MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK
Jún 2024

Vypracoval: CSIRT.SK

TLP: White

Kybernetickým priestorom v júni 2024 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

I. Čínska spoločnosť Funnull vo februári 2024 zakúpila doménu a GitHub účet populárnej webovej knižnice Polyfill.io. Bezpečnostní výskumníci v júni odhalili, že došlo k modifikácii zdrojového kódu knižnice tak, aby do webových stránok vkladala škodlivý kód umožňujúci presmerovanie používateľov a krádež citlivých údajov. Ohrozených bolo vyše 100 000 webových stránok.

II. Ruská ransomvérová skupina Qilin zaútočila na spoločnosť Synnovis, ktorá poskytuje rôzne diagnostické služby londýnskym nemocniciam. Útok mal za následok odloženie chirurgických zákrokov pre tisíce pacientov. Útočníci dodatočne zverejnili aj ukradnuté údaje, ktoré obsahovali citlivé údaje pacientov. Jedná sa o jeden z najzávažnejších incidentov v sektore zdravotníctva za rok 2024.

III. V kategórii incidentov súvisiacich s úspešnými prienikmi do systémov boli zaznamenané aj početné incidenty používateľov cloudovej platformy SNOWFLAKE, medzi ktorými boli aj významné spoločnosti ako napr. Ticketmaster alebo banka Santander. Útočníci zneužili staré, ale stále platné prihlasovacie údaje, čo zdôrazňuje potrebu zabezpečenia prístupov do cloudových platforiem. Používatelia by nemali zabúdať na nasadenie viacfaktorovej autentifikácie, používanie silných hesiel a ich pravidelnú zmenu.

IV. Počas júnových volieb do Európskeho parlamentu boli zaznamenané DDoS útoky, ktorých cieľom bolo zneprístupnenie webových stránok vládnych organizácií a iných významných subjektov v rámci členských štátov Európskej únie. K útokom sa prostredníctvom sociálnych sietí prihlásili prorusky orientované hacktivistické skupiny.

V. Spojené štáty americké zakázali používanie produktov od spoločnosti Kaspersky. Dôvodom sú obavy z väzieb na ruskú vládu a potenciál zneužitia údajov spracovávaných počas činnosti antivírusových riešení, ktoré zbierajú vzorky súborov a telemetriu zariadení. Vzhľadom na dlhodobo napäté vzťahy medzi USA a Ruskom možno tento krok považovať aj za súčasť geopolitického konfliktu týchto štátov.

Riešené incidenty na Slovensku a z našej činnosti

V mesiaci jún, ako súčasť svojich bežných činností sa Vládna jednotka CSIRT zaoberala predovšetkým phishingovými kampaňami, ktoré zasahovali jeho konštituenciu. Objavili sa aj situácie, keď boli e-mailové účty zamestnancov verejných inštitúcií kompromitované a útočníci z nich rozosielali phishingové e-maily na ďalšie organizácie v rámci konštituencie CSIRT.SK. Navyše sme zaznamenali, že prihlasovacie údaje do e-mailových účtov zamestnancov organizácií v rámci konštituencie CSIRT.SK boli na predaj na hackerských fórach.

V júni sa uskutočnila rozsiahla phishingová kampaň, ktorá vychádzala z kompromitovaných e-mailových účtov verejnej organizácie. Kampaň bola aktívna minimálne týždeň a vzhľadom na jej rozsah a cielenie CSIRT.SK rozposlal varovanie organizáciám vo svojej správe.

Jednotka pre kybernetickú bezpečnosť verejnej správy narazila na podvodné webové stránky, ktoré ponúkali investičné príležitosti. Tieto stránky zobrazovali video, ktoré bolo vytvorené pomocou umelej inteligencie a zneužívalo identitu slovenských politikov. Tieto známe tváre tak predstavovali fiktívne investičné príležitosti v spoločnostiach ako Slovnaft, Slovenská sporiteľňa a Orlen, čím sa snažili podvodu dodať ďalšiu dôveryhodnosť.

