ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

December 2018

Vypracoval: CSIRT.SK

TLP: White

Rok 2018 nám okrem iného priniesol aj niekoľko rekordov v oblasti kyberútokov. Odcudzených bolo niekoľko miliárd citlivých záznamov, pričom už v polovici roka toto číslo predstavovalo 173% odcudzených záznamov v predchádzajúcom roku. Prakticky na dennom poriadku dochádzalo k infiltráciám systémov súkromných spoločností, no odohrali sa tiež prieniky do databáz osobných údajov občanom na štátnej úrovni. Bezpečnostné incidenty súvisiace s únikmi dát často vznikali v dôsledky nedostatočného zabezpečenia serverov. Bezpečnostní výskumníci našli množstvo nezabezpečených databáz s citlivými údajmi, ktoré boli vystavené verejne na internete po dobu niekoľko týždňov, či aj dlhšie. Takýto incident najväčšieho rozsahu sa odohral v marci v Indii a verejne ponechané boli osobné údaje 1,1 miliardy indických občanov.

Cryptojacking, alebo zneužitie cudzieho hardvéru cez internetový prehliadač na ťažbu kryptomien bol tento rok tiež bežným druhom kyberútokov. Postihol používateľov tisícok webstránok, vrátane vládnych webov.

Veľmi rozšíreným typom útoku sa tento rok stal malvér určený na zber údajov o platobných kartách. Stalo sa tak najmä zásluhou kampane skupín známych pod spoločným názvom ako Magecart.

Spoločnosti zaoberajúce sa kybernetickou bezpečnosťou zverejnili svoje predpovede akým smerom sa budú uberať útočníci a aké kybernetické hrozby vyvstanú v roku 2019. Ich prehľad pripravil portál ZDNet. Veľkí hráči počítajú s ústupom cryptojackingu, ktorý nahradia šíriace sa kampane typu Magecart, infikujúce platobné portály internetových obchodov a zbierajúce údaje z platobných kariet. Naopak, expanzia ťažby kryptomien sa očakáva v cloudových prostrediach. Očakáva sa nárast aktivity súvisiacej s útokmi na IoT zariadenia (napr. routre), ich infekciou a budovaním botnetov. Útočníci sa pravdepodobne tiež zamerajú na spôsoby obchádzania honeypot serverov a iných detekčných bezpečnostných prvkov. DDoS útoky, majúce na svedomí nedostupnosť zariadení a služieb, budú pravdepodobne zneužívať nové protokoly. Predpokladá sa, že masívne ransomvérové kampane budú na ústupe a útočníci sa začnú zameriavať na väčšie spoločnosti, pri ktorých existuje väčšia pravdepodobnosť, že dostanú požadované výkupné. Autori malvéru sa zase stále viac zaujímajú o techniky, ktoré by dali ich kódu schopnosť vyhnúť sa antivírusovému softvéru. Vďaka rozvoju umelej inteligencie budú môcť takéto techniky vyvíjať a testovať efektívnejšie.

V oblasti kybernetických hrozieb, ktorých činiteľmi sú štáty, sa tiež očakáva nárast aktivity. Predpokladá sa, že viaceré štáty začnú budovať svoje obranné a prípadne útočné tímy. Možná je zvýšená priemyselná a ekonomická špionážna aktivita a využívanie elektronickej propagandy štátmi, ktoré doposiaľ podobné aktivity nerozvíjali. Očakáva sa aj predloženie niekoľkých medzinárodných dohôd upravujúcich pravidlá pre štátmi sponzorované kybernetické kampane, nakoľko rastie počet civilných obetí.

