pinewood

THE INTERSTELLAR COLLECTION

Januari 2025

Dreigingen & Ontwikkelingen

We see risks
before they hurt

Introductie

Pinewood monitort continu alle ontwikkelingen die naar voren komen uit het steeds ontwikkelende (cybersecurity-)landschap. Op maandeljkse basis bundelen wij al deze ontwikkelingen en halen hier steeds vier centrale thema's uit die gedurende die maand zijn opgevallen. We kijken daarbij niet alleen naar de ontwikkelingen die we binnen die centrale thema's hebben gezien, maar we vertalen dat ook in essentiële maatregelen die een organisatie moet hebben getroffen om afdoende beveiligd te zijn tegen de dreigingen van die maand.

Inhoudsopgave

Thema 1

Aanhoudende problemen met publiek ontsloten netwerkdevices

Een thema dat vrijwel elke maand weer terugkeert, is de problematiek rondom kwetsbaarheden in netwerkdevices en het misbruik hiervan. Daarbij gaat het in het bijzonder om systemen die via internet te benaderen zijn en waarvan aanvallers dankbaar misbruik maken in de vorm van een “opstapje” richting het (interne) netwerk van het slachtoffer. Regelmatig wordt dan ook bekend dat kwetsbaarheden in publiek bereikbare firewalls, VPN-systemen en andere apparatuur (zoals IP-camera’s) op verschillende manieren misbruikt zijn voor malafide doeleinden (zie kader “Misbruik van netwerkdevices in de praktijk”).

Misbruik van netwerkdevices in de praktijk

Dat kwetsbaarheden in publiek ontsloten netwerkdevices ook actief misbruikt worden, wordt wel duidelijk uit de recente dump van FortiGate-configuraties door de “Belsen Group”.
Diverse andere recente rapporten en incidenten onderschrijven dit echter ook:

- eSentire meldt dat aanvallers actief misbruik maken van gestolen inloggegevens om in te breken op de VPN-devices van organisaties. [1]
- De Franse toezichthouder voor gegevensbescherming (CNIL) heeft in kaart gebracht welke problemen ten grondslag lagen aan de datalekken die in 2024 bij haar werden gemeld. Daarbij geeft CNIL aan dat misbruik van kwetsbare software en kwetsbare configuraties op extern ontsloten systemen één van de belangrijkste oorzaken blijkt te zijn. [2]
- Trend Micro maakt recent melding van een IoT-botnet dat op zoek gaat naar kwetsbare wireless routers (en IP-camera’s) om deze vervolgens in te kunnen zetten voor DDoS-aanvallen. [3]
- Een ziekenhuis in Italië viel ten prooi aan de RagnarLocker-ransomware waarbij de aanvallers initieel wisten binnen te dringen door misbruik te maken van een kwetsbaarheid in een firewall van het ziekenhuis. [4]

Configuraties van meer dan 15.000 FortiGate-firewalls gepubliceerd

Een voorheen onbekende actor genaamd “Belsen Group” publiceerde de volledige configuraties van meer dan 15.000 FortiGate-firewalls, met daarin allerlei gevoelige informatie zoals firewallregels, gebruikersnamen, wachtwoorden en sleutelmateriaal. [5] Naast de (gratis) initiële verzameling van meer dan 15.000 firewalls, bood dezelfde groep later in de maand ook nog een aanvullende set van 1.000 “exclusieve targets” aan voor $500. [6] De gelekte configuraties werden al in oktober 2022 buitgemaakt door misbruik te maken van een (destijds pas ontdekte) kwetsbaarheid in de beheerinterface van FortiGate-devices (CVE-2022-40684). De configuraties lijken afkomstig vanaf FortiGate-devices vanuit (bijna) de hele wereld, maar veruit de meeste configuraties zijn te koppelen aan systemen in Mexico, de Verenigde Arabische Emiraten en Thailand. De configuraties van 464 devices lijken afkomstig te zijn van systemen in Nederland. Misbruik van de informatie in het lek is op verschillende manieren mogelijk, maar gedacht kan worden aan het opzetten van malafide VPN-tunnels en het ongeautoriseerd inloggen op management interfaces.

Nieuwe kritieke kwetsbaarheden verholpen in netwerkdevices

Naast de verouderde kwetsbaarheid in FortiGate, zoals misbruikt in eerder genoemd lek, verschenen er afgelopen maand ook weer een aantal nieuwe kritieke kwetsbaarheden die snelle actie vanuit beheerders vereisten om deze zo snel als mogelijk te patchen. Opvallend bij de nieuw gepubliceerde kwetsbaarheden is dat ze zich in veel gevallen bevinden in de (webgebaseerde) management interfaces van systemen en dat de kwetsbaarheden in veel gevallen al misbruikt werden voordat de leverancier een update kon uitbrengen (zogenoemde “zero day”-kwetsbaarheden).

	CVE-ID	Details
Ivanti Connect Secure en Ivanti Policy Secure [7, 8]	CVE-2025-0282	Kwetsbaarheid maakt het mogelijk op afstand willekeurige code uit te voeren zonder dat authenticatie vereist is. Actief misbruikt sinds midden december 2024.
FortiOS [9]	CVE-2024-55591	Een kwetsbaarheid in de beheer-interface van FortiOS stelde een kwaadwillende in staat om op afstand – zonder authenticatie – super-admin rechten te verkrijgen. Actief misbruikt sinds november 2024.
SonicWall Secure Mobile Access 1000 Appliances [10]	CVE-2025-23006	Een kwetsbaarheid in de beheer-interface stelt een kwaadwillende in staat om – zonder authenticatie – op afstand wilekeurige OS-commando’s uit te voeren. Actief misbruikt (onbekend sinds wanneer).
SonicWall SonicOS [11]	CVE-2024-53704	Een kwetsbaarheid in de authenticatie op SonicOS stelt een kwaadwillende in staat deze authenticatie via SSL-VPN-verbindingen te omzeilen.