Aj tento mesiac sa odohral útok typu DDoS na webstránky Ministerstva vnútra SR. Aktér nie je známy. VJ CSIRT zaznamenala aj ďalšie útoky na webové rozhrania. Masívny útok hrubou silou smeroval na e-mailové účty zamestnancov dvoch organizácií v konštituencii CSIRT.SK. Opäť chceme zdôrazniť dôležitosť zabezpečenia administrátorských rozhraní webových služieb, ktoré sú dostupné z internetu, aby sa predišlo neoprávneným pokusom o prihlásenie alebo narušeniu systémov. Najbežnejšie opatrenia zahŕňajú implementáciu viacfaktorovej autentifikácie, skrytie prihlasovacích rozhraní za VPN, obmedzenie prístupu z určitých IP adries alebo úplné zablokovanie prístupu k týmto rozhraniam z internetu, pokiaľ nie je absolútne nevyhnutné, aby boli verejne dostupné.

Vládnej jednotke CSIRT bol nahlásený aj jeden ransomvérový útok na klientsky počítač kamerového systému.

V rámci svojej proaktívnej činnosti VJ CSIRT informovala organizácie vo svojej konštituencii o únikoch e—mailových adries ich zamestnancov, ktoré boli zverejnené v rámci operácie Endgame. Jednotka vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles slúži tiež na monitoring dostupnosti webových domén.

Významné útoky vo svete

FBI s partnermi zaistil vyše 7 000 dešifrovacích kľúčov ransomvéru LOCKBIT



Americký Federálny úrad pre vyšetrovanie FBI informoval, že v rámci medzinárodnej akcie s označením OPERATION CRONOS sa podarilo zaistiť aj vyše 7000 dešifrovacích kľúčov obetí ransomvérovej skupiny LOCKBIT. Orgánom činným v trestnom konaní sa ešte v máji 2024 podarilo získať prístupy k časti infraštruktúry tejto skupiny a odhaliť identitu vodcu skupiny vystupujúceho pod aliasom LOCKBITSUPP. FBI postupne notifikuje obete a zároveň ich vyzýva na nadviazanie kontaktu za účelom dešifrovania zasiahnutých systémov.

Výskumníci demonštrovali postup exfiltrácie citlivých údajov z AI služby Microsoft Recall



Bezpečnostní výskumníci zverejnili proof-of-concept kód pre exfiltráciu údajov z kontroverznej AI služby Recall od spoločnosti Microsoft, ktorá mala byť súčasťou novej generácie počítačov s označením COPILOT+ s plánovaným dátumom vydania na 18. júna 2024. Služba Recall je súčasťou operačného systému Windows 11, ktorá v pravidelných intervaloch vytvára screenshoty obrazovky používateľa a prostredníctvom umelej inteligencie v nich umožňuje vyhľadávanie prostredníctvom textových dopytov. Bezpečnostná komunita ihneď po ohlásení služby vyjadrila pochybnosti so zabezpečením týchto údajov a potenciálnymi zásahmi do súkromia jej používateľov a predpovedala vznik nových útočných vektorov zameriavajúcich sa na exfiltráciu jej údajov. V nadväznosti na komunitnú spätnú väzbu Microsoft vydanie služby Recall odložila na dobu neurčitú.

Detailná analýza malvéru HEADLACE, ktorý používa ruská skupina APT28



Bezpečnostní výskumníci zo spoločnosti RECORDED FUTURE zverejnili detailnú analýzu phishingových kampaní ruskej štátom sponzorovanej skupiny APT28, ktorých cieľom je infekcia zariadení a systémov malvérom HEADLACE a následné získavanie citlivých údajov. Popísané techniky, taktiky a postupy skupiny sú v súlade s nedávno zverejnenou analýzou od CERT.PL a boli

taktiež zaznamenané aj v rámci phishingových kampaní v rámci kybernetického priestoru Slovenskej republiky.

