ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Február 2019

Vypracoval: CSIRT.SK

TLP: White

Bývalý zamestnanec si nahrá citlivé firemné údaje a predá ich konkurencii. Dodávateľ softvéru pridá do svojho produktu zadné vrátka, aby si navýšil zisky krádežou údajov. Čo si predstavíte pod slovným spojením „hrozba zvnútra“? Štúdia spoločnosti CA Technologies pre rok 2018 hovorí, že zo všetkých útokov zvnútra je vedomých menej ako polovica. Až 51% hrozieb vychádza z nedbalosti či nevedomosti zamestnancov, alebo je spôsobená únikom ich prihlasovacích údajov. Pritom 53% organizácií, ktoré sa prieskumu zúčastnili, zaznamenalo v roku 2018 aspoň jeden kybernetický bezpečnostný incident vychádzajúci zvnútra a až 90% organizácií sa takýmito incidentami cítilo ohrozených. Vyše 90% organizácií nejakým spôsobom monitorovalo používateľov a prístup k citlivým dátam.

Čo sa týka vnútorných bezpečnostných incidentov z nedbalosti, správa spoločnosti Dtex hovorí až o 64%, pričom 13% incidentov v štúdii súviselo s únikom prihlasovacích údajov a len 23% prípadov predstavovalo zámerné útoky. Podľa štúdie spoločnosti Egress Technologies až 83% spoločností sa vyjadrilo, že ich zamestnanci exponovalo dáta spoločnosti, alebo jej zákazníkov.

Ďalším faktorom, ktorý nahráva útočníkom, je priemerný čas, za ktorý organizácie aktualizujú svoje softvérové vybavenie a odstránia tak zo svojich systémov závažné zraniteľnosti. Takmer 70% zraniteľností je odstránených za čas dlhší ako štyri týždne, pričom až 55% sa natiahne na tri mesiace. 25% závažných zraniteľností ostáva neopravených priemerne 290 dní a menej závažné zraniteľnosti môžu ostať prítomné v systémoch aj viac ako rok po vydaní opráv.

Úspešný útok zvnútra môže vykonať aj útočník, ktorý nepochádza priamo z organizácie. Môže napríklad podvrhnúť na parkovisku spoločnosti USB kľúče so škodlivým kódom, ktoré zvedaví zamestnanci vložia do svojich pracovných staníc. Alebo priamo vstúpi do budovy spoločnosti predstierajúc, že je klient, zástupca klientskej spoločnosti, kuriér, uchádzač o zamestnanie, či dodávateľ služby. Týmto spôsobom boli vykonané útoky na východoeurópske banky, ktoré boli nazvané DarkVishnya. Útočníci v klientskych priestoroch a kanceláriách bánk rozmiestnili svoje zariadenia, ktoré pripojili do siete inštitúcie a následne na diaľku sieť kompromitovali. Využili lacné notebooky, Raspberry Pi, či nástroje na penetračné testovanie v tvare USB kľúčov, tzv. Bash Bunny. Okrem monitorovacích softvérových riešení sa na zmiernenie dopadu podobných útokov odporúča oddeliť segment siete prístupnej z klientskych priestorov od vnútorného segmentu siete organizácie.

Samozrejme, aj incidenty spôsobené zámerným konaním zamestnancov sú vážnou hrozbou. Spoločnosť DJI, ktorá ma troj-štvrtinový podiel na svetovom trhu s dronmi, takýmto spôsobom utrpela škodu 150 miliónov dolárov po tom, ako časť jej zamestnancov podvodne upravila ceny jej výrobkov. Banke Huaxia Bank zas softvérov manažér, ktorý bol zamestnancom v jej centre pre softvérový a technologický vývoj, ukradol milión dolárov zneužitím zraniteľnosti v jej bankomatoch. Podobné útoky zvnútra zažívajú aj štátne organizácie. Francúzska polícia zadržala pred niekoľkými mesiacmi dôstojníka, ktorý predával na darkwebe službu, ktorá využívala policajnú databázu na sledovanie mobilných zariadení podľa telefónneho čísla.

Portál DarkReading.com priniesol niekoľko tipov na možné opatrenia na zníženie pravdepodobnosti vzniku vnútorných bezpečnostných incidentov:

1) Starostlivosť a záujem o zamestnancov – ak sú zamestnanci nespokojní, ľahšie skĺznu, alebo sa nechajú presvedčiť, aby sa zapojili do škodlivej činnosti.
2) Bezodkladná blokácia prístupov do systémov po skončení pracovného pomeru so zamestnancom.
3) Prehľad o finančnej situácii zamestnancov - dlhy, alebo iná ťažká situácia môže zviesť k škodlivej aktivite, ktorá má potenciál vyprodukovať finančný zisk.
4) Sledovanie náhlych zmien v záujmoch a správaní zamestnancov – práca v nezvyčajných hodinách, alebo neskoro do večera, záujem o utajené materiály, a podobne.
5) Udeľovanie prístupu zamestnancom s najnižšími možnými právami.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci február riešil zväčša štandardné incidenty, najmä phishingové kampane na svoju konštituenciu a informoval inštitúcie o napadnutí malvérom tvoriacim botnety. Obdržal tiež informáciu o kompromitovaných slovenských IP adresách, ktorých vlastníkov informoval v spolupráci s NBÚ. Okrem toho CSIRT.SK riešil zraniteľnosti niekoľkých systémov verejnej správy, okrem iného systému eID, o ktorom informovali aj médiá. Riešený bol aj útok ransomvérom na jednu inštitúciu.

