MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Máj 2021

Vypracoval: CSIRT.SK

TLP: White

V mesiaci máj sa svet stretol s útokmi ransomvéru Conti. Tento ransomvér bol prvýkrát spozorovaný v ojedinelých útokoch v roku 2019. Útočníci stojaci za ním sú známi tým, že kompromitujú podnikové siete a šíria svoje pôsobenie bočnými kanálmi až kým nezískajú prístup k oprávneniam správcu domény. Tie im umožňujú nasadiť spúšťače ransomvéru bez akýchkoľvek súborov – injektovaním DLL knižníc. Conti funguje ako „ransomvér ako služba“ (Ransomware as a Service – RaaS), ktorý naberá hackerov, ktorí následne nasadzujú daný ransomvér za finančnú odmenu. Conti pravdepodobne prevádzkuje ruská kyberkriminálna skupina známa ako Wizard Spider.

Írsky výkonný úrad pre zdravotníctvo (HSE), štátny verejne financovaný systém zdravotnej starostlivosti, odstavil všetky systémy IT po tom, čo bola pri útoku ransomvérom Conti kompromitovaná jeho sieť. V minulosti tento ransomvérový gang zasiahol v decembri 2020 aj Škótsku agentúru pre ochranu životného prostredia (SEPA). Zverejnených bolo zhruba 1,2 GB ukradnutých údajov.

Skupina stojaca za ransomvérom Conti tvrdila, že mala prístup k sieti HSE viac ako dva týždne, a že dokázala ukradnúť 700 GB nezašifrovaných súborov vrátane informácií o zamestnancoch a pacientoch, finančných výkazov, miezd, zmlúv a ďalších. Skupina vyžadovala výkupné v hodnote takmer 20 miliónov amerických dolárov.

Útočníci sa pokúšali šifrovať aj systémy írskeho ministerstva zdravotníctva (DoH), avšak neúspešne. Sieť sa im však podarilo kompromitovať, pričom nasadili útočný nástroj Cobalt Strike. Ten mal slúžiť na následné nasadenie malvéru po sieti, čo však zablokovalo antivírusové riešenie.

Útočníci sa rozhodli vydať írskej zdravotnej službe HSE bezplatný dešifrovač, avšak ukradnuté údaje predávajú aj naďalej. Kým ministerstvo zdravotníctva dokázalo útok zablokovať, HSE musela vypnúť svoje systémy, aby tak zabránila šifrovaniu ďalších zariadení. Tento výpadok viedol k rozsiahlym narušeniam systému zdravotnej starostlivosti v krajine.

FBI identifikovala v priebehu minulého roka najmenej 16 útokov ransomvéru Conti zameraných na americké zdravotníctvo, orgány činné v trestnom konaní, pohotovostné lekárske služby a podobne. Obeťami ransomvéru Conti je viac ako 400 organizácií po celom svete, pričom viac ako 290 sa nachádza v USA.

Predpokladá sa, že Conti úzko súvisí s ransomvérom Ryuk. Ukázalo sa, že zdieľajú kód a oba sú založené na distribúcii pomocou botnetu TrickBot. Conti využíva simultánne až 32 vlákien procesora pre rýchlejšie šifrovanie. Svojmu radiču dáva možnosť preskočiť šifrovanie súborov na lokálnom systéme a šifrovať tie, ktoré sú zdieľané v sieti. Nakoniec Conti zneužije Windows Restart Manager na uvoľnenie súborov používaných aplikáciami.

Bezpečnostní výskumníci zo spoločnosti Sophos odporúčajú na ochranu proti ransomvérom monitorovať bezpečnosť siete, nepoužívať Remote Desktop protokol (prípadne ho používať cez VPN),

vzdelávať zamestnancov a využívať štandardnú metódu 3-2-1 na zálohovanie (3 kópie dát, použitím 2 rôznych systémov, pričom jeden z nich je offline).