Thema 2

Kwetsbare DNS-configuraties als oorzaak van incidenten

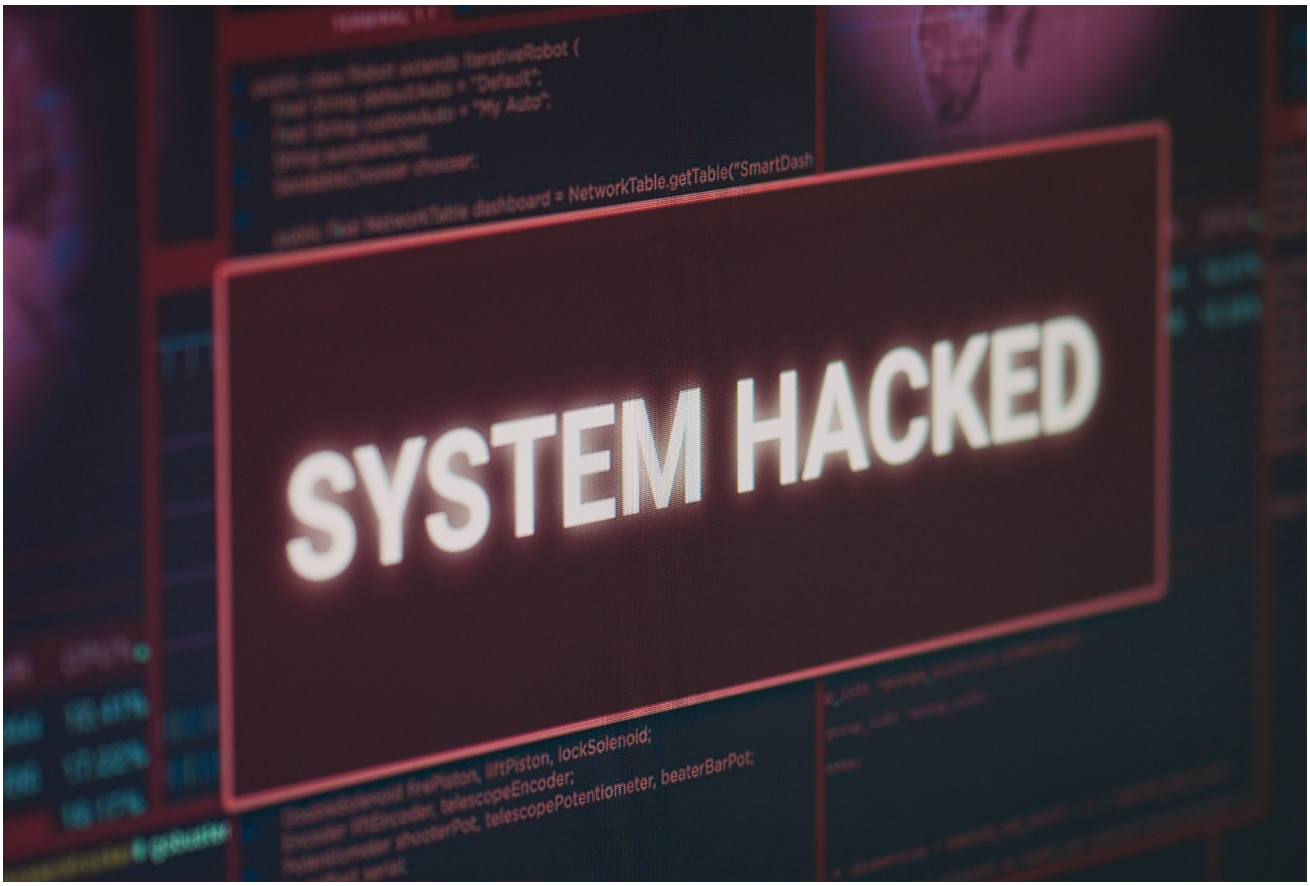
Het Domain Name System, kortweg DNS, bestaat al sinds begin jaren 80 van de vorige eeuw, maar nog altijd is DNS cruciaal voor internetverkeer én helaas vaak kwetsbaar ingericht. De kwetsbaarheden bij het gebruik van DNS ontstaan daarbij voornamelijk door slecht beheer en slechte configuraties, niet door kwetsbaarheden in DNS of de implementaties daarvan. Zulke slechte configuraties kunnen echter wel leiden tot diverse beveiligingsrisico's.

Misbruik van vergeten en verlopen domeinen

Aanvallers kunnen een slechte DNS-hygiëne – waarbij organisaties vergeten dat ze bepaalde domeinen in gebruik hebben of waarbij de registratie van domeinen verloopt – op verschillende manieren misbruiken voor malafide doeleinden, zo heeft F5 beschreven. [12]

Zo kunnen aanvallers deze domeinen misbruiken voor het uitvoeren van phishingaanvallen, waarbij het voor een slachtoffer lastig te herkennen is dat het om phishing gaat aangezien de verbinding verloopt via een domein dat daadwerkelijk van de aangevallen organisatie lijkt te zijn (en voorheen was). We zien dat phishingaanvallen nog altijd populair zijn, zeker de Actor-in-the-Middle-aanvallen waarbij een slachtoffer via het phishingdomein een legitieme inlogpagina bezoekt en de aanvaller al het verkeer daartussen kan onderscheppen. Uiteindelijk kan dit soort aanvallen resulteren in identiteitsdiefstal en het lekken van gevoelige informatie.