Spoločnosť Kaspersky očakáva nárast kybernetických hrozieb pre finančné inštitúcie a platobné systémy v regiónoch juhovýchodnej a strednej Ázie a strednej Európy, vzhľadom na nedostatočné bezpečnostné opatrenia. Očakávané sú aj prvé útoky s použitím uniknutých biometrických údajov a útoky na mobilné bankovníctvo, nakoľko k nim existuje dostatok nástrojov. Možné sú útoky využívajúce sieť dodávateľov a webové API rozhrania. Tiež sa očakávajú útoky s využitím pokročilých techník sociálneho inžinierstva cielené na pracovníkov organizácií s právami vykonávať prevody

peňazí. Koncom roka 2018 riešila spoločnosť Kaspersky vo východnej Európe útoky na banky, pri ktorých útočníci využili fyzické zariadenia, ktoré pripojili do infraštruktúry bánk. Jednalo sa o notebooku, zariadenia postavené na Raspberry Pi a tzv. Bash Bunny USB zariadeniach vo veľkosti USB kľúča, určených pre penetračné testovanie. Kampaň bola nazvaná DarkVishnya.

Očakáva sa nárast cielených phishingových útokov na spoločnosti, tzv. spear phishing, pri ktorých sa útočník vydáva za vyššie postaveného člena organizácie, nadriadeného zamestnanca, ktorému je e-mail určený. Dávajte si preto pozor a kontrolujte, či e-mail prišiel naozaj od osoby, ktorá je v podpise, resp. ktorej e-mailová adresa sa zobrazuje ako odosielateľ (najmä aj sa jedná o peňažné prevody a dôležité rozhodnutia). Nezabudnite na 5 najbežnejších techník spamerov a phisherov:

1) *Falošné notifikácie zo sociálnych sietí* – takáto notifikácia môže pôsobiť na nerozoznanie od skutočnej správy. Najlepšia prevencia pred odcudzením prihlasovacích údajov je kontrola, kam vedie poskytnutý link a z akej adresy e-mail prišiel.
2) *Bankový phishing* – vaša banka vás nikdy e-mailom nepožiada o prihlasovacie údaje, či údaje z vašej platobnej karty. Podvodníci však áno. Nasledovať e-mailový pokyn „prosím prihláste sa do svojho účtu cez link nižšie, aby ste obnovili prístup k vášmu účtu“ je istá cesta ako sa rýchlo zbaviť svojich peňazí.
3) *Falošné notifikácie od známych služieb a predajcov* – „kliknite na odkaz nižšie“ a prihláste sa do svojho účtu v Amazone (resp. zameň za ľubovoľnú známu službu)... a Vaše údaje má útočník. Prípadne ste práve stiahli do svojho zariadenia malvér.
4) *Falošné notifikácie od e-mailových služieb* – vaša e-mailová schránka je „preplnená“, alebo ju potrebujete „overiť“ prihlásením sa cez podvrhnutý formulár, alebo link. Váš poskytovateľ e-mailovej služby vás nikdy nebude žiadať o prihlasovacie údaje.
5) *Podvody typu „Nigérijský princ“* – pravdepodobne ste už obdržali nejeden e-mail, v ktorom odosielateľ tvrdí, že je významná, alebo bohatá osoba a potrebuje previesť veľkú finančnú čiastku mimo svojej krajiny. A práve vy ste jediný dôveryhodný človek a za svoju službu dostanete tučný podiel. Najprv však prosím pošlite niekoľko stoviek dolárov na poplatky za prevod pre fiktívnu banku.

Riešené incidenty na Slovensku a z našej činnosti

Mesiac december a sviatkové obdobie boli vzhľadom na počet bezpečnostných incidentov pokojnejšie. CSIRT.SK v tomto mesiaci riešil niekoľko štandardných incidentov, najmä phishingové kampane na svoju konštituenciu a informoval inštitúcie o napadnutí botmi.

CSIRT.SK vykonal niekoľko vyžiadaných penetračných testov webových stránok a systémov inštitúcií vo svojej konštituencii.

V rámci aktivít zameraných na zvyšovanie odbornej a vedomostnej úrovne tímu sa členovia analytického oddelenia zúčastnili na konferencii Black Hat Europe 2018.