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti, CSIRT.SK v mesiaci máj riešil najmä phishingové kampane zasahujúce jeho konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov. Útok ransomvéru z rodiny Phobos sa nevyhol jednej obci, ktorá však bola schopná väčšinu svojich dát obnoviť.

Medzi závažnejšie riešené incidenty patril pokus o prienik do infraštruktúry jedného konštituenta. Infikované zariadenie v sieti vykonávalo skenovanie infraštruktúry a pokúšalo sa v rámci nej komunikovať. Zariadenie bolo izolované a hlbší prienik nebol potvrdený. Podozrenie na škodlivú aktivitu riešila jednotka aj v ďalšej organizácii, kde zaistila obraz disku predmetného serveru a iné relevantné digitálne stopy a vykonala forenznú analýzu. Skúmanie preukázalo, že sa o škodlivú aktivitu nejednalo. Organizácii boli poskytnuté odporúčania, ktoré vyplynuli pri analýze.

Vishingové telefonáty z falšovaných telefónnych čísiel vrátane slovenských predvolieb sa objavili aj tento mesiac, opäť s tematikou technickej podpory spoločnosti Microsoft.

CSIRT.SK vykonal na vyžiadanie opakované analýzy zraniteľností do internetu vypublikovaných systémov niekoľkých zdravotníckych zariadení.

Jednotka upozornila svoju konštituenciu na databázu kompromitovaných emailových účtov, ktorú zaistil Europol počas akcie zameranej na rozbitie infraštruktúry botnetu Emotet. Organizáciám odporučila vykonať kontrolu pre výskyt účtov pomocou služby Have I Been Pwned.

CSIRT.SK tiež priamou cestou upozornil na kritickú zraniteľnosť CVE-2021-31166 v operačných systémoch Windows, CVE-2021-21985 v produkte VMware vCenter a indikátory kompromitácie skupiny Black Halo, zodpovednej za útok na dodávateľskú infraštruktúru SolarWinds. V rámci svojich proaktívnych činností pripravila návod na nasadenie politík pre mailservery SPF, DKIM a DMARC, pomáhajúcich pri ochrane pred podvrhutými e-mailami. Momentálne je dostupný na tomto odkaze.

Významné útoky vo svete

Poskytovateľ zdravotnej starostlivosti Scripps Health utrpel útok ransomvéru

Útok ransomvéru na neziskového poskytovateľa zdravotnej starostlivosti Scripps Health prinútil organizáciu pozastaviť prístup k jej online portálu. Po útoku boli služby pre pacientov offline a niektorí pacienti s kritickou starostlivosťou boli podľa správ miestnych médií presmerovaní do iných nemocníc. Interné oznámenie naznačovalo, že útok ransomvéru zasiahol počítačové systémy v dvoch nemocniciach vrátane prístupu k lekárskym snímkam.

Nový malvér Pingback sa zameriava na 64-bitové verzie operačného systému Windows

Nový malvér Pingback pre Windows využíva protokol ICMP na činnosti velenia a riadenia (C&C). Malvér sa zameriava na 64-bitové verzie operačného systému Windows a na zaistenie perzistencie využíva únos DLL. Predmetný škodlivý súbor má veľkosť 66 kB a nazýva sa oci.dll. Zvyčajne je presunutý do priečinku „System“ iným škodlivým procesom alebo vektorom útoku. Na načítanie tohto súboru je zneužitá služba Microsoft Distributed Transaction Control (msdtc). Pri spustení služba Windows msdtc vyhľadá na načítanie 3 knižnice DLL: oci.dll, SqlLib80.dll a xa80.dll. Výhodou použitia ICMP na komunikáciu je, že Pingback zostáva efektívne skrytý pred používateľom.

