Dark Web Scan-rapport (demoversie)

Contactpersoon **Acme Corp**: John Smith

Datum: 1 maart 2025

Version Control

Version	Description	Date	Author
1.0	Dark Web Scan Report	01-03-2025	*S. Jansen (OSEP, OSCP, CRTO, S7 RTO)*

INHOUDSOPGAVE

Inleiding

Dit rapport beschrijft de dark web-scan die is uitgevoerd voor Acme Corp. Het doel van dit rapport is om een gedetailleerd overzicht te geven van de gebruikte methodologieën, bevindingen en aanbevelingen die voortkomen uit de analyse.

De dark web-scan is uitgevoerd om inzicht te verkrijgen in mogelijke blootgestelde of gelekte informatie met betrekking tot Acme Corp. Hierbij is specifiek gekeken naar inloggegevens, bedrijfsgevoelige documenten, klant- en personeelsgegevens, en andere potentiële dreigingen die op ondergrondse marktplaatsen, forums en datalekdatabases circuleren.

In dit rapport worden de bevindingen systematisch gepresenteerd en geanalyseerd, waarbij de impact en risico's van de aangetroffen gegevens worden geëvalueerd. Daarnaast worden aanbevelingen gegeven om de digitale weerbaarheid van Acme Corp te verhogen, waaronder het verbeteren van wachtwoordbeheer, implementeren van aanvullende beveiligingsmaatregelen en het monitoren van verdere datalekken.

Dit rapport dient als een waardevol hulpmiddel voor stakeholders binnen Acme Corp, zoals het IT-beveiligingsteam, het management en andere relevante partijen, om proactieve stappen te ondernemen ter bescherming van bedrijfsinformatie en reputatie.

SCOPE

Deze scan richt zich op het identificeren van gelekte of misbruikte gegevens die verbonden zijn aan de organisatie binnen bekende dark web- en datalekbronnen. Het doel is om te detecteren of e-mailadressen, inloggegevens, of gerelateerde gevoelige informatie publiekelijk beschikbaar zijn, en zo vroegtijdige risico's op misbruik, phishing of accountovername te signaleren.

Onderstaande tabel geeft een overzicht van de domeinen die binnen de scope van dit onderzoek vallen:

#	Domein
1	Acme-corp.com
2	Admin.acme-corp.com

DRAAGWIJDTE

De scope van deze dark web-scan omvat een beknopte maar gerichte OSINT-analyse van ondergrondse digitale ecosystemen waarin potentiële dreigingen voor ACME CORP zich kunnen manifesteren. Dit onderzoek richt zich op het identificeren van gelekte of gecompromitteerde gegevens en het detecteren van mogelijke incidenten waarbij bedrijfsinformatie openbaar is geworden of te koop wordt aangeboden.

Het onderzoek richt zich specifiek op de volgende aspecten:

Analyse van relevante dark web-platformen:

Dit omvat forums, marktplaatsen, datalekdatabases en versleutelde communicatiekanalen waar cybercriminelen actief zijn en informatie wordt verhandeld.

Identificatie van gecompromitteerde gegevens:

Onderzoek naar gelekte inloggegevens, financiële informatie, klant- en personeelsgegevens, evenals andere bedrijfskritische gegevens die betrekking hebben op ACME CORP of gelieerde entiteiten.

Monitoring van bedreigingen en reputatierisico's:

Actief speuren naar vermeldingen van ACME CORP in criminele netwerken, waaronder geplande aanvallen, gerichte phishing-campagnes en potentiële insider threats.

Disclaimer: de scan richt zich uitsluitend op openbaar toegankelijke dark web-bronnen binnen de vooraf vastgestelde onderzoeksperiode. Privékanalen, end-to-end versleutelde netwerken en bronnen die juridische of technische beperkingen opleggen, vallen buiten de scope van dit onderzoek.

