MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

September 2022

Vypracoval: CSIRT.SK

TLP: White

Albánsko už vyše dvoch mesiacov čelí neustálym kybernetickým útokom. September však priniesol novú vlnu incidentov namierených proti vládnym inštitúciám. Práve počas septembra totiž Albánsko v dôsledku kybernetický útokov prerušilo diplomatické vzťahy s Iránom. Len pár dní neskôr Tirana ohlásila novú sériu útokov. Predpokladá sa preto, že išlo o odpoveď Teheránu na vývoj politickej situácie. K ráznemu kroku Albánska sa pridali aj Spojené štáty americké. Tie na Irán uvalili sankcie.

FBI atribuovala incident iránskej kyberkriminálnej skupine známej pod názvom *HomeLand Justice*. Práve táto skupina mala 14. júla napadnúť albánske informačné systémy a následne stáť za útokom v septembri. Z aktuálne dostupných informácií od albánskeho Ministerstva vnútra rovnako ako aj zo stanoviska FBI vyplýva, že by malo ísť o rovnakého páchateľa. Pri septembrovom incidente totiž išlo o vyžitie podobných taktík, techník a postupov (TTPs) ako tomu bolo pri tom júlovom.

Tentokrát sa však útočníci zamerali na informačné systémy polície. Bezpečnostný tím bol v dôsledku nútený vypnúť počítačové systémy v prístavoch, na letiskách a hraničných priechodoch. Podľa slov vlády sa všetky kybernetické útoky minuli svojmu účinku, keďže sa všetky systémy podarilo v relatívne krátkom čase obnoviť a nedošlo k žiadnemu trvalému vymazaniu dát.

Podľa najnovších zistení FBI a Agentúry pre kybernetickú bezpečnosť a bezpečnosť infraštruktúry (CISA) mali byť vládne systémy Albánska infikované približne 14 mesiacov pred útokom. Prvotný prístup do systémov mali teda útočníci získať ešte v priebehu minulého roku. Zneužitá bola zraniteľnosť CVE-2019-0604 na Microsoft SharePoint. Útočníci následne kompromitovali účet Microsoft Exchange, ktorý zneužili na exfiltráciu dát. Útočníci mali vďaka tomu získať prístup do vládnej siete, čo im umožňovalo získavať informácie z emailovej konverzácie. Bola taktiež detegovaná aktivita v rámci VPN organizácie, čo umožnilo mapovanie otvorených portov v infraštruktúre.

Útočníci po dlhých mesiacoch snáh o infiltrovanie sa do systémov napokon v júli začali s kybernetickou operáciou proti Tirane. Išlo konkrétne o inštaláciu malvéru určeného na šifrovanie súborov rovnako ako aj malvéru slúžiaceho na vymazanie diskov.

Siete boli navyše zasiahnuté ransomvérom. Ten zanechal v systémoch správu namierenú proti iránskej opozičnej strane Mujahideen-e Khalq (MEK), ktorej členom bolo v Albánsku a iných balkánskych krajinách poskytnuté útočisko. Ako odpoveď na snahu vlády eliminovať možné škody z incidentu, útočníci začali využívať deštruktívny malvér ZeroCleare. Skupina sa napokon k útoku 18. júla priznala, pričom postupne na verejnosť začali unikať informácie týkajúce sa ukradnutých dát z vládnych sietí.

FBI v spolupráci s CISA vydali sériu odporúčaní a príkladov dobrej praxe ako môžu štáty predchádzať podobným kybernetickým incidentom. Ide najmä o vypracovanie plánov ako postupovať v prípade útoku, rovnako ako aj o monitorovanie známych zraniteľností a návrh možných postupov pri ich zneužití. Dôraz by mal byť taktiež kladený na pravidelnú aktualizáciu antivírusových softvérov a monitorovanie nezvyčajne veľkých prenosov dát.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci september riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitácie e-mailového konta, z ktorého útočníci rozposielali phishingové e-maily. Vládna kyberbezpečnostná jednotka zaznamenala tento mesiac novú phishingovú resp. podvodnú kampaň zameranú na občanov Slovenskej republiky. Útočníci sa v nej snažia presvedčiť svoje obete, že ich kontaktuje slovenská pobočka Europolu kvôli prechovávaniu detskej pornografie a obdobným sexuálnym deliktom. Prílohou podvodných e-mailov je PDF dokument alebo obrázok fingovaného predvolania na súdne pojednávanie. CSIRT.SK zaznamenal viacero verzií prílohy s rôznou mierou dôveryhodnosti (jedna napríklad obsahovala časť slovenskej hymny). Slovenské úrady musia doručovať obdobné dokumenty, na to aby boli právne relevantné, v papierovej forme alebo cez ústredný portál verejnej správy – slovensko.sk. Podvodné e-maily sa dostali aj do schránok zamestnancov organizácií štátnej a verejnej správy.