Z americkej agentúry pre globálne médiá unikli osobné údaje o súčasných a bývalých zamestnancoch

Americká agentúra pre globálne médiá (USAGM) sa stala obeťou úniku údajov, pričom odhalené boli osobné údaje o súčasných a bývalých zamestnancoch. Dôvodom úniku je phishingový útok, ktorý sa udial ešte v decembri 2020. Tento phishingový útok umožnil útočníkovi získať prístup k emailovému účtu agentúry, ktorý obsahoval osobné údaje súčasných a bývalých zamestnancov USAGM, Voice of America a Office of

Cuba Broadcasting, ktorí v agentúre pracovali v rokoch 2013 až 2020. Uniknuté údaje zahŕňajú celé mená, čísla Social Security a podobne.

Malvér Moriya pre OS Windows umožňuje sledovať sieťový prenos

Neznámy útočník použil nový rootkit na nasadenie zadných vrátok do operačného systému Windows. Nový malvér Moriya umožňuje útočníkom sledovať sieťový prenos a posielať príkazy napadnutým hostiteľom. Spôsob, akým zadné vrátka dostávajú príkazy vo forme špeciálne vytvorených paketov skrytých v sieťovej premávke obetí bez použitia riadiaceho servera prispel k utajeniu útokov. Útočníci tiež nasadili ďalšie nástroje (China Chopper, BOUNCER, Termite a Earthworm) na napadnutých systémoch.

Mesto Tulsa bolo nútené vypnúť svoje systémy a služby kvôli útoku ransomvérom

Mesto Tulsa v Oklahome utrpelo útok ransomvéru, ktorý prinútil mesto vypnúť svoje systémy a služby, aby tak zabránili ďalšiemu šíreniu. Tulsa je druhé najväčšie mesto v Oklahome s približne 400-tisíc obyvateľmi. Starosta mesta tvrdí, že incident nemal vplyv na núdzové služby. Vypnutie mestských systémov však obyvateľom bráni v prístupe k online platobným systémom, elektronickej fakturácii a službám prostredníctvom emailu. Webové stránky pre mesto Tulsa, mestskú radu v Tulse, políciu v Tulse a celkovo 311 ďalších webových stránok tiež neboli k dispozícii kvôli údržbe.

Z webových stránok guard.me unikli osobné informácie poistencov

Poskytovateľ zdravotného poistenia pre študentov guard.me uviedol svoje webové stránky do režimu offline po tom, ako zraniteľnosť umožnila útočníkovi prístup k osobným informáciám poistencov. Uniknuté údaje zahŕňajú dátum narodenia, pohlavie, šifrované heslá. U niektorých študentov údaje zahŕňali tiež emailové adresy, adresy bydliska a telefónne čísla.

Guard.me uvádza, že chybu odstránili a že odolali ďalším pokusom o obídenie bezpečnostných opatrení. Poskytovateľ zdravotného poistenia tiež uvádza, že zavádza nové politiky pre zvýšenie bezpečnosti vrátane dvojfaktorovej autentifikácie.

Spoločnosť Domino's India údajne utrpela únik údajov o veľkosti 13TB

Spoločnosť Domino's India utrpela únik údajov po tom, čo sa útočník vlámal do jej systémov a predal ukradnuté údaje na hackerskom fóre. Útočník tvrdil, že predáva 13TB odcudzených údajov, vrátane podrobností o 180 miliónov objednávkach a 1 milióne kreditných kariet. Útočník predával údaje za približne 10 BTC a zdieľal vzorky databázy ukradnutých údajov. Uniknuté údaje zahŕňajú mobilné čísla, emailové adresy a GPS súradnice zákazníkov.

Útočníci získali prístup k projektom, ktoré používali ProjectWEB od Fujitsu

Kancelárie viacerých japonských agentúr boli kompromitované prostredníctvom nástroja na zdieľanie informácií spoločnosti Fujitsu – ProjectWEB. Spoločnosť Fujitsu uvádza, že útočníci získali neoprávnený prístup k projektom, ktoré používali ProjectWEB, a ukradli niektoré údaje o zákazníkoch. Získaním neoprávneného prístupu k vládnym systémom prostredníctvom ProjectWEB sa útočníkom podarilo získať najmenej 76-tisíc emailových adries vrátane konfigurácie emailového systému.