CSIRT.SK vykonal niekoľko vyžiadaných externých penetračných testov inštitúcií vo svojej konštituencii.

V rámci aktivít zameraných na zvyšovanie odbornej a vedomostnej úrovne tímu sa členovia CSIRT.SK zúčastnili na niekoľkých konferenciách a vzdelávacích podujatiach.

CSIRT.SK sa tiež venoval príprave novej vyhlášky Úradu podpredsedu vlády SR pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Významné útoky vo svete

Únik dát užívateľov služby bytového dizajnu Houzz

Internetový portál ponúkajúci služby interiérového dizajnu Houzz informoval o prieniku do svojich systémov a úniku súboru s citlivými dátami používateľov. Súbor obsahoval mená, domovské mestá a štáty, popisy, prihlasovacie údaje IP adresy a používateľské Facebook ID , ak sa používatelia prihlasovali cez sociálnu sieť. Presný počet zasiahnutých používateľov nie je známy, no mesačne stránku navštívi 40 miliónov záujemcov. Spoločnosť Houzz používateľov o prieniku informovala.

Útočníci vo Veľkej Británii odchytávali bankové SMS kódy pre 2-faktorovú autentifikáciu

Britská banka Metro Bank zaznamenala sériu útokov, aké sa odohrali v roku 2017 v Nemecku. Jednalo sa o krádež prostriedkov z účtov klientov, ktoré boli zabezpečené dvojfaktorovou autentifikáciou pomocou sms kódu. Útočníci najprv pomocou phishingu, keyloggeru, alebo trójskeho koňa získali prihlasovacie heslá do internet bankingu niekoľkých klientov. Následne zneužili zraniteľnosť telekomunikačného protokolu SS7, ktorý neoveruje, odkiaľ príde požiadavka na doručenie sms. Tak presmerovali a odchytili overovacie sms od banky a odoslali platby. Už nejakú dobu prevláda medzi bezpečnostnými expertmi názor, že 2-FA pomocou sms nie je bezpečná a odporúča sa používať inú formu, napríklad autentifikačnú aplikáciu, alebo hardvérový autentifikátor ako Yubikey.

Útok na diplomatov v Iráne upraveným spyvérom

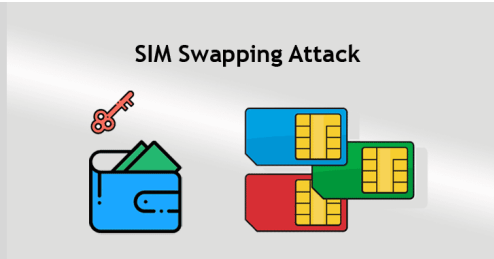
Iránska APT skupina s pseudonymom Chafer útočila na veľvyslancov v Iráne pomocou upraveného spyvéru Remexi. Na komunikáciu s malvérom využila mechanizmus Microsoft Background Intelligent Transfer Service (BITS) cez protokol http. Remexi

umožňuje získavať stlačené klávesy, screenshoty a dáta z internetových prehliadačov ako cookies a históriu. Nie je známe, akým spôsobom bol malvér šírený. Spoločnosti Kasperski a Symantec už nejaký čas sledujú vývoj tejto skupiny.

Nová varianta podvodu Sextortion

Nová odnož podvodu Sextortion sa objavila na internete v mesiaci Február. Jedná sa o kampaň podvodných e-mailov, v ktorých útočníci tvrdia, že obeť nahrali cez jej webkameru pri sledovaní sexuálne orientovaného obsahu. Pýtajú výkupné s hrozbou, že ak obeť nezaplatí, toto video rozpošlú všetkým jej kontaktom, ktoré získali z jej adresára. Nová varianta tvrdí, že útočníci nahrali na populárnu stránku xvideos.com škodlivý kód, ktorý dokáže nahrať obeť cez jeho kameru a súčasne ukradnúť údaje jej kontaktov z jej počítača. V skutočnosti sa však jedná len o podvod a takéto e-maili možno mazať. Neodporúča sa klikať na linky v nich, ktoré sľubujú náhľad inkriminovaného videa, nakoľko boli zaznamenané prípady šírenia ransomvéru a trójskych koní.