Významné útoky vo svete

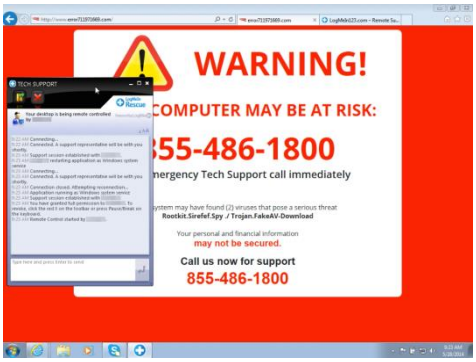
50 000 tlačiarní napadnutých kvôli propagovaniu youtubera

Používateľ s Twitterovou prezývkou TheHackerGiraffe získal kontrolu nad 50 000 tlačiarňami a multifunkčnými zariadeniami, aby vytlačil odkaz na podporu youtubera s prezývkou PewDiePie. Tomu hrozilo, že príde o prvenstvo v počte odberateľov jeho kanálu na úkor indickej spoločnosti T-Series. TheHackerGiraffe chcel svojím činom zároveň upozorniť majiteľov zraniteľných zariadení, aby ošetrili voľný prístup k nim z internetu cez porty 9100, 631 a 515. Zraniteľné sú stotisíce zariadení po celom svete. Útočník môže získať prístup k zariadeniam v sieti v ktorej sa tlačiareň nachádza, inštalovať malvér, či spôsobiť fyzické poškodenie tlačiarne. Podľa používateľa trvala celá akcia približne pol hodiny, pričom predtým sa o hackovanie tlačiarní nezaujímal.

Moskovská lanovka napadnutá ransomvérom hneď po otvorení

Prvá lanovka, ktorú vybudovali v Moskve, mala neslávne otvorenie. Niekoľko dní po jej spustení bol hlavný počítačový systém napadnutý a zašifrovaný ransomvérom. Útočník žiadal za dešifrovanie súborov nešpecifikovanú sumu v bitcoinoch. Prvý mesiac od spustenia lanovky sľubovala prevádzkujúca spoločnosť jazdy zdarma, čo prispelo k veľkému záujmu verejnosti.

16 falošných call centier a 39 zadržaných



Indická polícia vykonala razie v 16 miestach, kde operovali podvodníci vydávajúci sa za technickú podporu firiem ako Microsoft, Apple, Goole, Dell a HP. Zadržala 39 podvodníkov, teda o 15 viac ako pri októbrových raziách. Zaistila aj množstvo dôkazového materiálu. Microsoft sa vyjadril, že obdržal vyše 7000 správ od obetí tech-support podvodu. Podvodníci často využívajú tzv. techniku „typosquatting“, kedy zakúpia doménu pripomínajúcu známu legitímnu službu (napr. aple.com). Keď na takúto stránku obeť príde, vyskočia na ňu varovania o infekcii jej zariadenia malvérom, prípadne

tab so stránkou nie je možné zatvoriť. Podvodníci sa tak snažia obeť donútiť zavolať na fingované číslo technickej podpory, ktoré stránka ponúka.

Prienik do systémov služby Quora postihol 100 miliónov používateľov

Informačný portál Quora, ktorý umožňuje používateľom klásť rôzne otázky a dostávať na ne odpovede, bol napadnutý. Unikli pri tom osobné informácie 100 miliónov používateľov. Okrem iného sa jednalo o mená, e-mailové kontakty, šifrované heslá, informácie importované z iných webov, verejný obsah vrátane otázok, odpovedí a komentárov a neverejný obsah vrátane súkromných správ. Ako prenikol útočník na server nebolo v čase zverejnenia informácie známe. Quora informovala zasiahnutých používateľov cez e-mail a resetovala ich prihlasovacie heslá.

Nový ransomvér infikoval v Číne 100 000 zariadení

V Číne sa šíril nový druh ransomvéru, ktorý za štyri dni infokoval vyše 100 000 počítačov. Útočníkovi sa ho podarilo vložiť do distribúcie softvéru EasyLanguage, ktorý využíva množstvo vývojárov aplikácií. Všetky aplikácie skompilované cez kompromitovanú distribúciu EasyLanguage spôsobovali spolu s nimi inštaláciu ransomvéru. Útočník nevyžadoval platbu v bitcoinoch, ale v čínskych yuanoch cez aplikáciu WeChat Pay (jedná sa o sumu 110 yuanov, v prepočte asi 16 USD). Ransomvér okrem šifrovania súborov obsahoval aj funkcionalitu na odcudzenie používateľských hesiel z niekoľkých webstránok. Útočníka autority do piatich dní odhalili a chytili.