Útok na Commport Communications spôsobil škodu spoločnosti Canada Post

Spoločnosť Canada Post informovala 44 svojich veľkých komerčných zákazníkov o tom, že útok ransomvéru na poskytovateľa služieb tretej strany odhalil informácie o preprave pre ich zákazníkov. Dodávateľ tretej strany s názvom Commport Communications utrpel útok ransomvérom, pri ktorom útočníci pristupovali k údajom uloženým v jeho systémoch. Tieto prístupové údaje zahŕňajú údaje manifestu prepravy pre veľkých

balíkových obchodných zákazníkov, vrátane kontaktných informácií o odosielateľovi a príjemcovi, mien a poštových adries. Útok sa celkovo dotkol 44 komerčných zákazníkov Canada Post a 950 miliónov prijímajúcich zákazníkov.

Ruskí útočníci vedú phishingovú kampaň voči vládnym agentúram

Microsoft Threat Intelligence Center (MSTIC) zistilo, že ruskí hackeri koordinujú prebiehajúcu phishingovú kampaň zameranú na vládne agentúry po celom svete. Táto vlna útokov sa zamerala na približne 3-tisíc emailových účtov vo viac ako 150 rôznych organizáciách. Zatiaľ čo organizácie v USA boli obeťami najväčšieho množstva útokov, obete sa nachádzajú v najmenej 24 krajinách. Hackerská skupina Nobelium zasielala phishingové emaily pomocou napadnutého účtu Constant Contact (legitímna služba emailového marketingu) USAID.

Zo systémov poisťovne AXA útočníci údajne odcudzili 3TB údajov

Pobočky poisťovne AXA so sídlom v Thajsku, Malajzii, Hongkongu a na Filipínach boli zasiahnuté ransomvérom. Skupina útočníkov Avaddon tvrdí, že odcudzila 3TB citlivých údajov z prevádzok spoločnosti AXA. Medzi uniknuté údaje patria lekárske správy zákazníkov, kópie občianskych preukazov, výpisy z bankových účtov a podobne. Skupina sa tiež priznala, že vykonávala voči webovým stránkam tejto spoločnosti DDoS útoky.

Ransomvér Red Epsilon sa zameriava na neopravené servery Microsoft Exchange

Nový ransomvér Red Epsilon sa zameriava na neopravené servery Microsoft Exchange. Je napísaný v programovacom jazyku Go a predchádza mu sada Powershell skriptov, ktoré pripravujú systém na šifrovanie súborov. Po kompromitovaní siete sa hackeri dostanú k počítačom cez protokol RDP a pomocou Windows Management Instrumentation (WMI)

nainštalujú softvér a spustia skripty PowerShell, ktoré nakoniec nasadia Epsilon Red.

- **Nový ransomvérový gang známy ako N3TW0RM sa zameriava na izraelské spoločnosti.**
- **Zraniteľný ovládač Dell vystavuje stovky miliónov systémov riziku.**
- **Kritické chyby 21Nails Exim vystavujú milióny serverov útokom.**
- **Spoločnosť Twilio odhaľuje dopad útoku na dodávateľský reťazec spoločnosti Codecov.**
- **Pokus študenta stiahnuť si nelegálne softvér, viedol k útoku ransomvéru Ryuk na Európsky inštitút pre biomolekulárny výskum.**
- **Operátori ransomvéru Cuba sa spojili s operátormi malvéru Hancitor na získanie ľahšieho prístupu k kompromitovaným podnikovým sieťam.**
- **Chyba v softvéri Foxit Reader umožňuje útočníkom vykonávať škodlivý kód pomocou PDF súborov.**
- **Po útoku ransomvéru na spoločnosť Colonial Pipeline USA vyhlásilo stav núdze.**
- **Skupina stojaca za ransomvérom DarkSide zverejnila tlačovú správu, v ktorej uviedla, že je apolitická a pred útokom preveruje svoje ciele.**
- **USA a Austrália varujú pred stupňovaním útokov ransomvéru Avaddon.**
- **Novoobjavené chyby zabezpečenia známe ako FragAttacks ovplyvňujú všetky Wi-Fi zariadenia.**
- **Ransomvér MountLocker využíva API rozhrania Windows Active Directory na šírenie prostredníctvom sietí.**
- **Osobné údaje viac ako 100 miliónov používateľov systému Android boli vystavené do internetu v dôsledku rôznych nesprávnych konfigurácií cloudových služieb.**