Ransomvérový útok narušil poskytovanie služieb viacerých nemocníc v Londýne



Anglická spoločnosť SYNNOVIS, ktorá poskytuje rôzne diagnostické a laboratórne služby pre viacero nemocníc v Londýne, sa stala obeťou ransomvérového útoku ruskej skupiny QILIN. Nedostupnosť poskytovaných služieb negatívne ovplyvnila aj chod partnerských nemocníc, ktoré museli odložiť vykonávanie niektorých zdravotných úkonov. Zverejnených bolo približne 400 GB dát obsahujúcich citlivé údaje v rozsahu mien pacientov, dátumov narodenia a výsledkov krvných testov.

DDoS útoky proruských skupín počas volieb do Európskeho parlamentu

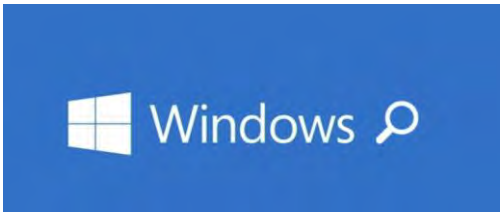


Prorusky orientované hacktivistické skupiny uskutočnili sériu DDoS útokov v súvislosti s voľbami do Európskeho parlamentu. Skupiny zoznam cieľov upravovali na základe štátov, v ktorých sa v daný deň uskutočňovali voľby. Ciele zahŕňali webové stránky organizácií EÚ, vládnych organizácií a politických strán členských štátov a vo viacerých prípadoch aj dopravné spoločnosti. Útoky na viaceré ciele boli úspešné, ale vzhľadom na dlhodobo nízku sofistikovanosť metodiky voľby cieľov nedošlo k relevantnému narušeniu priebehu volieb.

Phishingová kampaň cielená na používateľov platformy GITHUB

Bezpečnostní výskumníci upozornili na phishingové kampane s cieľom získania prístupov do účtov na platforme GITHUB. Útočníci obete kontaktujú prostredníctvom e-mailových správ s tematikou pracovných ponúk a upozornení na udalosti súvisiace so zabezpečením účtov. Webové stránky imitujúce prihlasovacie rozhranie platformy GITHUB umožňujú zber prihlasovacích údajov a priradenie ďalších OAuth aplikácií. Útočníci po získaní prístupu exfiltrujú obsah repozitárov, zmažú ho a následne žiadajú zaplatenie „výkupného“ za obnovu dát. S obeťou komunikujú prostredníctvom aplikácie Telegram.

Sofistikovaná phishingová kampaň zneužívajúca službu Windows Search



Bezpečnostní výskumníci zachytili phishingovú kampaň, v rámci ktorej útočníci na šírenie malvéru zneužívajú funkcionalitu WINDOWS SEARCH. URI protokoly „search-ms:“ a „search:“ aplikáciám umožňujú priamu interakciu so službou vyhľadávania vo Windows Explorer. Služba štandardne vyhľadáva výsledky lokálne na súborovom systéme zariadenia, ale prostredníctvom špecifických parametrov je možné vyvolať aj online hľadanie na externých zdrojoch. Útočníci túto funkciu zneužívajú na stiahnutie súboru BAT, ktorý zariadenia obetí infikuje malvérom. Jedná sa o nový a pomerne zaujímavý mechanizmus infekcie malwarom, ktorý môže byť mimoriadne nebezpečný v prostrediach postavených na platforme Windows.