CSIRT.SK prijal v septembri hlásenie o používaní nelegálnych crackovacích nástrojov v infraštruktúre organizácie v jeho konštituencii. Spolu s národnou jednotkou SK-CERT analyzoval závažnosť incidentu a možné škody. Predpokladanými dôsledkami boli napríklad únik citlivých informácií a vytvorenie zadných dvierok do infraštruktúry zneužiteľných útočníkmi, ktorí nástroje vytvorili. CSIRT.SK prijal tiež hlásenie úniku citlivých dokumentov tej istej organizácie, ktoré boli objavené na portáli uloz.to. Incidenty však spolu pravdepodobne nesúvisia.

Vládna jednotka CSIRT pokračovala v riešení rozsiahleho ransomvérového incidentu nahláseného v auguste. Ransomvér zasiahol veľký počet serverov a pracovných staníc. Jednotka vykonávala forenznú analýzu zaistených digitálnych stôp a analýzu možností obnovy infraštruktúry.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK poskytla organizáciám vo svojej konštituencii indikátory kompromitácie niekoľkých ransomvérových kampaní, získané od zahraničného partnera. Jednotka ďalej vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií v jej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje.

Významné útoky vo svete

Portugalsku boli ukradnuté utajované dokumenty z NATO



Útočníkom sa podarilo nabúrať do informačných systémov Generálneho štábu ozbrojených síl Portugalska a ukradnúť tak dokumenty s utajovanými skutočnosťami zo Severoatlantickej aliancie (NATO). Vláda však únik nedetegovala sama. Upozorniť naň mali americkí spravodajcovia, ktorí našli dokumenty predávané na darknete. Okrem počítačov Generálneho štábu boli kompromitované aj systémy Vojenského informačného a bezpečnostného centra rovnako ako aj Generálneho riaditeľstva pre zdroje národnej obrany. Dôvodom pre únik bolo porušenie odporúčaných bezpečnostných pravidiel, ktoré určujú ako by mal prebiehať prenos utajovaných dokumentov. Inštitúcie totiž nevyužívali integrovaný systém vojenských komunikácií. Namiesto toho používali nezabezpečené kanály. Vyšetrovaním incidentu bolo poverené Národné centrum kybernetickej obrany.

Útočníci využívajú zero-days zraniteľnosti na Microsoft Exchange Server



Spoločnosť Microsoft potvrdzuje zneužívanie 2 zero-days zraniteľností na svojich systémoch Exchange Server 2013, 2016 a 2019. Zraniteľnosti dovoľujú autentifikovanému útočníkovi, hoci aj s nízkymi privilégiami, vzdialene vykonávať kód prostredníctvom PowerShell. Prvotne sa predpokladalo, že by mohlo ísť o variáciu predchádzajúcich ProxyShell zraniteľností. Po prešetrení však bola táto alternatíva vylúčená. Útoky ako prvá nahlásila vietnamská kyberbezpečnostná firma GTSC. Malo ísť o snahu čínskej skupiny zneužiť zraniteľnosti s cieľom

ohroziť kritickú infraštruktúru začiatkom augusta. Zákazníci by však podľa slov spoločnosti nemali byť ohrození.

Za únikom dát spoločnosti Uber má stáť hackerská skupina Lapsus$



Uber obvinil kyberkriminálnu skupinu Lapsus$ z kybernetického útoku, ktorý mal za následok únik dát. Útočníkom sa podarilo vniknúť do interných systémov spoločnosti, odkiaľ stiahli internú komunikáciu a údaje z finančného oddelenia. Útok mal prebehnúť prostredníctvom zneužitia dodávateľa tretej stany. Útočníci mali získať prístupové údaje korporátu cez darknet, keďže systém dodávateľa bol predtým napadnutý malvérom. Hoci bolo konto poskytnuté dodávateľom chránené dvojfaktorovou autentifikáciou, po viacerých žiadostiach na prihlásenie dodávateľ napokon poskytol prístup. Útočníci tak získali oprávnenia na využívanie interných služieb ako G-Suite a Slack. Systémy spracúvajúce dáta verejnosti by však nemali byť zasiahnuté. Spoločnosť spolupracuje s FBI a Ministerstvom spravodlivosti USA na prešetrení daného incidentu.

