MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

September 2020

Vypracoval: CSIRT.SK

TLP: White

September. Vo väčšine krajín sveta sa začína či už školský, alebo akademický rok. Kvôli aktuálnej pandémii vo svete sú veľmi lukratívnym cieľom práve školy, prípadne videokonferenčné softvéry, ktoré používajú pri online výučbe. Vo svete došlo počas tohto mesiaca hneď k niekoľkým útokom na školy.

NCSC (Britské národné stredisko pre kybernetickú bezpečnosť) vydalo správu o náraste ransomvérových útokov voči vzdelávacím inštitúciám. Štúdia potvrdila, že tretina všetkých univerzít v Británii utrpela útok ransomvérom. NCSC odporúča mať vypracovaný plán reakcie na incidenty a mať pripravené mechanizmy, ktoré sú schopné obnoviť údaje z offline záloh.

Údaje od spoločnosti Check Point z oblasti kybernetickej bezpečnosti ukazujú, že útočníci používajú rôzne metódy a taktiky pri útokoch na sektor vzdelávania a výskumu v USA, Európe a Ázii. Inštitúcie sa najčastejšie stávajú obeťou DDoS, útokov cieliacich na získavanie citlivých informácií a možnosti vykonávať kód, pričom väčšina útokov sa zameriavala na inštitúcie v USA.

Školy v Severnej Karolíne utrpeli prienik so svojich systémov a únik osobných údajov po krádeži nezašifrovaných súborov počas útoku ransomvérom SunCrypt. Útočníci žiadali výkupné, ktoré im nebolo zaplatené, a tak zverejnili 5GB dát. Unikli osobné údaje učiteľov a študentov, a tiež citlivé dokumenty školského obvodu.

Práve tento ransomvér spôsobil škodu aj v Univerzitnej nemocnici New Jersey, pričom bolo zverejnených 1,7GB dát a celkovo 48 000 záznamov. Tieto dáta zahŕňajú autorizačné formuláre, kópie vodičských oprávnení, čísla sociálneho zabezpečenia (SSN), dátumy narodenia a podobne. Útok začal infekciou počítača zamestnanca nemocnice. Trójsky kôň TrickBot umožnil ransomvéru SunCrypt prístup do IT systémov nemocnice.

SunCrypt je ransomvér, ktorý sa inštaluje pomocou Powershell skriptu, podobného malvéru Netwalker. Nosičmi SunCryptu sú infikované emailové prílohy, torrentové webové stránky a škodlivé reklamy. Na šifrovanie súborov využíva algoritmus ChaCha20. Akonáhle je tento ransomvér nainštalovaný, pripája sa na riadiaci server a sprostredkúva informácie útočníkovi o priebehu útoku a obeti. Tvorcovia SunCryptu sa vyjadrili, že po útoku na Univerzitnú nemocnicu v New Jersey neplánujú viesť ďalšie útoky voči lekárskym subjektom.

Ďalším z útokov smerovaným na sektor vzdelávania bol útok na školský obvod v meste Hartford. Zasiahol IT systémy škôl a spôsobil ich výpadok. Technická podpora pracovala na obnove služieb, avšak nepodarilo sa im sprevádzkovať všetky systémy načas. Prvý deň nového školského roka musel byť odložený. Systém na komunikáciu s autobusovou spoločnosťou bol po útoku stále nefunkčný. Vzhľadom k útoku na viacero systémov bolo tiež nutné prerušiť online výučbu.

Zasiahnutá bola aj oblasť verejných škôl v okrese Fairfax. Útočníci zverejnili údaje o veľkosti 100MB, čo predstavuje 2% ukradnutých dát. Dáta získané pomocou ransomvéru Maze zahŕňali známky študentov, ako aj administratívne dokumenty. Je známe, že Maze stojí za významnými útokmi voči spoločnostiam Canon, LG Electronics a podobne.

Na sieti sa tiež našli dáta o študentoch zo školského obvodu v okrese Clark po tom, čo jeho správa odmietla zaplatiť výkupné. Tieto dáta sa na čiernom trhu objavili takisto po útoku ransomvérom Maze.