Početné prieniky do cloudovej platformy SNOWFLAKE



Bezpečnostní experti zo spoločnosti MANDIANT asociujú nedávne početné prieniky do systémov zákazníkov cloudovej platformy SNOWFLAKE s aktivitami finančne motivovanej hackerskej skupiny UNC5537. Útočníci na prienik do systémov zneužívajú uniknuté prihlasovacie údaje získané v rámci predchádzajúcej infekcie systémov obetí rôznymi rodinami malvéru. Nakoľko boli v rámci nedávnych incidentov zneužité platné prihlasovacie údaje ešte z roku 2020, incident zdôrazňuje potrebu pravidelnej zmeny hesiel, nasadenia viacfaktorovej autentifikácie a ďalších metód riadenia prístupu. Spoločnosť SNOWFLAKE v spolupráci so zákazníkmi zavádza povinné viacfaktorové overovanie pri prihlasovaní.

Spoločnosť GOOGLE zakročila voči operáciám Ruska, Číny, Pakistanu a Indonézie



Spoločnosť GOOGLE informovala, že v rámci boja proti zneužívaniu svojej infraštruktúry a služieb zakročila proti vplyvovým operáciám Číny, Ruskej federácie, Pakistanu a Indonézie. V súvislosti s identifikovanými kampaňami došlo k deaktivácii účtov a odstráneniu obsahu na platformách Ads, AdSense, Blogger, YouTube, Google News. Na základe zverejneného štatistického prehľadu sú v oblasti vplyvových operácií a šírenia dezinformácií z dlhodobého hľadiska najaktívnejšie práve Čína a Rusko.

TLP: White

Chyba v ransomvéri skupiny RANSOMHUB pre platformu VMware ESXi

Bezpečnostní výskumníci informovali, že skupina RANSOMHUB poskytujúca službu ransomware-as-a-service okrem verzií svojho ransomvéru pre operačné systémy Windows a Linux (naprogramované v jazyku GO) využíva aj verziu špecializovanú na šifrovanie virtualizovaných prostredí VMWARE ESXI (naprogramovanú v jazyku C++). Verzia pre ESXi podľa výskumníkov obsahuje chybu, ktorú možno využiť na vytvorenie nekonečnej slučky programu a zamedzenie spustenia samotného procesu šifrovania. Vládna jednotka CSIRT priebežne monitoruje aktivity tejto skupiny, pretože je aktívna aj v rámci kybernetického priestoru SR.

Zneužitie zraniteľnosti kryptoplatformy KRAKEN na krádež 3 miliónov dolárov

Platforma na obchodovanie s kryptomenami KRAKEN informovala o odstránení zero-day zraniteľnosti, ktorá používateľom umožňovala navýšenie prostriedkov v rámci peňaženky KRAKEN. Na základe zverejnených informácií sa jednalo o chybu používateľského rozhrania, ktorá sa do produkcie dostala v rámci poslednej aktualizácie a umožňovala nepovolenú manipuláciu s prostriedkami. Bezpečnostní výskumníci zo spoločnosti CERTIK údajne zraniteľnosť zneužili na získanie 3 miliónov dolárov, ktoré odmietli vrátiť. Spoločnosť KRAKEN toto správanie označila za neetické konanie a kontaktovala orgány činné v trestnom konaní.

Americká vláda zakázala používanie produktov spoločnosti KASPERSKY

Americká vláda zakázala využívanie produktov od spoločnosti KASPERSKY, vrátane produktov od jej partnerských a dcérskych spoločností. Rozhodnutie odôvodnili údajným prepojením spoločnosti na ruskú vládu a obavami zo zneužitia ich produktu v rámci kybernetických útokov. Od 20. júla 2024 spoločnosť nebude môcť predávať žiadne produkty občanom USA, bezpečnostné aktualizácie softvéru a detekčných signatúr pre antivírusové riešenia môže poskytovať do 29. septembra 2024. Do tohto dátumu majú všetci aktívni používatelia prejsť na riešenia od iných výrobcov.