LIMITATIES

De bevindingen in dit rapport dienen te worden beschouwd binnen de volgende beperkingen en randvoorwaarden:

- **Tijdslimieten**: De scan is uitgevoerd binnen een vooraf vastgestelde en beperkte tijdsperiode. Hierdoor is het mogelijk dat tijdelijke of zich snel ontwikkelende dreigingen, zoals nieuwe datalekken of plotselinge verschijningen van gecompromitteerde informatie, niet zijn gedetecteerd. Daarnaast kunnen bedreigingen die na de scanperiode zijn ontstaan, buiten de analyse vallen.
- **Toegankelijkheid van gegevens**: De analyse richt zich uitsluitend op openbaar beschikbare informatie binnen het dark web. Gesloten criminele netwerken, privéfora, versleutelde marktplaatsen en op uitnodiging toegankelijke communicatiekanalen zijn niet meegenomen in de scope van dit onderzoek. Hierdoor is het mogelijk dat bepaalde bedreigingen en transacties buiten het zicht van deze analyse zijn gebleven.
- **Scopebeperkingen**: De scan is gericht op gegevens die direct verband houden met Acme Corp, zoals gelekte bedrijfsgegevens, inloggegevens en gerelateerde vermeldingen. Mogelijke bredere dreigingen, zoals algemene trends binnen de dreigingsactorengemeenschap of indirecte indicatoren die kunnen wijzen op toekomstige risico's, zijn mogelijk buiten beschouwing gelaten.
- **Dynamische omgeving**: Het dark web is een snel veranderend ecosysteem waarin informatie continu wordt toegevoegd, verwijderd of verplaatst. De resultaten van deze scan vormen daarom een momentopname en kunnen op korte termijn veranderen. Nieuwe kwetsbaarheden of gelekte gegevens kunnen na de analyse alsnog opduiken, en eerder gevonden informatie kan inmiddels verplaatst of verwijderd zijn.

Deze beperkingen onderstrepen dat de dark web-scan een waardevol inzicht biedt, maar geen volledige garantie geeft op de detectie van alle bestaande en toekomstige bedreigingen. Het is daarom aan te raden om regelmatig aanvullende scans en monitoring uit te voeren om de digitale veiligheid van ACME CORP proactief te waarborgen.

MANAGEMENT SAMENVATTING

Dit rapport biedt een diepgaande analyse van de beveiligingsrisico's met betrekking tot gevonden kwetsbaarheden (CVE's), gelekte inloggegevens en webkwetsbaarheden. De bevindingen tonen aan dat er aanzienlijke risico's bestaan op ongeautoriseerde toegang, misbruik en potentiële aanvallen. Om deze risico's te minimaliseren, worden concrete aanbevelingen gedaan om de beveiliging te versterken en de digitale weerbaarheid te verbeteren.

BELANGRIJKSTE GEÏDENTIFICEERDE RISICO'S

Tijdens de dark web-scan zijn meerdere gevoelige gegevens aangetroffen die een potentieel risico vormen voor de organisatie. Dit omvat:

1. **Kwetsbaarheden in OpenSSH (CVE's)**

   Via een asset exposure-scan zijn 23 kwetsbaarheden geïdentificeerd, waaronder kritieke issues zoals buffer overflows, race conditions, en cryptografische zwakheden.

   I. **MOGELIJKE IMPACT:** Deze kwetsbaarheden kunnen leiden tot **denial-of-service (DoS)-aanvallen, ongeautoriseerde toegang** en **afluisteren van communicatie**.

2. **Gelekte Inloggegevens**

   Via het zoeken in Breached Databases zijn meerdere wachtwoorden en e-mailadressen aangetroffen. Inloggegevens van acme-corp.com zijn online gelekt.

   Daarnaast blijkt dat admin@acme-corp.com een **directeur is binnen de organisatie**, en zijn wachtwoord meerdere keren voorkomt in de gelekte datasets. Dit verhoogt het risico op **gerichte aanvallen tegen leidinggevenden** (zoals spear phishing of business email compromise).

   I. **MOGELIJKE IMPACT:** Hergebruik van wachtwoorden en zwakke wachtwoorden verhogen het risico op **accountovername en gerichte phishing-aanvallen**.

3. **Webkwetsbaarheden in WordPress-websites**

   De verouderde 'wc-gallery' WordPress-plugin bevat een kwetsbaarheid die cross-site scripting (XSS) mogelijk maakt. De externe WP-Cron-functionaliteit is ingeschakeld.

   I. **MOGELIJKE IMPACT:** Aanvallers kunnen een **kwaadaardige code injecteren** en een **Denial-of-Service-aanval (DoS)** uitvoeren.

STRATEGISCHE AANBEVELINGEN

Om de blootstelling van gevoelige informatie te beperken en de cyberweerbaarheid van ACME CORP te verhogen, worden de volgende maatregelen aanbevolen:

✅ **Beveiliging van OpenSSH verbeteren**: Updaten naar de nieuwste versie, zwakke protocollen uitschakelen, MFA implementeren en SSH-toegang beperken via een VPN of bastion host.