Útočníci kradli 4 roky kanadskému kvetinárstvu platobné dáta

Kanadská online pobočka kvetinárstva 1-800-Flowers bola štyri roky zdrojom údajov o platobných kartách pre neznámych útočníkov. Spolu exfiltrovali záznamy o 75 000 objednávkach. Nie je jasné, akým spôsobom ostal tento prienik nepovšimnutý takú dlhú dobu, no jednou z možností je miskonfigurácia, alebo zraniteľnosť prítomná v online systémoch.

Botnet útočí na WordPress stránky, ovládol už 20 000

Útočníci ovládajúci botnet zostavený z 20 000 kompromitovaných WordPress webstránok využívajú tieto stránky na útočenie na ďalšie WordPress portály. Spoločnosť WordFence zaznamenala koncom minulého roka 5 miliónov pokusov o prihlásenie za mesiac z takýchto kompromitovaných webstránok. Jedná sa o slovníkové útoky. Príkazy a informácie o nových cieľoch útokov sú rozposielané štyrmi kontrolnými servermi cez sieť vyše 14 000 prenajatých proxy serverov infikovaným WordPress stránkam. Pokusy o prihlásenie sú smerované na XML-RPC autentifikačné rozhranie, preto sa odporúča používať bezpečnostný modul pre WordPress (resp. firewall), blokujúci brute-force a slovníkové útoky.

Nezabezpečená databáza vystavuje internetu osobné dáta 66 miliónov osôb

Aj tento mesiac výskumník Bob Diachenko odhalil nezabezpečenú databázu MongoDB. Obsahovala osobné údaje vyše 66 miliónov osôb, ktoré vyzerali ako pozbierané zo siete LinkedIn. Okrem iného pozostávali z mien, súkromných a pracovných e-mailových adries, telefónnych čísel a pracovnej histórie osôb. Vlastníka databázy sa nepodarilo nájsť, no databáza už nie je verejná. To však nevylučuje možnosť, že sa údaje v nej obsiahnuté v budúcnosti opäť objavia na verejnosti.

Druhá kritická zraniteľnosť Google+ postihuje takmer 53 miliónov používateľov

Spoločnosť Google objavila za posledné mesiace už druhú veľkú zraniteľnosť vo svojej službe Google+, ktorá exponovala osobné údaje takmer 53 miliónov používateľov. Konkrétne sa jednalo o mená, e-mailové adresy, vek a povolanie. Opäť sa jednalo o vývojársku API, konkrétne funkciu „People:get“, poskytujúcu vývojárom základné informácie spojené s používateľským účtom. V novembrovej aktualizácii existovala chyba, ktorá cez toto volanie sprístupnila aplikáciám osobné údaje aj používateľov s neverejnými profilmi. Napriek tomu, že žiadne údaje pravdepodobne neboli zneužité a spoločnosť zraniteľnosť odstránila za 6 dní, na základe tohto incidentu posunula ukončenie

používateľskej verzie služby Google+ na apríl tohto roku a oznámila vypnutie API v tejto verzii za 90 dní od objavenia.

30 krajín sveta a prihlasovacie údaje 40 000 občanov do vládnych systémov

Phishingová kampaň, šíriaca malvér exfiltrujúci prihlasovacie údaje, zasiahla vyše 40 000 obetí zo štátnej správy a vládnych organizácií 30 krajín sveta. Oznámil to ruský bezpečnostný tím CERT Group-IB. Útočníci prostredníctvom e-mailu šírili spyware ako Pony, AZORult či Qbot. Najviac exfiltrovaných prihlasovacích údajov pochádzalo z Talianska, Saudskej Arábie a Portugalska. Postihnuté boli aj účty zamestnancov na vládnych stránkach Francúzska, Maďarska, Chorvátska, Poľska, Rumunska, Švajčiarska, Bulgarska, Nórska, Izraelu a Gruzínska. Group-IB kontaktovala bezpečnostné tímy postihnutých krajín. Exfiltrované údaje môžu útočníci použiť na prístup k utajovaným dátam a k získaniu prístupu do interných systémov vládnych organizácií.

