadači zobrazí upozornenie na falošnú informačnú aplikáciu o COVID-19, údajne pochádzajúcej od Svetovej zdravotníckej organizácie (WHO) a používateľ je vyzvaný aby si túto aplikáciu stiahol. Používateľ si však namiesto aplikácie stiahne trójskeho koňa Oski, ktorý je schopný z infikovaného počítača sťahovať údaje. Po spustení tento malvér zbiera informácie o súboroch cookie, históriu prehliadača, informácie o platbách, bitcoin peňaženkách a rôzne iné informácie.

Vo viacerých krajinách boli občanom posielané aj informačné SMS správy o COVID-19, výnimkou nie je ani Slovensko, kde tieto správy rozosielalo Ministerstvo zdravotníctva a Ministerstvo vnútra. Americká agentúra pre kybernetickú bezpečnosť a infraštruktúru (CISA) a Britské národné stredisko pre kybernetickú bezpečnosť (NCSC) vydali varovania o podvodných SMS správach od odosielateľov „COVID" a „UKGOV", ktoré obsahujú odkazy na phishingové stránky.

Ďalším opatrením, ktoré sa týka aj Slovenskej republiky, je práca z domu. Kvôli aktuálnej situácii je v mnohých štátoch prikázaná karanténa a práca z domu, ak je to možné. Výnimkou sú zvyčajne iba neodkladné návštevy potravín či lekára. S prácou z domu prirodzene narástol záujem o online komunikačné platformy, ako sú Zoom či Microsoft Teams. To podnietilo rozposielanie phishingových e-mailov obsahujúcich malvér s názvami podobnými týmto platformám. Príkladom môže byť „zoom-us-zoom_##########.exe" alebo „microsoft-teams_V#mu#D_##########.exe".

Neoddeliteľnou súčasťou vypuknutia napätej situácie ohľadom COVID-19 je šírenie dezinformácií. Na internete sa objavujú klamlivé informácie o pôvode koronavírusu a o príčinách karantény. Môžeme sa tak nepravdivo dočítať napríklad o tom, že umývanie rúk, či nosenie rúška nám nepomôže pri ochrane pred COVID-19, alebo dokonca že celá pandémia je výmysel a žiadny vírus neexistuje. Objavujú sa tiež rôzne články o tom, ako sa jednotlivé štáty obviňujú u koho a za akým účelom vlastne vírus vznikol.

V neposlednom rade útočníci používajú ransomvér. Medzinárodná organizácia kriminálnej polície (Interpol) takisto pomáha členským štátom pri zmierňovaní a vyšetrovaní cielených útokov na nemocnice a zdravotnícke zariadenia. Interpol vydal varovanie týkajúce sa útokov súvisiacich s COVID-19 v ktorom informuje, že útočníci sa zameriavajú na nemocnice a ďalšie inštitúcie v prvej línii boja proti COVID-19. Príkladom je ransomvérový útok na jedno z najväčších testovacích laboratórií v Českej republike. Napadnutá Fakultná nemocnica v Brne bola počas incidentu nútená vypnúť nemocničný systém a presunúť niektoré plánované operácie do Fakultnej nemocnice sv. Anny.

Ako sa teda môžeme brániť proti spomínaným útokom?

- Pri sťahovaní aplikácií si dôkladne skontrolujte predajcu aplikácie, prípadne vôbec nesťahujte do mobilu aplikácie týkajúce sa COVID-19. Pri akomkoľvek podozrení, nezadávajte do žiadnej aplikácie či webovej stránky svoje citlivé či platobné údaje.
- Pri phishingových e-mailoch a SMS správach platia rovnaké pravidlá ako v situácii mimo súčasnej pandémie – kontrolujte odosielateľa, gramatiku v správach a neotvárajte, nesťahujte neznáme prílohy. Ak sa odosielateľ tvári ako oficiálna inštitúcia, skontrolujte si kontakt uvedený v správe na webe. Takéto kontakty by mali byť verejne dostupné.
- Ak si chcete zistiť informácie o aktuálnej situácii týkajúcej sa tejto tematiky, použite dôveryhodné zdroje od oficiálnych inštitúcií či autorít. Na vyhľadávanie takýchto informácií môžete využiť napríklad webové stránky Ministerstva zdravotníctva SR, Úradu verejného zdravotníctva, Úradu podpredsedu vlády SR pre investície a informatizáciu alebo stránku Svetovej zdravotníckej organizácie.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci marec riešil najmä phishingové kampane na svoju konštituenciu. Okrem toho CSIRT.SK pokračoval v riešení wiper útoku na databázu svojho konštituenta, spojeného s požiadavkou o výkupné za navrátenie zmazaných dát a ich nezverejnenie.

