ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

TLP: White

Mesačná správa CSIRT.SK

August 2018

Mesiac august sa z pohľadu útokov na slovenskú vládnu infraštruktúru niesol v znamení phishingových kampaní. Niektoré boli úspešné, iné nie. Útočníci napríklad kompromitovali e-mailovú schránku zamestnanca jedného úradu, ktorého presvedčili, aby zadal svoje prihlasovacie údaje na podvodnú stránku. Z jeho schránky ďalej šírili podvodné e-maily do siete Govnet. Z toho vyplýva, že pravidelné preškolovanie zamestnancov ohľadom phishingu nikdy nie je na škodu. CSIRT.SK na svojich webstránkach k tomu ponúka zábavnou formou koncipovaný phishingový test (https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html).

Vo svete tento mesiac vďaka výskumníkov zo spoločnosti Check Point Research vyplávala na povrch botnetovská kampaň, nazvaná „Black“. Výskumníci predpokladajú, že pozostáva minimálne z dvoch fáz, počas ktorých sa šíri malvér určený na vytvorenie podmienok pre organizovanie masívnych útokov. Doteraz bolo zaznamenaných 100 000 infikovaných zariadení, čo podľa výskumníkov predstavuje len špičku ľadovca. Situáciu je teda potrebné monitorovať, aby sme dokázali reagovať na prípadné hrozby s dostatočným predstihom.

Iný výskumník zase v spojení s kauzou obrovského úniku osobných a lekárskych údajov 2 miliónov pacientov mexickej spoločnosti Hova Health a Efimed odhalil 54 000 ďalších nezabezpečených databáz voľne prístupných z internetu. Všetkým inštitúciám spravujúcim citlivé údaje odporúčame, aby si skontrolovali svoje implementované databázové riešenia a postupy s ich narábaním, a odhalili tak prípadné bezpečnostné nedostatky ako prví.

Bohužiaľ ani zabezpečenie javiace sa ako špičkové nemusí byť vždy tak silné, ako si myslíme. Tento mesiac sa o tom presvedčila napríklad spoločnosť Reddit, ktorej zamestnancom útočník odpočúval SMS komunikáciu. Zachytil kódy posielané v rámci 2-faktorovej autentifikácie a odcudzil citlivé informácie mnohých používateľov zo serverov spoločnosti.

Nakoniec si musíme uvedomiť, že jedným z najefektívnejších opatrení, ktoré mám pomôžu zabrániť útokom a s nimi súvisiacim finančným aj reputačným škodám, je vhodne nastavená politika aktualizovania. Štatistika od spoločnosti Ponemon Institute hovorí, že 47% svetových finančných inštitúcií, ktoré utrpeli prienik do svojich systémov, nemali nainštalované aktualizácie, aj keď boli v tom čase už dostupné. Pritom až 37% inštitúcií zároveň vedelo, že sú zraniteľní. Prieskumu sa zúčastnilo 3000 odborníkov na IT bezpečnosť z celého sveta, z toho takmer 500 pôsobiacich vo finančných inštitúciách.

Riešené incidenty na Slovensku

CSIRT.SK nezaznamenal tento mesiac žiaden významný útok na infraštruktúru SR. V mesiaci august riešil prevažne phishingové kampane na svoju konštituenciu a informoval inštitúcie o napadnutí botmi. Okrem toho sa pripravoval na možný rozsiahly DDoS útok na svoju konštituenciu.

Významné útoky vo svete

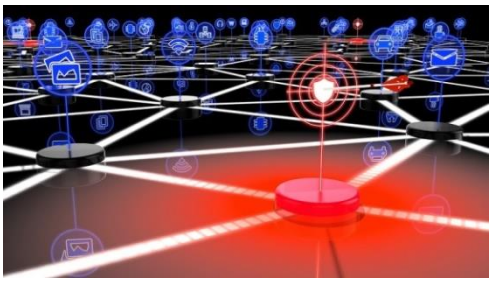
Krádež citlivých údajov servera Reddit

Spoločnosť Reddit začiatkom augusta oznámila, že v júni zaznamenala prielom do svojich systémov a únik údajov niektorých používateľov. Jedná sa o e-mailové adresy a zálohu databázy z toku 2007, v ktorej sa okrem iného nachádzali prihlasovacie údaje vrátane hašovaných a saltovaných hesiel, e-mailové adresy, používateľský obsah a súkromné správy. Útočník sa dostal do systému po kompromitácii niekoľkých zamestnaneckých účtov v systémoch poskytovateľov zdrojového kódu a cloudových služieb. Odpočúvaním SMS správ sa dostal k jednorazovým kódom dvojfaktorovej autentifikácie.

