MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Marec 2022

Vypracoval: CSIRT.SK

TLP: White

V mesiaci marec bola vo veľkej miere aktívna skupina útočníkov, ktorá je známa pod názvom LAPSUS$. Predmetná skupina vykonávala rôzne útoky voči organizáciám vrátane spoločnosti NVIDIA, Samsung, Octa, Microsoft a Ministerstvo zdravotníctva v Brazílii. LAPSUS$ získava citlivé údaje z IT systémov a následne sa vyhráža ich zverejnením. Skupina bola prvýkrát spozorovaná v decembri roku 2021, pričom sa vo všeobecnosti zameriava na veľké vládne a komerčné organizácie pôsobiace v telekomunikačnom, hardvérovom sektore alebo hernom priemysle.

Jedným z veľkých útokov uvedenej skupiny bola kompromitácia spoločnosti NVIDIA. Ukradnutých bolo viac ako 71-tisíc prihlasovacích údajov zamestnancov. Medzi uniknuté údaje patria e-mailové adresy a NTLM hashe hesiel, z ktorých mnohé boli prelomené. Skupina sa vyhrážala napadnutej spoločnosti únikom informácií o hardvérových špecifikáciách. Spoločnosť sa na margo vyhlásení útočníkov vyjadrila, že nenašla žiadne dôkazy o útoku ransomvéru.

Ďalší z radu útokov zamerala skupina na spoločnosť Samsung. Skupina ukradla približne 190GB údajov a zverejnila ich prostredníctvom internetového protokolu Torrent, ktorý funguje na báze siete s vzájomným sprístupňovaním. Uniknuté údaje útočníci rozdelili do 3 archívov s vágnym popisom,. Prvý má obsahovať zdrojový kód a údaje k rôznym položkám. Druhý obsahuje okrem údajov aj zdrojový kód a údaje súvisiace so zabezpečením a šifrovaním zariadenia. Posledný archív obsahuje rôzne repozitáre z GitHubu. Spoločnosť Samsung potvrdila, že útočníci získali prístup do systémov a tiež prístup k zdrojovému kódu používaného v smartfónoch Galaxy.

Obeťou tejto skupiny sa stal aj argentínsky gigant elektronického obchodu MercadoLibre. Útočníci tvrdia, že získali prístup k 24-tisíc repozitárov zdrojového kódu MercadoLibre a Mercado Pago. Telegramový kanál prevádzkovaný spoločnosťou Lapsus$ zverejnil 7. marca prieskum, v ktorom používateľov žiadal, aby hlasovali za spoločnosť, ktorej údaje by mali útočníci zverejniť ako ďalšie. Medzi potenciálnymi obeťami boli tiež spoločnosti Impresa a Vodafone. Skupiny ako LAPSUS$ na rozdiel od šifrovania dôverných súborov, kradnú a uchovávajú údaje, ktoré následne zverejňujú v prípade, že nie sú splnené ich požiadavky.

Veľký dopad mal útok na spoločnosť Okta, ktorá je poskytovateľom autentifikačných služieb a riešení správy identity a prístupu (Identity and access management – IAM). Skupina získala prístup k backendovým administratívnym konzolám a údajom o zákazníkoch. Spoločnosť tvrdí, že identifikovala pokus o kompromitáciu účtu zákazníckej podpory už v januári tohto roku. Na základe vyšetrovania však neexistujú žiadne ďalšie dôkazy, ktoré by naznačovali škodlivú aktivitu po tomto incidente.

