eRemote

Kwetsbaarheden in Microsoft Defender Updates bij Groeiende Geopolitieke Onrust

1. Introductie

Microsoft Defender speelt een cruciale rol als een dominante endpoint security oplossing, met name in omgevingen waar Windows besturingssystemen een significant marktaandeel bezitten, zoals in Nederland. Het hoge marktaandeel van Windows, geschat rond de 74% [1], vestigt Microsoft Defender als een fundamentele beveiligingslaag voor een omvangrijke gebruikersgroep. Deze dominantie maakt het update mechanisme een zeer aantrekkelijk doelwit voor kwaadwillende actoren die streven naar een wijdverspreide impact. Een succesvolle compromittering van het update systeem van Defender zou potentieel een groot deel van de computers in Nederland kunnen treffen, wat het tot een strategisch objectief maakt voor tegenstanders, vooral in tijden van geopolitieke spanning.

Het escalerende mondiale geopolitieke landschap, gekenmerkt door toegenomen spanningen en conflicten [5], heeft directe implicaties voor het cyberdomein, dat transformeert in een stille slagveld.[5] Geopolitieke instabiliteit voedt een toename van door staten gesponsorde cyberoperaties [5], waarbij natiestaten in toenemende mate cybercapaciteiten inzetten voor spionage, verstoring en het bereiken van strategische voordelen. Dit verhoogt het risico voor kritieke software zoals antivirusoplossingen. Naarmate traditionele oorlogsvoering het risico op escalatie met zich meebrengt, bieden cyberaanvallen een minder direct toewijsbare en potentieel impactvollere manier voor landen om invloed uit te oefenen en schade toe te brengen aan hun tegenstanders. Beveiligingssoftware, als hoeksteen van digitale verdediging, wordt een primair doelwit voor dergelijke operaties.

De specifieke bezorgdheid van de gebruiker in Nederland met betrekking tot de veiligheid en potentiële kwetsbaarheden van Microsoft Defender updates in deze verhoogde geopolitieke context is pertinent. Nederland, als een technologisch geavanceerd land en lid van internationale allianties, zou een doelwit kunnen zijn voor cyberoperaties. De veiligheid van de digitale infrastructuur, die sterk afhankelijk is van Windows en Defender, is daarom een legitieme zorg. De convergentie van een dominant beveiligingsproduct, een technologisch geavanceerd gebruikersbestand in Nederland en een steeds volatielere geopolitieke omgeving waarin cyberoorlogvoering een groeiende realiteit is, onderstreept de validiteit van deze bezorgdheid.

Het doel van dit rapport is om een gedetailleerde analyse op expertniveau te bieden van het Microsoft Defender updateproces, potentiële kwetsbaarheden te identificeren die kunnen worden misbruikt, met name in de context van groeiende geopolitieke onrust, en bruikbare aanbevelingen te doen om deze risico's voor gebruikers en organisaties in Nederland te beperken.

2. Microsoft Defender Update Architectuur en Proces

Microsoft Defender ontvangt updates doorgaans automatisch via Windows Update [10], wat een handig en frequent kanaal is. Deze afhankelijkheid maakt de veiligheid van de Windows Update infrastructuur zelf echter cruciaal. Elke compromittering daarvan zou wijdverspreide gevolgen kunnen hebben. Als een dreigingsactor controle zou krijgen over delen van het Windows Update systeem, zouden ze potentieel kwaadaardige updates kunnen verspreiden die vermomd zijn als

legitieme, wat niet alleen het besturingssysteem maar ook geïntegreerde beveiligingscomponenten zoals Defender zou treffen.

Gebruikers kunnen handmatig updates initiëren via de Windows Beveiliging app [10], wat een zekere mate van controle biedt. Dit is echter afhankelijk van de alertheid van de gebruiker en tijdig handelen. In een geopolitiek geladen scenario zouden gebruikers het doelwit kunnen worden van social engineering tactieken om legitieme updates uit te stellen of te vermijden, of om valse updates te installeren. Aanvallers zouden publieke angst of onzekerheid tijdens geopolitieke gebeurtenissen kunnen misbruiken om desinformatie over updates te verspreiden, waardoor gebruikers onveilige keuzes zouden kunnen maken met betrekking tot hun antivirusbescherming.

Voor organisaties kunnen beheerders updates centraal beheren [10], wat consistentie en tijdige implementatie kan waarborgen. Dit vormt echter ook een centraal aanvalspunt. Het compromitteren van de update server of beheerconsole zou aanvallers in staat kunnen stellen om kwaadaardige updates over het gehele netwerk te verspreiden. In een geopolitiek conflict zouden organisaties specifiek het doelwit kunnen zijn, en hun update infrastructuur zou een primair doelwit kunnen zijn voor tegenstanders die streven naar het verstoren van operaties of het verkrijgen van toegang tot gevoelige gegevens.