Únik zdravotných záznamov miliónov ľudí v Mexiku

Databáza od spoločnosti MongoDB s osobnými lekárskymi údajmi 2 miliónov ľudí bola voľne dostupná na internete. Výskumník Bob Diachenko ju našiel pomocou vyhľadávača Shodan, pričom zistil, že je prístupná komukoľvek z možnosťou editovať vstupy bez autentifikácie heslom. Obsahovala osobné údaje ako meno, dátum narodenia, adresa, postihnutie, a zdravotné poistenie. Databázu priradili podľa e-mailov administrátorov spoločnostiam Hova Health (Mexiko) a Efimed (nepodarilo sa identifikovať). Napriek tomu, že spoločnosť MongoDB svoj softvér zabezpečila pred piatimi rokmi, Diachenko sa vyjadril, že podľa vyhľadávača Shodan existuje na internete 54 000 takýchto nezabezpečených databáz.

Masívna kampaň Black botnet používajúca malvér Ramnit



Bola odhalená masívna botnetová kampaň s názvom Black, využívajúca malvér Ramnit. Za dva mesiace bolo infikovaných 100 000 systémov. Výskumníci predpokladajú, že sa jedná o prvú fázu kampane, kedy útočníci budujú sieť infikovaných proxy serverov, pravdepodobne prostredníctvom spamových kampaní. Takéto serveri spolu dokážu vytvoriť vysoko centralizovaný botnet. To umožňuje funkcionalita Ramnit, vkladajúca do systémov zadné dvierka. V druhej fáze môže byť do napadnutých systémov inštalovaný malvér Ngioweb, v praxi multifunkčný proxy server s dvomi vrstvami šifrovania. Takto pripravený systém umožňuje prevádzať rôznorodé masívne útoky, od DDoS, cez nepovolenú ťažbu kryptomien, šírenie ransomware, až po krádež informácií.

Štatistika: takmer u polovice kompromitovaných finančných inštitúcií bol útok úspešný vďaka zanedbaniu aktualizovania zraniteľností

Štatistický prieskum medzi 3000 profesionálmi v oblasti počítačovej bezpečnosti ukázal, že 47% obetí prieniku do systémov sa stalo obeťami, pretože neaplikovali bezpečnostné aktualizácie, ktoré v čase prieniku boli k dispozícii. Okrem toho, 37% obetí vedelo, že ich systém je zraniteľný ešte pred útokom. Vyše polovica respondentov sa vyjadrila, že časový priestor medzi vydaním aktualizácie a útokom sa skrátil za posledné dva roky o 27%. 66% sa vyjadrilo, že útočníci predbiehajú inštitúcie v oblasti technológie. Veľkému množstvu útokov sa však dá zabrániť implementovaním vhodnej aktualizačnej politiky. Ďalšie údaje a popis sú dostupné v správe z výskumu:
https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ar-ponemon-financial-report.pdf

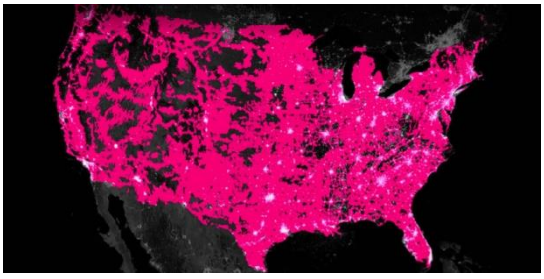
Únik informácií o konfiguračných nastaveniach veľkého množstva zariadení z GoDaddy

Spoločnosť GoDaddy zaznamenala únik informácií o konfigurácii 24 000 systémov vo svojej hostingovej infraštruktúre. Dôvodom bola konfiguračná chyba v Amazon S3 úložisku, kde boli dokumenty umiestnené. Únik okrem iného zahŕňa hostname, informácie o operačnom systéme, hardvérové parametre, pracovná náplň a oblasť Amazon Web Services. Tieto informácie môžu byť použité útočníkmi na vytipovanie vhodných cieľov.