Unikli daňové identifikačné čísla 120 miliónov brazílskych občanov

Chybou v konfigurácii servera Apache boli po neurčitú dobu verejne prístupné daňové identifikačné čísla 120 miliónov občanov Brazílie, ktoré sú potrebné pre otvorenie bankového účtu, podanie žiadosti o pôžičku, či založenie firmy. Tieto čísla boli párované k ďalším citlivým údajom, ako banková a volebná história osoby, pôžičky, registračné číslo voliča, adresa, kontakty na osobu a rodinu, zmluva a údaje o zamestnaní, či dátum narodenia. Nie je známe, prečo sa tieto údaje nachádzali na serveri tretej strany, ani či sa k nim dostali nepovolané osoby skôr, ako bol server zabezpečený.

Chyba v API Facebooku sprístupnila fotografie takmer 7 miliónov používateľov

Photos API je funkcia, ktorá v službe Facebook povoľuje po odsúhlasení používateľov prístup k ich fotografiám na ich „Timeline“. Chyba v softvérovej aktualizácii tejto služby spôsobila, že Photos API funkcia povoľovala dva týždne prístup aj k fotografiám, ktoré sa nachádzali vo „Facebook Stories“, „Marketplace“ a tiež neuverejneným. Takýto prístup dostalo 1500 aplikácií

a zraniteľnosť zasiahla 6,8 milióna používateľov. Spoločnosť Facebook týchto používateľov o incidente informovala.

Desiatky tisíc serverov s aplikáciou Jenkins otvorené útočníkom

Napriek niekoľko mesiacov dostupnej aktualizácii je približne 78 000 serverov s vývojárskou aplikáciou Jenkins stále zraniteľných. Dve opravené zraniteľnosti povoľovali útočníkom získať administrátorské práva a prihlásiť sa s použitím neplatných prihlasovacích údajov. Tak mohli útočníci exfiltrovať dáta, prevziať kontrolu nad serverom, či ťažiť kryptomeny. Minulý rok sa podarilo útočníkom na Jenkins serveroch počas niekoľkých mesiacov vyťažiť kryptomenu Monero v hodnote 3,4 milióna USD.

Čínski hackeri ukradli tajné informácie námorníctvu USA

Americké vojenské námorníctvo vydalo koncom roka správu o kybernetických hrozbách, v ktorej sa spomínajú aj útoky na zazmluvnené firmy. Útočníci začiatkom roka ukradli 64 GB citlivých dát US Navy uložených v sieti nešpecifikovaného dodávateľa. V polovici roka zas útočníci prenikli do systémov ďalšieho dodávateľa vojenského námorníctva USA a ukradli tajné plány na nadzvukovú strelu určenú na likvidáciu lodí ponorkami. Pravdepodobný pôvod oboch útokov je v Číne. Stopy vedú ku skupine Temp.Periscope (Leviathan).

Prienik do systémov NASA

Agentúra NASA v decembri oznámila, že v októbri neznámi útočníci prenikli do systémov serverov, na ktorých boli uložené osobné údaje bývalých a súčasných zamestnancov, vrátane čísiel sociálneho poistenia. Agentúra incident oznámila postihnutým osobám, začala forenzné vyšetrovanie a práce na zabezpečení serverov.

Prienik do platobných terminálov reťazca Caribou Coffee

Americký reťazec obchodov s kávou Caribou Coffee ohlásil bezpečnostný incident postihujúci 239 obchodných miest, teda asi 40% prevádzok. Útočníci prenikli do platobných systémov spoločnosti. Zasiahnutí sú zákazníci platiaci v postihnutých prevádzkach v období od konca augusta do začiatku decembra, ktorým mohli uniknúť údaje o platobných kartách.

