Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

End of Week

vrijdag 7 juni 2024

Toegestane verspreiding: TLP:GREEN
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:GREEN en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Voor u ligt de End Of Week van week 23, vandaag mag ook de dag zijn dat Tetris al 40 jaar bestaat, laten wij op deze heugelijke dag stil staan bij de nieuwsberichten van afgelopen week.

We nemen u in deze End Of Week mee door de nieuwsberichten van de afgelopen week.

Inloggegevens meerdere klanten van Cloud opslag bedrijf Snowflake aangeboden

Vorige week maakte we al melding van een mogelijk datalek bij Ticketmaster waarbij 560 miljoen klantgegevens worden aangeboden. Deze week komen daar nog een aantal andere bedrijven bij en is duidelijk geworden dat het om klanten van het cloud opslag bedrijf Snowflake gaat. Hierdoor werd er in eerste instantie vanuit gegaan dat het om een lek bij Snowflake zelf ging, maar er zijn nu steeds meer aanwijzingen dat de inloggegevens van de klanten van Snowflake zijn buitgemaakt met behulp van zogenaamde infostealer malware. Zo ontdekte journalisten van TechCrunch deze week enkele honderden login gegevens die mogelijk van klanten van Snowflake zijn. [1]

Nederland zal NIS2-richtlijn jaar te laat invoeren: 'versnellen kan niet'

Nederland zal de Europese beveiligingsrichtlijn NIS2 een jaar te laat invoeren, met een verwachte inwerkingtreding in het tweede of derde kwartaal van 2025. Deze richtlijn, een herziening van de NIS-richtlijn uit 2016, beoogt betere implementatie en aanpassing aan nieuwe ontwikkelingen in cyberbeveiliging. Door de NIS2 wordt samenwerking en informatie-uitwisseling tussen EU-landen verbeterd, en een Europese kwetsbaarheidsdatabase opgezet. Minister Yesilgöz gaf aan dat versnellen niet mogelijk is, ondanks kritiek vanuit de Tweede Kamer. De vertraging werd besproken tijdens een debat over de nationale weerbaarheid tegen buitenlandse dreigingen. Yesilgöz benadrukte de complexiteit van de wet en wees op de inspanningen die al zijn geleverd. Ook andere landen zoals Frankrijk en Duitsland hebben de richtlijn nog niet uitgewerkt.[2]

---

[1] https://techcrunch.com/2024/06/05/snowflake-customer-passwords-found-online-infostealing-malware/?guccounter=1

[2] https://www.security.nl/posting/844067/Nederland+zal+NIS2-richtlijn+jaar+te+laat+invoeren%3A+%27versnellen+kan+niet%27

PostNL introduceert antiphishingcode voor e-mails

PostNL introduceert een antiphishingcode voor e-mailcommunicatie, waarmee klanten kunnen controleren of een mail daadwerkelijk van PostNL afkomstig is. Klanten kunnen via hun PostNL-account zelf een antiphishingcode instellen. Deze code, een woord of korte zin van maximaal twintig tekens, verschijnt bovenaan elke legitieme e-mail van PostNL na activatie. Het kan tot 24 uur duren voordat de code in e-mails verschijnt. Deze maatregel is bedoeld om cybercriminaliteit tegen te gaan en de echtheid van e-mails te waarborgen. Het concept van antiphishingcodes wordt al door meerdere grote cryptoplatformen gebruikt.[3]

Nieuwe V3B-phishingkit richt zich op klanten van 54 Europese banken

Cybercriminelen promoten een nieuwe phishingkit genaamd 'V3B' op Telegram, gericht op klanten van 54 grote financiële instellingen in landen als Ierland, Nederland, en Duitsland. De kit kost tussen $130 en $450 per maand en biedt geavanceerde functies zoals obfuscatie, lokalisatie-opties, en ondersteuning voor 2FA en OTP. Volgens onderzoekers van Resecurity heeft het Telegram-kanaal van V3B al meer dan 1.250 leden. De kit bevat professioneel vertaalde pagina's en kan zowel bankgegevens als creditcardgegevens onderscheppen. Het admin paneel stelt fraudeurs in staat om via een chatsysteem in real-time interactie met slachtoffers te hebben en OTP's te verkrijgen. Gestolen informatie wordt via de Telegram API naar de criminelen verzonden. Een opvallende functie is QR code login jacking, die gebruikmaakt van bekende inlogmethoden om legitimiteit te simuleren. V3B ondersteunt ook PhotoTAN en Smart ID om geavanceerde authenticatietechnologieën te omzeilen. Phishingkits zoals V3B maken het voor minder ervaren criminelen mogelijk om zeer schadelijke aanvallen uit te voeren. Onlangs werd een van de grootste PhaaS-operaties, LabHost, ontmanteld door de autoriteiten, waarbij 37 mensen werden gearresteerd.[4]