✅ **Gelekte credentials aanpakken**: Wachtwoordreset forceren, MFA verplicht stellen, sterke wachtwoorden gebruiken en security awareness-trainingen uitvoeren.

✅ **WordPress-websites beveiligen**: De kwetsbare plugin **verwijderen of updaten**, toegangsrechten beperken en een **Web Application Firewall (WAF)** implementeren.

✅ **WP-Cron beveiligen**: Externe WP-Cron uitschakelen en vervangen door een server-side cronjob, terwijl monitoring en rate-limiting worden toegepast om misbruik te voorkomen.

✅ **Uitvoeren van een penetratietest (pentest):** Een grondige pentest laten uitvoeren om kwetsbaarheden binnen het netwerk, webapplicaties en systemen te identificeren. Dit omvat onder andere: testen op misconfiguraties, zwakke authenticatiemethoden en kwetsbare software. Actief aanvallen simuleren om te beoordelen of ACME CORP bestand is tegen gerichte cyberaanvallen. Op basis van de resultaten gerichte beveiligingsmaatregelen implementeren.Door deze maatregelen te implementeren, kan ACME CORP het risico op misbruik van gevoelige informatie aanzienlijk verkleinen en haar weerbaarheid tegen cyberdreigingen vergroten.

METHODOLOGIE

De dark web-scan is uitgevoerd door middel van een combinatie van geautomatiseerde tools en handmatige analyse, waarbij OSINT (Open Source Intelligence) en SOCMINT (Social Media Intelligence) technieken zijn toegepast. Dit hybride proces zorgt voor een effectieve detectie van gelekte of gecompromitteerde gegevens en biedt een nauwkeurig inzicht in potentiële dreigingen.

De methodologie omvat de volgende stappen:

1. Gegevensverzameling

- Systematisch doorzoeken van het dark web met behulp van gespecialiseerde crawlers en zoekmachines zoals Ahmia, OnionScan en dark web-indexeringsdiensten.
- Toepassen van OSINT- en SOCMINT-methoden om informatie te verzamelen van ondergrondse forums, marktplaatsen en chatplatformen (zoals Telegram en IRC).
- Gebruik van threat intelligence-platformen en commerciële databanken voor het identificeren van recente datalekken die mogelijk verband houden met ACME CORP.

2. Analysetechnieken

- Zoekwoordgebaseerde detectie: Gebruik van specifieke zoektermen en aangepaste filters om te zoeken naar vermeldingen van ACME CORP, e-mailadressen, domeinen en andere gerelateerde entiteiten.
- Patroonherkenning: Identificeren van terugkerende datalekstructuren, zoals combinaties van e-mailadressen en wachtwoorden, of financiële gegevens die overeenkomen met bekende fraudepatronen.
- Kruisverwijzing met bekende datalekken: Vergelijken van aangetroffen gegevens met bekende breached databases

3. Validatie van Bevindingen

- Correlatie van meerdere gegevensbronnen: Verificatie van aangetroffen informatie door middel van kruisanalyse tussen verschillende dark web-platformen en OSINT-tools.
- Authenticiteitscontrole: Controleren of gelekte gegevens daadwerkelijk operationeel zijn door middel van metadata-analyse en checksum-verificatie.
- Verificatie via secundaire bronnen: Afstemmen van bevindingen met eerdere bekende dreigingen, cybercrime-rapporten en threat intelligence-feeds om de relevantie en betrouwbaarheid te waarborgen.

4. Rapportagestandaarden

- Industrienormen en frameworks: De rapportage is afgestemd op toonaangevende cybersecurity-frameworks, waaronder:
    - NIST Cybersecurity Framework (CSF)
    - MITRE ATT&CK voor dreigingsanalyse
    - ISO 27001-normen voor informatiebeveiliging
    - OWASP Top 10 en CIS Controls voor best practices
- Traceerbaarheid en reproduceerbaarheid: Alle stappen van het scanproces zijn gedocumenteerd om de betrouwbaarheid en herhaalbaarheid te garanderen. Dit maakt het mogelijk om de resultaten te reproduceren en eventuele nieuwe bevindingen efficiënt te verifiëren.