V rámci proaktívnej činnosti vykonal CSIRT.SK neinvazívne skenovanie a varoval svoju konštituenciu pred rizikami spojenými so zariadeniami dostupnými z internetu, ktoré majú povolené zraniteľné verzie protokolu SMB. Kvôli zvýšenej aktivite útočníkov počas krízy COVID-19 spojenej najmä so šírením ransomvéru cez phishingové kampane varoval zdravotnícky sektor pred hroziacimi útokmi. V rámci varovania tiež informoval o krokoch vedúcich k zabezpečeniu systémov ohrozených organizácií a k významnému zníženiu ich zraniteľnosti. CSIRT.SK vykonal tiež sken zraniteľností do internetu publikovaných portov na IP adresách svojej konštituencie. Jednotlivým organizáciám poslal reporty s požiadavkou opravy nájdených zraniteľností.

Významné útoky vo svete

Spoločnosti Marriott International uniklo 5,2 milióna záznamov o klientoch

Medzinárodná sieť hotelov Marriott International oznámila, že došlo k úniku údajov až 5,2 milióna zákazníkov. Predpokladá sa, že už od polovice januára boli prihlasovacie údaje dvoch zamestnancov použité na prístup k informáciám o hotelových hosťoch. Uniknuté údaje zahrňovali kontaktné údaje (meno, adresa, email, telefónne číslo), informácie o vernostnom účte (číslo účtu a zostatok bodov), osobné údaje ako pohlavie, deň a mesiac narodenia, preferencie izieb a podobne. Marriott tvrdí, že citlivé údaje, ako heslá, informácie o platobných kartách, PIN kódy ani cestovné pasy neunikli. Pre zákazníkov bol spustený portál, na ktorom zistia, či a aké ich údaje boli medzi uniknutými dátami.

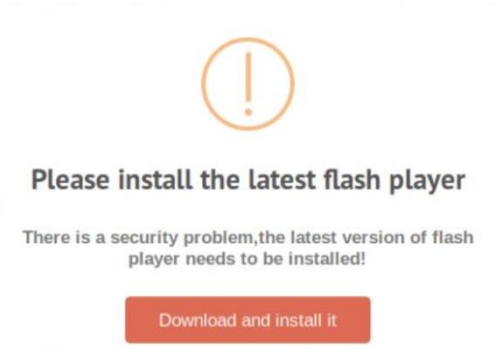
Trójsky kôň Zeus Sphinx sa šíri prostredníctvom phishingovej kampane súvisiacej s COVID-19.

Bankový trójsky kôň sa po troch rokoch nečinnosti objavil v rámci koronavírusovej phishingovej kampane, ktorá je počas súčasnej pandémie najčastejšou témou väčšiny útokov. Podľa odborníkov zo spoločnosti IBM-X-Force sa v decembri začali objavovať úpravy malvéru Sphinx. Je to kmeň škodlivého softvéru, ktorý bol zaznamenaný v auguste roku 2015, keď bol využitý na útok na niekoľko britských finančných cieľov. Je založený na trójskom koni Zeus v2. Tento malvér sa pokúša zbierať údaje pomocou sociálneho inžinierstva. Jeho cieľom je získanie autorizačných kódov a prístupových údajov k bankovým účtom. Keď infikovaní požívatelia pristupujú na stránku online bankovníctva, malvér modifikuje webstránku tak, že údaje, ktoré používateľ zadá sa automaticky posielajú na riadiaci server útočníkovi. V súčasnosti phishingové maily tejto kampane obsahujú formulár a nabádajú obeť k jeho vyplneniu, kvôli získaniu vládnej pomoci v čase koronavírusovej pandémie.

Osobné údaje obyvateľov Gruzínska boli uverejnené online

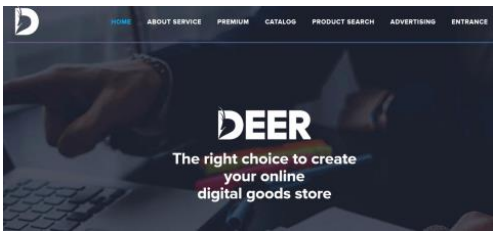
Osobné údaje viac ako 4,9 milióna Gruzíncov, vrátane mŕtvych občanov boli zverejnené na hackerskom fóre. Obsahovali informácie ako napríklad celé meno, bydlisko, dátum narodenia, identifikačné číslo a číslo mobilného telefónu. Boli zverejnené vo forme databázy Microsoft Access s kapacitou 1,04 GB. Tento únik bol prvýkrát zaznamenaný spoločnosťou Under the Breach, čo je služba monitorovania a prevencie únikov údajov. Zdroj údajov však zostáva záhadou. Pôvodne existovalo podozrenie, že tento únik pochádzal z Gruzínskej ústrednej volebnej komisie (CEC), avšak uniknuté dáta obsahujú informácie, ktoré daná komisia nezhromažďuje. Prípad momentálne podlieha vyšetrovaniu. Používateľ, ktorý súbor zverejnil na fóre hackerov, tvrdí, že pochádza z oficiálneho vládneho portálu voters.cec.gov.ge. Jedná sa o vládnu službu, ktorá umožňuje voličom overiť a aktualizovať svoje registračné záznamy.