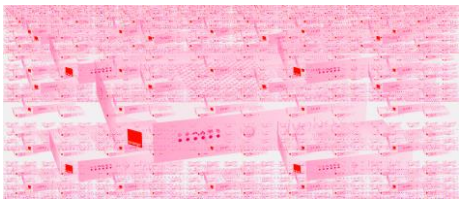
India povolila 10 organizáciám monitorovať a dešifrovať dáta svojich občanov

Koncom roka vydala indická vlád nariadenie, ktoré dovoľuje desiatim agentúram legálne odchytávať, monitorovať a dešifrovať informácie vytvorené, odoslané, prijaté, alebo uložené na ľubovoľnom počítači. V praxi toto nariadenie dovoľuje indickým autoritám sledovať prijímanú a odosielanú komunikáciu všetkých svojich občanov. Zákon bude pravdepodobne napadnutý na súde ako protiústavný.

Únik dát pol milióna študentov a zamestnancov školstva v San Diego

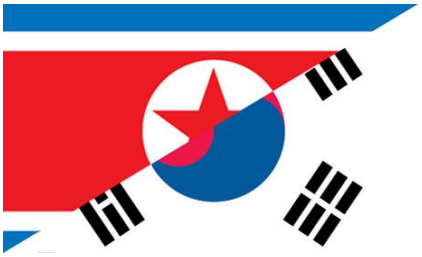
Prienik do systémov San Diego Unified School District zasiahol pol milióna študentov od školského roku 2008/2009, rodičov a zamestnancov. Okrem iného unikli mená, dátumy narodenia, adresy, e-mailové a telefonické kontakty, čísla sociálneho poistenia / študentské identifikačné čísla, a tiež informácie o študentoch vrátane rozvrhov a zdravotného stavu. Útočníci využili phishingové e-maily na získanie prístupu do siete organizácie. Do systémov mali prístup od začiatku roka do novembra. Organizácia sa o prieniku dozvedela v októbri a potichu viedla vyšetrovanie, aby útočníkov nevyplašila. Poškodené osoby boli o incidente informované a systémy zabezpečené.

Modemy Orange v Španielsku a Francúzsku sprístupňujú prihlasovacie údaje



Výskumník Troy Mursch zistil, že približne 19 500 Orange Livebox modemov obsahuje niekoľko rokov starú zraniteľnosť, kvôli ktorej dokáže útočník ľahko získať SSID, heslo potrebné pre pripojenie na wifi sieť a geografickú polohu siete. Užívatelia často používajú rovnaké heslo aj pre prístup do administrátorského rozhrania. Okrem útokov na malú vzdialenosť na zaujímavé ciele, ku ktorým je útočník ochotný pricestovať je tak možné vytvárať zo zraniteľných routerov aj botnety. Mursch oznámil, že existuje aspoň jeden útočník skenujúci takéto zariadenia spoločnosti Orange. Väčšina zraniteľných zariadení sa nachádzalo v Španielsku a Francúzsku. Kód zneužívajúci niekoľko zraniteľností Orange Livebox zariadení je verejne dostupný.

Útočníci ukradli informácie o 997 severokórejských utečencoch

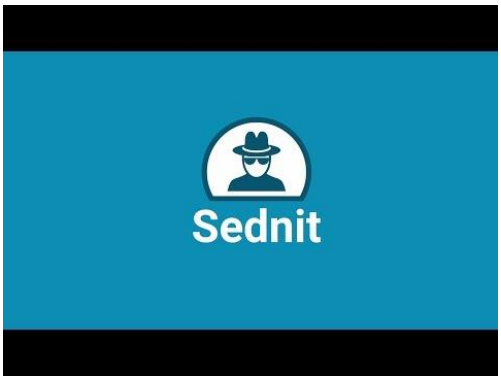


Prienik do databázy juhokórejského centra podpory utečencov znamenal únik osobných informácií vrátane umiestnenia 997 severokórejských utečencov v provincii Severný Gyeongsang. Nie je známe, či za útokom stojí náhodný útočník, alebo niektorá zo severokórejských vládou sponzorovaných skupín, a teda či sú utečenci v priamom ohrození života.

