MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Október 2021

Vypracoval: CSIRT.SK

TLP: White

Október si už od nepamäti spájame s kybernetickou bezpečnosťou. Je to mesiac, kedy sa vo veľkej miere rôzne inštitúcie snažia zvyšovať bezpečnostné povedomie za účelom zvýšenia bezpečnosti na internete. V USA a v Európe sa v tomto mesiaci spúšťajú kampane, vďaka ktorým sa obyvateľstvo môže dozvedieť v krátkom časovom okamihu množstvo zaujímavých informácií z tejto oblasti.

Od roku 2003 je október „mesiacom povedomia o kybernetickej bezpečnosti“ v USA. Cybersecurity and Infrastructure Security Agency (CISA) a National Cyber Security Alliance (NCSA) tento rok zvolili motto „Do Your Part. #BeCyberSmart.“, ktorého cieľom je povzbudiť jednotlivcov a organizácie, aby chránili online priestor, v ktorom sa pohybujú. Zdôrazňujú, že dôležitá je osobná zodpovednosť a prijímanie proaktívnych opatrení za účelom zvyšovania kybernetickej bezpečnosti.

CISA taktiež ponúka rôzne zdroje na použitie v komunitách na podporu silnej celoštátnej kybernetickej bezpečnosti. Materiály sú bezplatné a je možné si ich prispôsobiť. Na vytvorenie efektívnej kampane CISA a NCSA vytvorili 4 témy, na ktoré sa počas mesiaca október zameriavali:

1. Be Cyber Smart – Zaoberanie sa základmi kybernetickej bezpečnosti; ako zlepšiť bezpečnosť smart zariadení a zariadení pripojených k internetu a podobne.
2. Fight The Phish! – Zameranie sa na rozpoznávanie phishingových pokusov, ktoré môžu viesť k odhaleniu a následne zneužitiu zraniteľností – napríklad k nasadeniu ransomvéru alebo iného malvéru.
3. Explore. Experience. Share. – V 3. týždni je vhodné poukázať na to, akí dôležití sú bezpečnostní profesionáli v online svete.
4. Cybersecurity First – Je nutné zdôrazniť, že kybernetická bezpečnosť by mala byť prioritou a nie len akýmsi dodatkom.

V roku 2012 bol október taktiež vyhlásený za „Európsky mesiac kybernetickej bezpečnosti“ (ECSM). Jedná sa o každoročnú kampaň Európskej Únie, ktorá je venovaná poskytovaniu aktuálnych informácií o bezpečnosti. Počas celého mesiaca sa v celej Európe koná množstvo aktivít práve na zvyšovanie bezpečnostného povedomia v online priestore. Kampaň je koordinovaná agentúrou ENISA a Európskou Komisiou.

Hlavným sloganom tejto kampane je „‘Think Before U Click’ #ThinkB4UClick“. Dve hlavné témy kampane ECSM2021 sú:

1. Prvá pomoc, pokyny, čo robiť, ak sa niekto stane obeťou kybernetického útoku a
2. byť v kyber-bezpečí doma.

Vzhľadom k tomu, že kvôli pandémii koronavírusu sme nútení pracovať formou „homeoffice“, je tento rok viac než nutné, aby občania boli vzdelávaní v oblasti kybernetickej bezpečnosti. Hlavnými cieľmi je zabezpečiť, aby používatelia a organizácie boli informovaní o potenciálnych rizikách, a aby v online svete ostali v bezpečí.

TLP: White

Je dôležité, aby sa každý z nás v tejto oblasti vzdelával nie len počas októbra, ale v priebehu celého roka.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci október riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Jednotka riešila tiež prípad kompromitovanej schránky zamestnanca inštitúcie vo svojej konštituencii, ktorú útočníci zneužili na rozposielanie phishingových e-mailov. Po zablokovaní konta a zmene hesla sa incident neopakoval.