Andere malafide zaken waartoe het hebben van verlopen of vergeten domeinen kunnen leiden zijn het verkrijgen van digitale certificaten voor subdomeinen onder deze domeinen, het onderscheppen van verkeer naar deze domeinen (bijvoorbeeld verouderde API-koppelingen die naar deze domeinen verwijzen en e-mail) en het aanbieden van malafide content (malware) op de domeinen.



Onvolledige of ontbrekende inrichting van e-mailprotocollen

Het Computer Emergency Response Team CIRCL uit Luxemburg stuurde óók een waarschuwing uit voor misbruik van onjuist geconfigureerde domeinen, maar richtte zich daarbij voornamelijk op de gebrekkige configuratie van e-mailprotocollen in DNS. [13] Grofweg bestaan er drie protocollen waarmee binnen DNS de beveiliging van e-mail voor een domein kan worden ingericht: SPF, DKIM en DMARC (zie kader).

SPF, DKIM en DMARC

SPF (Sender Policy Framework) controleert of een mailserver gemachtigd is om e-mails te verzenden namens een bepaald domein, waardoor spoofing wordt voorkomen.

DKIM (DomainKeys Identified Mail) voegt een digitale handtekening toe aan e-mails, zodat de ontvanger kan verifiëren dat de e-mail echt van de afzender komt en niet is aangepast.

DMARC (Domain-based Message Authentication, Reporting, and Conformance) bouwt voort op SPF en DKIM en bepaalt hoe e-mails die deze verificaties niet doorstaan, moeten worden behandeld (bijv. markeren als spam of blokkeren). Een essentieel onderdeel is alignment, waarbij een ontvangende mailserver controleert of het afzenderadres (From-header) overeenkomt met de domeinen die door SPF en DKIM worden gevalideerd.

Dit voorkomt dat aanvallers e-mails verzenden met vervalste afzenderadressen en biedt betere bescherming tegen phishing en spoofing.

De waarschuwing vanuit CIRCL heeft vooral betrekking op SPF en geeft aan dat ongebruikte of slecht geconfigureerde domeinen een groot beveiligingsrisico vormen, omdat aanvallers deze kunnen misbruiken voor het versturen van phishing of spam. Dit is mogelijk op het moment dat een domein überhaupt niet over een SPF-configuratie beschikt of indien deze onvoldoende strikt is ingesteld. Volgens CIRCL maken aanvallers dankbaar misbruik van dit soort tekortkomingen om bijvoorbeeld phishing en frauduleuze facturen uit te sturen, waarbij de doelwitten veelal partners, leveranciers of klanten van een organisatie zijn.

Pinewood monitoort via de dienst External Attack Surface Management (EASM) de e-mailrecords (SPF, DMARC, DKIM) van aangesloten klanten.
Daarbij komt dit soort issues vaak aan het licht. Dit zijn enkele zaken die binnen deze dienst zijn opgevallen:

- Vrijwel elke organisatie is eigenaar van één of meerdere domeinen waarop géén SPF en/of DMARC is ingericht en die misbruikt kunnen worden voor spoofing.
- De belangrijkste reden waarom dit niet is ingericht, is omdat de organisatie de betreffende domeinen niet gebruikt voor legitieme e-mail. Het is echter van belang om wel mailrecords aan te maken voor deze domeinen om malaifide gebruik te voorkomen!
- Om spoofing van domeinen te voorkomen is het belangrijk om tevens een DMARC-policy te koppelen aan alle domeinen en hierop een policy van reject (of minimaal quarantine) te definiëren. Dit zorgt ervoor dat spoofed e-mails in het geheel niet door mailservers geaccepteerd worden of in quarantine worden geplaatst. We zien in de praktijk echter dat veel organisaties nog gebruikmaken van een none-policy (geen actie ondernemen bij afwijkingen) waardoor spoofing mogelijk blijft en DMARC in feite volledig ineffectief wordt ingezet.

Incidenten met foutief geconfigureerde DNS

Infoblox beschrijft in een artikel massaal misbruik te hebben waargenomen van domeinen waarop SPF onjuist is ingericht. [14] Dit misbruik vindt plaats vanuit een botnet van gekaapte MikroTik-routers waarbij de aanvaller deze routers inzet om via e-mail de malware verder te verspreiden. De e-mails doen zich voor als meldingen vanuit DHL (met valse DHL-facturen), met als doel om slachtoffers te laten klikken op geïnfecteerde bijlagen. Voor het versturen van deze e-mails maakt het botnet gebruik van zo'n 20.000 domeinen waarop SPF onjuist of niet is ingericht. Een voorbeeldconfiguratie die Infoblox daarbij beschrijft, is dat de zogenoemde SPF-policy (die bepaalt wat een mailserver moet doen als niet voldaan wordt aan de eisen zoals

beschreven in SPF) staat ingesteld op +all; deze instelling zorgt ervoor dat de eisen niet afgedwongen worden en mailservers mails nog steeds zullen accepteren, ook al voldoen deze niet aan hetgeen in het SPF-record gemeld staat.