Spoločnosť Microsoft taktiež potvrdila, že jeden z účtov jej zamestnancov bol kompromitovaný, čo umožnilo útočníkom nahliadnuť k časti zdrojového kódu a ukradnúť ho. Skupina zverejnila 37GB zdrojového kódu ukradnutého zo servera Azure DevOps. Hoci Microsoft nezverejnil, ako bol účet napadnutý, poskytol všeobecný prehľad o taktikách, technikách a postupoch (TTP) skupiny LAPSUS$ pozorovaných pri viacerých útokoch. Spoločnosť Microsoft odporúča posilniť implementáciu

viacfaktorovej autentifikácie, využiť moderné autentifikačné možnosti pre VPN siete, posilniť a monitorovať zabezpečenie cloudových úložísk a tiež zvyšovať bezpečnostné povedomie ohľadom útokov prostredníctvom sociálneho inžinierstva.

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci marec riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitácie e-mailového konta. Jednotka riešila prípad rozsiahlej spear-phishingovej kampane spojenej s únikom legitímnej komunikácie medzi viacerými organizáciami v konštituencii CSIRT.SK, aj súkromných spoločností. O phishingovej kampani jednotka CSIRT.SK informovala aj na svojej webovej stránke. Jednotka začala preverovať pravdepodobné miesta úniku. Podľa zistení útočníci okrem iného zneužívali zraniteľnosti mailserverov Microsoft Exchange (CVE-2021-26855, ProxyLogon) pre kompromitáciu mailservera a získanie obsahu komunikácie na ňom uloženej. Následne podvodnú správu s odkazom na škodlivý súbor priložili do vlákna ako odpoveď na túto komunikáciu a posielali ju pôvodným adresátom. Týmto spôsobom získali phishingové správy vyššiu dôveryhodnosť.

Negatívne dôsledky kybernetických útokov súvisiacich s vojnou na Ukrajine dopadli aj na územie Slovenskej republiky. Malvér, ktorý poškodil telekomunikačné zariadenia Viasat na Ukrajine a paralyzoval komunikáciu vyše 5000 nemeckých veterných turbín, spôsobil zákazníkom spoločnosti Softel výpadok satelitného internetového pripojenia. Zasiahnutých výpadkom bolo aj niekoľko slovenských obcí.

V rámci svojej proaktívnej činnosti jednotka zdieľala so svojou konštituenciou indikátory kompromitácie malvéru Trickbot a informácie o oprave kritických a závažných zraniteľností produktov spoločnosti Microsoft. Informovala o modeloch routerov Asus, zneužívaných APT skupinou Sandworm pre operáciu botnetu Cyclops Blink. Jednotka CSIRT.SK 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

V obchode Google Play bol nájdený nový bankový malvér SharkBot

Bankový malvér SharkBot sa vydával za antivírusové riešenie s možnosťou prečistenia systému. Nájdený bol v obchode Google Play. Medzi najnovšie funkcie malvéru patria injekcie, keylogging, zachytávanie SMS správ a tiež vzdialené ovládanie zariadenia. SharkBot zneužíva povolenia „Accessibility“ a následne si podľa potreby udelí ďalšie povolenia. Malvér taktiež prijíma príkazy z riadiaceho servera na vykonanie rôznych akcií, ako napríklad poslanie SMS správy na konkrétne číslo, zakázanie optimalizácie batérie, stiahnutie súboru a ďalšie.

Spoločnosti Rompetrol sa útočníci vyhrážajú zverejnením ukradnutých údajov

Sieť čerpacích staníc Rompetrol sa stala obeťou útoku ransomvéru Hive. Dcérska spoločnosť KMG International, ktorá pôsobí v 15 rôznych krajinách ohlásila, že bojuje s komplexným kybernetickým útokom. Útočníci žiadajú výkupné vo výške 2 milióny dolárov, pričom sa vyhrážajú zverejnením ukradnutých údajov. Webové stránky KMG a Rompetrol a aplikácia Fill&Go boli po útoku nedostupné. Spoločnosť uviedla, že útok zasiahol väčšinu IT služieb. O skupine Hive je známe, že využíva rôznorodý súbor taktík, techník a postupov, čo organizáciám sťažuje obranu pred jej útokmi.