10 rokov pre útočníka kradnúceho telefónne čísla



20 ročný útočník priznal svoju vinu a prijal trest 10 rokov odňatia slobody za krádež vyše 5 miliónov dolárov v kryptomenách. To sa mu podarilo odcudzením telefónnych čísel 40-tich obetí s využitím sociálneho inžinierstva u ich mobilných operátorov. Útočník tvrdil, že stratil svoju SIM kartu a požiadal o vydanie novej s pôvodným číslom. V súčasnosti existuje niekoľko podobných súdnych procesov.

Smrť riaditeľa a strata hesla k 145 miliónom dolárov

Najväčšia kanadská bitcoinová burza QuadrigaCX ohlásila stratu kryptomeny v hodnote 145 miliónov USD po tom, ako náhle zomrel jej zakladateľ, ktorý mal ako jediný prístup k offline úložiskám, kde bola kryptomena uložená. Analýza spoločnosti Crypto Medication však priniesla indície, že firma vlastnila aktíva v podstatne nižšej hodnote, ako vykazovala. Môže sa jednať o tzv. „exit scam“, teda plán úniku z trhu s peniazmi klientov.

SpeakUp – schyľuje sa k novému masívnemu kybernetickému útoku?

Bezpečnostná spoločnosť Check Point zverejnila na konferencii v Las Vegas svoje pozorovanie malvéru SpeakUp. Jedná sa o sofistikovaného trójskeho koňa, ktorý využíva komplexný balík spôsobov infekcie obete a vytvára v napadnutom systéme zadné vrátka. Napadnutých bolo vyše 70 000 linuxových serverov po celom svete, vrátane cloudových zariadení. Malvér sťahuje na napadnuté systému softvér na ťažbu kryptomeny Monero, XMRig a servery sú tak využívané na ťažbu. To sa však javí vzhľadom na veľkosť operácie ekonomicky nezaujímavé. Preto spoločnosť predpokladá, že sa jedná o testovaciu fázu pred nasadením nebezpečnejšieho malvéru.

Identifikovali útočníka stojaceho za minulomesačným únikom dát „Collection #1“

Výskumníci spoločnosti Recorded Future oznámili, že identifikovali útočníka, ktorý v januári 2019 zverejnil masívnu databázu uniknutých párov emailových adries a hesiel s názvom Collection #1. Pravdepodoben teda ide o pomerne nového člena undergroundových internetových fór s pseudonymom „C0rpz“, ktorý sa k úniku prihlásil ako prvý, ešte 7. januára. Dáta však pravdepodobne neodcudzil sám, ale iba vytvoril predmetnú kolekciu.

Únik dát reštauračnej siete Huddle House

Sieť reštaurácií s vyše 300 pobočkami Huddle House utrpela únik informácií o kreditných kartách svojich zákazníkov. Útočníci prenikli do PoS systémov, ktoré využívala a nainštalovali tam malvér zbierajúci údaje z magnetického pásika kariet. Získali tak mená, čísla kariet, expiračné dátumy, servisné kódy a bezpečnostné kódy. Incident môže zasahovať platobné karty, ktoré boli používané od augusta 2017.

Z predaja stiahli detské hodinky odhaľujúce ich geografickú polohu

Európska Komisia vydala podnet na stiahnutie detských smart-hodiniek Safe-KID-One od spoločnosti Enox z predaja kvôli závažným nedostatkom produktu, ktoré môžu dovoliť útočníkom sledovať polohu detí a vzdialene s nimi komunikovať. Hodinky majú umožňovať rodičom kontrolovať polohu svojich detí pomocou GPS zariadenia v hodinkách a mobilnej aplikácie. Komunikácia medzi aplikáciou a backend serverom však nie je šifrovaná, čo umožňuje prístup k dátam nepovolaným osobám.

Únik dát Eskom, hlavného dodávateľa elektriny v Južnej Afrike

Najväčší dodávateľ elektrickej energie v Južnej Afrike, spoločnosť Eskom, spravoval databázu svojich klientov vrátane údajov k ich platobným kartám, ktorú ponechal nezabezpečenú a dostupnú z internetu. Zároveň jeden z vysoko postavených zamestnancov mal vo svojom počítať trójskeho koňa, ktorý exfiltroval jeho citlivé údaje. Získal ho spustením falošnej inštalácie hry SIMS 4. Spoločnosť na incidenty zareagovala, až keď bezpečnostní výskumníci využili ako komunikačný kanál verejný Twitter.

Čínska skupina APT10 zodpovedná za útok na nórsku Visma

Nórska spoločnosť Visma, poskytujúca cloudové služby pre európske spoločnosti, sa stala cieľom útoku čínskej

skupiny APT10. Útočníci použili RAT malvér Trochilus a zadné dvierka Uppercut a odcudzili vnútorné údaje firmy. Údaje klientov neboli zasiahnuté, no útočníci sa pripravovali na rozšírenie prieniku do ich vnútorných sietí. Útok však bol pomerne skoro odhalený samotnou spoločnosťou.