Microsoft biedt ook de mogelijkheid om updates handmatig te downloaden van hun website.[10] Hoewel dit in specifieke situaties nuttig kan zijn, introduceert het ook een risico als gebruikers worden misleid om updates van onofficiële of gecompromitteerde bronnen te downloaden, vooral tijdens perioden van verhoogde geopolitieke spanningen waarin desinformatie zich snel kan verspreiden. Dreigingsactoren zouden valse websites kunnen creëren die de update portal van Microsoft nabootsen om malware te verspreiden, inspelend op de angst van gebruikers in onzekere tijden.

Microsoft Defender ontvangt frequent security intelligence updates, soms meerdere keren per dag [10], om gelijke tred te houden met het evoluerende dreigingslandschap. Deze hoge frequentie is weliswaar gunstig voor de bescherming, maar betekent ook dat een grote hoeveelheid updates veilig moet worden geleverd en geverifieerd. Elke verstoring of compromittering van deze snelle updatestroom zou systemen kwetsbaar kunnen maken voor zero-day aanvallen, een risico dat kan worden versterkt tijdens geopolitieke crises. Als een door de staat gesteunde actor een vertraagde of gemanipuleerde security intelligence update zou kunnen injecteren, zouden ze een kans kunnen creëren om systemen te misbruiken voordat de legitieme update wordt toegepast.

Naast de frequente security intelligence updates brengt Microsoft ook maandelijks platform- en engine-updates uit.[10] Deze updates bevatten vaak kritieke beveiligingsfixes en verbeteringen. Vertragingen bij het toepassen van deze updates, hetzij door administratief toezicht, hetzij door opzettelijke vermijding door gebruikers die bang zijn voor gecompromitteerde updates tijdens geopolitieke onrust, zouden systemen kunnen blootstellen aan bekende kwetsbaarheden die actief kunnen worden misbruikt door door de staat gesteunde actoren. Tegenstanders zouden de release van deze maandelijkse updates kunnen volgen om snel systemen te identificeren en te misbruiken die niet zijn gepatcht, vooral als de geopolitieke spanningen hoog zijn en cyberaanvallen worden verwacht.

Microsoft slaat gegevens die door Defender for Endpoint voor Europese gebruikers worden verzameld, op binnen de EU.[21] Hoewel dit belangrijk is voor gegevensprivacy en compliance, staat het los van de veiligheid van het updateproces zelf. De locatie van de gegevensopslag voorkomt of vermindert niet direct kwetsbaarheden in de manier waarop updates worden gemaakt, ondertekend en gedistribueerd. De focus op data-residentie, hoewel cruciaal voor naleving van regelgeving, mag het even belangrijke aspect van het waarborgen van de integriteit en veiligheid van de software-updates zelf niet overschaduwen, vooral in de context van geopolitieke cyberdreigingen.

3. Beveiligingsfuncties en Integriteitscontroles in het Updateproces

Microsoft gebruikt SHA-2 digitale handtekeningen voor alle security intelligence updates sinds oktober 2019.[10] Dit is een kritieke beveiligingsmaatregel die helpt de authenticiteit en integriteit van de updates te waarborgen. Systemen die SHA-2 niet ondersteunen, ontvangen deze updates niet meer, waardoor ze potentieel kwetsbaar blijven. In een geopolitiek scenario zouden tegenstanders kunnen proberen systemen met verouderde software te misbruiken die dit ondertekeningsmechanisme niet ondersteunen. De afhankelijkheid van SHA-2 ondertekening biedt een sterke verdedigingslaag tegen ongeautoriseerde wijzigingen of nabootsing van updates. De kracht van deze verdediging hangt echter af van de veiligheid van de private sleutels van Microsoft.

Gebruikers met voldoende technische expertise kunnen de digitale handtekeningen van gedownloade updatebestanden handmatig verifiëren.[15] Dit biedt een extra zekerheidslaag, maar is voor de meeste gebruikers geen praktische stap. Tijdens perioden van geopolitieke onzekerheid zou het aanmoedigen van gebruikers in kritieke sectoren om dergelijke verificatie uit te voeren een verstandige maatregel kunnen zijn. Hoewel handmatige verificatie een optie is, is de effectiviteit ervan beperkt door het aantal gebruikers dat de nodige vaardigheden en bewustzijn bezit om dit uit te voeren.