Deze methodologische aanpak biedt ACME CORP een diepgaand inzicht in de dreigingen die voortkomen uit dark web-activiteiten, en draagt bij aan een strategische besluitvorming om de organisatie beter te beschermen tegen cyberrisico's.

BEVINDINGEN

Security analyse & risico's van gevonden CVE's, gelekte credentials en webkwetsbaarheden

Dit document bevat een uitgebreide analyse van de gevonden kwetsbaarheden (CVEs), gelekte inloggegevens en webkwetsbaarheden. De risico's worden geanalyseerd en er worden aanbevolen maatregelen gegeven om de beveiliging te verbeteren.

Voor gedetailleerde technische informatie, zoals lijsten met specifieke CVE's, domeinspecifieke credentials en output van OSINT-tools, wordt verwezen naar de bijlagen achterin dit rapport. Deze bevatten de volledige ruwe data en scanresultaten ter ondersteuning van de bevindingen in dit hoofdstuk.

Analyse van gevonden CVE's

Op verschillende IP-adressen gekoppeld aan ACME CORP zijn open services aangetroffen, waaronder verouderde webapplicaties en services zoals Apache, nginx en PHP. In totaal zijn 5 kwetsbaarheden (CVE's) vastgesteld die misbruikt kunnen worden voor onder meer remote code execution, cross-site scripting en privilege escalation.

Risicoanalyse van gevonden CVE's

- **CVE-2023-25690:** Apache HTTP Server - mod_rewrite buffer overflow (kan leiden tot DoS of RCE)
  - **Risico:** Kan leiden tot denial-of-service of remote code execution bij specifieke rewrite-configuraties.
- **CVE-2022-37434:** PHP Zip module - integer overflow bij verwerking ZIP-archieven
  - **Risico:** Mogelijk misbruikbaar via ZIP-bestanden, kan leiden tot heap corruption en code execution.
- **CVE-2023-29383:** WordPress Core - XSS via shortcode rendering
  - **Risico**: Maakt XSS mogelijk via shortcode-verwerking; misbruikbaar voor sessiekaping of credential harvesting.
- **CVE-2022-21661:** WordPress - Stored XSS via post slugs in bepaalde configuraties
  - **Risico:** Kwaadwillenden kunnen persistent JavaScript injecteren met impact op beheerdersaccounts.
- **CVE-2021-41773:** Apache HTTP Server path traversal in bepaalde configuraties
  - **Risico**: Stelt aanvallers in staat om buiten de webroot bestanden te benaderen en mogelijk code uit te voeren.

Analyse van gelekte credentials

Er zijn meerdere gelekte wachtwoorden en e-mailadressen gevonden via *Breached Databases*. Dit vormt een groot beveiligingsrisico, vooral als wachtwoorden hergebruikt worden.

Risicoanalyse per domein.

- **Acme-corp.com** :500 gelekte wachtwoorden aangetroffen op pastebin groot risico op account overname
- **Admin.acme-corp.com**: door de aanwezigheid van een publiek toegangelijk backup bestand, is een plain text admin wachtwoord gevonden. Dit wachtwoord geeft toegang tot de wordpress website. Risico is kritiek op account overnamen.

Analyse van webkwetsbaarheden

Tijdens de scan zijn meerdere kwetsbaarheden aangetroffen binnen een WordPress-installatie. De plugin wc-gallery blijkt verouderd en bevat een bekende stored XSS-kwetsbaarheid. Daarnaast is de externe WP-Cron-functionaliteit ingeschakeld, wat DoS-aanvallen mogelijk maakt. Verder is een publiek toegankelijke back-upbestand (backup_2023-11-01.zip) aangetroffen, waarin een config-bestand werd gevonden met een admin-wachtwoord in plaintext.

Kwetsbaarheid in wc-gallery plugin

De plugin 'wc-gallery' is verouderd en bevat een bekende kwetsbaarheid:

- **CVE-2022-4795:** Galerijen van Angie maakt <= 1.67 - Contributor+ opgeslagen XSS via shortcode
    - **Risico:** Aanvallers met een minimaal 'contributor' account kunnen kwaadaardige scripts injecteren via shortcodes. Dit kan worden misbruikt om andere gebruikers aan te vallen of sessies te kapen.