Dva najvážnejšie októbrové incidenty, ktoré jednotka riešila, boli spojené s ransomvérom. Zasiahnuté boli dve inštitúcie verejnej správy. V oboch prípadoch bol rozsah ransomvérového útoku devastačný, vzhľadom na nedostatočnú implementáciu princípov najlepšej praxe kybernetickej bezpečnosti a na chýbajúce offline zálohy. Šťastie v nešťastí mala jedna z dvojice inštitúcií, keď sa rozhodla komunikovať s páchateľmi. Títo sa vyjadrili, že nemali v úmysle útočiť na organizácie verejnej správy, a tak poskytli dešifrovacie kľúče zdarma. Inštitúcia tak získala naspäť svoje dáta. Obe organizácie sa však nevyhli kompletnej prestavbe svojej IT infraštruktúry. CSIRT.SK poskytol odporúčania pre dosiahnutie kvalitnejšieho zabezpečenia.

Jednotka ďalej riešila prípad zraniteľného webového formulára v správe organizácie v jej konštituencii. Dohliadala tiež na preverenie hlásenia od NBÚ, ktoré sa týkalo informácie z aukcií na útočníckych webových fórach. V ponuke bol prístup ku kompromitovanému zariadeniu v majetku organizácie v konštituencii CSIRT.SK. Výsledky vyšetrovania naznačili, že ponuka bola pravdepodobne falošná.

CSIRT.SK informoval niekoľko organizácií svojej konštituencie o zraniteľnostiach ich mailserverov. Primárnym cieľom kampane bolo odhaliť a dohliadnuť na odstránenie neošetrených zraniteľností serverov Microsoft Exchange.

V rámci svojej proaktívnej činnosti jednotka pokračovala v kampani na platforme Achilles, zameranej na odhaľovanie a odstraňovanie zraniteľností verejne dostupných systémov organizácií jej konštituencie. Taktiež školila zamestnancov týchto organizácií. Témou boli základy informačnej bezpečnosti a bežné hrozby, s ktorými sa účastníci môžu stretnúť v pracovnom aj súkromnom živote. Účastníci získali informácie, ako tieto hrozby rozpoznávať a ako sa pred nimi brániť. Prezentácia ku školeniu je dostupná na našej webstránke.

Významné útoky vo svete

Spoločnosti Neiman Marcus uniklo približne 4,3 milióna údajov o zákazníkoch

Spoločnosť Neiman Marcus sa stala obeťou úniku údajov, ktorý zasiahol približne 4,3 milióna zákazníkov. K úniku došlo v máji roku 2020, kedy útočník získal prístup k veľkému počtu prihlasovacích údajov, a získal tak prístup k citlivým údajom o zákazníkoch. Uniknuté údaje zahŕňajú používateľské mená, heslá, čísla kreditných kariet, bezpečnostné otázky a odpovede na ne, kontaktné informácie a ďalšie. V systémoch neboli uložené CVV čísla, čo sťažuje útočníkom použitie ukradnutých údajov o platobných kartách. Spoločnosť vynútila resetovanie hesiel k účtom dotknutých zákazníkov.

Servery Confluence sú pod paľbou útokov ransomvéru Atom Silo

Ransomvér Atom Silo sa zameriava na zraniteľnosť v serveroch Confluence. Úspešným zneužitím dochádza k vzdialenému vykonávaniu príkazov na predmetných serveroch. Skupina stojaca za týmito útokmi používa takmer identický ransomvér ako je LockFile, ktorý sa podobá tomu, ktorý využíva skupina LockBit. Po kompromitácii zraniteľných serverov a inštalácii zadných vrátok útočníci inštalujú ďalšie zadné vrátka pomocou bočného načítania DLL knižníc. Atom Silo sa úspešne vyhýba detekcii pred spustením samotného ransomvéru, ktorý zahŕňa známe techniky, avšak používané novými spôsobmi. Útočníci na zraniteľných serveroch taktiež ťažili pomocou XMRig kryptomenu Monero.

Útočníci šifrujú virtuálne stroje na serveroch VMware ESXi

Útočníci využívajú skript napísaný v programovacom jazyku Python na šifrovanie virtuálnych strojov hostených na serveroch VMware ESXi. Bezpečnostní výskumníci zo spoločnosti Sophos objasnili, že celý proces šifrovania sa začína približne tri hodiny po

počiatočnej kompromitácii. Pre prvotný prístup útočníci kompromitovali účet TeamViewer, ktorý nemal nastavenú viacfaktorovú autentifikáciu, a bežal na pozadí na počítači patriacom používateľovi s povereniami správcu domény. Podľa výskumníkov spoločnosti Sophos skript obsahuje viacero pevne zakódovaných šifrovacích kľúčov a nástroj na generovanie ešte väčšieho počtu kľúčov, čo ich viedlo k záveru, že ran somvér vytvára jedinečný kľúč pri každom spustení.