De bekende internetjournalist Brian Krebs wist te melden dat er zich jarenlang een typo bevond in de DNS-records voor het domein az.mastercard.com, een subdomein onder het mastercard.com-domein [15] Een onderdeel van de DNS-configuratie voor een domein is de verwijzing naar één of meerdere nameservers (DNS-servers) die queries voor het domein kunnen beantwoorden. MasterCard maakt hiervoor gebruik van vijf verschillende nameservers van Akamai die allen te benaderen zijn via het akamai.net domein. Het bleek echter dat bij de vermelding van één van die nameservers de “t” op het einde van de naam ontbrak door een typo, waardoor deze verwees naar het (niet-geregistreerde) akamai.ne-domein. Een beveiligingsonderzoeker registreerde dit domein (wat onderdeel uitmaakt van de .ne TLD van Niger) en zag vervolgens honderdduizenden DNS-queries tot zich komen. Door malafide antwoorden te geven op deze queries had hij allerlei verkeer richting het az.mastercard.com-domein kunnen onderscheppen. Gelukkig lijkt het erop dat dit probleem niet eerder door malafide actoren is opgemerkt en er uiteindelijk geen schade is geweest.

```
└─# dig +tcp @dns1.mastercard.com az.mastercard.com

; <<>> DiG 9.19.17-2~kali1-Kali <<>> +tcp @dns1.mastercard.com az.mastercard.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45077
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 6d51066062f6102a13bff6c8678149d366a3aabb89779394 (good)
;; QUESTION SECTION:
;az.mastercard.com.             IN      A

;; AUTHORITY SECTION:
az.mastercard.com.      3600    IN      NS      a1-29.akam.net.
az.mastercard.com.      3600    IN      NS      a7-67.akam.net.
az.mastercard.com.      3600    IN      NS      a22-65.akam.ne.
az.mastercard.com.      3600    IN      NS      a26-66.akam.net.
az.mastercard.com.      3600    IN      NS      a9-64.akam.net.

;; Query time: 92 msec
;; SERVER: 216.119.218.53#53(dns1.mastercard.com) (TCP)
;; WHEN: Fri Jan 10 11:24:51 EST 2025
;; MSG SIZE  rcvd: 191
```

A DNS lookup on the domain az.mastercard.com on Jan. 14, 2025 shows the mistyped domain name a22-65.akam.ne.

Het foutieve DNS-record. Bron: https://krebsonsecurity.com/2025/01/mastercard-dns-error-went-unnoticed-for-years/

Thema 3

Aanvallen op Amazon S3

Amazon S3 (Simple Storage Service) is een cloudopslagdienst van Amazon Web Services (AWS) voor het opslaan en ophalen van data via het internet. Het wordt wereldwijd gebruikt door bedrijven, overheden en ontwikkelaars en is populair voor onder andere back-ups, big data-analyse, hosting van statische websites en machine learning-toepassingen. Afgelopen maand zagen we diverse dreigingen rondom Amazon S3 voorbijkomen.

Ransomware-aanvallen vanuit “Codefinger”

Organisaties die data opslaan in Amazon S3 kregen te maken met de dreiging van dataversleuteling. Een groep genaamd “Codefinger”, heeft het voorzien op de S3-instances van organisaties en maakt gebruik van standaard versleutelingstechnieken binnen S3 om de opgeslagen data onbruikbaar te maken voor de eigenaar. [16] Voor de initiële toegang tot S3-instances maakt de aanvaller misbruik van publiek gelekte AWS-sleutels waarmee het mogelijk is om data in betreffende S3-instances zowel te lezen als te schrijven. Vervolgens maakt de aanvaller gebruik van de standaard aanwezige AWS Server-Side Encryption functionaliteit om de data in de S3-instance onleesbaar te maken (te versleutelen). De sleutel om de data weer leesbaar te maken, houdt de aanvaller uiteraard alleen voor zichzelf. Pogingen om de data weer te ontsleutelen, zullen voor het slachtoffer vruchteloos zijn zolang deze niet beschikt over deze sleutel. De aanvaller voert de druk vervolgens nog iets verder op door via een andere standaard AWS-functionaliteit (“Amazon S3 Object Lifecycle Management’) in te stellen dat alle data na 7 dagen automatisch verwijderd zal worden. Door dit extra pressiemiddel hoopt de aanvaller uiteraard dat het slachtoffer bereid zal zijn om de losgeldsom te betalen die de aanvaller via dit type ransomwareaanval heeft geëist.