Kamerové systémy Guardzilla umožňujú sledovať majiteľov

Systém Guardzilla All-In-One Video Security System určený na zabezpečenie a video monitoring domácností, konkrétne kamera typu GZ501W, obsahuje natvrdo naprogramované heslo pre prístup do cloudového úložiska Amazon S3, kde sa ukladá záznam. To znamená, že všetci užívatelia tohto systému majú rovnaké heslo a vedia sa dostať k videozáznamom ľubovoľného používateľa. Do vydania zdrojového článku nebola výrobcom vydaná opravná aktualizácia a odporúčané bolo vypnúť cloudovú funkcionalitu.

Prvý UEFI rootkit vlastní APT Sednit



„UEFI rootkity boli v posledných rokoch študované a viedli sa o nich rozsiahle diskusie, no prakticky neexistovali dôkazy o reálnych kampaniach zameraných na kompromitáciu systémom touto cestou.“, informoval výskumník firmy ESET, Frédéric Vachon. Skupina APT28, známa aj ako Sednit, Sofacy, či Fancy Bear však mení hru. Upravila bezpečnostný nástroj LoJack pre obete krádeží laptopov, a vytvorila z neho UEFI malvér LoJax. Tento rootkit využíva veľkú časť pôvodnej funkcionality, t.j. vzdialená kontrola súborov a nenápadné odosielanie svojej polohy. Vďaka tomu, že sa nahráva do UEFI, získava perzistenciu a nenápadnosť. Nahrá sa pred naštartovaním operačného systému a na jeho odstránenie je potrebné vymeniť matičnú dosku, alebo prepísať UEFI novou verziou. Malvér sa šíri najmä prostredníctvom phishingových e-mailov.

Útok ransomvérom na mediálne spoločnosti, vydanie denníkov zdržané

Kybernetický útok zasiahol spoločnosť Tribune Publishing publikujúcu niekoľko významných amerických denníkov a Los Angeles Times a zdržal tak ich sobotňajšie tlačené vydania. Zasiahnuté boli Wall Street Journal, New York Times, Los Angeles Times, Chicago Tribune, Baltimore Sun, Lake County News-Sun, Post-Tribune, Hartford Courant, Capital Gazette a Carroll County Times. Podľa všetkého útočníci využili ransomvér Ryuk.

Závažné zraniteľnosti bežných softvérových produktov

Zneužívaná zero-day zraniteľnosť Flash Player dovoľuje ovládnuť systém

Bezpečnostní experti zachytili pokus o zneužitie kritickej zero-day zraniteľnosti v Adobe Flash Player, ktorá pomocou chyby použitia odalokovaného miesta v pamäti môže viesť k možnosti vzdialene vykonávať kód a prebrať kontrolu nad systémom obete. Útočníci na to využili ovládací prvok Flash ActiveX v hlavičke škodlivého dokumentu Microsoft Office, ktorý následne rozbalil a nainštaloval do systému zadné dvierka.

Kritická chyba v Kubernetes ponúka administrátorské práva

Nástroj Kubernetes obsahuje kritickú zraniteľnosť, ktorá dovoľuje neautentifikovanému útočníkovi bez práv získať administrátorské práva ku API, alebo „clustru“ v cloude. Nachádza sa v Kubernetes API serveri, ktorý po prijatí upravenej požiadavky vyvolávajúcej chybu ponechá spojenie k „podu“ otvorené. Útočník môže potom „podu“ posielať požiadavky bez ďalšej autorizácie, čo mu umožní vykonávať ľubovoľný kód, získavať dáta, či sabotovať cloudovú službu.