Trójsky kôň Aberebot sa vracia pod názvom Escobar obohatený o nové funkcie

Bankový trójsky kôň pre Android s názvom Aberebot sa vrátil pod názvom Escobar s novými funkciami. Malvér je schopný ukradnúť viacfaktorové overovacie kódy z aplikácie Google Authenticator. Medzi ďalšie nové funkcie patrí prevzatie kontroly nad zariadením prostredníctvom VNC, nahrávanie zvuku, fotografovanie a ďalšie. Hlavným cieľom trójskeho koňa

Escobar je ukradnúť údaje, vďaka ktorým by útočníci boli schopní prevziať kontrolu nad bankovými účtami, získať dostupné zostatky a vykonávať neautorizované transakcie.

Spoločnosti DENSO údajne unikli údaje o veľkosti 1,4TB

Spoločnosť DENSO, ktorá dodáva automobilové komponenty značkám ako Toyota, Mercedes-Benz, Ford či Honda, sa stala obeťou kybernetického útoku. Útočníci napadli podnikovú sieť v Nemecku, pričom spoločnosť zareagovala ihneď a útočníkov odrezala od zvyšku sieťových zariadení. Kým spoločnosť uvádza, že útok nespôsobil škody, útočníci stojaci za ransomvérom Pandora tvrdia, že ukradli údaje o veľkosti 1,4TB. Medzi ukradnuté údaje patria informácie o objednávkach, technické schémy, zmluvy o mlčanlivosti a ďalšie. Ransomvér Pandora je nová operácia, ktorá bola spustená v marci tohto roku.

Malvér Serpent sa zameral na francúzske organizácie

Francúzske organizácie sa stali terčom nových zadných vrátok s názvom Serpent. Serpent je nasadený ako skript v programovacom jazyku Python a umožňuje útočníkom vzdialene ovládať infikované systémy, exfiltrovať údaje, sťahovať a spúšťať ďalšie nástroje. Bezpečnostná spoločnosť Proofpoint odhalila použitie Chocolatey na inštaláciu zadných vrátok a ďalších nástrojov na vykonanie prieniku do systému. Útoky sa začínajú phishingovými e-mailami, ktoré obsahujú ako prílohu wordovský dokument s makrami. Útočníci využívajú v e-mailoch tému GDPR.

Ransomvér Conti zaútočil na platformu Shutterfly

Platforma Shutterfly sa stala obeťou útoku ransomvéru Conti. Sieť bola kompromitovaná v decembri roku 2021. Útočník znefunkčnil niektoré systémy a získal prístup k niektorým údajom v predmetných systémoch. Ukradnuté dokumenty mohli obsahovať osobné

informácie ako mená, informácie o platoch a odmeňovaní a ďalšie. Na internete sa vyskytli vzorky údajov ukradnutých zo služby Shutterfly, ktoré obsahovali dokonca aj právne zmluvy, informácie o bankovom a obchodnom účte a iné. Skupina stojaca za ransomvérom od útoku zverejnila približne 7GB údajov.

Mars Stealer je nový variant malvéru na kradnutie informácií

Malvér Mars Stealer sa objavil ako redizajn malvéru Oski. Jedná sa o novo spustený variant malvéru na exfiltráciu informácií. Malvér využíva Google Ads na udelenie vysokého hodnotenia klonovaným škodlivým stránkam pre OpenOffice vo výsledkoch vyhľadávania v Kanade. Inštalačný súbor pre OpenOffice je v skutočnosti Mars Stealer, ktorý je vybavený šifrovačom Babadeda alebo zavádzačom Autoit. Medzi kradnuté informácie patria údaje o automatickom dopĺňaní prehliadača, údaje o rozšíreniach prehliadača, kreditné karty, IP adresu, kód krajiny a časové pásmo.