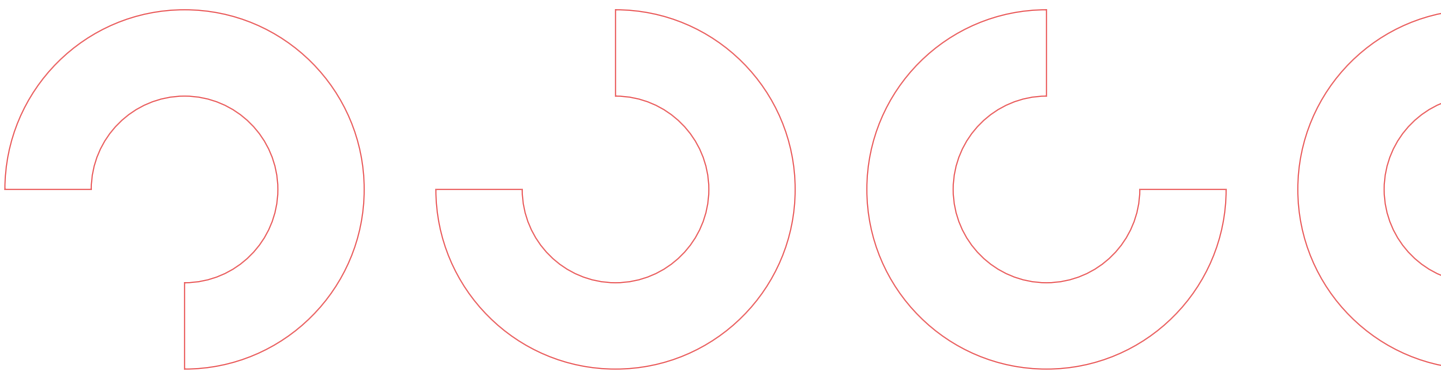
Misbruik van vergeten S3-instances

Naast de problemen die zich kunnen voordoen met ingebruikzijnde S3-instances kunnen er ook problemen ontstaan met S3-instances waarvan een organisatie niet langer meer gebruikmaakt en die het wellicht allang is vergeten. Onderzoekers van WatchTowr besloten op zoek te gaan naar zulke vergeten S3-instances om te zien welke schadelijke effecten dit mogelijk zou kunnen hebben. [17] In hun zoektocht vonden ze ongeveer 150 S3-instances die voorheen in gebruik waren door commerciële en open-source software en overheden, maar die inmiddels niet meer actief (en niet meer geregistreerd) waren. De onderzoekers registreerden deze S3-instances nu op hun eigen naam om te zien wat voor verzoeken hier nog op uit zouden komen. De resultaten waren verrassend te noemen, want in 2 maanden tijd ontvingen ze op de geregistreerde instances maar liefst 8 miljoen HTTP-verzoeken.

Door vast te leggen om wat voor verzoeken het ging, ontdekten ze dat – ondanks het feit dat de S3-instances al enige tijd niet meer bestonden– allerlei systemen op het internet nog steeds op zoek waren naar bijvoorbeeld softwareupdates, Windows-/Linux-/MacOS-bestanden, images van virtual machines, Javacript-bestanden en SSL-VPN-configuraties. Hoewel de onderzoekers dit niet hebben gedaan, hadden ze hierop kunnen antwoorden met malafide versies van bestanden en zwakke configuraties om daarmee via de overgenomen instances systemen te infecteren met malware en/of deze kwetsbaar te maken. Belangrijk te beseffen is dat dit soort problemen – die kunnen leiden tot grootschalige supply chainaanvallen – zich niet alleen voordoen met Amazon S3, maar net zo goed met andere opslagservices in de cloud.

Incidenten met S3-instances

Twee organisaties ondervonden recent de gevolgen van een compromittatie van hun S3-instance: hotelmanagementplatform Otelier en leverancier van locatie-intelligentie Gravy Analytics. Beiden zagen de data op hun S3-instance ten prooi vallen aan aanvallers met een groot datalek als gevolg. In het geval van Otelier wisten de aanvallers in eerste instantie in te breken op het (interne) ticketingsysteem van de organisatie door inloggegevens hiervoor via malware buit te maken van een medewerker. [18] Nadat toegang was verkregen tot dit systeem, wisten de aanvallers vervolgens binnen tickets in dit systeem de benodigde informatie te vinden om ook toegang te verkrijgen tot de S3-instances van de organisatie. De aanvallers wisten 7,8 terabyte aan informatie buit te maken waarmee ze zonder succes probeerden om het slachtoffer af te persen. Onduidelijk is nog hoe gevoelig exact de informatie in de dataset is, maar naar verluidt zou de dataset o.a. reserveringsinformatie, transacties, e-mails van medewerkers en andere interne data bevatten. In het geval van Gravy Analytics is nog niet bekendgemaakt hoe de aanvallers toegang wisten te verkrijgen tot de S3-instance van het bedrijf. De criminelen achter de aanval beweren 17 terabyte aan informatie te hebben verzameld, waarbij het voornamelijk lijkt te gaan om lokatiegegevens van mobiele telefoons die verzameld zijn via apps als Tinder, Grindr, Candy Crush en Subway Surfers. [19, 20]



Thema 4

Opvallend veel meldingen m.b.t. DDoS-aanvallen

DDoS-aanvallen vinden doorlopend plaats, maar in veel gevallen wordt hier weinig ruchtbaarheid aan gegeven omdat een aanval maar heel kortdurend was of weinig impact sorteerde. Afgelopen maand ondervonden een aantal Nederlandse organisaties echter duidelijk hinder van DDoS-aanvallen en meldden diverse bedrijven nog altijd een toename in frequentie en hevigheid van dit soort aanvallen te zien.