Niektoré letecké spoločnosti nešifrujú dáta cestujúcich

Bezpečnostní výskumníci spoločnosti Wandera zistili, že osem leteckých spoločností, Southwest, Air France, KLM, Vueling, Jetstar, Thomas Cook, Transavia, a Air Europa, posiela cez svoje elekronické portály nešifrované odkazy na check-in. Odkazy presmerovávajú na rezervačnú stránku, kde sú ich adresáti už prihlásení. To môže útočníkom na tej istej sieti ako obeť umožniť prehliadať detaily o letoch a letenkách obete, a tiež v istých prípadoch tieto údaje meniť. Získať môžu aj osobné informácie vrátane mien, e-mailových kontaktov, čísiel pasov a podobne.

500% nárast v kompromitácii pracovných e-mailových účtov

Štvrťročná správa spoločnosti Proofpoint o hrozbách hovorí, že medzi štvrtými kvartálmi 2017 a 2018 narástol počet kompromitácií pracovných e-mailových účtov takmer o 500% a počet e-mailových podvodov takmer o 230%. E-maily obsahujúce škodlivé odkazy prevyšovali správy so škodlivými prílohami v pomere 3:1. Najčastejšie e-mailom šíreným malvérom boli bankové trójske kone. O 442% vzrástli aj podvody vydávajúce sa za používateľskú podporu na sociálnych médiách. Zaujímavým zistením je aj fakt, že ťažba kryptomien zneužitím služby Coinhive vzrástla 23-násobne.

Prienik do siete austrálskeho parlamentu

Austrálsky parlament informoval o nešpecifikovanom bezpečnostnom incidente, resp. prieniku do svojej siete, pričom odmietli uviesť podrobnosti. Údajne nedošlo k prístupu k citlivým dátam. Preventívne boli zmenené všetky heslá. Incident vyšetrovala agentúra Australian Signals Directorate (ASD) a jej zložka Australian Cyber Security Centre.

Chladiace systémy nemocníc a obchodov nechránené

Resource Data Management

Výskumníci spoločnosti Safety Detective sa zamerali na inteligentné chladiace systémy spoločnosti Resource Data Management. Tieto systémy sa dajú pripojiť na internet a využívajú ich potravinové reťazce, farmaceutické spoločnosti, aj poskytovatelia zdravotnej starostlivosti. Výskumníci zistili, že je možné sa do nich jednoduchým spôsobom nabúrať cez http protokol, cez porty 9000, 8080, 8100 a 80. Nakoľko po inštalácii správcovia často ponechávajú prednastavené prihlasovacie meno a heslo, je možné sa cez webový prehliadač prihlásiť do administrátorského rozhrania a meniť chladiace nastavenia.

Švajčiarsko odmeňuje za prienik do svojho online volebného systému

Švajčiarska pošta spustila program odmeňovania za nájdenie zraniteľností vo švajčiarskom volebnom systéme. Testovanie prebieha od roku 2004. Tento rok okrem akreditovanej spoločnosti, ktorá vykonáva penetračné testy, je k testovaniu prizvaná celosvetová verejnosť. Etickí hackeri, ktorí nájdu zraniteľnosti vedúce k nedetekovateľnej manipulácii volieb, si môžu zarobiť 30 000 – 50 000 USD. Detekovateľné metódy manipulácie im zarobia až do 20 000 USD, chyby na strane servera až 10 000 USD, chyby volebného systému 5000 USD a konfiguračné chyby servera 100 USD.

Únik dát používateľov webov Instagram, OkCupid a Mumsnet

Všetky tri webové služby zažili vo februári únik používateľských dát. Každá iným spôsobom. Výskumník Oliver Hough objavil voľne dostupnú databázu obsahujúcu 14,5 milióna užívateľských vstupov z Instagramu, zozbieraných z účtov používateľov v októbri 2018. Zoznamka OKCupid únik dát dementovala po tom, ako jej používatelia začali nahlasovať nabúranie svojich účtov. Útočníci v nich zmenili heslá a e-mailové kontakty, čím legitímnych používateľov vymkli. Naopak, diskusná stránka Mumsnet ohlásila únik údajov spôsobený problémovou migráciou na cloud. Užívatelia prihlásení medzi 5. a 7.2. sa mohli dostať na cudzí účet, nakoľko sa prihlasovacie údaje a účty medzi sebou pomiešali.

Útočníci kompletne vymazali dáta e-mailovej služby VFEmail aj so zálohami

E-mailová služba VFEmail.net utrpela zničujúci kybernetický útok, pri ktorom útočníci sformátovali disky na jej serveroch. Útok nebol motivovaný finančne, nakoľko útočníci nepožadovali výkupné. Spoločnosť prišla o všetky dáta svojich užívateľov. Webstránka spoločnosti bola opäť spustená, no ďalšie služby ostali nefunkčné. Americkí používatelia VFEmail pravdepodobne ostanú s prázdnymi e-mailovými schránkami.