Kwetsbaarheid in WP-Cron (denial of service)

De externe WP-Cron functionaliteit is ingeschakeld, wat een potentieel risico vormt voor een DoS-aanval (Denial of Service). Aanvallers kunnen het cron-systeem misbruiken om het systeem te overbelasten door herhaaldelijk requests te sturen naar wp-cron.php.

Publiek toegankelijk wordpress backup bestand

Verder is een publiek toegankelijke back-upbestand (backup_2023-11-01.zip) aangetroffen, waarin een config-bestand werd gevonden met een admin-wachtwoord in plaintext.

- **Risico:** Volledige compromittering van het admin-account via gelekt wachtwoord.

BEGRIPPENLIJST

- **Dark Web**

  Een verborgen deel van het internet dat alleen toegankelijk is via gespecialiseerde software zoals Tor. Hier worden vaak illegale activiteiten uitgevoerd, waaronder de handel in gestolen gegevens.
- **OSINT (Open Source Intelligence)**

  Het verzamelen van informatie uit openbare bronnen zoals websites, sociale media en datalekken om potentiële dreigingen te analyseren.
- **SOCMINT (Social Media Intelligence)**

  Een vorm van OSINT waarbij informatie wordt verzameld van sociale media-platforms om digitale dreigingen en risico's te identificeren.
- **Datalekdatabase**

  Een verzameling van gegevens die zijn buitgemaakt bij cyberaanvallen en beschikbaar zijn op het dark web of gespecialiseerde forums.
- **Gecompromitteerde gegevens**

  Informatie (zoals inloggegevens, financiële data of bedrijfsgevoelige documenten) die is gelekt of gestolen en mogelijk door kwaadwillenden wordt misbruikt.
- **Threat Intelligence**

  Inlichtingen over cyberdreigingen, vaak afkomstig van gespecialiseerde bronnen zoals beveiligingsfirma's of overheidsinstanties, om organisaties te helpen aanvallen te voorkomen.
- **Shodan-scan**

  Een zoekmachine en scanningstool die apparaten en servers op het internet opspoort en kwetsbaarheden identificeert.
- **CVE (Common Vulnerabilities and Exposures)**

  Een internationaal erkend systeem voor het registreren van bekende kwetsbaarheden in software en hardware.
- **Buffer Overflow**

  Een kwetsbaarheid waarbij een programma meer gegevens verwerkt dan het aankan, wat kan leiden tot crashes of het uitvoeren van kwaadaardige code.
- **Race Condition**

  Een kwetsbaarheid waarbij een systeem foutief omgaat met gelijktijdige processen, waardoor aanvallers toegang kunnen krijgen tot gevoelige informatie of systemen kunnen manipuleren.

- **Cryptografische zwakte**

  Een zwakte in een versleutelingstechniek die aanvallers in staat stelt om versleutelde data te ontsleutelen of te manipuleren.
- **Cross-Site Scripting (XSS)**

  Een webkwetsbaarheid waarbij een aanvaller schadelijke scripts in een website injecteert om gebruikersgegevens te stelen of sessies over te nemen.
- **Denial-of-Service (DoS) aanval**

  Een aanval waarbij een website of dienst wordt overbelast met verkeer, waardoor deze tijdelijk onbruikbaar wordt.
- **Web Application Firewall (WAF)**

  Een beveiligingsmechanisme dat webapplicaties beschermt tegen aanvallen zoals XSS en SQL-injecties door kwaadwillend verkeer te filteren.
- **WP-Cron**

  Een ingebouwd WordPress-mechanisme voor het plannen van taken, dat kan worden misbruikt door aanvallers om overbelasting en DoS-aanvallen te veroorzaken.
- **Bastion Host**

  Een speciaal beveiligde server die als toegangspunt dient voor een netwerk en de blootstelling aan bedreigingen minimaliseert.
- **MFA (Multi-Factor Authentication)**

  Een beveiligingsmethode waarbij meerdere verificatiestappen nodig zijn om toegang te krijgen, zoals een wachtwoord in combinatie met een eenmalige code via sms of een authenticator-app.
- **Phishing**

  Een vorm van cybercriminaliteit waarbij aanvallers zich voordoen als betrouwbare partijen om slachtoffers te misleiden en gevoelige gegevens te verkrijgen.
- **Rate-Limiting**

  Een beveiligingsmaatregel waarbij het aantal verzoeken dat een gebruiker in een bepaalde tijd kan indienen wordt beperkt om misbruik zoals brute-force aanvallen te voorkomen.