Opravená zneužívaná kritická zero-day zraniteľnosť vo Windows

Spoločnosť Microsoft opravila v rámci decembrového balíka aktualizácií aktívne zneužívanú zero-day zraniteľnosť, ktorá dovoľuje vo viacerých verziách operačného systému Windows zvýšenie práv. To môže viesť k úniku informácií, umožneniu vzdialene vykonávať kód a ovládnutiu zraniteľného systému.

Magellan: zraniteľnosť v SQLite postihuje webové prehliadače a iné aplikácie

Zraniteľnosť v databázovej knižnici SQLite nazvaná Magellan umožňuje útočníkom spôsobiť zlyhanie programu, čítať jemu alokovanú pamäť, alebo vzdialene vykonávať ľubovoľný kód. Vzhľadom na masívne rozšírené používanie SQLite sú postihnuté milióny aplikácií, od webových prehliadačov postavených na platforme Chromium, cez IoT zariadenia, po Android a iOS aplikácie.

TLP: White

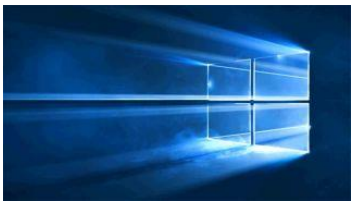
WordPress obsahuje niekoľko závažných chýb. Môžu spôsobiť únik používateľských hesiel.

Spoločnosť WordPress opravila vo verziách 4.x a 5.0 sedem závažných zraniteľností, z ktorých niektoré môžu viesť až k prevzatiu kontroly nad webstránkou. Jedná sa o tri XSS zraniteľnosti, zraniteľnosť umožňujúcu únik údajov, chyby narábania s objektmi a zraniteľnosti umožňujúce neautorizované zásahy do obsahu.

Kritická zero-day zraniteľnosť v prehliadači Internet Explorer

Spoločnosť Microsoft vydala mimoriadnu opravnú aktualizáciu na zero-day zraniteľnosť v prehliadači Internet Explorer, ktorá umožňuje vykonávanie ľubovoľného kódu. Zraniteľnosť je aktívne zneužívaná. V spojení s niektorou zero-day zraniteľnosťou navyšujúcou práva na úroveň systému, opravenou v predchádzajúcich mesiacoch, dokáže útočník získať úplnú kontrolu nad zraniteľným systémom.

Tretia zero-day zraniteľnosť v OS Windows od SandboxEscapera



Twitterový používateľ s pseudonymom SandboxEscaper zverejnil v poradí už tretiu zero-day zraniteľnosť v operačnom systéme Microsoft Windows, ktorá dovoľuje zvýšenie práv a čítanie ľubovoľných súborov na úrovni systémových práv. Zatiaľ neexistuje opravná aktualizácia.

Zraniteľnosť prehrávača VideoLAN VLC

Zraniteľnosť s označením CVE-2018-19857 v prehrávači VideoLAN VLC môže viesť k podtečeniu premennej typu integer a umožniť útočníkovi vykonávanie ľubovoľného kódu v kontexte aplikácie. Funkcia „ReadKukiChunk()“ premieňa vrátenú hodnotu na neoznačenú premennú typu integer. Chyba môže nastať, keď aplikácia číta pamäť z neinicializovaného ukazovateľa pri spracovaní cookie v súboroch CAF. Aktualizácia je dostupná.

Zraniteľnosť firewallu Cisco Adaptive Security Appliance

Zraniteľnosť Cisco ASA označená ako CVE-2018-15465 nesprávne vyhodnocuje používateľské práva, čo môže viesť ku vzdialenému zvýšeniu práv. Útočník na to môže využiť špeciálne upravené HTTP požiadavky odosielané cez HTTPS, vďaka čomu môže okrem iného získavať súbory zo zraniteľného zariadenia, alebo zamieňať softvérové zálohy (image). Aktualizácia je dostupná.

Mesačník zraniteľností December 2018

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
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
    - Kubernetes
    - Zraniteľnosti modulov WordPress
    - Magellan (SQLite)
    - Wordpress

https://www.csirt.gov.sk/aktualne-7d7.html?id=173