Čínske spoločnosti čelia rovnakým bezpečnostným hrozbám, ako západné

Grady Summers na základe svojich skúseností porovnal hrozby, ktorým čelia čínske a americké spoločnosti. Konštatoval, že hrozby smerujúce na východ sú prakticky rovnaké, ako západné. Čínske spoločnosti však okrem iného majú rozsiahlejšie bezpečnostné tímy a pracujú s novšími technológiami a využívajú inovatívny prístup k riešeniu týchto hrozieb. Preto môžu byť zdrojom inšpirácie pre ďalšie štáty.

Masívna kampaň šíri malvér z Brazílie až do Európy

Výskumníci spoločnosti Cybereason Nocturnus Research zachytili novú kampaň šíriacu trójskeho koňa Astaroth z Brazílie do niektorých častí Európy. Kampaň je veľmi dobre maskovaná, nakoľko pre svoju činnosť využíva legitímne binárne súbory resp. procesy, tzv. LOLBin prístup (Living Off the Land Binaries). Jedným z nich je súbor aswrundll.exe, ktorý využíva antivírový produkt Avast. Predchádzajúce kampane sa softvéru Avast vyhýbali, no tentokrát ho útočníci využili pre šírenie malvéru. Ďalší proces, unins000.exe patriaci spoločnosti GAS Tecnologia, využíva malvér na nebadané exfiltrovanie osobných údajov. Okrem iného zaznamenáva stlačenie kláves, odpočúva systémové volania a zbiera dáta z clipboardu.

Vyše 600 + 127 + 93 miliónov účtov z desiatok stránok na predaj na Darkwebe

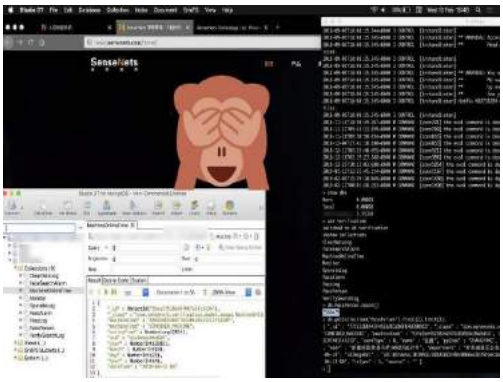
Na darkwebovom obchode Dream Market sa objavila rozsiahla databáza údajov k účtom 617 miliónov zákazníkov 16 webových stránok. Zodpovedný je za to pravdepodobne pakistanský útočník s prezývkou „gnosticplayers“. Následne ponúkol na predaj ďalších 127 miliónov účtov z 8 webstránok. Útočník tým neskončil a o niekoľko dní pridal tretiu databázu účtov obsahujúcu 93 miliónov záznamov z ďalších 8 webstránok. Vyhlásil, že celkovo chce predať vyše miliardy účtov. Jeho pohnútkami sú financie, no tiež protest proti uväzneniu „talentovaného“ člena hackerskej skupiny Apophis Squad.

Únik osobných údajov vyše 6 miliónov používateľov zoznamky Coffee Meets Bagel

Zoznamovacia služba Coffee Meets Bagel oznámila prienik do svojich systémov, ktorý znamenal únik osobných údajov vyše 6 miliónov používateľov registrovaných pred májom 2018. Unikli mená, e-mailové kontakty, vek, pohlavie a dátum registrácie používateľov. Únik je spojený s rozsiahlou databázou ponúkanou na darkwebe na predaj v prvej polovici mesiaca (viď predchádzajúci odsek).

TLP: White

Voľne prístupná čínska databáza pre sledovanie občanov



Holandský bezpečnostný výskumník Victor Gevers objavil z internetu dostupnú MongoDB databázu čínskej firmy SenseNets obsahujúcu citlivé záznamy vyše 2,5 milióna osôb. Po ohlásení spoločnosť databázu zabezpečila. Okrem iného sa v databáze nachádzali aj GPS súradnice, kde bola daná osoba spozorovaná. Tieto pravdepodobne zodpovedali verejným kamerám a vykazovali aktívnu činnosť – 6,7 miliónov súradníc zapísaných za predchádzajúcich 24 hodín. Súradnice ukazovali na miesta v provincii Xinjiang, kde sa nachádza menšina Uygurských moslimov, voči ktorým čínske autority pristupujú rozporuplným spôsobom. Databáza teda slúžila na aktívne sledovanie tohto minoritného obyvateľstva.

17 000 aplikácií pre Android permanentne sleduje svojich používateľov

Výskumníci z International Computer Science Institute vydali štúdiu, ktorá hovorí, že minimálne približne 17 000 aplikácií pre Android nedodržuje politiku súkromia Google a napriek používateľskému nastaveniu zákazu personalizácie stále zaznamenáva online aktivitu pre reklamné účely. Využívajú k tomu reklamné ID a perzistentné identifikátory užívateľského zariadenia. Spoločnosť Google sa vyjadrila, že porušovanie svojich politík berie vážne, vykonáva kontroly aplikácií a zasahuje, ak nespĺňajú dané politiky.