Útok cez webovú knižnicu zasiahol vyše 100 000 webových stránok



Bezpečnostní výskumníci informovali o supply chain útoku, v rámci ktorého došlo ku kompromitácii vyše 100 000 webových stránok po celom svete. Útočník zakúpil doménu POLYFILL.IO a modifikoval skripty, aby vykonávali presmerovanie na škodlivé webové stránky. Škodlivá stránka v súčasnosti už nie je dostupná, nakoľko ju doménový registrátor NAMECHEAP deaktivoval. VJ CSIRT spustila kampaň na kontrolu webových stránok v rámci svojej konštituencie a na svojej webovej stránke zverejnila varovanie aj s odporúčaniami ako minimalizovať obdobné hrozby.

Útočníci prenikli do systému CSAT americkej CISA

Americká CISA potvrdila, že v januári 2024 došlo ku kompromitácii systému CSAT (Chemical Security Assesment Tool). Na prienik do systému útočníci zneužili zraniteľnosti v produkte Ivanti Connect Secure, ktoré im umožnili vytvorenie webshellu. Dáta v systéme sú šifrované prostredníctvom šifrovacieho algoritmu AES256, obsahujú informácie o identifikovaných bezpečnostných zraniteľnostiach, programoch fyzickej bezpečnosti a taktiež aj osobné údaje používateľov systému. CISA nepotvrdila, že by došlo aj k exfiltrácii dát, ale používateľom odporučila preventívnu zmenu prihlasovacích údajov.

Ruská APT29 prenikla do interných systémov spoločnosti TEAMVIEWER

Spoločnosť TEAMVIEWER na základe výsledkov vyšetrovania prieniku do svojich interných systémov z júna 2024 vyhlásila, že za útokom stojí ruská štátom sponzorovaná skupina APT29. Na prienik do korporátnej siete útočníci zneužili prihlasovacie údaje zamestnanca spoločnosti, ktoré skupina získala bližšie neuvedeným spôsobom. Incident neohrozil samotných používateľov služby, nakoľko sú korporátne a produkčné systémy spoločnosti striktne oddelené v rámci segmentácie.

- Spoločnosť Microsoft ohlásila postupné ukončenie podpory NTLM autentifikácie a odporučila prechod na bezpečnejšie metódy autentifikácie ako Kerberos a Negotiate.
- Ruskí hackeri kompromitovali systémy poľskej tlačovej agentúry PAP a zverejnili falošné správy o vyhlásení čiastočnej mobilizácie občanov.

TLP: White

- Bezpečnostní výskumníci v rámci analýzy Microsoft Visual Studio Code odhalili vyše 1200 zásuvných modulov, ktoré obsahovali škodlivý kód.
- Kritická bezpečnostná zraniteľnosť v PHP pre Windows je aktívne zneužívaná na šírenie ransomvéru TellYouThePass.
- Čínska hackerská skupina Velvet Ant aktívne zneužíva zraniteľnosti F5 BIG-IP zariadení na získanie prístupu do siete, zaistenie perzistencie a realizáciu ďalších útokov.
- Úspešnosť kampane, v rámci ktorej musí obeť manuálne skopírovať a spustiť PowerShell skript, dokazuje, že človek naďalej zostáva najslabším článkom phishingu.
- Francúzska agentúra pre kybernetickú bezpečnosť ANSSI zverejnila report o aktivitách ruskej APT29 cielených na francúzske subjekty v oblasti diplomacie.
- Americká FBI upozornila pred podvodnými kampaňami, v rámci ktorých útočníci kontaktujú obete krypto podvodov ohľadom vrátenia ukradnutých prostriedkov.
- Štátom sponzorované APT skupiny zameriavajúce sa na kyberšpionáž čoraz častejšie nasadzujú ransomvér za účelom maskovania činnosti a odvedenia pozornosti.
- Ransomvérová skupina Lockbit nesprávne identifikovala obeť svojho útoku, v rámci ktorého došlo k exfiltrácii 33 TB dát americkej banky.
- Hackerské skupiny aktívne zneužívajú open-source malvér Rafel Rat na infekciu mobilných zariadení so zastaranými verziami operačného systému Android.
- Európska únia na svoj sankčný zoznam pridala 6 osôb, ktoré sú asociované s kybernetickými útokmi na kritickú infraštruktúru členských štátov EÚ.
- Holandsko zverejnilo tlačovú správu o činnosti čínskych hackerských skupín, ktoré v rokoch 2022 až 2023 aktívne zneužívali zraniteľnosti na šírenie malvéru Coathanger.