Údajne unikol zdrojový kód služby Twitch a údaje o používateľoch

Zdrojový kód služby Twitch a citlivé údaje používateľov údajne unikli online. Útočník zdieľal torrentový odkaz vedúci k archívu o veľkosti 125GB, ktorý údajne obsahoval údaje ukradnuté z približne 6-tisíc interných Git repozitárov predmetnej služby. Útočník uviedol, že uniknuté údaje zahŕňajú celú stránku twitch.tv, klientov pre mobily, stolné počítače a videoherné konzoly, súpravy SDK a interné služby AWS a ďalšie. Twitch potvrdil, že k úniku naozaj došlo, a že pracujú na jeho vyriešení.

Útočníci využívajú trójskeho koňa ShellClient v rámci útokov na letecké a telekomunikačné spoločnosti

Útočníci využívajú tichý malvér ShellClient proti leteckým a telekomunikačným spoločnostiam. Bezpečnostní výskumníci odhalili, že títo útočníci vedú špionážne kampane minimálne od roku 2018. ShellClient je trójsky kôň so vzdialeným prístupom (RAT). Malvér sa na infikovaných počítačoch maskuje ako „RuntimeBroker.exe“, čo je legitímny proces, ktorý pomáha so správou povolení pre aplikácie z obchodu Microsoft Store. Malvér je pripisovaný skupine MalKamak, novej iránskej útočníckej skupine s jedinečnými vlastnosťami, ktoré ju odlišujú od ostatných známych iránskych útočníkov.

Malvér FontOnLake sa zameriava na linuxové systémy

Malvér FontOnLake infikuje linuxové systémy prostredníctvom nástrojov s trójskym koňom. FontOnLake má viacero modulov, ktoré sa navzájom ovplyvňujú a umožňujú komunikáciu s operátormi škodlivého softvéru, kradnú citlivé údaje a zostávajú skryté v systéme. Výskumníci zo spoločnosti ESET našli viacero vzoriek malvéru nahraného do skenovacej služby VirusTotal počas minulého roka, pričom prvá sa objavila v máji 2020. Medzi nástroje, ktoré útočník pozmenil na účel distribúcie malvéru FontOnLake patria cat, kill, sftp a sshd.

Útočník tvrdí, že ukradol viac ako 60GB súborov a databáz spoločnosti Acer

Spoločnosť Acer potvrdila, že sa stala obeťou útoku, ktorý nazvala izolovaným. Napadnuté boli systémy popredajných služieb v Indii. Incident nemal žiaden podstatný vplyv na operácie spoločnosti a kontinuitu podnikania. Útočník na populárnom hackerskom fóre potvrdil, že ukradol viac ako 60GB súborov a databáz zo serverov spoločnosti Acer. Ukradnuté údaje zahŕňajú klientske, firemné, finančné a prihlasovacie údaje patriace maloobchodníkom a distribútorom spoločnosti Acer z Indie. Tento rok ide už o druhý prípad, kedy boli narušené počítačové systémy tejto spoločnosti.

Ransomvér zasiahol spoločnosť Sinclair Broadcast Group

Spoločnosť Sinclair Broadcast Group, ktorá vlastní stovky miestnych televíznych staníc v USA potvrdila, že sa stala obeťou ransomvéru. Incident spôsobil narušenie reklamných operácií a vyradenie miestneho vysielania. Útok viedol k úniku údajov, avšak zatiaľ nie je známe, konkrétne ktorých údajov sa únik dotýka. Spoločnosť nezverejnila detaily o útoku, ale potvrdila, že prehodnocuje nastavenie bezpečnostných politík.