Ransomvér Maze sa spočiatku distribuoval pomocou exploitových súprav (Fallout EK a Spelevo EK) a spamu so škodlivými prílohami. Tento ransomvér je jeden z prvých, ktorý hrozil únikom údajov obetí v prípade, že zasiahnuté spoločnosti odmietli spolupracovať. Maze je 32-bitový binárny súbor zvyčajne zabalený ako „exe“ alebo „dll“. Malvér využíva aj triky na zmarenie statickej alebo dynamickej analýzy.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci september riešil štandardne najmä phishingové kampane na svoju konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov.

Vládna jednotka riešila aj medializovaný prípad úniku osobných dát občanov testovaných na ochorenie COVID-19. Títo sa na testovanie registrovali cez aplikáciu Moje eZdravie, ktorá patrila Národnému centru zdravotníckych informácií (NCZI). Etickí hackeri spoločnosti Nethemba, ktorí zraniteľnosť objavili, stiahli 130 000 záznamov obsahujúcich osobné údaje desiatok tisíc občanov. Analýza logov, ktorú sme vykonali za celé dostupné časové obdobie nepotvrdila, že by došlo k úniku údajov tretím stranám. Zraniteľnosť bola zároveň v krátkom čase NCZI odstránená.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK kontaktovala organizácie vo svojej konštituencii, u ktorých zistila, že nepoužívajú na svojich weboch protokol TLS (HTTPS), alebo nemali vynútené presmerovanie z HTTP na tento zabezpečený protokol, či platný certifikát. Varovala pred špionážnou kampaňou skupiny Fancy Bear, zameranou na krádež údajov vládnych inštitúcií. Kampaň šírila malvér predstierajúc školiace materiály NATO a bola pozorovaná v Azerbajdžane. Jednotka varovala aj pred podvodnou kampaňou, v ktorej sa útočníci vydávali za rôzne zvučné APT skupiny. Svojim obetiam sa vyhrážali útokom DDoS a krádežou údajov, pokiaľ nezaplatia výkupné vo forme Bitcoinov. Textácia šírených správ sa nápadne podobala dlhotrvajúcej kampani zvanej Sextortion.

Na svojich webstránkach publikovala jednotka svoju analýzu 13-tich open-source aj proprietárnych telekonferenčných produktov pre prácu na diaľku. V štúdii zohľadnila širokú škálu kritérií, pričom svoje odporúčania sústredila okolo dvoch modelových situácií. Prvá zohľadňovala prácu zamestnancov formou home office s obmedzeným prístupom k zamestnávateľom poskytnutej výpočtovej technike, druhá zas výučbu na diaľku.

Významné útoky vo svete

Iránski útočníci predávajú prístup ku kompromitovaným spoločnostiam

Bola spozorovaná iránska skupina hackerov, ktorá sa snažila predávať prístup k napadnutým sieťam spoločností. Skupina útočníkov bola identifikovaná ako Pioneer Kitten (Fox Kitten, Parisite). Na získanie prístupu do firemných sietí využívala zraniteľnosti vo VPN sieťach a rôznych ďalších sieťových prvkov. Po získaní prístupu do siete Pioneer Kitten sprostredkovali prístup ďalším skupinám ako APT33, APT34, Chafer a podobne. O nejaký čas neskôr bola táto skupina spozorovaná pri predaji daných údajov na čiernom trhu.

Ransomvér Maze šifruje súbory cez virtuálne systémy, aby zabránil jeho detekcii

Prevádzkovatelia ransomvéru Maze si osvojili techniku, ktorá umožňuje šifrovanie súborov zariadenia z virtuálneho stroja. Predchodcom tohto ransomvéru je Ragnar Locker, ktorý využíval na šifrovanie virtuálne systémy s operačným systémom Windows XP. V spoločnosti Sophos bol detegovaný útok ransomvérom Maze trikrát, pričom dvakrát bol blokovaný funkciou Sophos Intercept X. Na tretíkrát Maze nasadil na zariadenie MSI súbor, ktorý nainštaloval softvér VirtualBox VM a následne aj virtuálny systém s prispôsobeným operačným systémom Windows 7.