Watering-Hole útok sa zameriava na obete s ázijskou etnicitou



Rozsiahla kampaň zameraná na používateľov operačného systému Windows, ktorí patria do určitej náboženskej a etnickej skupiny, využíva sériu webových stránok, ktoré nabádajú k falošnej aktualizácii nástroja Adobe Flash. Podľa analýzy spoločnosti Kaspersky sú príslušné stránky legitímnymi webmi, ktoré boli napadnuté. Spoločnosť zistila, že existuje takmer 10 kompromitovaných webstránok, ktoré sú využívané cieľovou skupinou - verejné orgány, charitatívne organizácie a iné. Tie obsahujú Javascript kód, ktorý nabáda používateľov, aby si stiahli aktualizáciu Flash, no po kliknutí na "Inštalovať" sú do zariadenia stiahnuté 4 škodlivé .exe súbory, medzi ktorými sú aj "zadné vrátka" do systému pre útočníka.

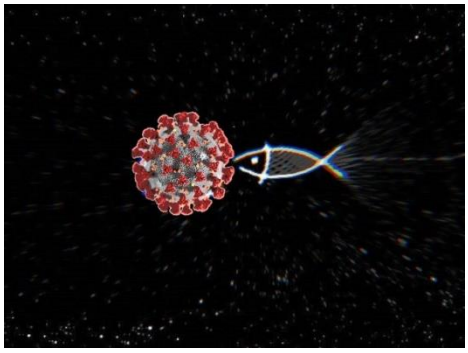
FBI vypína ruskú online platformu Deer.io



FBI dnes zrušila ruskú počítačovú platformu známu ako DEER.IO, ktorá hosťuje stovky online obchodov, v ktorých sa predávajú nelegálne výrobky a služby. Údajný ruský hacker Kirill Victorovich Firsov bol zatknutý ako správca tejto stránky. Bol obvinený zo spáchania trestných činov spojených s útočením na americké spoločnosti s cieľom získať osobné informácie zákazníkov.

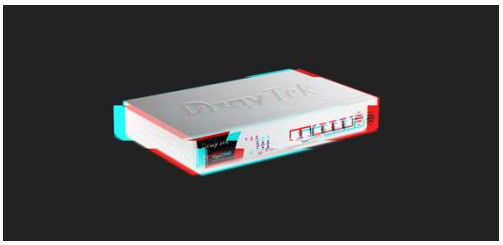
TLP: White

Phishingový e-mail tvrdiaci, že ste boli vystavení koronavírusu



Bola zaznamenaná nová phishingová kampaň, ktorá predstiera, že email pochádza z miestnej nemocnice. Príjemcovi tvrdí, že bol vystavený koronavírusu a že je potrebné ho otestovať. Je nabádaný k tomu, aby si vytlačil priloženú prílohu EmergencyContact.xlsm a priniesol ju so sebou na najbližšiu pohotovostnú kliniku na testovanie. Keď obeť túto prílohu otvorí, zobrazí sa výzva "Povoliť obsah" na zobrazenie chráneného dokumentu. Ak používateľ povolí obsah, spustia sa škodlivé makrá na stiahnutie škodlivého softvéru a jeho vykonanie. Tento spustiteľný súbor sa vloží do legitímneho systémového súboru msiexec.exe, aby sa zabránilo jeho detekcii. Malvér vyhľadáva a kradne kryptomenové peňaženky, získa zoznam programov spustených v počítači, kradne súbory cookie webového prehliadača a podobne.

Hackeri zneužívajú zero-day zraniteľnosti v zariadeniach Draytek a zameriavajú sa na podnikové siete



Čínska bezpečnostná firma Qihoo 360 vydala správu, podľa ktorej najmenej dve samostatné skupiny útočníkov využívali dve kritické zraniteľnosti prepínačov, vyrovnávačov zaťaženia, smerovačov a brán VPN spoločnosti DrayTek Vigor. Tieto zraniteľnosti (CVE-2020-8515) súvisia so vzdialeným vykonávaním kódu na napadnutom zariadení a boli využité na odpočúvanie sieťového prenosu a inštaláciu zadných vrátok. Prvá skupina útočníkov zneužila zraniteľnosť v mechanizme šifrovaného prihlasovania sa pomocou RSA na zariadení DrayTrek, aby skryla škodlivý kód v poli pre používateľské meno. Pomocou neho potom sledovali sieťovú prevádzku. Druhá skupina útočníkov využila chybu v procese "rtick" na vytvorenie zadných vrátok v napadnutých zariadeniach.