Iránske čerpacie stanice sa stali obeťou kybernetického útoku

Iránske čerpacie stanice (National Iranian Oil Products Distribution Company) prestali fungovať pre kybernetický útok, ktorý zasiahol celú distribučnú sieť. Zákazníkom sa zobrazovala správa „cyberattack 64411“, čo je zjavne odkazom na kybernetický útok, ktorý sa udial v júli a narušil iránsku vlakovú dopravu. Na digitálnych billboardoch sa zobrazovala správa „Khamenei! Where's our fuel?“ a „Free fuel in Jamaran station“. Iránska Najvyššia rada pre kyberpriestor sa domnieva, že incident by mohol byť sponzorovaný štátom, avšak nevedno ktorým.

Skupina FIN7 sa snaží nalákať legitímnych IT špecialistov na pozíciu „penetračných testerov“

Útočníci zo skupiny FIN7 vytvárajú falošné spoločnosti zaoberajúce sa kybernetickou bezpečnosťou, pričom vykonávajú sieťové útoky pod zámienkou penetračného testovania. Skupina chcela prilákať legitímnych IT špecialistov, ktorí by nevedomky vykonávali falošné „penetračné testovanie“. Výskumíci z Gemini Advisory zistili, že webová stránka pre falošnú spoločnosť Bastion Security pozostávala z ukradnutého a znovu skompilovaného obsahu z iných webových stránok. Zdá sa, že cieľom skupiny bolo preskúmanie siete a následné nasadenie ransomvéru. Medzi nástroje, ktoré útočníci využívali patria napríklad Carbanak alebo Lizar/Tirion.

Spoločnosť BrewDog vystavila údaje o svojich zákazníkoch na dobu dlhšiu ako rok a pol

BrewDog, škótsky reťazec pivovarov a krčiem vystavil do internetu údaje o 200-tisíc svojich zákazníkoch a akcionároch. Vystavenie trvalo dlhšie ako rok a pol, pričom údaje unikli z mobilnej aplikácie firmy, ktorá poskytuje prístup k informáciám, zľavám v baroch a podobne. Problém spočíva v API aplikácie, konkrétne v jej autentifikačnom systéme založenom na tokenoch. Tokeny boli napevno zakódované do mobilnej aplikácie namiesto toho, aby sa do nej preniesli po úspešnej

autentifikácii používateľa. Údaje, ktoré boli voľne dostupné sú meno, dátum narodenia, emailová adresa, pohlavie a ďalšie. Potenciálny útočník by dokonca mohol získať nekonečné bezplatné pivo a zľavy generovaním QR kódov z účtov.

- **Austrálsky minister vnútra predstavil „Akčný plán austrálskej vlády pre ransomvér“.**
- **Botnet MyKings sa stále aktívne šíri a zarába veľké množstvo financií.**
- **Nový ransomvér Yanluowang sa využíva v útokoch proti podnikovým subjektom.**
- **Nová APT skupina ChamelGang sa zameriava na palivový, energetický a letecký priemysel.**
- **Platforma Coinbase informovala tisícky svojich používateľov o ukradnutí finančných prostriedkov z ich účtov.**
- **Útočníkov, ktorí napadli ransomvérom viac ako 100 spoločností, zatkli na Ukrajine.**
- **Útočníci používajú novoobjavený UEFI bootkit na nasadenie zadných vrátok do systémov Windows od roku 2012.**
- **Spoločnosť Syniverse potvrdila roky trvajúci únik údajov.**
- **Noviny a online médiá v Spojenom kráľovstve s názvom „The Telegraph“ nezabezpečili jednu zo svojich databáz, čo spôsobilo únik údajov o veľkosti 10TB.**
- **APT skupina FIN12 útočí na zdravotníctvo pomocou ransomvéru.**
- **Facebooková stránka Navy Warship bola napadnutá útočníkmi, aby mohla streamovať hru Age of Empires.**
- **Spoločnosť Google varuje 14-tisíc používateľov emailovej služby Gmail pred ruskými útočníkmi.**
- **Trójsky kôň Hydra sa zameriava na nemeckú banku Commerzbank.**

