Cybercrimeinfo (ccinfo.nl) Bekijk de webversie

Nieuwsbrief 342

Reading in □□ or another language

Phishing-as-a-service: de nieuwe dreiging voor bedrijven en gebruikers met 2FA

Phishing-as-a-service (PaaS) transformeert de manier waarop cybercriminelen phishing-aanvallen uitvoeren door kant-en-klare aanvalstools te commercialiseren. Dit model biedt zelfs niet-technische criminelen de mogelijkheid om geavanceerde phishing-aanvallen, zoals de Rockstar 2FA-campagnes, uit te voeren. Deze campagnes richten zich specifiek op gebruikers met tweefactor-authenticatie (2FA), waarbij criminelen 2FA-codes onderscheppen via valse inlogpagina's. Ondanks de extra beveiligingslaag van 2FA, blijven dergelijke aanvallen effectief en benadrukken ze de noodzaak voor bedrijven en individuen om hun beveiligingsmaatregelen te versterken. Bewustwording, educatie en het gebruik van hardwarematige authenticators zijn cruciaal om deze groeiende dreiging het hoofd te bieden.

Lees verder

Reading in □□ or another language

Online fraude in 2024: Hoe cybercriminelen steeds slimmer te werk gaan

In november 2024 kwam Volexity met een alarmerende ontdekking: de "nearest neighbor-aanval". Deze geavanceerde tactiek, toegepast door een Russische APT-groep, maakt gebruik van nabijgelegen Wi-Fi-netwerken om ongemerkt toegang te krijgen tot doelwitten. Anders dan traditionele aanvallen maakt deze methode gebruik van bestaande netwerken in de directe omgeving van het slachtoffer. Door gebruik te maken van automatische verbindingsinstellingen van moderne apparaten, kunnen aanvallers zonder interactie gevoelige informatie bemachtigen, zoals wachtwoorden en documenten. Deze aanval benadrukt het groeiende belang van fysieke nabijheid in cyberaanvallen en onderstreept de noodzaak voor organisaties om hun netwerkbeveiliging en bewustwording rondom openbare Wi-Fi-netwerken te versterken.

Lees verder

Reading in □□ or another language

Gevangenisblauwdrukken gelekt op het darkweb: gevolgen voor nationale veiligheid

Recentelijk zijn gedetailleerde blauwdrukken van meer dan 20 gevangenissen in Engeland en Wales gelekt op het darkweb. Dit incident heeft ernstige bezorgdheid gewekt bij zowel media als autoriteiten. Gevangenissen zijn cruciale infrastructuren en de blootstelling van deze gevoelige informatie kan leiden tot potentiële inbraken, ontsnappingen en gerichte aanvallen. Het lek benadrukt de groeiende dreiging van cyberaanvallen op kritieke infrastructuur, waarbij zwakke digitale beveiliging een belangrijke rol speelt. Het incident onderstreept de noodzaak van robuuste cybersecuritymaatregelen en internationale samenwerking om dergelijke bedreigingen effectief aan te pakken.

Lees verder

Reading in □□ or another language

Slachtofferanalyse en Trends van Week 47-2024

De afgelopen week markeerde opnieuw een periode van intensieve cyberaanvallen en datalekken, waarbij bedrijven wereldwijd kwetsbaar bleken voor geavanceerde dreigingen. In België werd Zalando getroffen door een ernstig datalek, terwijl ransomware-aanvallen de Belgische bedrijven BusinessTraining.be en Euromedix.com hard raakten. Wereldwijd hebben ransomware-groepen zoals Akira en Eldorado een spoor van schade achtergelaten, met slachtoffers variërend van kleine bedrijven tot grote instellingen zoals gemeentelijke administraties. Nieuwe malware zoals Glove Stealer en het Water Barghest Botnet onderstrepen de voortdurende evolutie van bedreigingen. Deze gebeurtenissen benadrukken het belang van continue cyberbeveiliging en bewustwording voor zowel bedrijven als individuen in deze snel veranderende digitale wereld.

Lees verder

Reading in □□ or another language

Vraag van de week: Slim speelgoed - Hoe veilig zijn de digitale speeltjes voor onze kinderen?

Met de opkomst van slimme apparaten thuis groeit de bezorgdheid onder ouders over de veiligheid van digitale speeltjes voor kinderen. Interactieve poppen, robots en andere IoT-verbonden speelgoed bieden nieuwe speel- en leerervaringen, maar brengen ook serieuze cyberveiligheidsrisico's met zich mee. Deze apparaten verzamelen vaak persoonlijke gegevens zoals stemopnames en locatiegegevens, die kunnen worden blootgesteld aan cybercriminelen. Ouders worden aangemoedigd om de beveiligingsinstellingen van deze apparaten zorgvuldig te controleren, regelmatig software-updates uit te voeren en de privacyverklaringen grondig te lezen. Fabrikanten worden opgeroepen om strengere beveiligingsnormen te hanteren en transparant te zijn over gegevensverwerking. Alleen door gezamenlijke inspanningen kunnen we een veilige digitale omgeving voor onze kinderen waarborgen.