Austrálskej telekomunikačnej spoločnosti Optus boli odcudzené dáta zákazníkov



Austrálska spoločnosť Optus čelila rozsiahlemu kybernetickému útoku. Počas neho boli ukradnuté citlivé údaje zákazníkov ako čísla občianskych preukazov či emailové adresy. V ohrození sa nachádza 10 miliónov aktuálnych zákazníkov, pričom odcudzené mali byť aj dáta tých bývalých. Útočník navyše zverejnil viac ako 10 tisíc záznamov získaných pri útoku žiadajúc o 1 miliónové výkupné. V opačnom prípade mali byť zverejnené aj dáta všetkých ostatných zákazníkov. Po rozsiahlej verenej publicite však útočník požiadavku na výkupné stiahol a ospravedlnil sa spoločnosti za spôsobené škody. Hacker mal

údajne vymazať všetky ukradnuté dáta z jeho zariadení. Na preniknutie do systémov a získanie dát bol pravdepodobne využitý API endpoint. Spoločnosť spolupracuje s Austrálskou Federálnou políciou na prešetrení incidentu.

Útok na Americkú leteckú spoločnosť má za následok únik dát



Americké aerolínie informovali verejnosť o úniku dát, ktorý bol spôsobený kybernetickým útokom. Útočník najskôr zaslal phishingové emaily zamestnancom, v dôsledku čoho získal prístup do ich emailových účtov. Kompromitácia mala prebehnúť prostredníctvom protokolu IMAP umožňujúceho prenesenie obsahu z mailových schránok na iné zariadenie. Zasiahnuté účty navyše obsahovali aj citlivé údaje ako telefónne číslo či číslo identifikačných dokumentov niektorých zákazníkov. Spoločnosť incident odhalila až po hlásení od svojich zamestnancov, ktorých účty boli zneužité na rozosielanie ďalších phishingových emailov. Zasiahnutých bolo približne 1700 ľudí.

Wintermute prišlo v dôsledku kybernetického útoku o 160 miliónov USD



Globálnemu tvorcovi krypto trhu Wintermute bolo počas kybernetického útoku odcudzených 160 miliónov amerických dolárov v kryptomenách. Išlo o vykonanie série neautorizovaných transakcií, vďaka ktorým si útočník previedol viac ako 66 kryptomien do svojej peňaženky. Útočník mal využívať operácie decentralizovaného financovania (DeFi) spoločnosti. Doposiaľ však nie je známe ako presne prienik do systému prebiehal. Predpokladá sa, že išlo o zneužitie zraniteľností Profanity. Wintermute v odpovedi na útok oznámila, že hackerovi za odhalenie zraniteľnosti zaplatí, a to bez akýchkoľvek právnych následkov.

Hackerská skupina Gamaredon útočí na ukrajinskú vládu



Ruská skupina Gamaredon spustila rozsiahlu špionážnu kampaň proti Ukrajine. Malvérom sú zasiahnutí najmä zamestnanci vlády, orgány činné v trestnom konaní a obranné inštitúcie. Ide o snahu získať informácie týkajúce sa vojny. Využívaný je nový typ malvéru určeného na kradnutie informácií zo systémov a kybernetickú špionáž. Gamaredon využila svoju typickú stratégiu- spear phisingovú kampaň na získanie prvotného prístupu. Stalo sa tak využitím LNK súborov, PowerShellu a VBScriptu, čo umožnilo následné infikovanie zariadení už spomenutým malvérom.