Zdrojový kód pre Windows XP SP1 a ďalšie verzie operačného systému údajne unikli online

Zbierka zdrojového kódu o veľkosti 43GB bola zverejnená na fóre 4chan. Údajne je v tomto torrente zahrnutý zdrojový kód pre Windows XP, Windows Server 2003 a iné ďalšie staršie verzie operačného systému. Obsah zahŕňa tiež zbierku videí týkajúcich sa konšpiračných teórií o Billovi Gatesovi. Po sieti koluje tiež súbor vo formáte 7zip o veľkosti 2,9GB, ktorý obsahuje zdrojový kód len pre systémy Windows XP a Windows Server 2003.

Útočníci aktívne zneužívajú kritickú chybu na viac ako 300 tisíc weboch WordPress

Útočníci zneužívajú kritickú chybu zabezpečenia pri vzdialenom vykonávaní kódu. Chyba umožňuje útočníkom nahrávať skripty a vykonávať ľubovoľný kód na weboch WordPress, ktoré používajú zraniteľné verzie doplnkov File Manager. Tento doplnok je momentálne nainštalovaný na viac ako 700 000 weboch WordPress a chyba zabezpečenia ovplyvňuje všetky verzie medzi 6.0 a 6.8. Wordfence Web Application Firewall zablokoval cez 450 tisíc pokusov o zneužitie. Útočníci sa pokúšali nahrať PHP súbory do priečinku wp-content/plugins/wp-file-manager/lib/files/.

Malvér MrbMiner infikoval tisícky MSSQL databáz

Botnet s názvom MrbMiner sa šíril skenovaním internetu na MSSQL servery. Následne sa pokúšal opakovaným skúšaním účtu správcu s rôznymi heslami dostať do systému. Po prekonaní hesla bol stiahnutý súbor „assm.exe“, ktorý bol použitý na zavedenie mechanizmu perzistencie a na pridanie účtu za účelom vytvorenia zadných vrátok. Posledným krokom procesu infikovania bolo pripojenie sa k riadiacemu serveru a stiahnutie aplikácie, ktorá ťaží kryptomenu Monero (XMR) zneužívaním zdrojov miestneho servera a generovaním mincí XMR na účty kontrolované útočníkmi.

Šifrovaná e-mailová služba Tutanota trpí útokmi DDoS

Služba Tutanota zaznamenala sériu útokov DDoS zameraných na webovú stránku a ďalších jej poskytovateľov DNS. To spôsobilo výpadky na niekoľko hodín mnohým používateľom Tutanoty. Výpadok ešte prehĺbila skutočnosť, že rôzne servery DNS pokračovali v ukladaní nesprávnych položiek pre doménu do medzipamäte. Tento incident spôsobil problémy niekoľkým stovkám používateľov, ale v krátkom čase bol odstránený obmedzením „nadmerne reagujúceho bloku IP“ zodpovedného za útok.

Nový malvér „Alien“ môže ukradnúť heslá z 226 aplikácií na Androide

Výskumníci v oblasti kybernetickej bezpečnosti objavili a analyzovali nový malvér s názvom Alien pre Android. Má širokú škálu funkcií, ktoré mu umožňujú ukradnúť údaje z 226 aplikácií. Tento nový trójsky kôň je založený na zdrojovom kóde malvéru Cerberus. Je aktívny od začiatku roka 2020 a na čiernom trhu je ponúkaný ako malvér ako služba (MaaS). Je schopný zobrazovať falošné prihlasovacie obrazovky, zbierať heslá, tiež poskytovať prístup k zariadeniu a mnoho ďalších funkcií.

150 miliónov dolárov ukradnutých zo singapurskej burzy kryptomien KuCoin

Burza kryptomien KuCoin oznámila, že identifikovala množstvo veľkých výberov v Bitcoinoch, ERC-20 a iných kryptomien zo svojich peňaženiek. V tejto veci začala vyšetrovanie, pričom pozastavila službu vkladov a výberov. Deň na to v aktualizácii jej majitelia oznámili, že lokalizovali niektoré peňaženky, do ktorých boli finančné prostriedky prevedené a pracujú na ich zablokovaní. Veľké množstvo odcudzených kryptomien a tokenov bolo zmrazených, avšak suma väčšia ako 150 miliónov dolárov bola prevedená mimo KuCoin Ethereum peňaženky.