De ontdekking van CVE-2023-24934 [24] toont aan dat zelfs met digitale handtekeningen kwetsbaarheden kunnen bestaan binnen de software zelf die kunnen worden misbruikt om beveiligingsfuncties te omzeilen. Dit incident, dat de potentie had om bedreigingen te verwijderen en toegestane bestanden te manipuleren, werd door Microsoft verholpen, wat het belang van continue monitoring en patching benadrukt, vooral in het licht van potentiële geopolitieke cyberdreigingen. Deze kwetsbaarheid onderstreept dat beveiliging een gelaagde aanpak is. Hoewel een veilige updatelevering cruciaal is, is de veiligheid van de software die wordt bijgewerkt even belangrijk.

Microsoft hanteert Safe Deployment Practices (SDP) [39] voor zijn updates, waaronder interne tests en geleidelijke uitrol. Dit helpt het risico te beperken dat een gecompromitteerde update een groot aantal gebruikers tegelijkertijd treft. Echter, geavanceerde, gerichte aanvallen, mogelijk door door de staat gesteunde actoren tijdens geopolitieke onrust, kunnen dit proces nog steeds omzeilen, vooral als ze systemen in de vroege stadia van de uitrol kunnen identificeren en targeten. Hoewel SDP een beveiligingslaag toevoegt, is het niet waterdicht tegen vastberaden en vindingrijke tegenstanders die hun aanvallen kunnen afstemmen om deze waarborgen te omzeilen.

Microsoft Defender is afhankelijk van verbindingen met specifieke Microsoft servers voor cloudgebaseerde bescherming en updates.[41] Deze gecentraliseerde aanpak helpt de bronnen van

updates te controleren en vermindert het risico dat gebruikers naar kwaadaardige servers van derden worden geleid. In een scenario van extreme geopolitieke spanning kan de mogelijkheid dat deze Microsoft servers zelf het doelwit worden van geavanceerde aanvallen echter niet volledig worden uitgesloten. Hoewel het direct aanvallen van de update-infrastructuur van Microsoft een hoge drempel is, zouden door de staat gesteunde actoren met aanzienlijke middelen een dergelijke optie in een extreme crisis kunnen overwegen.

4. Potentiële Kwetsbaarheden en Dreigingscenario's

Software update processen, inclusief die van antivirusoplossingen, zijn vatbaar voor supply chain aanvallen.[6] Geopolitieke instabiliteit zou het risico kunnen vergroten dat natiestaten proberen de ontwikkelings- of distributiekanalen van Microsoft te infiltreren om Defender updates te compromitteren, wat potentieel zou leiden tot een wijdverspreide implementatie van malware. De SolarWinds aanval [45] dient als een grimmige herinnering aan de potentiële impact van dergelijke aanvallen. Een succesvolle compromittering van de supply chain zou aanvallers in staat stellen om kwaadaardige code in legitieme updates in te bedden bij de bron, waardoor detectie uiterst moeilijk wordt voor eindgebruikers en zelfs beveiligingssoftware.

Hoewel digitale handtekeningen de kans op succesvolle MITM-aanvallen op Microsoft Defender updates aanzienlijk verminderen [46], kunnen kwetsbaarheden in de implementatie van het updateproces of een compromittering van de ondertekeningssleutels nog steeds worden misbruikt door geavanceerde aanvallers, vooral die met staatsniveau middelen en motivaties tijdens geopolitieke conflicten.[47] De historische kaping van eScan antivirus updates [54] toont de reële mogelijkheid van dergelijke aanvallen aan. Aanvallers zouden kunnen zoeken naar zwakke plekken in de communicatieprotocollen die voor updates worden gebruikt of proberen gebruikers te misleiden om valse certificaten te accepteren, hoewel dit laatste steeds moeilijker wordt met moderne browserbeveiligingsfuncties.

CVE-2023-24934 [24] illustreert dat zelfs met veilige updatelevering kwetsbaarheden binnen Microsoft Defender zelf kunnen worden misbruikt. In een geopolitiek geladen omgeving zouden dergelijke omzeilingen kunnen worden gebruikt door gerichte malware die via legitieme updates wordt geleverd om detectie te ontwijken. Door de staat gesteunde actoren zouden bijzonder geïnteresseerd kunnen zijn in het misbruiken van dergelijke kwetsbaarheden om spionage of sabotage uit te voeren zonder de waarschuwingen van Defender te activeren.