Club Penguin-fans braken in op Disney's Confluence-server en stalen 2,5 GB aan gegevens

Club Penguin-fans hebben een Disney Confluence-server gehackt om informatie over hun favoriete spel te stelen, maar hebben per ongeluk 2,5 GB aan interne bedrijfsgegevens bemachtigd. Club Penguin was een MMO-spel van 2005 tot 2018, oorspronkelijk gemaakt door New Horizon Interactive en later gekocht door Disney. Ondanks de sluiting in 2017 en 2018, leven privéservers van het spel voort, beheerd door fans en onafhankelijke ontwikkelaars. Op 4Chan werd een link gedeeld naar een 415 MB groot archief met 137 PDF's met interne informatie over Club Penguin. Deze gegevens zijn meer dan zeven jaar oud en interessant voor fans van het spel.
De gehackte gegevens omvatten echter veel meer dan alleen Club Penguin-documentatie. De hackers hebben 2,5 GB aan data over Disney's bedrijfsstrategieën, advertentieplannen, Disney+, interne ontwikkeltools, zakelijke projecten en infrastructuur gestolen. Een bron meldde dat deze informatie oorspronkelijk werd gezocht om Club Penguin-gegevens te vinden, maar

[3] https://tweakers.net/nieuws/222766/postnl-introduceert-antiphishingcode-voor-e-mails.html

[4] https://www.bleepingcomputer.com/news/security/new-v3b-phishing-kit-targets-customers-of-54-european-banks/

leidde tot een breder scala aan gevoelige informatie. Disney's interne ontwikkeltools, Helios en Communicore, werden onthuld in de documenten. Hoewel het Club Penguin-materiaal oud is, bevat de rest van de gegevens recente informatie, waaronder gegevens van 2024. Disney heeft nog niet gereageerd op verzoeken om commentaar.[5]

De websites van CDA, PVV en FVD zijn donderdag een tijdje niet of slechter bereikbaar geweest vanwege ddos-aanvallen. Russische hackers van de groep HackNet hebben de aanval op Telegram opgeëist.

Bij een DDoS-aanval sturen hackers zoveel verkeer naar een website dat deze niet meer bereikbaar is. Dit gebeurde donderdagochtend bij Nederlandse politieke partijen, maar de aanvallen zijn inmiddels afgeslagen en de websites zijn weer bereikbaar. De groep HackNet, actief vanuit Rusland, claimde de verantwoordelijkheid op Telegram en dreigde door te gaan met aanvallen op Nederlandse websites. Cybersecurityexpert Dave Maasland van ESET benadrukt dat DDoS-aanvallen vooral bedoeld zijn om twijfel en angst te zaaien in de samenleving, ondanks dat ze vaak weinig daadwerkelijke schade aanrichten. Het creëren van een gevoel van onbehagen is precies wat de aanvallers willen bereiken, zodat mensen uit angst gaan handelen.[6]

[5] https://www.bleepingcomputer.com/news/security/club-penguin-fans-breached-disney-confluence-server-stole-25gb-of-data/

[6] https://www.nu.nl/tech/6315777/hackers-leggen-websites-politieke-partijen-plat-op-dag-van-europese-verkiezingen.html?referrer=https%3A%2F%2Ftaranis.arp.ncsc.nl%2F

Beveiligingsadviezen

Zie voor een actueel overzicht: https://advisories.ncsc.nl/advisories

NCSC-2024-0241 [v1.00][M/H]	Kwetsbaarheden verholpen in FortiNet FortiWebManager
NCSC-2024-0240 [v1.00][M/H]	Kwetsbaarheden verholpen in Google Android en Samsung Mobile
NCSC-2024-0239 [v1.00][M/H]	Kwetsbaarheden verholpen in Solarwinds Platform

Wat was er nog meer in het nieuws

Russische misdaadgroep verantwoordelijk voor cyberaanval op Londense ziekenhuizen, zegt expert

Een cybercriminele groep genaamd Qilin wordt verantwoordelijk gehouden voor een ransomware-aanval op belangrijke ziekenhuizen in Londen, waardoor operaties en tests werden stopgezet. De aanval op Synnovis, een pathologiedienstenbedrijf, veroorzaakte een ernstige verstoring van de capaciteit. Qilin staat bekend als een ransomware-as-a-service groep die malware verhuurt aan andere criminelen en de doelwitten selecteert. Het gemiddelde losgeldbedrag voor ransomware is het afgelopen jaar met 500% gestegen tot $2 miljoen, met onderzoek naar de impact van de cyberaanval door de Britse National Cyber Security Centre en NHS-functionarissen.[7]