Spoločnosť Adafruit zistila, že na GitHube sa nachádza verejne dostupný repozitár obsahujúci citlivé údaje

Spoločnosť Adafruit zistila, že na GitHube sa nachádza verejne dostupný repozitár, ktorý obsahuje citlivé údaje o používateľských účtoch. Spoločnosť sa obáva, že mohlo dôjsť k neoprávnenému prístupu k predmetným údajom. Verejne dostupný súbor obsahoval informácie ako mená, emailové adresy, fakturačné adresy, detaily objednávok a stav zadania objednávok. K potenciálnemu úniku údajov došlo z úložiska bývalého zamestnanca spoločnosti. Spoločnosť si nie je vedomá zneužitia vystavených údajov. Používatelia, ktorých sa potenciálny únik mohol dotknúť, by mali zostať ostražití pred phishingovými útokmi, ktoré môžu dané informácie zneužívať.

V obchode Google Play pre Android sa vyskytuje bankový trójsky kôň TeaBot

V obchode Google Play sa opäť objavil bankový trójsky kôň TeaBot. Vystupoval tam ako aplikácia s názvom „QR Code & Barcode – Scanner“ a infikoval viac ako 10-tisíc zariadení. Aplikácia sa javila ako legitímna pomôcka na skenovanie QR kódov. Po nainštalovaní si aplikácia vyžiada aktualizáciu prostredníctvom kontextovej správy, pričom aktualizácia sa stiahne z externého zdroja. Spoločnosť Cleafy vystopovala zdroj sťahovania aktualizácií – 2 úložiská na GitHube patriace používateľovi „feleanicusor“.

Na Ukrajine vyčíňa nový malvér CaddyWiper

Bezpečnostní výskumníci objavili nový malvér zameraný na ukrajinské organizácie. Malvér CaddyWiper odstraňuje údaje zo zariadení v napadnutých sieťach. CaddyWiper je navrhnutý na mazanie údajov v doménach Windows, avšak ak sa jedná o radič domény, údaje sa nevymažú. Pravdepodobne sa jedná o taktiku, ktorá slúži na udržanie prístupu do sietí organizácií. Malvér bol nasadený v rámci útokov v ten istý deň, ako bol skompilovaný. CaddyWiper je štvrtý malvér na mazanie údajov nasadený pri útokoch na Ukrajinu od začiatku roku 2022.

- **Monongalia Health System sa stal obeťou útoku, ktorý mohol viesť k odcudzeniu údajov.**
- **Spoločnosť Avast zverejnila bezplatný dešifrovač pre obete ransomvéru HermeticRansom.**
- **Skupina pre analýzu hrozieb spoločnosti Google varovala viacerých používateľov Gmailu, že sa stali terčom phishingových útokov skupiny APT31.**
- **Malvér BazarBackdoor sa šíri prostredníctvom kontaktných formulárov na webových stránkach.**

- **Útočníci stojaci za ransomvérom LockBit zaútočili na spoločnosť Bridgestone Americas.**
- **Poskytovatelia zdravotníckych služieb v Alabame a Colorade sa stali obeťami kybernetického útoku. Útok ovplyvnil viac ako 500-tisíc pacientov.**
- **Nesprávne nakonfigurované databázy Firebase odhalili údaje v tisícoch mobilných aplikácií.**
- **Skupina útočníkov DarkHotel sa zameriava na luxusné hotely v Macau v Číne.**
- **TransUnion South Africa zverejnila, že útočníci narušili jeden z ich serverov pomocou ukradnutých prihlasovacích údajov.**
- **FBI a ministerstvo financií varovali organizácie v Spojených štátoch pred útokmi ransomvéru AvosLocker.**
- **Bezpečnostný výskumník z Ukrajiny odhalil nový zdrojový kód malvéru z operácie ransomvéru Conti.**
- **V obchode Google Play sa nachádza škodlivá aplikácia, ktorá kradne prihlasovacie údaje k Facebooku.**
- **Spoločnosť ELTA, štátny poskytovateľ poštových služieb v Grécku, sa stala obeťou útoku ransomvéru.**
- **Viac ako 200 škodlivých npm balíčkov sa zameriava na vývojárov Azure.**
- **Malvér Vidar sa objavil v novej phishingovej kampani, ktorá zneužíva súbory pomocníka Microsoft HTML.**
- **Chyba áut značky Honda umožňuje útočníkom odomknúť a naštartovať auto pomocou „replay“ útoku.**
- **Útočníci stojaci za malvérom Purple Fox využívajú vo svojich útokoch FatalRAT.**
- **Spoločnosť Microsoft uviedla, že ukrajinské siete boli napadnuté malvérom, ktorý pomenovali FoxBlade.**
- **Twitterový účet Reality Winnerovej napadli útočníci, pričom sa zamerali na novinárov v prominentných mediálnych organizáciách.**