Exponovaná databáza záznamov medicínskych telefonických hovorov

Výskumník spoločnosti IDG, Lars Dobos, objavil z internetu voľne dostupnú databázu 2,7 miliónov záznamov telefonických hovorov na švédsku zdravotnú asistenčnú linku 1177. Spolu sa jednalo o 170 000 hodín. Server navyše obsahoval podľa vyhľadávača Shodan 23 zraniteľností objavených v rozpätí rokov 2013-2018. V záznamoch sa niekedy nachádzali čísla sociálneho poistenia, či telefónne čísla volajúcich. Správca servera po oznámení nálezu server zabezpečil.

Generátor falošného textu tvorí uveriteľné správy

Výskumníci z think-tanku Elona Muska, OpenAI, vytvorili AI nástroj, ktorý dokáže zobrať človekom napísanú vetu a dotvoriť podľa nej článok, ktorý vyzerá veľmi dôveryhodne. Pritom sa jedná o fikciu. Tvorcovia zverejnili len okliešteňú verziu, nakoľko sa obávajú, že ich produkt by bol ľahko zneužiteľný na písanie veľkého množstva dezinformačných článkov.

Únik údajov platobných kariet klientov 137 reštaurácií

NORTH COUNTRY
BUSINESS PRODUCTS
Trusted Point of Sale Solutions Provider

Ďalší prienik do PoS systémov oznámený v mesiaci február zasiahol zákazníkov 137 reštaurácií v americkom Stredozápade, ktorí platili kartou v období 3.1.-24.1.2019. Spoločnosť North Country Business Products oznámila, že vyšetrovanie koncom januára preukázalo, že útočníkom sa podarilo rozšíriť malvér skenovací kreditné karty do PoS terminálov časti ich zákazníckych prevádzok. Malvér mohol exfiltrovať kompletné údaje z kreditných a debetných kariet potrebné pre vykonanie platby. Spoločnosť poskytla zasiahnutým osobám ochranu proti podvodu a krádeži identity. Taktiež zriadila asistenčnú a informačnú telefonickú linku.

Voľne prístupná databáza pol milióna obyvateľov indického Dilí

Transerve

Bezpečnostný výskumník Bob Diachenko objavil z internetu dostupnú MongoDB databázu bez zabezpečenia heslom. Obsahovala 4,1 GB citlivých dát vyše 458 000 osôb z indického Dilí. Indície naznačujú, že sa jednalo o databázu spoločnosti Transerve Technologies, ktorá poskytuje služby v oblasti smart city a zberu dát. Jedna tabuľka databázy obsahovala registrovaných používateľov s e-mailovými kontaktmi, hashmi hesiel a používateľskými menami pre administrátorský prístup. Iné tabuľky obsahovali tiež informáciu o zdravotnom stave, vzdelaní, či geolokačnú polohu. Diachenko musel problém riešiť prostredníctvom indického CERTu, nakoľko spoločnosť na e-mailovú komunikáciu neodpovedala.

TLP: White

Databáza kreditných kariet v hodnote 3,5 milióna USD na predaj; nie jediná

Dva súbory ukradnutých platobných údajov ku kreditným kartám boli ponúknuté na predaj na portáli Joker's Stash. Jeden obsahoval platobné údaje takmer 70 000 pakistanských občanov, pričom 96% z nich pochádzalo z banky Meezan Bank. Karty boli ponúkané aj s pin kódmi a ponúkaná cena za jednu bola 50 USD, pričom štandardné ceny sa pohybujú v rozsahu 10-40 USD. Druhá várka, nazvaná „DaVinci Breach", obsahovala platobné údaje vyše 2,15 milióna zákazníkov amerických bánk.

Hlavnou obeťou útokov typu „credential stuffing" obchodníci

Akamai

Out-evolve, out-pace and out-scale
credential stuffing attackers.

Podľa správy „2019 State of the Internet" spoločnosti Akamai sa v druhej polovici roku 2018 stal komerčný sektor hlavným cieľom útokov typu „credential stuffing", teda automatizovaných pokusov napárovať uniknuté prihlasovacie údaje z jedného portálu na iné. Tieto útoky sú úspešné, ak používatelia recyklujú svoje prihlasovacie údaje. Podľa správy sa formuje trend, ktorý využíva botov na útočenie na účty e-shopov. Tieto urobia rýchle nákupy a ich operátori tovar predajú. Najčastejším cieľom útokov sú obchody s oblečením. Spoločnosť Akamai pozorovala za 8 mesiacov roku 2018 takmer 28 miliárd pokusov o zneužitie prihlasovacích údajov, pričom 10 miliárd smerovala na online obchody.