Lees verder

Reading in □□ or another language

Nijkerk - Helpdesk fraude

In juni werd een echtpaar uit Assendelft slachtoffer van bankhelpdeskfraude. Een oplichter deed zich voor als bankmedewerker en wist met een verzonnen verhaal de bankpassen van het echtpaar te bemachtigen. Vervolgens gebruikte de verdachte deze om geld van hun rekening op te nemen. De politie zoekt naar de dader en vraagt het publiek om tips. Bewakingsbeelden tonen de verdachte tijdens het plegen van de fraude. Dit incident benadrukt het belang van waakzaamheid bij verdachte telefoontjes en het beschermen van persoonlijke bankgegevens.

Lees verder

Reading in □□ or another language

Verbeter je cyberveiligheid: Test je kennis met onze interactieve quizzen

Verken de wereld van cybersecurity en het darkweb met onze interactieve quizzen op CyberCrimeInfo. Of je nu een beginner bent of een doorgewinterde expert, onze quizzen bieden een leuke en uitdagende manier om je kennis uit te breiden.

Wat kun je verwachten?

- **Leer in je eigen tempo:** Ontdek en test je vaardigheden wanneer het jou het beste uitkomt.
- **Ontvang feedback:** Krijg gedetailleerde feedback na elke quiz, zodat je precies weet waar je staat en waar je nog kunt verbeteren.
- **Verdien speciale erkenning:** Behaal een perfecte score en ontvang speciale erkenning voor je prestaties.

Ben je klaar om je kennis te testen en jezelf te meten met anderen? Begin vandaag nog aan je leerreis en vraag je toegangscode aan!

Naar quizzen

De Perfecte Score Club!

Topscorer	Punten	Wanneer
Joost W.	10	04-08-2024
Jasper	10	23-05-2024
Johan	10	16-03-2024
Philip S.	9	17-03-2024
Maxim	9	16-03-2024
Aart	7	21-06-2024
Thijs	7	09-04-2024
Kenan	7	30-03-2024

NIEUW TOEGEVOEGD

Maximaal te behalen **punten: 20**
Aantal deelnemers tot nu toe: 948 (+1)

Totaal overzicht De Perfecte Score Club!

Reading in □□ or another language

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,
In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Wij zijn een onafhankelijke organisatie, gedreven door vrijwilligers, die zich inzet voor het informeren en beschermen van het publiek tegen de gevaren van het digitale tijdperk.
Jouw donatie maakt het verschil. Hier is waarom:

1. **Onafhankelijke en Belangrijke Bron van Informatie:** Cybercrimeinfo is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en preventiemethoden.
2. **Bijdragen aan Bewustwording en Preventie:** Door te doneren help je ons in de missie om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen bij aan het voorkomen van digitale misdrijven.
3. **Ondersteuning van Onze Operationele Kosten:** Donaties worden direct gebruikt voor het hosten van de website en het vernieuwen van onze technologische middelen. Dit stelt ons in staat om op de voet te volgen hoe cybercriminelen opereren en jullie te informeren over de nieuwste digitale gevaren.

Elke bijdrage, hoe klein ook, is van onschatbare waarde in onze continue strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.
We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Doneren kan via de **doneer pagina** (Kies nu zelf het bedrag dat je wilt doneren!) of via onderstaande QR code.

Met vriendelijke groet,
Het team van Cybercrimeinfo

Doneer | Cybercrimeinfo.nl (ccinfo.nl)

Doneer pagina

Geen budget? Geen probleem!

Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!

Laat jouw stem horen: Steun ons met een Google review!

Wij streven er voortdurend naar om de zichtbaarheid en bereikbaarheid van Cybercrimeinfo te verbeteren. Een fantastische manier waarop jij ons hierbij kunt helpen, is door een review achter te laten op Google. Jouw feedback is onmisbaar voor ons en helpt anderen om ons makkelijker te vinden.
Het plaatsen van een recensie is simpel en kost slechts een minuutje van je tijd. Klik op de volgende link om jouw ervaringen te delen: **Schrijf een review**.
Elke review draagt bij aan onze missie om iedereen beter te informeren over cyberveiligheid. Jouw steun is voor ons ontzettend waardevol! Hartelijk dank voor je betrokkenheid.

Non-profit team Cybercrimeinfo

Share Tweet Share Pinterest