DDoS-aanvallen op DigiD en SURF

Zowel DigiD als SURF (de ict-coöperatie van Nederlandse onderwijs- en onderzoeksinstellingen) kregen te maken met DDoS-aanvallen die uiteindelijk resulteerden in het tijdelijk uitvallen en verminderd bereikbaar zijn van diensten. Naast DigiD raakten ook andere digitale diensten van Logius ombereikbaar, waarbij Logius spreekt van een “uitzonderlijk hoog volume” aanvallen die zorgden voor overbelasting van het netwerk. [21] Ook de aanvallen op SURF (op 15, 16 en 17 januari 2025) leidden tot overbelasting van netwerken en het onbeschikbaar raken hiervan. [22]

Trend: meer en zwaardere aanvallen

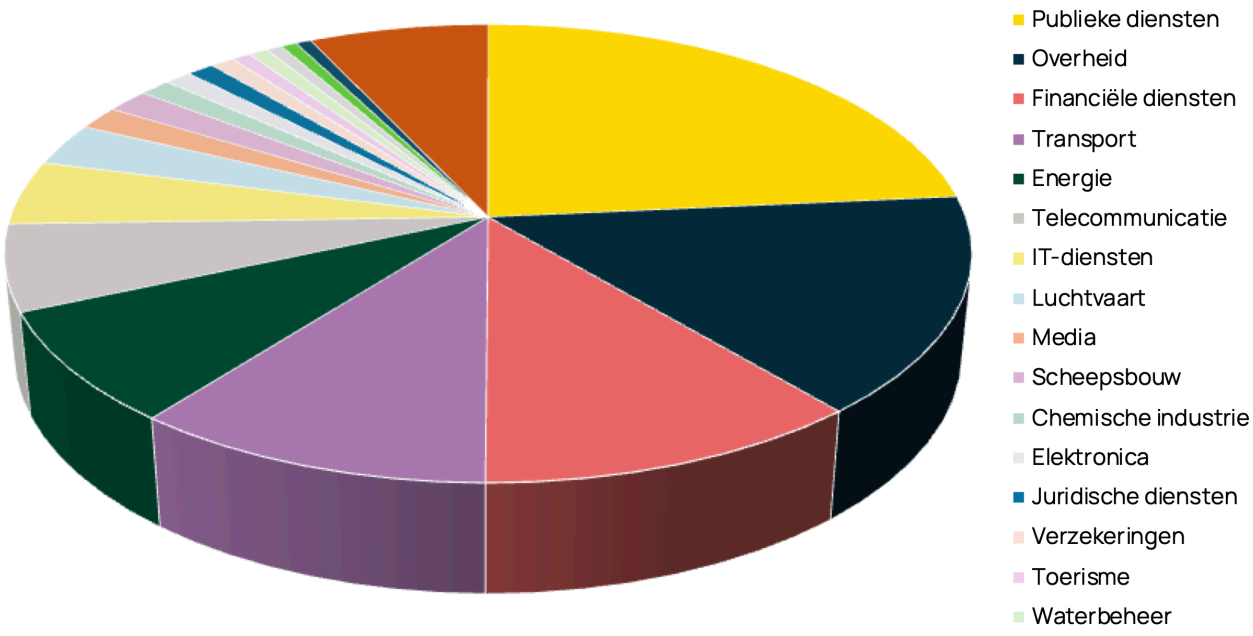
Trend Micro meldt een toename in DDoS-aanvallen te zien, waarbij de meest recent waargenomen golf zich voornamelijk richtte op Japanse bedrijven (internetproviders, financiële instellingen en een luchtvaartmaatschappij). [23] De aanvallers maken hierbij gebruik van een IoT-gebaseerd botnet waar continu nieuwe devices aan worden toegevoegd door misbruik te maken van zwakke wachtwoorden of kwetsbaarheden op deze devices.

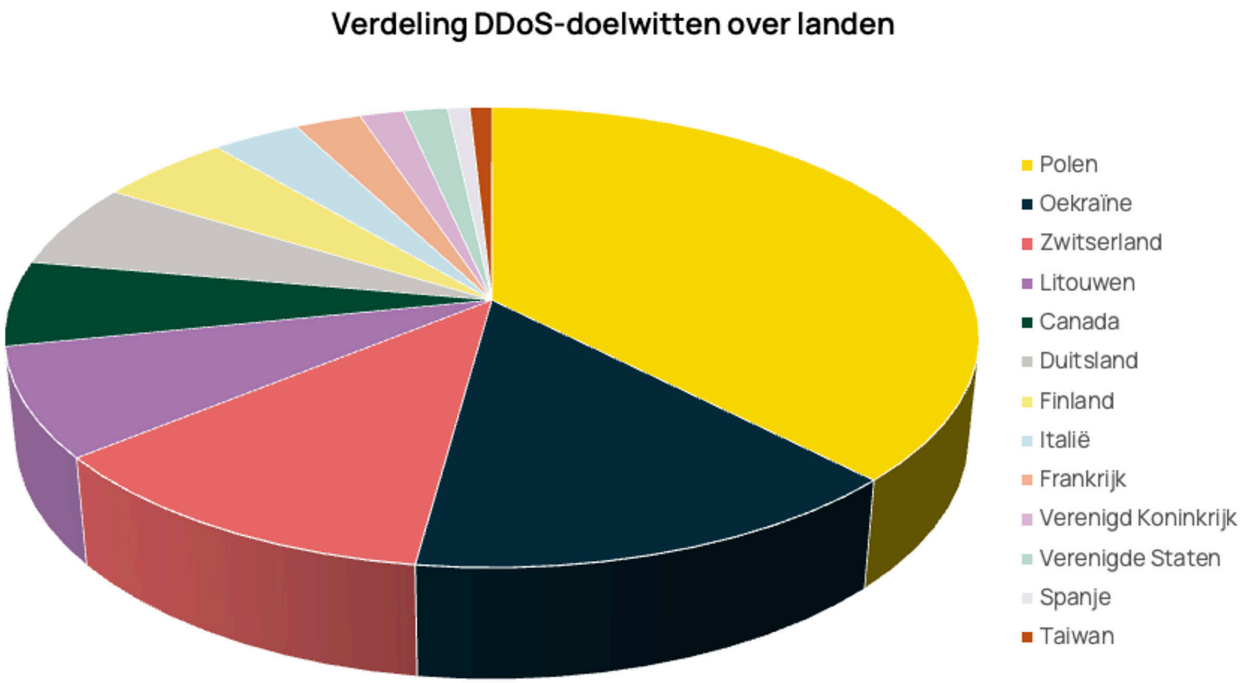
Cloudflare zegt in 2024 53% meer DDoS-aanvallen te hebben gezien in vergelijking met een jaar eerder. Bovendien registreerde Cloudflare steeds zwaardere aanvallen. [24] Alleen al in het vierde kwartaal van 2024 zag Cloudflare 420 “hypervolumetrische” aanvallen die zich kenmerken door een aanval met meer dan 1 miljard packets per seconde en een bandbreedte van meer dan 1 terabits per seconde. Daarnaast zag Cloudflare ook een record sneuvelen, want een recordaanval ter grootte van 5,6 terabits per seconde was zwaarder dan ooit gezien.