Lazarus útočí na energetické spoločnosti v štátoch Severnej Ameriky a v Japonsku



Severokórejská APT skupina Lazarus útočí prostredníctvom troch typov remote access trojans (RATs) na poskytovateľov energií vo svete. Podľa výskumníkov z Cisco sa útočníkom podarilo vniknúť do systémov energetických spoločností v priebehu obdobia od februára do júla tohto roku. Využívať pritom mali známe zraniteľnosti VMWare Horizon. Následne boli napadnuté zariadenia infikované rôznymi typmi malvéru ako VSingle a YamaBot. Použitá bola aj nová verzia trójskeho koňa MagicRAT, ktorá slúži na kradnutie dát z infikovaných zariadení.

Zero-day zraniteľnosť umožnila napadnutie viac ako 280 tisíc Wordpress webstránok



Hackeri zneužívajú jednu zo zraniteľností na najnovších verziách Wordpressu. Ide konkrétne o zero-day zraniteľnosť v prémiovom module zvanom WPGateaway**,** ktorú je možné zneužiť na prevzatie kontroly na webom. Táto zraniteľnosť umožňuje neautentifikovanému používateľovi

zmeniť privilégiá a pridať tak nového administrátora stránky. Podľa dostupných informácií sa podarilo bezpečnostnému tímu Wordfence zablokovať 4,6 milióna útokov namierených na 280 tisíc stránok.

Akamai odvrátila najväčšie DDoS útoky v histórii Európy



Spoločnosť Akamai detegovala zatiaľ najrozsiahlejší pokus o znedostupenie služby (DDoS) v Európe po predchádzajúcich závažných incidentoch v júli. Podľa aktuálnych zistení by za oboma útokmi mal stáť rovnaký aktér. Útočníci zahltili stránky Európskych organizácií obrovským množstvom falošných požiadaviek, čo spôsobilo nedostupnosť jednotlivých služieb. Zasiahnutých bolo celkovo šesť dátových centier v Severnej Amerike a Európe.

- **Útočníci zverejnili dáta pacientov z francúzskej nemocnice.**
- **Smart Links na sociálnej sieti LinkedIn sú zneužívané na phishingové útoky.**
- **SQL servery spoločnosti Microsoft boli napadnuté ransomvérom FARGO.**
- **Hackerská skupina Metador útočí na organizácie v Afrike a na Blízkom východe za účelom kybernetickej špionáže.**
- **Čínski hackeri zneužili zadné vrátka LOWZERO na špionáž namierenú proti Tibetu.**
- **Ruská hackerská skupina Sandworm sa prestrojená za ukrajinské telekomunikačné spoločnosti snaží šíriť malvér.**
- **Eset objavil novú kyberšpionážnu skupinu Worok, ktorá sa zameriava na entity v Ázii.**
- **Spoločnosť Elbit Systems of America potvrdzuje únik dát spôsobený ransomvérovým útokom.**

- **Ukrajinská polícia zatkla členov kyberkriminálnej skupiny predávajúcej 30 miliónov účtov na darknete.**
- **Cisco pripisuje nedávne zverejnenie uniknutých dát ransomvéru Yanluowang, ktorým firmu napadli útočníci ešte v máji.**
- **Štáty naprieč Blízkym východom boli zasiahnuté malvérom skrytým v logu Windows.**
- **APT skupina Lazarus využíva falošnú ponuku práce na inštaláciu malvéru do operačného systému MacOS.**
- **Útočníkom sa podarilo získať viac ako 50 tisíc dát zákazníkov firmy Revolut.**
- **Malvér Chromeloader podľa spoločnosti VMware predstavuje značné riziko.**
- **Pôvodní členovia kyberkriminálnej skupiny Conti majú stáť za útokmi na Európu a Ukrajinu.**
- **Interpolu sa podarilo rozpustiť medzinárodnú kriminálnu organizáciu zaoberajúcu sa kybernetickým sexuálnym vyhrážaním.**
- **Zdravotníckym spoločnostiam boli podľa FBI odcudzené milióny USD počas kybernetických útokov.**
- **Útočníci zneužili smrť kráľovnej Alžbety na phishingové kampane.**
- **Hackerská skupina Webworm využíva na útoky upravené verzie starého malvéru.**
- **Ruská skupina APT28 zneužíva pohyb myši v produktoch Microsoft PowerPoint na infikovanie zariadenia malvérom.**
- **Skupina LeakBase zverejnila dáta vyše 16 miliónov používateľov platformy Swachh City.**
- **GitHub varuje používateľov pred phishingovou kampaňou, ktorá využíva notifikácie CircleCI.**
- **Citlivé dáta zákazníkov portugalskej leteckej spoločnosti TAP Air Portugal boli odcudzené počas útoku.**