Skupina útočníkov OldGremlin útočí na rôzne odvetvia podnikových sietí v Rusku

Skupina OldGremlin podnikala viacstupňové útoky na veľké podnikové siete bánk, výrobcov a vývojárov softvéru a lekárskych laboratórií v Rusku. Táto skupina sa neskôr zamerala aj na iné geografické oblasti z dôvodu, aby sa znížili šance na ich zatknutie. Aktéri týchto útokov využívali vo svoj prospech svetové udalosti ako krízu COVID, alebo prebiehajúce protesty v Bielorusku. Skupina začala útoky v marci tohto roka a pokračuje v nich dodnes. Vo svojich útokoch využíva škodlivý kód na tvorbu zadných vrátok TinyNode a TinyPosh, pričom cieľom je šifrovať súbory pomocou ransomvéru TinyCryptor.

Majiteľ spoločnosti Luxottica potvrdil útok ransomvéru

Spoločnosť Luxottica údajne utrpela kybernetický útok, ktorý viedol k prerušeniu jej činnosti v Taliansku a Číne. Stránky značiek Ray-Ban, Sunglass Hat, LensCrafters, EyeMed a Pearle Vision prestali fungovať. Spoločnosť Luxottica mala radič Citrix ADX zraniteľný voči kritickej chybe CVE-2019-19781. Táto zraniteľnosť je populárna medzi útočníkmi, ktorí používajú ransomvér.

Činnosť vládneho poskytovateľa služieb v USA Tyler Technologies bola prerušená z dôvodu útoku ransomvérom

Webové stránky spoločnosti Tyler Technologies zobrazovali správu o údržbe a na Twitteri zdieľali, že majú technické ťažkosti. Tyler Technologies utrpela útok ransomvérom s názvom RansomExx. Jedná sa o pozmenenú verziu ransomvéru Defray777, pričom zaznamenané boli napríklad útoky na Texaské ministerstvo dopravy a spoločnosť Konica Minolta. Nie je známe či pomocou tohto ransomvéru boli kradnuté aj osobné údaje.

Malvér CDRThief kradne podrobnosti o hovoroch zo softvérového prepínača (softswitch)

Spoločnosť ESET odhalila malvér CDRThief, ktorý sa zameral na konkrétnu platformu Linux VoIP. Malvér svoju činnosť začína pokusom o vyhľadanie konfiguračných súborov softvérových prepínačov zo zoznamu vopred určených adresárov s cieľom získať prístup k databáze MySQL. Hlavným cieľom tohto malvéru je zisk citlivých údajov zo softvérového prepínača vrátane podrobností o hovoroch a databáze. CDRThief útočí konkrétne na softvérové prepínače VOS2009 a 3000 od spoločnosti Linknat. Útočníci šifrovaním svojej škodlivej činnosti zabraňujú vykonávaniu statickej analýzy.

- **Útočníci kompromitovali niekoľko e-mailových účtov nórskeho parlamentu (Stortinget)**
- **Útočníci zneužívajú službu Google DNS prostredníctvom protokolu HTTPS na sťahovanie škodlivého softvéru**
- **Poskytovatelia internetových služieb rôznych krajín Európy zaznamenali útoky typu DDoS**
- **Televízia CNN-News18 v Indii bola údajne hacknutá, aby poprela tvrdenia ohľadom útoku na PayTM Mall**
- **Argentínska vláda bola zasiahnutá ransomvérom Netwalker**
- **Pomocou nástroja CRYLOGGER bolo odhalených 306 aplikácií Androidu, ktoré obsahovali chyby**
- **TeamTNT útočí na cloudové inštancie platforiem Docker a Kubernetes zneužitím nástroja Weave Scope na monitorovanie cloudu**
- **Nesprávna konfigurácia cloudu vo firme Razer potenciálne vystavila 100 000 používateľov phishingu a ďalším podvodom**
- **Tisíce online obchodov napájaných z Magenta boli napadnuté**
- **Čínska skupina hrozieb RedDelta podnikala kybernetické útoky proti katolíckym inštitúciám**
- **Útok ransomvérom v nemeckej nemocnici viedol k smrti pacienta**
- **Bola odhalená iránska útočnícka skupina, ktorá vyvinula špeciálny malware pre Android schopný zachytávať a kradnúť kódy dvojfaktorovej autentifikácie (2FA) zasielané prostredníctvom SMS**
- **Ruskí hackeri používajú falošné výcvikové dokumenty NATO na narušenie vládnych sietí**
- **Spoločnosť Warner Music Group informovala zákazníkov webových stránok svojho elektronického obchodu, že mohlo dôjsť k úniku údajov, ktoré utrpel externý poskytovateľ služieb**