AANBEVELINGEN

Op basis van de gevonden kwetsbaarheden adviseren we gerichte maatregelen om de risico's te minimaliseren. De aanbevelingen in dit hoofdstuk helpen bij het verbeteren van de beveiliging en het verkleinen van de kans op misbruik door kwaadwillenden. Door deze stappen tijdig te implementeren, kan de organisatie haar digitale weerbaarheid aanzienlijk versterken. In onderstaand overzicht vindt u per onderdeel de aanbevolen maatregelen.

Gevonden CVE's

- ✅ Upgrade OpenSSH naar de nieuwste stabiele versie.
- ✅ Schakel zwakke encryptieprotocollen en ongebruikte authenticatiemethoden uit.
- ✅ Gebruik MFA en sterke authenticatiemethoden zoals ed25519 SSH keys.
- ✅ Overweeg een alternatieve toegangsmethode (VPN of bastion host) om directe SSH-exposure te vermijden.

Gelekte credentials

- ✅ Forceer een wachtwoordreset voor alle gelekte accounts.
- ✅ Schakel MFA in voor alle accounts.
- ✅ Gebruik sterke wachtwoorden en verplicht periodieke updates.
- ✅ Implementeer een wachtwoordmanager om hergebruik te voorkomen.
- ✅ Voer interne security awareness-trainingen uit om phishing te verminderen.

Wc-galerij

- ✅ Verwijder of vervang de 'wc-gallery' plugin als deze niet strikt noodzakelijk is.
- ✅ Controleer of er een beveiligingspatch beschikbaar is en update de plugin indien mogelijk.
- ✅ Beperk de rechten van gebruikers zodat alleen vertrouwde accounts content kunnen plaatsen.
- ✅ Gebruik een Web Application Firewall (WAF) om XSS-exploits te detecteren en blokkeren.

WP-Cron

✅ Schakel externe WP-Cron uit door de regel `define('DISABLE_WP_CRON', true);` toe te voegen aan `wp-config.php`.

✅ Gebruik een server-side cronjob als vervanging voor WP-Cron om de site minder kwetsbaar te maken.

✅ Implementeer rate-limiting via een firewall of beveiligingsplugin om herhaalde toegangspogingen te beperken.

✅ Monitor serverlogs op verdachte activiteit die wijst op misbruik van WP-Cron.

De bevindingen in dit rapport tonen aan dat Acme Corp een verhoogd risico loopt door gelekte gegevens en gecompromitteerde netwerktoegang. Zonder een grondige analyse en passende beveiligingsmaatregelen blijft het bedrijf kwetsbaar voor cybercriminelen. Een penetratietest is een essentiële stap om kwetsbaarheden in de IT-infrastructuur en applicaties te identificeren voordat kwaadwillenden deze kunnen exploiteren.

- **Voorkomen van cyberaanvallen**: Een pentest helpt bij het tijdig opsporen en verhelpen van beveiligingslekken, waardoor de kans op misbruik door aanvallers aanzienlijk wordt verminderd.

- **Naleving van regelgeving**: Organisaties zoals Acme Corp moeten voldoen aan regelgeving zoals AVG/GDPR en ISO 27001. Een pentest draagt bij aan compliance door beveiligingsrisico's in kaart te brengen en te mitigeren.

- **Bescherming van bedrijfsgegevens**: Het voorkomen van datalekken is cruciaal om reputatieschade en financiële verliezen te minimaliseren. Door kwetsbaarheden proactief aan te pakken, wordt de kans op het uitlekken van klant- en bedrijfsgegevens verlaagd.

- **Versterken van de algehele cyberweerbaarheid**: Door realistische aanvalsscenario's te simuleren, krijgen IT-teams waardevolle inzichten in de effectiviteit van bestaande beveiligingsmaatregelen en kunnen zij hun responsstrategieën optimaliseren.

Naast periodieke OSINT-onderzoeken is het aan te raden om regelmatig een pentest uit te voeren. Dit helpt om een actueel beeld te behouden van de beveiligingsstatus van Acme Corp en tijdig te anticiperen op nieuwe dreigingen. Voor een complete beveiligingsstrategie is een combinatie van pentesting, continue monitoring en security awareness-training noodzakelijk.

Door een integrale aanpak te hanteren, kan Acme Corp zich beter wapenen tegen toekomstige cyberdreigingen en de impact van mogelijke aanvallen minimaliseren.