Závažné zraniteľnosti bežných softvérových produktov

Zero-day zraniteľnosti produktov Mozilla

Spoločnosť Mozilla opravila dve zero-day zraniteľnosti, ktoré sa týkali vybraných produktov. Zraniteľnosti sú vysokej závažnosti s CVSS skóre 8.4.

Kritické zraniteľnosti produktov Veeam

Spoločnosť Veeam vydala aktualizácie svojich produktov Veeam Backup & Replication, ktoré opravujú štyri novoobjavené zraniteľnosti. Tieto zraniteľnosti by mohli byť zneužité na kompromitáciu podnikovej infraštruktúry. Opravy boli vydané pre verzie Veeam Backup & Replication 10 a 11. Spoločnosť Veeam odporúča používateľom starších verzií produktov migráciu na podporované verzie.

Kritické zraniteľnosti tlačiarní HP umožňujú vzdialene vykonávať kód

Spoločnosť Hewlett Packard vydala opravné aktualizácie pre stovky modelov tlačiarní a multifunkčných zariadení, v ktorých bolo objavených niekoľko kritických zraniteľností. Tieto chyby umožňujú vzdialené vykonávanie kódu, spôsobenie nedostupnosti systému a únik informácií.

Zraniteľnosť služby Redis

V službe Redis pre distribúcie Linux rodiny Debian bola nájdená kritická zraniteľnosť s CVSSv3 skóre 10. Zraniteľnosť umožňuje vzdialene vykonávať kód a zneužíva ju botnet Muhstik.

TLP: White

Kritické zraniteľnosti Cisco

V produktoch Cisco boli opravené 3 kritické a viacero závažných zraniteľností.

CVE-2022-20754: Zraniteľnosť v klastrovom databázovom rozhraní API Cisco Expressway Series a Cisco TelePresence VCS by mohla umožniť overenému vzdialenému útočníkovi s oprávneniami na čítanie/zápis do aplikácie vykonávať útoky prechodom cez adresár a prepisovať súbory v operačnom systéme ako root.

CVE-2022-20755: Zraniteľnosť vo webovom rozhraní správy zariadení Cisco Expressway Series a Cisco TelePresence VCS by mohla umožniť overenému vzdialenému útočníkovi s oprávneniami na čítanie/zápis do aplikácie vykonať ľubovoľný kód v operačnom systéme ako root.

CVE-2021-1577: Zraniteľnosť v koncovom bode API Cisco Application Policy Infrastructure Controller (APIC) a Cisco Cloud Application Policy Infrastructure Controller (Cloud APIC) by mohla umožniť neoverenému vzdialenému útočníkovi čítať alebo zapisovať do ľubovoľných súborov.

Mesačník zraniteľností Marec 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 závažné zraniteľnosti
    - Zero-day zraniteľnosti produktov Mozilla
    - Kritické zraniteľnosti produktov Veeam
    - Kritické zraniteľnosti tlačiarní HP umožňujú vzdialene vykonávať kód
    - Zraniteľnosť služby Redis

https://www.csirt.gov.sk/posts/2826.html?csrt=14023307582223161535