Web spoločnosti Tupperware bol napadnutý a zobrazoval falošný formulár na kradnutie kreditných kariet

Útočníci sa zacielili na oficiálnu stránku Tupperware, ktorá má v priemere takmer milión mesačných návštev. Na stránke platby za tovar vložili falošný formulár v nádeji, že ukradnú údaje o kreditných kartách zákazníkov. Výskumníci spoločnosti Malwarebytes objavili, že daný iframe načítaval obsah z domény deskofhelp(.)com, ktorá bola vytvorená 9.marca a zdieľa hostingový server s viacerými phishingovými stránkami. Tupperware problém vyriešil a platobný formulár sa momentálne načíta z legitímnej domény cybersource.com, ktorú vlastní spoločnosť Visa.

Útoky na smerovače D-Link a Linksys s cieľom presmerovať používateľov na stránky zamerané na koronavírus so škodlivým softvérom

Skupina útočníkov kompromituje smerovače D-Link a Linksys a mení nastavenia DNS s cieľom nasmerovať používateľov týchto zariadení na falošné stránky súvisiace s COVID-19. Tie šíria škodlivý softvér. Podľa spoločnosti Bitdefender využívajú útočníci útok hrubou silou, aby uhádli heslo správcu cielených smerovačov. Akonáhle sa im to podarí, zmenia predvolené nastavenia DNS a nasmerujú zariadenie na svoje vlastné servery. Ak sa používateľ pokúsi prejsť na konkrétnu doménu, je presmerovaný na web útočníkov, ktorý ho vyzýva k inštalácii informačnej aplikácie s tematikou koronavírusu. Spoločnosti Bitdefender a Bleeping Computer uviedli, že táto aplikácia nainštaluje verziu trójskeho koňa Oski, ktorého primárnou funkciou je ukradnúť prihlasovacie údaje z prehliadačov a súbory krypto-peňaženiek.

Ryuk ransomvér sa naďalej zameriava na nemocnice

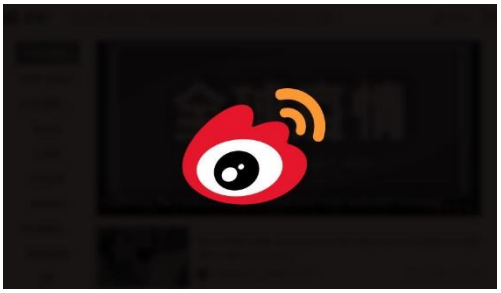
Portál Bleeping Computer minulý týždeň oznámil, že kontaktoval šesť kriminálnych skupín využívajúcich ransomvér na vydieranie obetí. Odpovedali im len dve z nich - DoppelPaymer a Maze - a oznámili, že sa nebudú v čase pandémie podieľať na útokoch na nemocnice a iné zdravotnícke organizácie. Jednou zo skupín bola organizácia za ransomvérom Ryuk, ktorá však nikdy neodpovedala. Avšak naďalej sa zameriava na nemocnice. Naposledy útok zaznamenal americký poskytovateľ zdravotnej starostlivosti.

TLP: White

Čínski hackeri využívajú chyby Cisco smerovačov a Citrix ADC v masívnej špionážnej kampani

Skupina čínskych útočníkov APT41 zneužíva zraniteľnosti v Citrix NetScaler / ADC, smerovačoch Cisco a Zoho ManageEngine Desktop Central na rozsiahlu špionážnu kampaň. Cieľom boli desiatky spoločností zamerané na rôzne priemyselné odvetvia, vrátane bankovníctva a financií, zdravotníctva, médií, ropy a zemného plynu. APT41 sa tiež zameralo na mnoho svetových krajín. Zneužilo známu zraniteľnosť (CVE-2019-19781) v zariadeniach Citrix Application Delivery Controller (ADC) a Citrix Gateway. Neskôr boli využité zraniteľnosti v smerovačoch Cisco RV320, ktoré umožňujú vzdialené vykonávanie kódu. Nakoniec bola spozorovaná zneužívaná zraniteľnosť v nástroji Zoho ManageEngine Desktop Central. V ňom útočníci využili zraniteľnosť CVE-2020-10189 na spustenie škodlivého softvéru na zariadení.

Ukradnuté údaje 538 miliónov používateľov Weibo sú na predaj na dark webe



Osobné údaje viac ako 538 miliónov používateľov čínskej sociálnej siete Weibo sú k dispozícii na online predaj. V reklamách pridaných na dark webe útočníci tvrdia, že napadli Weibo ešte v polovici roka 2019 a získali databázu používateľov tejto sociálnej siete. Medzi osobné údaje patria skutočné mená, používateľské mená, pohlavie, poloha a u niektorých používateľov aj telefónne čísla. Heslá však v tejto databáze neboli zahrnuté, čo vysvetľuje nízku cenu - iba 250 dolárov za celú databázu.