Útok MageCart na Topps.com

Topps®

Spoločnosť Topps ohlásila prienik do svojich systémov. Útočníci na webstránku spoločnosti pridali škodlivý kód, ktorý bol aktívny v období 19. november 2018 – 9. január 2019. Jednalo sa o skript typu MageCart. Potvrdil to aj výskumník spoločnosti RiskIQ Yonathan Klijnsma, ktorý spojil útok so skupinou MageCart Group 4. Útočníci sa v danom období dostali ku kontaktným údajom zákazníkov, ako aj platobným údajom.

Dow Jones Watchlist dostupný vďaka nezabezpečenej databáze

A opäť nezabezpečená databáza voľne dostupná z internetu. Tentokrát Elasticsearch databáza o veľkosti 4,4 GB obsahovala Dow Jones Watchlist, ktorý využívajú mnohé svetové spoločnosti pri uzatváraní kontraktov a vykonávaní transakcií. Databázu objavil výskumník Bob Diachenko, ktorý okamžite informoval Dow Jones. Obsahovala vyše 2,4 milióna záznamov, okrem iného identity politicky exponovaných osôb z celého sveta, vládne sankčné zoznamy, osoby spájané s vysokým zločinom.

Softvérová zraniteľnosť odhaľuje serveri útočníkov

Jednoduchá chyba v serverovom komponente pentesterského nástroja Cobalt Strike určeného na simulovanie kybernetického útoku umožnila expertom zo spoločnosti Fox-IT niekoľko rokov sledovať činnosť kyber-kriminálnych skupín. Nástroj sa totiž v priebehu času mimo penetračných testerov stal obľúbeným ako u zločineckých skupín, tak aj u štátmi podporovaných skupín. Chyba bola v januári 2019 v novej verzii nástroja opravená, no útočníci zväčša využívajú nelegálne verzie bez aktualizácií. Preto bude v najbližšej dobe možné efektívne oddeliť legitímnych a škodlivých používateľov.

Ruskej továrni na trollov sformátovali disky

Oddelenie amerického ministerstva obrany, US Cyber Command, viedla deň pred priebežnými voľbami (midterm) útok voči ruskej spoločnosti Internet Research Agency, prezývanej Ruská továreň na trollov. Spoločnosť je známa šírením dezinformácií a ovplyvňovaním pomocou falošných komentárov na rôznych fórach. Útok bol motivovaný obavami, že by spoločnosť mohla zasiahnuť do volebného procesu. Útočníkom sa podarilo zničiť interný serverový RAID kontroler a sformátovať dva zo štyroch pevných diskov k nemu pripojených. Získali tiež prístup k zálohovým

serverom spoločnosti, prenajatým v Estónsku a Švédsku, na ktorých tiež sformátovali disky.

Závažné zraniteľnosti bežných softvérových produktov

Dirty Sock - vytvorte si v Linuxe rootovský účet

Zraniteľnosť Dirty Sock postihuje distribúcie Linuxu používajúce službu snapd, najmä Ubuntu, a dovoľuje lokálne zvýšenie práv. Je tak možné vytvoriť nový účet s právami root, pričom útočník k tomu môže využiť škodlivý balíček .snap, ktorý obeť stiahne a nainštaluje.

WordPress: doplnok Simple Social Buttons dovoľuje prevziať kontrolu nad stránkou

Modul pre WordPress "Simple Social Buttons" nekontroluje dostatočne užívateľské práva a umožňuje tak meniť inštalačné nastavenia aj užívateľom s najnižšími právami. Registrovaný užívateľ môže ovládnuť administrátorský účet, alebo celú webstránku.

WordPress: vzdialené vykonávanie kódu

Šesť rokov stará kritická zraniteľnosť umožňujúca vzdialené vykonávanie kódu bola nájdená v CMS WordPress. K vykonávaniu PHP kódu môže dôjsť zneužitím možnosti traverzovania medzi priečinkami a vloženia lokálneho súboru (local file inclusion). Útočník môže prevziať kontrolu nad serverom, na ktorom webstránka beží. WordPress používa až 33% internetových stránok.

Kritická zraniteľnosť v CMS Drupal dovoľuje vzdialené vykonávanie kódu

Spoločnosť Drupal vydala aktualizácie na kritickú zraniteľnosť vo svojom CMS umožňujúcu vzdialene vykonávať PHP kód a následne prevziať kontrolu nad webstránkou. Zraniteľnosť sa nachádza vo verziách 8.x a niektorých prídavných moduloch. Krátko po vydaní opráv boli zaznamenané pokusy o jej zneužitie a implantovanie skriptov na ťažbu kryptomien do zraniteľných webstránok.