- **Malvér Flubot pre Android sa šíri prostredníctvom falošných bezpečnostných aktualizácií.**
- **Ekvádorská banka Banco Pichincha sa stala obeťou kybernetického útoku.**
- **Botnet FreakOut sa po novej aktualizácii zameriava na zraniteľné video DVR zariadenia.**
- **Phishingová kampaň využíva matematické symboly v logách spoločností, aby sa vyhla odhaleniu.**
- **Chyby v platforme OpenSea NFT umožňujú útočníkom kradnúť kryptomeny z peňaženiek.**
- **Izraelská nemocnica sa stala obeťou útoku ransomvéru.**
- **Ransomvér zasiahol SCADA systémy v 3 vodných zariadeniach v USA.**
- **Phishingová kampaň MirrorBlast zneužíva dokumenty Excel na kompromitáciu organizácií poskytujúcich finančné služby.**
- **FBI varuje pred falošnými vládnymi stránkami slúžiacimi na krádež finančných a osobných údajov.**
- **APT skupina Lyceum sa zameriava na tuniské firmy.**
- **Nová varianta botnetu PurpleFox používa WebSockets na komunikáciu s riadiacim serverom.**
- **Bezplatná VPN služba Quickfox vystavila údaje o viac ako 1 milióne používateľov.**

Závažné zraniteľnosti bežných softvérových produktov

Kritická zraniteľnosť produktu VMware VCenter

Spoločnosť WMware varuje pred kritickou zraniteľnosťou svojho produktu VMware vCenter. Chyba sa nachádza v nástroji VMware Analytics, ktorý dokáže prijať škodlivý súbor bez akejkoľvek autentifikácie, zapísať ho kdekoľvek na disk a následne spustiť s oprávneniami správcu. Zraniteľnosť je triviálne zneužiteľná a preto VMware apeluje na administrátorov systémov VMware, aby bezodkladne vykonali kroky k zabezpečeniu svojej infraštruktúry. Aktuálne je postup zneužitia zraniteľnosti už voľne dostupný na internete.

Kritická zraniteľnosť Apache HTTP server

Apache Software Foundation vydala dôležité opravy kritickej zraniteľnosti, ktorá umožňuje potenciálnemu útočníkovi odosielať požiadavky a získať prístup k súborom na backende webového servera. Zraniteľnosť sa nachádza len vo verzii Apache 2.4.49. Úspešným zneužitím zraniteľnosti môže prísť k úniku binárnych súborov ako sú napríklad CGI skripty, či zmapovaniu súborov mimo publikovaných web root súborov. Zraniteľnosť je aktívne zneužívaná útočníkmi. CSIRT.SK odporúča bezodkladnú aktualizáciu zraniteľných systémov.

Spoločnosť Apple vydala záplatu pre kritickú zero-day zraniteľnosť

Spoločnosť Apple opravuje kritickú zraniteľnosť vyskytujúcu sa v iOS a iPadOS, ktorá je aktívne zneužívaná. Chyba súvisí s poškodením pamäte v komponente IOMobileFrameBuffer. Zneužitím môže dôjsť k vykonávaniu ľubovoľného kódu s oprávneniami jadra.

Závažné zraniteľnosti Cisco

V produktoch Cisco bolo opravených viacero závažných zraniteľností. Zraniteľnosti ovplyvňujú Cisco AnyConnect Secure Mobility Client pre Linux a Mac OS, Cisco Small Business 220 Series Smart Switches, Cisco Intersight Virtual Appliance, softvér Cisco IOS XR pre smerovače série ASR 9000, softvér Cisco Adaptive Security Appliance (ASA), softvér Firepower Threat Defense (FTD), softvér Firepower Management Center (FMC) a ďalšie. Úspešným zneužitím týchto zraniteľností môže dôjsť napríklad k vzdialenému prechádzaniu adresárov, narušeniu dostupnosti služby, vzdialenému vykonaniu kódu alebo injektovaniu príkazov.

Závažná zraniteľnosť Intel

Závažná zraniteľnosť CVE-2021-0186 v SDK aplikáciách Software Guard Extensions (SGX) môže umožniť eskaláciu privilégií prostredníctvom lokálneho prístupu. Súvisí s nesprávnym overením vstupu v SDK aplikáciách SGX skompilovaných pre procesory s podporou SGX2. Spoločnosť Intel vydala bezpečnostné záplaty na zmiernenie tejto potenciálnej zraniteľnosti.

Mesačník zraniteľností Október 2021

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné závažné zraniteľnosti
    - Kritická zraniteľnosť produktu VMware VCenter
    - Kritická zraniteľnosť Apache HTTP server

https://www.csirt.gov.sk/posts/2611.html?csrt=6658460021841249842