Ransomvér Netwalker infikuje používateľov pomocou phishingu súvisiaceho s koronavírusom

MalwareHunterTeam našiel prílohu využitú v novej phishingovej koronavírusovej kampani, ktorá na napadnuté zariadenie nainštaluje ransomvér s názvom Netwalker. Ten bol predtým nazývaný Mailto a nedávno sa stal zas aktívnym. Spomenutá príloha má názov „CORONAVIRUS_COVID-19.vbs“ a obsahuje spustiteľný kód na extrahovanie a spustenie ransomvéru. Po jeho aktivovaní začne šifrovať súbory v zariadení a k šifrovaným súborom pripojí náhodnú koncovku. Obete potom nájdu súbor s názvom [koncovka]-Readme.txt, ktorá obsahuje pokyny na zaplatenie výkupného.

Nový variant botnetu Mirai s názvom Mukashi sa zameriava na ZyXEL NAS zariadenia

Nová verzia neslávneho botnetu Mirai využíva nedávno odhalenú kritickú zraniteľnosť v sieťových úložných zariadeniach (NAS) spoločnosti ZyXEL. Využíva útok hrubou silou pomocou rôznych kombinácií prihlasovacích údajov na prihlásenie sa do produktov ZyXEL v snahe prevziať nad nimi kontrolu a pridať ich do siete infikovaných zariadení. Ak sa úspešne prihlási, informuje o tom riadiaci server ovládaný útočníkom. Takáto sieť sa neskôr využíva na DDoS útoky. Zraniteľných je viacero zariadení vo verzii do 5.21. Mukashi využíva "command injection" zraniteľnosť s označením CVE-2020-9054. Táto chyba spočíva v programe „weblogin.cgi“ a potenciálne umožňuje útočníkom vzdialené vykonanie kódu.

- **Nemocnica v Brne bola zasiahnutá kybernetickým útokom v čase prepuknutia COVID-19**
- **Kritická RCE chyba ovplyvňuje milióny sieťových zariadení založených na OpenWrt**
- **Útočníci použili miestne spravodajské weby na inštaláciu spywaru na telefónoch iPhone**
- **Útočníci ohrozujú e-mailové účty zamestnancov spoločnosti T-Mobile z ktorých môžu ukradnúť dáta zákazníkov.**

- Rozsiahla databáza s viac ako 200 miliónmi demografických záznamov a informácií o nehnuteľnostiach bola voľne prístupná na webe
- Spoločnosti Virgin Media Data unikli podrobnosti o 900 000 zákazníkoch
- Útoky LVI: Nové zraniteľné miesta v procesoroch Intel ohrozujú dátové centrá
- Android malvér kradnúci cookie súbory zneužíva Facebookové účty
- Europol zatkol 26 zlodejov, ktorí využili krádeže SIM kariet k odcudzeniu 3,5 milióna eur
- Nový modul pre TrickBot – bankový trójsky kôň, využíva útok hrubou silou na nezabezpečené RDP
- Aplikácii priznaní Whisper unikla takmer miliarda záznamov
- Poskytovateľovi údajov o menách 'Open Exchange Rates' unikli údaje
- Tesco posiela bezpečnostné upozornenie 600 000 držiteľom Clubcard
- Poskytovateľovi Wi-fi pripojenia na železničných staniciach v Británii unikli údaje o cestujúcich
- Microsoft zhodil globálnu sieť zombie botov Necurs
- Skupina BEC (Business Email Compromise) útočníkov používa podvodné maily s tématikou COVID-19 na nabádanie obetí, aby poslali peniaze na účty podvodníkov
- Kybernetický útok DDoS zasiahol Americké ministerstvo zdravotníctva
- Finančným spoločnostiam uniklo 425 GB citlivých dokumentov a údajov o zákazníkoch prostredníctvom otvorenej databázy.
- Dve zero-day zraniteľnosti antivírového programu Trend Micro boli zneužité útočníkmi

- **Informácie o zákazníkoch spoločnosti Rogers poskytujúcej internetové pripojenie unikli prostredníctvom nezabezpečenej databázy**

- **Na hackerských fórach sa predáva 12 GB dát, ktoré získal ransomvér Sodinokibi**

- **Stránka donášky potravín Lieferando.de v Nemecku čelila DDoS útoku**

- **DDoS botnety zneužívali tri zero-day zraniteľnosti vo videorekordéroch LILIN**

- **Univerzite medicíny v Utahu unikli údaje**

- **Spoločnosť General Electric (GE) odhalila, že osobné údaje niektorých zamestnancov mohli byť ohrozené v dôsledku úniku údajov, ktorý utrpela spoločnosť Canon Business Process Services**