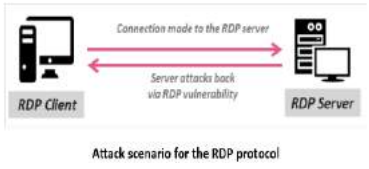
Zraniteľnosti obľúbených manažérov hesiel

Bezpečnostný tím spoločnosti Independent Security Evaluators skúmal zraniteľnosti štyroch obľúbených manažérov hesiel. Odhalil chyby pri odstraňovaní citlivých údajov z pamäte. Technikami memory scraping sa im podarilo získať hlavné heslo, aj heslá načítané do pamäte zo šifrovanej databázy. Pre zneužitie zraniteľností je však potrebný lokálny prístup k počítaču obete. Sami autori štúdie však odporúčajú naďalej používať softvér na manažment hesiel.

Vzdialené vykonávanie kódu v LibreOffice a OpenOffice

Kritická zraniteľnosť v open-source konkurencii MS Office – LibreOffice a OpenOffice umožňuje útočníkom vzdialene vykonávať kód zneužitím chyby traverzovania priečinkov. Stačí, ak obeť otvorí špeciálne upravený dokument .ODT, v ktorom je vložený neviditeľný odkaz. Prejdením kurzoru myši cez odkaz sa spustí lokálny pythonovský súbor, ktorý v konzole vykoná útočníkov škodlivý príkaz.

Kritické chyby RDP klientov umožňujú prevziať kontrolu nad zariadením



Attack scenario for the RDP protocol

V protokole pre vzdialené pripojenie RDP bolo nájdených viacero závažných zraniteľností, umožňujúcich prevzatie kontroly nad zariadením obete. Po pripojení na zariadenie útočníka môže tento vzdialene vykonávať kód, či spôsobovať poškodenie pamäte. Útočník môže traverzovať medzi priečinkami, či kompromitovať celú lokálnu sieť. Jedna zo zraniteľností napríklad umožňuje využitím funkcie „Clipboard“ preniesť súbory zo škodlivého servera do pripojeného zariadenia obete.

Ako hacknúť smartfón cez PNG obrázok

V mobilných operačných systémoch Android 7.0 až 9.0 boli nájdené zraniteľnosti, ktoré umožňujú vykonávať ľubovoľný kód jednoduchým otvorením obrázku vo formáte .PNG na zraniteľnom zariadení. Komponent zodpovedný za spracovanie PNG obrázkov obsahoval chybu spôsobujúcu pretečenie haldy. Útočníkovi tak

stačilo odoslať špeciálne upravený obrázok ukrývajúci škodlivý kód, ktorý obeť otvorila.

Kritická zraniteľnosť v runC dáva možnosť uniknúť z kontajneru a získať práva root

V utilite pre príkazový riadok, runC, bola nájdená kritická zraniteľnosť, ktorá dáva útočníkovi možnosť uniknúť z kontajneru, získať rootovský prístup k hostiteľským zariadeniam a kompromitovať ďalšie kontajnery. Zraniteľnosť zasahuje niekoľko open-source systémov pre manažovanie kontajnerov, vrátane Kubernetes, Docker, ContainerD, Podman a CRI-O. Zneužiť ju môže útočník s rootovským prístupom ku kontajneru, alebo škodlivý kontajner.

Kritické chyby v produktoch Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco Meeting Server (CVE-2019-1676): pri spracovaní volania Session Initiation Protocol nenastáva dostatočné overovanie správ, čo je možné zneužiť pri DoS útokoch.
Cisco Web Security Appliance (CVE-2019-1672): Nesprávne narábanie s SSL šifrovanou prevádzkou vedie k možnosti vzdialene obísť zabezpečenie a vykonávať neautorizovanú činnosť.
Cisco Aironet Active Sensor (CVE-2019-1675): nástroj obsahuje prednastavené heslo, ktoré ak je používané, dovoľuje útočníkom reštartovať zariadenie a spôsobiť tak DoS podmienky.
Cisco Firepower 9000 Series (CVE-2019-1700): zraniteľnosť umožňujúca vykonávať vzdialene DoS útoky zneužitím logickej chyby v komponente FPGA.
Cisco HyperFlex (CVE-2018-15380): používateľský vstup nie je vhodne ošetrený, čo umožňuje vzdialene injektovať príkazy.
Cisco HyperFlex (CVE-2019-1664): nevhodná kontrola autentifikácie umožňuje lokálne obísť prístupové práva.
Cisco Unity Connection (CVE-2019-1685): kvôli nedostatočne ošetrenému užívateľskému vstupu je možné vykonať XSS útok.
Cisco IP Phone série 7800 a 8800 (CVE-2019-1684): nevhodné overovanie LLDP paketov umožňuje vytvoriť DoS podmienky.

Mesačník zraniteľností Február 2019

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
    - Dirty Sock (Linux)
    - WordPress
    - Simple Social Buttons (doplnok pre WordPress)
    - Manažéry hesiel
    - Drupal

https://www.csirt.gov.sk/aktualne-7d7.html?id=181