- **Elektronický obchod Mercari utrpel únik údajov, ku ktorému došlo v dôsledku útokov na Codecov.**
- **Bankový malvér Bizarro sa zameriava na 70 bánk v Európe a Južnej Amerike.**
- **Spoločnosť Air India potvrdila únik údajov súvisiaci s útokom na spoločnosť SITA.**
- **Objavujú sa nové aktualizované verzie ransomvéru Zeppelin.**
- **Spoločnosť Bose potvrdila únik údajov po útoku ransomvéru.**
- **Výskumníci objavili novú phishingovú kampaň BazarCall, ktorá obchádza systémy na detekciu hrozieb.**
- **Čínske skupiny útočníkov pokračujú v zavádzaní nových kmeňov malvérov po zneužití zraniteľností v Pulse Secure VPN.**
- **Spoločnosť JBS Foods bola nútená po kybernetickom útoku pozastaviť výrobu.**
- **Švédska agentúra pre verejné zdravie (Folkhälsomyndigheten) uviedla do offline stavu databázu SmiNet po niekoľkých pokusoch o útok.**
- **Na používateľov peňaženiek Trust Wallet a MetaMask sa zameriavajú phishingové útoky na Twitteri.**
- **FBI varuje pred scammermi, ktorí sa zameriavajú na rodiny nezvestných osôb.**

Závažné zraniteľnosti bežných softvérových produktov

QNAP NAS – celosvetovo zneužívané zraniteľnosti sieťových úložísk

CSIRT.SK prináša súhrn zraniteľností a informácie o aktuálnych a minulých ransomvérových kampaniach, ktoré cielia na zariadenia QNAP NAS. Zariadenia, ktoré poskytujú sieťové úložisko s prístupom z internetu sú veľkým lákadlom pre útočníkov. Závažné bezpečnostné zraniteľnosti môžu umožniť potencionálnym útočníkom prevziať kontrolu nad zraniteľným NAS zariadením, odcudziť dáta, zneužiť zariadenie na šírenie rôzneho malvéru, a tak kompromitovať rozsiahlejšiu časť infraštruktúry organizácie.

V softvéri Cisco SD-WAN vManage bolo opravených 5 zraniteľností

Spoločnosť Cisco vydala opravné aktualizácie pre 5 zraniteľností v softvéri Cisco SD-WAN vManage, pričom 2 z nich sú kritické. Vo všeobecnosti tieto zraniteľnosti môžu neautentifikovanému útočníkovi umožniť vzdialené vykonanie kódu alebo získať prístup k citlivým informáciám. Autentifikovanému lokálnemu útočníkovi umožňujú eskalovať privilégiá alebo získať neautorizovaný prístup k aplikáciám.

Spoločnosť Cisco opravila 2 zraniteľnosti v softvéri HyperFlex HX

V softvéri Cisco HyperFlex HX boli nájdené a opravené 2 zraniteľnosti. Vo všeobecnosti tieto chyby môžu útočníkovi umožniť vzdialene vykonať ľubovoľný kód ako administrátor alebo používateľ tomcat8. Zraniteľné sú zariadenia Cisco so softvérom HyperFlex HX verzie 4.0, 4.5 a nižšej ako 4.0.