- **Škodlivý softvér vytvorený rusky hovoriacimi útočníkmi bol použitý pri útokoch proti najmenej dvom európskym spoločnostiam vo farmaceutickom a výrobnom priemysle**

- **Nový ransomvér s názvom CoronaVirus slúži ako krytie pre trójskeho koňa Kpot, ktorý kradne heslá**

- **Unikli údaje o miliónoch nakupujúcich na stránkach eBay a Amazon**

- **Hackeri získali 1,6 milióna dolárov za údaje o platobných kartách z napadnutých online obchodov**

- **Ruskí hackeri zo skupiny Turla využili dve doteraz nezdokumentované časti škodlivého softvéru pri "watering hole" útoku**

- **Holandská vláda stratila pevné disky s údajmi 6,9 milióna registrovaných darcov orgánov**

- **Bývalý pracovník CIA je obviňovaný z úniku tajných útočných nástrojov na WikiLeaks**

- **Útok „Spear-Phishing“ láka obete na stiahnutie Koadic RAT posielaním falošného súboru s výsledkami HIV testov**

- **Informácie o zákazníkovi unikli vďaka chybe protokolu NordVPN, nevyžaduje sa žiadna autentifikácia**

- **Koodo Mobile, ktorý vlastní spoločnosť Telus bola obeťou krádeže dát, ktoré sú teraz na predaj**

- **DoppelPaymer ransomvér bol využitý na krádež údajov od dodávateľa spoločností SpaceX, Tesla**

Závažné zraniteľnosti bežných softvérových produktov

ZyXEL vydal opravu zero-day zraniteľnosti ovplyvňujúcej jeho NAS zariadenia

Zraniteľnosť CVE-2020-9054, ovplyvňuje množstvo NAS a firewall zariadení od spoločnosti ZyXEL. Umožňuje vzdialené vykonávanie kódu bez potreby interakcie na zariadení cez vkladanie príkazov počas autentifikácie. Spoločnosť vydala aktualizácie, ale niektoré staršie zraniteľné zariadenia aktualizované nebudú. Na internete je dostupný exploit.

Útočníci masovo hľadajú zraniteľné Microsoft Exchange servery

Závažná zraniteľnosť umožňujúca vzdialene vykonávať kód sa týka všetkých verzií Microsoft Exchange servera. Pri inštalácii zlyhá tvorba unikátnych kryptografických kľúčov a použijú sa statické kľúče ktoré majú všetky servery rovnaké, čo možno využiť po autentifikácii na spúšťanie príkazov a kódu so SYSTEM oprávnením v rámci komponentu Exchange Control Panel a na manipuláciu s e-mailovými správami na serveri.

OpenSMTPD má dve vážne zraniteľnosti, na obe je už záplata

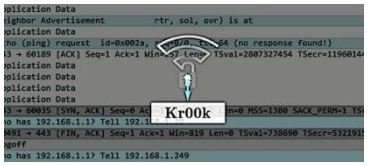
Zraniteľnosti sa týkajú mail servera OpenSMTPD. Prvá je stredne závažná zraniteľnosť, ktorá umožňuje bez privilégií čítať prvý riadok súborov, alebo v istých prípadoch celé súbory používateľov. Druhá je kritická zraniteľnosť umožňujúca čítanie pamäte mimo povolených hodnôt. Pochádza ešte z roku 2015 a umožňuje vzdialenému útočníkovi vykonávať shell príkazy, ktoré vloží do SMTP obálky. Po aktualizácii z mája 2018 môže útočník vykonávať príkazy aj s právami root.

Let's Encrypt zruší 3 milióny potenciálne nesprávne vydaných TLS certifikátov

Certifikačná autorita Let's Encrypt do 4. marca 21:00 zrušila 3 milióny TLS certifikátov ktoré mohli byť vydané nesprávne. Vlastníci domén môžu špecifikovať certifikačnú autoritu ktorá môže pre ich domény vydávať certifikáty. Let's Encrypt tieto dáta kontroluje každých 30 dní. Okrem toho ich kontroluje aj maximálne 8 hodín pred vydaním nového certifikátu. Pri tejto kontrole sa kvôli chybe pri certifikáte ktorý má platiť na viacero domén skontrolovala len jedna z nich. Certifikáty, ktorých sa táto chyba dotýka, budú zrušené.