- Škodlivá aplikácia Tik Tok Pro je propagovaná útočníkmi za účelom prevzatia základných funkcií zariadenia ako je snímanie fotiek, čítanie, odosielanie SMS správ a podobne

- Ransomvér AgeLocker útočí na zariadenia NAS spoločnosti QNAP, pričom šifruje súbory na zariadení a v niektorých prípadoch kradne dáta obete

- Hostitelia AirBnB hlásia, že majú neúmyselný prístup k súkromným schránkam, ktoré nesúvisia s ich účtami

- V štáte Washington prijímajú proaktívne opatrenia, pretože súkromné aj verejné subjekty v celom štáte boli vystavené phishingovým útokom

- Vo svete sa objavil nový ransomvér Mount Locker, ktorý využíva na šifrovanie ChaCha20 a na šifrovanie šifrovacieho kľúča zabudovaný verejný kľúč RSA-2048

- Ransomvér zasiahol americkú spoločnosť Arthur J. Gallagher (AJG), ktorá sprostredkúva poistenie a riadenie rizík

- Spoločnosť Universal Health Services (UHS) bola nútená vypnúť niektoré systémy kvôli útoku ransomvérom Ryuk

- Newyorský fitness reťazec Town Sports utrpel únik údajov po zverejnení databázy obsahujúcej údaje o viac ako 600 000 osobách

- Útočníci kombináciou sociálneho inžinierstva, výmeny SIM kariet a softvéru pre vzdialený prístup vyprázdnili bankové účty najmenej trom osobám

- Spyware FinSpy určený pre macOS a Linux sa zameriava na egyptské organizácie

- Chyba v implementácii viacfaktorovej autentifikácie spoločnosti TikTok pre webové rozhranie umožňuje útočníkom obísť ju

- Google odstránil z Play Store 17 aplikácií, ktoré boli infikované malvérom Joker

- Microsoft odstránil 18 aplikácií Azure Active Directory, ktoré boli zneužívané čínskou skupinou GADOLINIUM

- Útočník našiel spôsob, ako nahrávať PDF súbory na webstránky UNESCO a WHO

- Šíri sa phishingový útok, ktorý vyzýva zamestnancov rôznych firiem, aby aktualizovali Windows 7 na Windows 10

TLP: White

- **Francúzska prepravná spoločnosť CMA CGM bola zasiahnutá útokom ransomvérom**
- **Švajčiarska firma Swatch Group identifikovala útok na svoju organizáciu**
- **V USA bola odhalená podvodná emailová kampaň, ktorá viedla k odcudzeniu 15 miliónov dolárov**
- **Bol odhalený nový variant spywaru pre Android, ktorý sleduje aplikácie ako WhatsApp a Telegram**
- **Nový útok Raccoon umožňuje dekódovanie pripojení TLS**
- **Škodlivá tretia strana získala osobné údaje o zhruba 46 000 veteránoch, pričom porušenie ochrany údajov sa týkalo online aplikácie týkajúcej sa Centra finančných služieb (FSC)**
- **Unikli mená a osobné údaje viac ako 1 000 bieloruských policajných dôstojníkov v reakcii na násilné policajné zásahy proti protivládnym demonštráciám**
- **Databáza fóra Webmaster vystavila doi internetu dáta o 800 tisíc užívateľoch zahŕňajúc emailové adresy, mená a ďalšie údaje**
- **Došlo k odhaleniu osobných údajov používateľov 70 rôznych webov slúžiacich na zoznamovanie sa**
- **Niekoľko stoviek domén britskej vlády bolo nájdených na spamových blacklistoch, čo spôsobuje značné problémy s emailovou komunikáciou**
- **Dvaja členovia podporného tímu spoločnosti Shopify sa pokúsili získať podrobnosti o transakciách so zákazníkmi od majiteľov obchodov vo svoj prospech**
- **Aj napriek tomu, že spoločnosť ArbiterSports zabránila šifrovaniu súborov ransomvérom, unikli dáta o 540 tisíc registrovaných členoch**