- **Austrália, Veľká Británia, Kanada a Spojené štáty americké obviňujú Irán zo zapájania sa do ransomvérových útokov a kybernetického vydierania.**

- **Spoločnosť Starbucks v Singapure utrpela únik dát zasahujúci 219 tisíc zákazníkov.**

- **Útočníci využívajú populárne videohry na šírenie malvéru Erbium slúžiaceho na odcudzenie citlivých údajov.**

- **Nový malvér NullMixer infikuje zariadenia Windows svojimi rôznymi odnožami.**

- **Menšina Ujgurov v Číne má byť podľa výskumníkov dlhoročne špehovaná prostredníctvom mobilného spyware.**

- **Hackeri zneužili zraniteľnosť Sophos Firewall pri útokoch na juhoázijské organizácie.**

Závažné zraniteľnosti bežných softvérových produktov

Zero-day zraniteľnosti servera Microsoft Exchange

Vietnamskí výskumníci zo spoločnosti GTSC pred troma týždňami informovali spoločnosť Microsoft cez iniciatívu Trend Micro Zero Day o zraniteľnostiach, ktoré sa podobajú staršej zraniteľnosti ProxyShell. V produkte Microsoft Exchange a jeho súčasti Outlook Web app (OWA) boli objavené dve zraniteľnosti, pre ktoré aktuálne nie je dostupná bezpečnostná oprava, no existuje spôsob dočasnej opravy. Potenciálny vzdialený a autentifikovaný útočník by mohol zneužitím zraniteľností prevziať kontrolu nad serverom a nasadiť škodlivý webshell. Výskumníci zo spoločnosti GTSC nateraz nezverejnili podrobnejšie technické informácie o zraniteľnostiach, postup zneužitia zraniteľnosti je však verejne dostupný.

Kritická zneužívaná zraniteľnosť Sophos Firewall



Kritická zero-day zraniteľnosť v Sophos Firewall umožňuje útočníkom vzdialene vykonávať kód. Spoločnosť Sophos vydala opravu pre podporované verzie svojho produktu.

Microsoft v rámci Patch Tuesday opravil závažnú aktívne zneužívanú zraniteľnosť vo Windows



Spoločnosť Microsoft vydala v septembri 2022 balík opráv pre operačné systémy Windows opravujúcich 63 zraniteľností. 5 z nich dostalo hodnotenie kritická. Dve zraniteľnosti sú typu zero-day, pričom jedna je aktívne zneužívaná.

Závažná zraniteľnosť v HP Support Assistant

Spoločnosť HP opravila závažnú zraniteľnosť v nástroji HP Support Assistant, ktorá umožňuje útočníkom eskalovať privilégiá škodlivého kódu na úroveň SYSTEM.

Kritické zraniteľnosti sieťových dátových úložísk QNAP a Zyxel

Spoločnosť QNAP opravila nešpecifikovanú kritickú zraniteľnosť vo svojom produkte Photo Station pre úložiská NAS, ktorú aktívne zneužíva skupina Deadbolt vo svojej ransomvérovej kampani. Spoločnosť Zyxel opravila vo firmvéri svojich zariadení NAS kritickú zraniteľnosť umožňujúcu jednoduchým spôsobom vzdialené vykonávanie kódu.

Google opravil ďalšiu zero-day zraniteľnosť v prehliadači Chrome, zraniteľný aj Microsoft Edge

Google opravil ďalšiu zero-day zraniteľnosť v prehliadači Chrome, zraniteľný aj Microsoft Edge. Spoločnosť Google vydala opravu v poradí šiestej tohtoročnej zero-day zraniteľnosti svojho internetového prehliadača Chrome. Zraniteľnosť je aktívne zneužívaná a útočníkovi dáva možnosť obísť bezmečnostné obmedzenia. Podľa niektorých zdrojov je zraniteľný tiež prehliadač Microsoft Edge.

Mesačník zraniteľností september 2022

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 tohto mesačné závažné zraniteľnosti
   - HP Support Assistant
   - Sophos Firewall
   - sieťové dátové úložiská QNAP a Zyxel
   - server Microsoft Exchange

https://www.csirt.gov.sk/posts/3090/