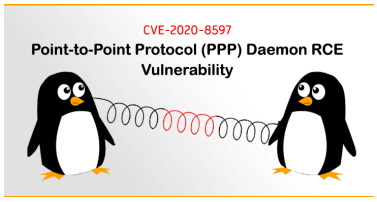
TLP: White

Kr00k zraniteľnosť zasahuje až miliardu zariadení



Zraniteľnosť CVE-2019-15126 sa nachádza vo WiFi čipoch vyrobených spoločnosťami Broadcom a Cypress, používanými v koncových zariadeniach, routeroch a prístupových bodoch. Zraniteľnosť spôsobuje, že čip použije nulový dočasný kľúč na šifrovanie paketov, ktoré odošle po odpojení z WiFi siete. Dáta z týchto paketov môže útočník odchytiť a využiť pri ďalších útokoch.

PPPD má 17 rokov starú kritickú zraniteľnosť umožňujúcu vzdialene vykonávať kód



Implementácia Point-to-Point protokolu – PPPD v mnohých distribúciách systému Linux má zraniteľnosť pretečenia medzipamäte, ktorá umožňuje útočníkovi po poslaní deformovaného EAP paketu vzdialene vykonávať kód na serveri alebo klientovi. Útočník nemusí byť autentifikovaný a PPPD príjme aj nevyžiadané pakety. Útočníkov kód sa môže vykonať s root oprávneniami.

Zero-day zraniteľnosť Zoho ManageEngine umožňuje vzdialené vykonávanie kódu

Služba Zoho ManageEngine Desktop Central, slúžiaca na manažment vzdialených zariadení, nesprávne kontroluje vstupné dáta od používateľa. Takto môže softvér deserializovať nedôveryhodné dáta, čo útočníkovi dáva možnosť vykonávať kód s oprávneniami SYSTEM alebo root bez potreby autentifikácie na zraniteľnom zaradení a prevziať kontrolu nad spravovanými zariadeniami.

Kritická zraniteľnosť typu „wormable“ umožňuje vzdialené vykonávanie kódu v Microsoft Server Message Block 3.1.1

Microsoft

Spoločnosť Microsoft zverejnila 10. marca upozornenie ADV200005, týkajúce sa kritickej zraniteľnosti zneužiteľnej na vzdialené vykonávanie kódu v protokole Microsoft Server Message Block 3.1.1 (SMBv3). Táto zraniteľnosť je spôsobená chybou spracúvania skomprimovaných škodlivých dátových paketov. Neautentifikovanému útočníkovi umožňuje zneužitie tejto chyby vykonávať ľubovoľný kód v kontexte aplikácie. Útok môže byť vedený na SMBv3 servery, aj klientov.

TLP: White

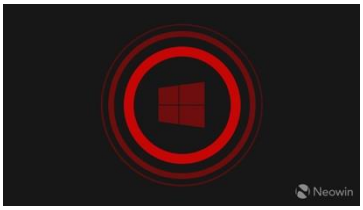
Kritická zraniteľnosť v produktoch VMware umožňuje vykonávanie kódu z hosťovaného systému

V produktoch od spoločnosti VMware boli nájdené 3 zraniteľnosti. Prvé dve zraniteľnosti sa týkajú VMware Workstation a Fusion. Prvá zraniteľnosť súvisí s použitím odalokovaného miesta v pamäti a umožňuje z hosťovaného systému vykonávať kód v hostiteľskom systéme. Druhá umožňuje eskaláciu privilégií na hosťovaných systémoch Linux, ktoré používajú virtuálnu tlač. Tretia zraniteľnosť zasahuje len hostiteľské systémy Windows a produkty VMware Workstation, Horizon Client a VMRC a umožňuje lokálnemu používateľovi vykonávať príkazy ako ktorýkoľvek používateľ. Všetky zraniteľnosti sú v najnovších verziách produktov zaplátané.

Avast a AVG AntiTrack umožňuje Man-in-the-Middle útok na HTTPS prevádzku

Program AntiTrack ktorého kód zdieľajú spoločnosti Avast a AVG, slúžiaci na zvýšenie ochrany súkromia, nekontroluje validitu HTTPS certifikátov serverov. Keďže program funguje ako proxy a prehliadaču posiela svoj vlastný certifikát ktorému prehliadač dôveruje, stránky s nedôveryhodným certifikátom sú vyhodnotené ako dôveryhodné. Okrem toho AntiTrack používa protokol TLS 1.0 aj keď je v prehliadači zakázaný a napriek nastaveniam prehliadača degraduje sady šifier na zastaralé a slabšie, ktoré neumožňujú dopredné zabezpečenie.

Dve neopravené kritické zero-day RCE zraniteľnosti zasahujú všetky verzie systému Windows



Spoločnosť Microsoft vydala upozornenie týkajúce sa bezpečnosti používateľov operačného systému Windows. Upozorňuje na dve nové kritické zero-day zraniteľnosti, ktoré umožňujú útočníkovi vzdialenú kontrolu nad napadnutými zariadeniami. Obe zraniteľnosti sú obmedzene zneužívané pri cielených útokoch a ovplyvňujú všetky podporované verzie operačného systému Windows. Nachádzajú sa v knižnici na analýzu písiem Windows Adobe Type Manager Library, ktorá nesprávnym spôsobom spracúva špeciálne vytvorené písmo Adobe Type 1 PostScript.