Závažné zraniteľnosti bežných softvérových produktov

Polyfill.io – z bežnej webovej knižnice malvér

Po odkúpení domény Polyfill.io, ktorá poskytuje knižnicu pre webové aplikácie polyfill.js, sa zistilo, že nový majiteľ upravil funkcionalitu skriptu tak, aby presmerovával požívateľov na škodlivé webstránky. Odporúčame prestať danú knižnicu používať, alebo nahradiť jej zdroj dôveryhodným zdrojom.

Aktívne zneužívaná zraniteľnosť umožňuje získanie obsahu súborov zo SolarWinds Serv-U

Spoločnosť SolarWinds vydala bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú zraniteľnosť v platforme na prenos súborov Serv-U. Zraniteľnosť umožňujúcu prechádzanie adresárov možno zneužiť na čítanie obsahu súborov na hostiteľskom systéme.

Kritické bezpečnostné zraniteľnosti vo VMware vCenter Server

Spoločnosť BROADCOM vydala bezpečnostné aktualizácie, ktoré opravujú 3 bezpečnostné zraniteľnosti v produkte VMware vCenter Server. Z nich 2 sú označené ako kritické. Zraniteľnosti možno zneužiť na eskaláciu privilégií a vzdialené vykonanie kódu.

Kritická zraniteľnosť PHP zneužívaná na šírenie ransomvéru

Vývojári skriptovacieho jazyka PHP vydali bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť. Chyba súvisí s konverziou kódovania znakov cez funkciu Windows Best-Fit a prostredníctvom injekcie príkazov ju možno zneužiť na vzdialené vykonanie kódu. Zraniteľnosť je v súčasnosti aktívne zneužívaná na šírenie ransomvéru TellYouThePass.

Microsoft v rámci júnového Patch Tuesday opravil kritickú zraniteľnosť v MSMQ

Spoločnosť Microsoft vydala v júni 2024 balík opráv pre portfólio svojich produktov opravujúci 51 zraniteľností, z ktorých 18 umožňuje vzdialené vykonávanie kódu. Kritická bezpečnostná zraniteľnosť sa nachádza v produkte Microsoft Message Queuing.

TLP: White

Zraniteľnosti v produktoch Veeam

Spoločnosť Veeam vydala bezpečnostné aktualizácie na svoje produkty Backup & Replication, Agent for Windows a Service Provider Console, ktoré opravujú viacero zraniteľností umožňujúcich obchádzanie bezpečnostných prvkov, eskaláciu privilégií alebo vzdialené vykonanie kódu.

Grafické procesory ARM Mali majú aktívne zneužívanú zraniteľnosť



Aktívne zneužívaná zraniteľnosť ovládača grafických procesorov ARM Mali Valhall a Bifrost umožňuje lokálnemu útočníkovi bez oprávnení získať prístup k dealokovanej pamäti. Zraniteľnosť možno zneužiť na vykonanie kódu alebo získanie neoprávneného prístupu k citlivým údajom.

Mesačník zraniteľností Jún 2024

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
   - Polyfill.io, BootCDN, Bootcss, Staticfile
   - SolarWinds Serv-U
   - VMware vCenter Server
   - PHP pre Windows
   - Microsoft Azure, 365 Apps for Enterprise, Authentication Library, Dynamics 365, Office, Outlook, SharePoint, Visual Studio, Windows, Windows Server
   - Veeam Backup & Replication, Veeam Agent for Windows, Veeam Service Provider Console
   - Bifrost GPU Kernel Driver, Valhall GPU Kernel Driver

https://www.csirt.gov.sk/posts/1084.html