Dreiging vanuit NoName057(16)

Eén van de bekendere actoren op het gebied van DDoS-aanvallen is NoName057(16). Deze pro-Russische groepering voert DDoS-aanvallen uit middels het zogenoemde “DDoSia”-project. Doorlopend publiceert de groep een lijst van nieuwe doelwitten waarop de DDoS-aanvallen zich moeten richten. [23] Deze lijsten zijn voor iedereen in te zien en geven dus een goed beeld van waar de aanvallen zich op dit moment op richten. Recent zijn er geen Nederlandse organisaties/websites op de lijst van deze groepering geplaatst, maar dit kan uiteraard op elk moment veranderen. Om een beter beeld te krijgen van de doelwitten van deze groep, hebben we de gepubliceerde doelwitten van januari 2025 op een rijtje gezet. Daaruit blijkt dat de meeste doelwitten gerelateerd zijn aan overheidsinstellingen (publieke diensten en overheid), gevolgd door organisaties binnen de financiële dienstverlening. Nederlandse organisaties kwamen afgelopen maand dus niet voor in de target-lists die wordt aangevoerd door Polen, Oekraïne en Zwitserland.

Verdeling DDoS-doelwitten over sectoren




Verdeling DDoS-doelwitten over landen
Polen
Oekraïne
Zwitserland
Litouwen
Canada
Duitsland
Finland
Italië
Frankrijk
Verenigd Koninkrijk
Verenigde Staten
Spanje
Taiwan

Maatregelen

Op basis van de thema's kunnen we een aantal essentiële maatregelen benoemen die organisaties zouden moeten implementeren om beschermd te zijn tegen de beschreven dreigingen:

Op basis van de thema's kunnen we een aantal essentiële maatregelen benoemen die organisaties zouden moeten implementeren om beschermd te zijn tegen de beschreven dreigingen:

- **Inventariseer en monitoor continu alle publiek ontsloten assets van de organisatie**
  Het is belangrijk om continu een up-to-date inzicht te hebben in alle assets die de organisatie richting internet ontsluit. Assets waarvan je niet afweet, kun je ook niet beschermen is daarbij het idee. Het gaat om allerlei soorten assets waaronder domeinen, certificaten, IP-adressen, cloud resources (Amazon S3 buckets bijvoorbeeld!) en meer. Nadat alle assets afdoende zijn geïnventariseerd, is het van belang te monitoren of de configuraties ervan nog steeds correct en strikt genoeg zijn. Daar waar de configuratie niet afdoende blijkt, dient men zo snel mogelijk wijzigingen door te voeren om dit te repareren. Niet meer in gebruik zijnde resources ruimt men volledig op of houdt men gecontroleerd in stand om malafide overname te voorkomen (hygiëne).

- **Dwing het gebruik van MFA af op alle extern ontsloten accounts (bijvoorbeeld cloud en VPN)**
  Het gebruik van multifactor-authenticatie voorkomt in veel gevallen ongeautoriseerde toegang tot netwerken en systemen. Het is daarom van belang om extern ontsloten accounts te voorzien van MFA, waardoor het niet meer mogelijk is hierop in te breken met alleen een gebruikersnaam en wachtwoordcombinatie. In sommige gevallen zal het niet mogelijk zijn om op alle accounts MFA toe te passen (bijvoorbeeld voor serviceaccounts) en zijn aanvullende maatregelen vereist om misbruik ervan te voorkomen (denk aan IP whitelisting). Gezien de steeds geavanceerdere vormen van phishing, is het bovendien belangrijk om zoveel mogelijk te kiezen voor "phishingresistente" MFA-oplossingen, in ieder geval voor accounts met hoge rechten. Tot slot is het van belang om de toegang tot accounts te monitoren om zo in een zo vroeg mogelijk stadium misbruik van accounts te kunnen detecteren.