Únik medicínskych záznamov na Augusta University Health

Spoločnosť Augusta University Health informovala tento mesiac o prieniku do svojich systémov. Prvotný útok vystopovala v roku 2017, kedy niekoľko zamestnancov poskytlo svoje prihlasovacie údaje útočníkom v rámci phishingovej kampane. Spoločnosti unikli citlivé údaje 417 000 pacientov a študentov. Okrem iných sa jednalo o mená, adresy, dátumy narodenia, výsledky laboratórnych testov, diagnózy, používané lieky, záznamy o operáciách, informácie o zdravotnom a sociálnom poistení a vodičské preukazy.

Krádež údajov 2 miliónov zákazníkov T-Mobile



T-Mobile oznámil, že 20. augusta spozoroval a zastavil prienik do svojich serverov v USA. Uniknúť mohli informácie 2 miliónov klientov (takmer 3% klientely). Jedná sa o mená, kontaktné údaje a údaje o účtoch. Čísla kreditných kariet, sociálneho poistenia, ani heslá údajne neunikli. Podľa vyjadrenia T-Mobile útočníci prenikli na servery spoločnosti cez API.

Investície do kryptomien cez Atlas Quantum ohrozené

Spoločnosť zaoberajúca sa investíciami do kryptomien Atlas Quantum ohlásila únik dát 261 000 svojich používateľov. Údaje obsahovali mená, telefónne čísla, e-mailové adresy a sumy na účtoch. K odcudzeniu aktív ani odtajneniu bezpečnostných prvkov nedošlo.

Únik informácií cez mobilnú aplikáciu leteckej spoločnosti Air Canada

Osobné údaje a údaje o pasoch 20 000 používateľov mobilnej aplikácie spoločnosti Air Canada bolo vystavených útočníkom pri prieniku do ich účtov. Spoločnosť zaznamenala nezvyklú aktivitu prihlasovania a zablokovala všetkých svojich 1,7 milióna účtov.

Predaj osobných údajov 130 miliónov zákazníkov čínskej hotelovej spoločnosti

Osobné údaje 130 miliónov klientov Huazhu Hotels Group Ltd boli na predaj na darknete za 8 BTC. Odcudzená databáza obsahovala aj kontaktné údaje, údaje o platobných kartách a identifikačných dokladoch, a tiež údaje o pobyte zákazníkov. Bezpečnostná firma Zibao vyhlásila, že chybu pravdepodobne urobili vývojári hotelovej spoločnosti, ktoré uložili kópiu predmetnej databázy na server GitHub.

Závažné zraniteľnosti bežných softvérových a hardvérových produktov

Zraniteľnosť v Microsoft Edge, ktorá vás môže pripraviť o súbory

Bol prezentovaný útok využívajúci zraniteľnosť v politike SOP v aplikáciách Microsoft Edge a Windows Mail and Calendar. Útok umožňuje ukradnúť súbory obete pomocou upraveného súboru v HTML formáte, ktorý obeť lokálne spustí v uvedených aplikáciách.

Perzistencia malvéru s pomocou Microsoft COM objektov

Útočník dokáže získať perzistenciu a neviditeľnosť pre svoj malvér zneužitím fantómových COM objektov zaznamenaných v registroch ako dôveryhodné. Tak dokáže vykonať ľubovoľný kód bez toho, aby bol detegovaný bezpečnostným softvérom.

Kritická zraniteľnosť v knižnici Symfony ovplyvňuje framework Drupal

Bola nájdená zraniteľnosť v knižnici Symfony, ktorú využíva redakčný framework Drupal.Chyba sa nachádza aj v komponentoch frameworku Zend. Táto zraniteľnosť súvisí s podporou zastaralých HTTP hlavičiek a umožňuje vzdialenému útočníkovi potenciálne obísť kontrolu prístupových práv.

Zraniteľnosť v Linuxovom jadre dovoľuje DoS útok

Zraniteľnosť v jadre systému Linux dovoľuje útočníkovi vykonať DoS útok odoslaním série vhodne upravených paketov v rámci otvorenej TCP relácie, pričom každý paket prinúti jadro vykonať sekvenciu systémovo náročných výpočtov.

Faxploit: Ako ovládnuť sieť odoslaním faxu

Odoslaním upraveného obrázku faxom na zraniteľné zariadenie dokáže útočník získať nad ním kontrolu. Ak je toto zariadenie zapojené do siete, útočník do nej môže ľahko preniknúť a kompromitovať ju. Na úspešné vykonanie útoku stačí faxové číslo a nie je potrebné internetové pripojenie.