Závažné zraniteľnosti bežných softvérových produktov

Cisco vWAAS obsahuje predvolené statické administrátorské prihlasovacie údaje

Cisco Virtual Wide Area Application Services (vWAAS) je služba na optimalizáciu pre cloudovú infraštruktúru. Táto služba je dodávaná v zariadeniach Cisco s predvolenými statickými údajmi ktoré môže vzdialený neautentifikovaný útočník využiť na prihlásenie sa do administrátorského konta.

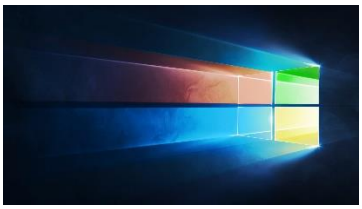
Expert z Google Project Zero odhalil 3 zraniteľnosti Apache Web Server

Felix Wilhelm z Google Project Zero objavil viacero zraniteľností na webovom serveri Apache. Spoločnosť Apache Foundation vydala záplatu adresovanú týmto zraniteľnostiam, ktoré by mohol potenciálny útočník za určitých podmienok zneužiť na vykonanie ľubovoľného kódu, alebo zapríčinenie nedostupnosti služby (DoS) zlyhaním servera.

Cisco Jabber obsahuje kritickú zraniteľnosť umožňujúcu vzdialené vykonávanie kódu

Aplikácia Cisco Jabber obsahuje XSS zraniteľnosť, ktorá sa dá využiť na vzdialené spustenie programov s právami prihláseného používateľa. Na zneužitie zraniteľnosti je potrebné, aby Jabber využíval protokol XMPP s povoleným rozšírením XHTML-IM.

Útočníci aktívne zneužívajú zraniteľnosť operačného systému Windows nazvanú „Zerologon“



Spoločnosť Microsoft v auguste 2020 vydala bezpečnostnú aktualizáciu pre 120 zraniteľností operačného systému Windows Server, z ktorých boli dve zero-day. V rámci tejto aktualizácie Microsoft upozorňuje na aktívne zneužívanie kritickej zraniteľnosti nazvanej „Zerologon“.

Nezabezpečený server Microsoft Bing spôsobuje únik vyhľadávacích dotazov a údajov o polohe

Microsoft Bing pre mobilné zariadenia spôsobuje únik dát. Aj napriek tomu, že neboli odhalené žiadne osobné informácie, uniklo dostatok údajov na to, aby bolo možné prepojiť vyhľadávacie dotazy a polohy s konkrétnymi používateľmi. Nie je celkom známe koľkých používateľov sa to presne týkalo, ale iba v službe Google Play je zaznamenaných viac ako 10 miliónov stiahnutí aplikácie Bing. Táto chyba bola opravená 16. septembra 2020.

Zraniteľnosti Intel

V produktoch Intel nebola opravená žiadna kritická zraniteľnosť. Závažná bola opravená jedna s CVSS skóre 7.6:
CVE-2020-24457: Jedná sa o logickú chybu vo firmvéri systému BIOS pre 8., 9. a 10. generáciu procesorov Intel® Core™. Umožňuje neautentizovanému používateľovi potenciálne povoliť eskaláciu privilégií, narušenie dostupnosti služby (DoS) alebo zverejnenie informácií.

Mesačník zraniteľností September 2020

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

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Flash Player, Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
    - Cisco vWAAS obsahuje predvolené statické administrátorské prihlasovacie údaje
    - Expert z Google Project Zero odhalil 3 zraniteľnosti Apache Web Server
    - Cisco Jabber obsahuje kritickú zraniteľnosť umožňujúcu vzdialené vykonávanie kódu
    - Útočníci aktívne zneužívajú zraniteľnosť operačného systému Windows nazvanú „Zerologon“

https://www.csirt.gov.sk/aktualne-7d7.html?id=226