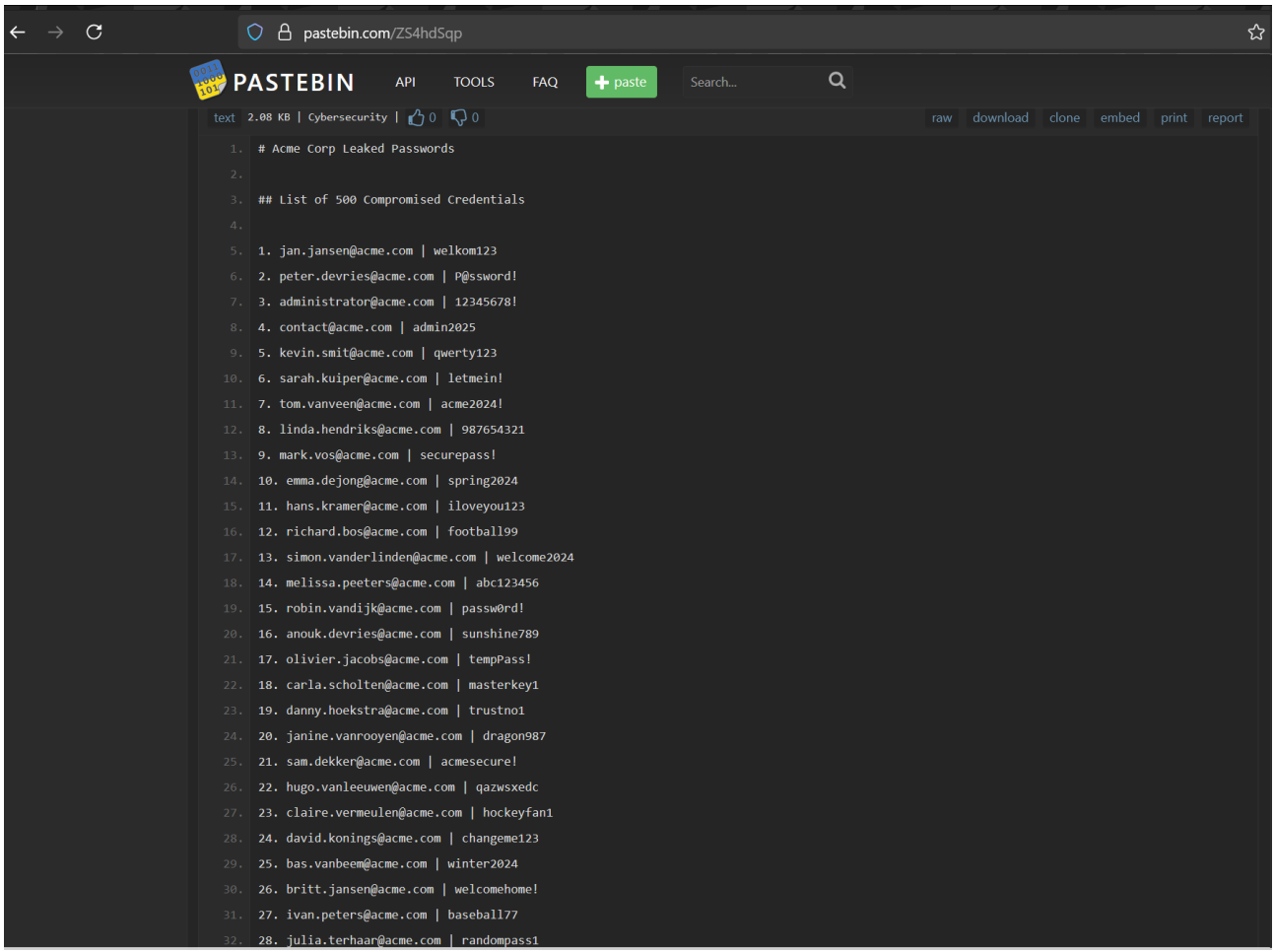
BIJLAGEN

Bewijs:

Acme Corp toegang te koop aangeboden op bekend hacker forum

Bron: https://hackerforum.io

Geraadpleegd op: 03-03-2025 om 09:05 uur



Lijst van gelekte wachtwoorden van Acme Corp

Geraadpleegd op: 03-03-2025 om 09:05 uur

Bron leaked https://pastebin.com/ZS4hdSqp