Protokoly medicínskych zariadení dovoľujú meniť životné funkcie pacienta

Protokoly používané na prenos dát medzi medicínskymi prístrojmi nie sú dostatočne preskúmané z hľadiska bezpečnosti. Ukazuje sa však, že aspoň niektoré sú veľmi slabo chránené a ich zraniteľnosti sa dajú okrem úniku citlivých údajov jednoducho zneužiť na odosielanie falošných údajov o pacientovom stave. Monitorujúci personál tak môže byť vmanipulovaný k podniknutiu krokov priamo ohrozujúcich pacientov život, alebo k vynaloženiu výdavkov na nepotrebné vyšetrenia.

Augustový balík záplat od Microsoftu obsahuje opravy dvoch aktívne zneužívaných zero-day zraniteľností

Microsoft vydal augustový balík opráv. Obsahuje opravy 60 zraniteľností rôznych produktov od Windows a Office, cez internetové prehliadače, až po frameworky a vývojárske nástroje. 19 z nich je klasifikovaných ako kritické, 39 ako dôležité. Ostatné dve z nich sú aktívne zneužívané zraniteľnosti umožňujúce vzdialené vykonávanie kódu.

Foreshadow: nové zraniteľnosti procesorov Intel

Boli odhalené nové zraniteľnosti kategórie Spectre týkajúce sa procesorov Intel. Tieto zraniteľnosti súvisia so exekúciou, na ktorú je možné previesť útok analýzou postranného kanálu. Útočník môže získať dáta z oblastí pamäte pomocou technológie SGX, a tiež odhaliť informácie o jadre operačného systému, SMM a virtuálnych systémoch.

Zraniteľnosť v PHP otvára WordPress-ovské (a iné) webstránky útočníkom

Zraniteľnosť v jazyku PHP, spojená so serializáciou a deserializáciou dát, postihuje redakčné systémy využívajúce PHP. Jedným z nich je aj WordPress. Útočník môže zabaliť škodlivý súbor do PHAR archívu, nahrať ho na server a spustiť na ňom sériu operácií, čím získa možnosť spúšťať na cieľovom serveri ľubovoľný kód a ovládnuť ho.

Kritická zraniteľnosť frameworku Apache Struts 2 umožňuje vzdialené vykonávanie kódu

Kritická zraniteľnosť vo frameworku Apache Struts umožňuje pri určitej pomerne bežnej konfigurácii útočníkom vzdialene vykonávať kód a prevziať kontrolu nad zraniteľným webserverom. Vzhľadom na závažnosť zraniteľnosti sa odporúča okamžitá aktualizácia systémov využívajúcich Apache Struts.

Hacker informoval o zero-day zranieľnosti vo Windows 10

Užívateľ na svojom Twitterovom konte zverejnil informáciu a odkaz na kód zneužívajúci zero-day zraniteľnosť v Microsoft Windows task scheduler. Táto existuje vo Windows 10 a Windows server 2016, no nie je vylúčená ani v iných verziách operačného systému. Lokálnemu útočníkovi dovoľuje získať privilégiá systému.

Kritické zraniteľnosti Cisco

Prime Collaboration Provisioning – nedostatočné overenie požiadavky na zmenu hesla umožňuje útočníkom zmeniť administrátorské heslo a vyvolať tak podmienky DoS.
Web Security Appliance, Unified Communications Manager, TelePresence Video Communication Server Expressway a Small Business 300 Series (switche) – nevhodná sanitizácia užívateľského vstupu vo webovskom ovládacom interfejse umožňuje prevádzať XSS útoky. Útoční môže odcudziť autentifikačné súbory cookie a použiť ich pri ďalšom útoku.

Kritická zraniteľnosť Microsoft Visual Studio

Aplikácia Visual Studio nedostatočne overuje zdrojové údaje špeciálne vytvoreného projektu. To umožňuje útočníkom vzdialene vykonávať kód. Neúspešný pokus o zneužitie môže viesť k podmienkam DoS.

Kritické zraniteľnosti VMware

Horizon View Client – zraniteľnosť označená CVE-2018-6970 umožňuje čítať pamäť mimo povoleného rozsahu, čím môže dôjsť k úniku informácií. Problém sa nachádza v knižnici Message Framework.
Fusion, Workstation – zraniteľnosť CVE-2018-6973 umožňuje zápis mimo povoleného rozsahu pamäte, čo môže útočník zneužiť na lokálne vykonávanie kódu. Neúspešný pokus o zneužitie môže viesť k podmienkam DoS.

Mesačník zraniteľností August 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
6. Iné tohtomesačné závažné zraniteľnosti
    - Foreshadow, PHP, Apache Struts 2

TLP: White