Oekraïne vermoed dat hackers SyncThing-tool misbruiken om gegevens te stelen

Het Computer Emergency Response Team van Oekraïne (CERT-UA) heeft een nieuwe campagne genaamd "SickSync" gerapporteerd, gelanceerd door de UAC-0020 (Vermin) hackergroep tegen de Oekraïense strijdkrachten. Vermin maakt gebruik van de legitieme bestandssynchronisatiesoftware SyncThing in combinatie met malware genaamd SPECTR om gevoelige informatie te stelen. De aanval begint met een phishing-e-mail die een RARSFX-archief bevat met een wachtwoordbeveiligd bestand genaamd "turrel.fop.wolf.rar." De malware, inclusief SPECTR, wordt uitgevoerd bij het openen van het bestand, waardoor gegevens worden gestolen en overgedragen naar de aanvaller. CERT-UA waarschuwt dat interactie met SyncThing's infrastructuur een indicatie kan zijn van een compromis en adviseert onderzoek om infecties op te sporen en te elimineren.[8]

Ransomhub Gang claimd de hack van de telecommunicatiegigant Frontier Communications

De RansomHub ransomware-groep beweert de gegevens van meer dan 2 miljoen klanten van het Amerikaanse telecombedrijf Frontier Communications te hebben gestolen. De gestolen gegevens, in totaal 5 GB, omvatten namen, e-mailadressen, burgerservicenummers, credit scores, geboortedata en telefoonnummers. Ondanks een twee maanden durende waarschuwing van de groep, heeft Frontier Communications volgens hen geen actie ondernomen om de klantgegevens te beschermen. De groep dreigt de gestolen gegevens te publiceren als er binnen negen dagen geen losgeld wordt betaald, na een vergelijkbare aanval op veilinghuis Christie's waarbij gegevens van minstens 500.000 klanten werden blootgesteld.[9]

Zyxel brengt noodpatch uit voor kritiek lek in end-of-life NAS-systemen

Zyxel heeft een noodpatch uitgebracht voor

[7] https://www.theguardian.com/technology/article/2024/jun/05/russian-group-behind-london-hospitals-cyber-attack-says-expert

[8] https://www.bleepingcomputer.com/news/security/ukraine-says-hackers-abuse-syncthing-tool-to-steal-data/

[9] https://securityaffairs.com/164126/data-breach/ransomhub-gang-hacked-frontier-communications.html

kritieke kwetsbaarheden in de niet-ondersteunde NAS326 en NAS542 systemen, waardoor aanvallers de apparaten op afstand kunnen overnemen, inclusief een backdoor-account. Vijf kwetsbaarheden werden ontdekt door onderzoekers van Outpost24, waarvan drie het uitvoeren van commando's of code door een ongeauthenticeerde aanvaller mogelijk maken. Het beveiligingslek CVE-2024-29972 betreft een backdoor-account dat door een aanvaller op afstand kan worden ingeschakeld, waarvan het wachtwoord uniek is maar kan worden afgeleid uit het MAC-adres. Zyxel adviseert gebruikers om de beschikbare firmware-updates te installeren om deze kwetsbaarheden te verhelpen.[10]

Bugs in Cisco Webex Meetings gebruikt voor ongeautoriseerde toegang

Cisco heeft aangekondigd dat verschillende bugs in Cisco Webex Meetings zijn gebruikt voor ongeautoriseerde toegang tot meeting-informatie en metadata van bepaalde klanten in een datacenter in Frankfurt. Deze problemen zijn inmiddels opgelost en een fix is wereldwijd uitgerold op 28 mei. Cisco heeft geen specifieke details verstrekt over de bugs of het 'gerichte beveiligingsonderzoek' dat werd genoemd in de security-advisory. Klanten waarbij er pogingen waren om toegang te krijgen tot hun meeting-informatie zijn ingelicht, en sinds de patches zijn toegepast, zijn er geen verdere inbreuken waargenomen.[11]

UWV eerder dit jaar getroffen door inbraak op commercieel videoplatform

Het UWV is eerder dit jaar slachtoffer geworden van een inbraak op een commercieel videoplatform dat het gebruikt voor videogesprekken met cliënten in het buitenland, volgens de Stand van uitvoering sociale zekerheid juni 2024. De inbraak heeft mogelijk geleid tot het lekken van persoonsgegevens, zoals naam en e-mailadres, van 378 cliënten, tolken en medewerkers van het UWV. Na ontdekking heeft de leverancier het videoplatform afgesloten, een datalek gemeld bij de Autoriteit Persoonsgegevens, en zijn de betrokkenen geïnformeerd.[12]

10 https://www.security.nl/posting/844314/Zyxel+komt+met+noodpatch+voor+kritiek+lek+in+end-of-life+NAS-systemen?channel=rss

11 https://www.security.nl/posting/844327/Bugs+in+Cisco+Webex+Meetings+gebruikt+voor+ongeautoriseerde+toegang?channel=rss

12 https://www.security.nl/posting/844639/UWV+eerder+dit+jaar+getroffen+door+inbraak+op+commercieel+videoplatform

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

juni ’24

TLP:GREEN