F5 Networks – zariadenia BIG-IP obsahujú závažnú bezpečnostnú zraniteľnosť

Výskumníci spoločnosti Silverfort objavili závažnú bezpečnostnú zraniteľnosť v produkte BIG-IP spoločnosti F5 Networks.

Zraniteľnosť existuje z dôvodu nedostatočnej implementácie protokolu Kerberos v manažmente prístupu APM produktov BIG-IP. Úspešné zneužitie zraniteľnosti by mohlo útočníkovi umožniť obísť proces autentifikácie, neoprávnene sa prihlásiť k rôznym službám, či administrátorskej konzole zariadenia, a tak kompromitovať celú infraštruktúru organizácie.

Spoločnosť Dell opravuje závažnú zraniteľnosť, ktorá postihuje milióny zariadení

Výskumníci zo spoločnosti SentinelLabs objavili zraniteľnosti v ovládači nachádzajúcom sa v miliónoch zariadení od spoločnosti Dell. Zraniteľnosti v ovládači existujú už od jeho prvého vydania v roku 2009. Potenciálnemu útočníkovi umožňujú eskaláciu privilégií či vykonanie kódu s oprávneniami jadra. Môžu sa nachádzať vo všetkých zariadeniach, ktoré používali obslužné programy pre aktualizáciu, ako napríklad Dell Command Update, Dell System Inventory Agent, Alienware Update či Dell Platform Tags.

Microsoft opravil 55 zraniteľností, z toho 3 zero-day

Spoločnosť Microsoft vydala balík opráv Patch Tuesday, v ktorom opravila 55 zraniteľností. Z nich 50 označila ako vysoko závažné a 4 ako kritické. 3 zraniteľnosti sú typu zero-day, no zatiaľ neboli aktívne zneužívané. Väčšina najzávažnejších chýb zabezpečenia umožňuje vzdialené vykonávanie kódu, či zvýšenie oprávnení útočníka.

Vo VMware vRealize Business for Cloud sa vyskytuje kritická zraniteľnosť

Spoločnosť VMware opravila kritickú zraniteľnosť vyskytujúcu sa v produkte vRealize Business for Cloud. Zneužitím tejto chyby môže dôjsť k vzdialenému vykonaniu kódu neautentifikovaným útočníkom.

Kritická zraniteľnosť produktu VMware vCenter Server

Zraniteľnosť sa nachádza na serveri VMware vCenter Server. Chyba existuje z dôvodu nedostatočného overenia vstupu v doplnku vSAN Health Check, ktorý je predvolene povolený na serveri vCenter. Zraniteľnosť je možné zneužiť, ak je na serveri dostupný port 443. Potenciálny útočník so sieťovým prístupom na port 443 by mohol vykonávať ľubovoľné príkazy s neobmedzenými oprávneniami v základnom hostiteľskom operačnom systéme, ktorý je hostiteľom servera vCenter. Zároveň aktualizácia rieši aj zraniteľnosť v mechanizme autentifikácie niekoľkých doplnkov servera.

Mesačník zraniteľností Máj 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 Flash Player, Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
    - QNAP NAS – celosvetovo zneužívané zraniteľnosti sieťových úložísk
    - V softvéri Cisco SD-WAN vManage bolo opravených 5 zraniteľností
    - Spoločnosť Cisco opravila 2 zraniteľnosti v softvéri HyperFlex HX
    - F5 Networks – zariadenia BIG-IP obsahujú závažnú bezpečnostnú zraniteľnosť
    - Spoločnosť Dell opravuje závažnú zraniteľnosť, ktorá postihuje milióny zariadení
    - Microsoft opravil 55 zraniteľností, z toho 3 zero-day
    - Vo VMware vRealize Business for Cloud sa vyskytuje kritická zraniteľnosť
    - Kritická zraniteľnosť produktu VMware vCenter Server

https://www.csirt.gov.sk/wp-content/uploads/2021/06/2021_05_mesacnik.pdf?csrt=3761693077297449191