- **Zorg voor een goed ingericht patchmanagementproces**
  Het is van groot belang om kritieke kwetsbaarheden zo snel mogelijk weg te nemen door het installeren van een patch of het doorvoeren van een workaround. Aanvallers zijn continu op zoek naar nieuwe kwetsbaarheden en zijn in staat deze binnen korte tijd uit te buiten, dus snelle response is essentieel. In sommige gevallen vindt misbruik al plaats voordat de kwetsbaarheid überhaupt bekend is (en dus nog geen patches of workarounds beschikbaar zijn), waardoor ook aanvullende maatregelen (zoals het strikt segmenteren van het netwerk) van belang zijn om de impact van kwetsbaarhedenmisbruik te verkleinen. Ook hierbij is het van belang dat de organisatie een duidelijk beeld heeft van de software en systemen die het op internet ontsluit (het eerste punt) zodat bij het bekendworden van nieuwe kwetsbaarheden ook direct duidelijk is óf een organisatie kwetsbaar is en zo ja, op welke plekken.

- **Mailprotocollen zijn toegepast op alle domeinen**
  Om misbruik van domeinen van een organisatie te voorkomen, is het van belang dat SPF (en liefst ook DMARC) is toegepast op alle domeinen die in eigendom zijn van de organisatie. Dit geldt niet alleen voor de domeinen die de organisatie ook daadwerkelijk voor e-maildoeleinden inzet, maar voor alle domeinen. Bovendien dient daarbij continu monitoring plaats te vinden van de SPF- en DMARC-configuraties om eventueel tijdig problemen hierin te kunnen detecteren. Daarnaast is het verstandig om actief DMARC-rapportages vanuit mailservers te ontvangen en te verwerken om op die manier misbruik van domeinen en configuratiefouten vast te kunnen stellen.

[1] https://esentire-dot-com-assets.s3.amazonaws.com/assets/resourcefiles/eSentire-TRU-Report-The-Modern-Threat-Actors-Playbook-How-Initial-Access-and-Ransomware-Deployment-Trends-are-Shifting-in-2025.pdf
[2] https://www.cnil.fr/fr/violations-massives-de-donnees-en-2024-quels-sont-les-principaux-enseignements-mesures-a-prendre
[3] https://www.trendmicro.com/en_us/research/25/a/iot-botnet-linked-to-ddos-attacks.html
[4] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10086523
[5] https://doublepulsar.com/2022-zero-day-was-used-to-raid-fortigate-firewall-configs-somebody-just-released-them-a7a74e0b0c7f
[6] https://cyberplace.social/@GossiTheDog/113924035304156708
[7] https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US
[8] https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day?e=48754805
[9] https://www.fortiguard.com/psirt/FG-IR-24-535
[10] https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002
[11] https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003
[12] https://www.f5.com/labs/articles/threat-intelligence/the-dangers-of-dns-hijacking
[13] https://www.circl.lu/pub/tr-92/
[14] https://blogs.infoblox.com/threat-intelligence/one-mikro-typo-how-a-simple-dns-misconfiguration-enables-malware-delivery-by-a-russian-botnet/
[15] https://krebsonsecurity.com/2025/01/mastercard-dns-error-went-unnoticed-for-years/
[16] https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c
[17] https://labs.watchtowr.com/8-million-requests-later-we-made-the-solarwinds-supply-chain-attack-look-amateur/
[18] https://www.bleepingcomputer.com/news/security/otelier-data-breach-exposes-info-hotel-reservations-of-millions/
[19] https://fido.nrk.no/8a09133d2b14a7e72c31006ef2611b22fd78d7c6bfd7cc62f7d35f13b3c2d338/Datatilsynet_Unacast_Security%20Incident%20Notification_Redacted.pdf
[20] https://www.theregister.com/2025/02/06/gravy_analytics_data_breach_suit/
[21] https://www.logius.nl/actueel/update-grootschalige-ddos-aanvallen-op-logius-diensten
[22] https://www.surf.nl/en/news/update-ddos-attack-surf-network
[23] https://www.trendmicro.com/en_us/research/25/a/iot-botnet-linked-to-ddos-attacks.html
[24] https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/
[25] https://witha.name/data/

pinewood
THE INTERSTELLAR COLLECTION

Hoe helpt Pinewood?

Pinewood is een honderd procent Nederlands bedrijf met 30 jaar specialistische ervaring in cybersecurity. Pinewood heeft een eigen SOC in Delft. Daar werken hoogopgeleide, Nederlandstalige security-analisten. Zij houden 24 uur per dag, zeven dagen per week de systemen en netwerken van onze klanten nauwlettend in de gaten. De security-experts van Pinewood slaan een brug tussen techniek en beleid, zodat ze complexe analyses uit de techniek direct kunnen omzetten naar strategische en beleidsmatige maatregelen.

Wij beseffen dat elke klant anders is. Wij richten ons uiteraard op de bekendste digitale risico's en dreigingen maar leveren ook maatwerk dat voldoet aan de specifieke eisen van uw organisatie. Pinewood detecteert en analyseert niet alleen, maar speelt tevens een adviserende rol. Bij dit advies staan aspecten zoals sector- of klant specifieke dreigingen, wet- en regelgeving en versterken van uw weerbaarheid centraal.

Wilt u meer weten over het SOC van Pinewood of over onze security diensten?

Neemt u dan contact met ons op via 015 251 36 36 of stuur een e-mail naar sales@pineood.nl

Wij staan u graag te woord.

Pinewood BV.
Delftechpark 35
2628 XJ, Delft

015 251 36 36
info@pinewood.nl
www.pinewood.nl

NEN 7510
INFORMATIEBEVEILIGING
IN DE ZORG

ISO