Zraniteľnosti VMware

V produktoch VMware bolo opravených viacero rozličných kritických a závažných zraniteľností:
CVE-2020-3947: VMware Workstation a Fusion obsahujú zraniteľnosť po použití vo vmnetdhcp.
CVE-2020-3948: Linux Guest virtuálne stroje pracujúce na serveroch VMware Workstation a Fusion obsahujú zraniteľnosť zvyšujúcu lokálne privilégiá kvôli nesprávnym povoleniam súborov v aplikácii Cortado Thinprint.
CVE-2019-5543: V prípade VMware Horizon Client pre Windows, VMRC pre Windows a Workstation pre Windows je priečinok obsahujúci konfiguračné súbory pre službu VMware USB zapisovateľný pre všetkých používateľov.

Kritické zraniteľnosti produktov Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco FXOS and NX-OS Software (CVE-2020-3172): Zraniteľnosť by mohla umožniť neautentifikovanému útočníkovi vykonať ľubovoľný kód ako root alebo spôsobiť stav odmietnutia služby (DoS).
Cisco TelePresence Management Suite (CVE-2020-3185): Kvôli nesprávnemu overovaniu vstupu, je vo webovom rozhraní možné vykonanie ľubovoľného HTML a skriptovacieho kódu v rámci postihnutej aplikácie, čo potenciálne umožňuje útočníkovi ukradnúť prihlasovacie údaje zo súborov cookie.
Cisco FXOS and UCS Manager Software (CVE-2020-3167): Zraniteľnosť je spôsobená nedostatočným overením vstupu. Jej zneužitie útočníkovi umožňuje vykonávať ľubovoľné príkazy v operačnom systéme s právami aktuálne prihláseného používateľa.
Cisco FXOS and UCS Manager Software Local Management (CVE-2020-3171): Zraniteľnosť je spôsobená nedostatočným overením vstupu. Jej zneužitie útočníkovi umožňuje vykonávať ľubovoľné príkazy v operačnom systéme s právami aktuálne prihláseného používateľa.
Cisco IOS XR Software (CVE-2020-3190): Zneužitie zraniteľnosti umožňuje útočníkovi vymazanie IPsec pamäte alebo spôsobenie stavu odmietnutia služby (DoS).
Multiple Cisco Products (CVE-2020-3164): Viaceré produkty spoločnosti Cisco sú náchylné na chybu zabezpečenia typu odmietnutia služby (DoS), pretože nedokážu overiť hlavičky HTTP požiadaviek. Útočníci môžu tento problém zneužiť a spôsobiť, že zariadenie spotrebuje nadmerné prostriedky procesora, čo používateľom spôsobí odmietnutie služby.
Cisco Email Security Appliance (CVE-2020-3181): Kvôli nedostatočnej kontrole alokácie systémovej pamäte je aplikácia náchylná na zraniteľnosť na diaľku, útočník tak môže spôsobiť stav

odmietnutia služby (DoS).
Cisco Identity Services Engine (CVE-2020-3157): Zneužitie zraniteľnosti umožňuje útočníkovi vykonať ľubovoľný kód v prehliadači prihláseného používateľa, čím sa môže dostať k prihlasovacím údajom zo súborov cookie.
Cisco WebEx Meetings Client (CVE-2020-3182): Zraniteľnosť sa vyskytuje v konfigurácii protokolu multicast DNS, útočník môže tento problém využiť na získanie citlivých informácií.

Mesačník zraniteľností Marec 2020

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
   - ZyXEL oprava zero-day zraniteľnosti ovplyvňujúcej jeho NAS zariadenia
   - Zraniteľné Microsoft Exchange servery
   - OpenSMTPD má dve vážne zraniteľnosti
   - Kr00k zraniteľnosť zasahuje až miliardu zariadení
   - Kritická zraniteľnosť Ghostcat zasahuje Apache Tomcat
   - PPPD má 17 rokov starú kritickú zraniteľnosť umožňujúcu vzdialene vykonávať kód
   - Zero-day zraniteľnosť Zoho ManageEngine umožňuje vzdialené vykonávanie kódu
   - Kritická zraniteľnosť umožňuje vzdialené vykonávanie kódu v Microsoft Server Message Block
   - Kritická zraniteľnosť v produktoch VMware umožňuje vykonávanie kódu z hosťovaného systému
   - Dve neopravené kritické zero-day RCE zraniteľnosti zasahujú všetky verzie systému Windows

https://www.csirt.gov.sk/aktualne-7d7.html?id=210