De succesvolle kaping van het update mechanisme van eScan [54] om malware te verspreiden dient als een verontrustend precedent. Hoewel eScan niet zo wijdverspreid is als Microsoft Defender, zou de techniek potentieel kunnen worden aangepast voor prominentere doelwitten, vooral door goed gefinancierde en geavanceerde actoren tijdens perioden van geopolitieke spanningen. Het feit dat de kwetsbaarheid in eScan minstens vijf jaar bestond, onderstreept de noodzaak van rigoureuze en voortdurende beveiligingsaudits van updateprocessen. Dit incident belicht een potentieel aanvalsvector die aantrekkelijk zou kunnen zijn voor door de staat gesteunde groepen die een groot aantal systemen heimelijk willen compromitteren.

Natiestaten beschikken over de geavanceerde capaciteiten en strategische motivaties om kritieke software zoals Microsoft Defender te targeten.[5] In een geopolitiek conflict zou het compromitteren van het update mechanisme van Defender een significant voordeel kunnen opleveren door hen in

staat te stellen bescherming uit te schakelen of malware te implementeren op een breed scala aan systemen in doelwittenlanden, waaronder Nederland. De potentiële impact van een dergelijke aanval op de nationale veiligheid en kritieke infrastructuur maakt het een plausibel dreigingsscenario dat moet worden overwogen.

APT-groepen, vaak gelinkt aan natiestaten, staan bekend om hun geavanceerde en persistente aanvallen.[44] Het compromitteren van een Microsoft Defender update zou een effectieve manier kunnen zijn voor hen om heimelijk, langdurige toegang te krijgen tot doelwitsystemen in Nederland voor spionage, datadiefstal of toekomstige disruptieve activiteiten, vooral gezien de hoge prevalentie van Windows in het land. Updates bieden een legitiem en frequent kanaal voor softwarewijzigingen, waardoor ze een ideale vector zijn voor het implementeren van persistente malware die gedurende lange perioden detectie kan ontwijken.

Verhoogde geopolitieke spanningen kunnen leiden tot een toename van de algemene cyberactiviteit, inclusief potentiële false flag operaties.[5] Dit zou het moeilijker kunnen maken om aanvallen op Microsoft Defender updates nauwkeurig toe te schrijven, wat mogelijk leidt tot verwarring en een afname van het gebruikersvertrouwen in legitieme updates, wat onbedoeld de kwetsbaarheden zou kunnen vergroten. Als gebruikers wantrouwend worden tegenover updates vanwege het geopolitieke klimaat, zouden ze de installatie ervan kunnen uitstellen of vermijden, waardoor ze juist kwetsbaarder worden voor bekende bedreigingen.

Tijdens perioden van intense geopolitieke conflicten zou het risico op insider threats of dwang gericht op individuen met toegang tot de update infrastructuur van Microsoft kunnen toenemen.[65] Een politiek gemotiveerde insider of een gedwongen persoon zou potentieel de update inhoud of processen kunnen manipuleren, wat zou leiden tot de verspreiding van gecompromitteerde software. Het Amerikaanse verbod op Kaspersky antivirus [66] vanwege zorgen over Russische overheidsinvloed, hoewel niet direct een voorbeeld van update manipulatie, illustreert de geopolitieke dimensie van vertrouwen in beveiligingssoftware. Hoewel Microsoft waarschijnlijk strenge beveiligingsmaatregelen heeft om dergelijke scenario's te voorkomen, kan de mogelijkheid niet volledig worden uitgesloten, vooral in de context van staatsactoren met aanzienlijke middelen en invloed.

5. Geopolitieke Context en Versterkte Risico's

Het cyberdomein is een kritiek front geworden in geopolitieke conflicten, waarbij door de staat gesteunde aanvallen in toenemende mate essentiële diensten en organisaties targeten.[5] Microsoft Defender, als een wijdverspreid beveiligingsproduct, zou een waardevol doelwit kunnen zijn voor dergelijke aanvallen, vooral die gericht zijn op het verstoren of verkrijgen van toegang tot systemen in landen met tegengestelde geopolitieke belangen dan het land van de aanvaller. De onderlinge verbondenheid van de mondiale digitale infrastructuur betekent dat een aanval op een beveiligingsproduct in het ene land wereldwijde gevolgen zou kunnen hebben, waardoor het een strategisch instrument in cyberoorlogvoering is.

Door de staat gesteunde cyberactoren beschikken over aanzienlijke middelen en geavanceerde technische vaardigheden [5], waardoor ze potentieel geavanceerde exploits kunnen ontwikkelen die gericht zijn op het Microsoft Defender updateproces en die mogelijk de mogelijkheden van typische cybercriminelen overstijgen. Hun motivaties zijn vaak afgestemd op nationale strategische

doelstellingen, waaronder spionage, sabotage of het verkrijgen van persistente toegang tot kritieke infrastructuur in andere landen, zoals Nederland. De persistente en goed gefinancierde aard van deze actoren maakt hen een bijzonder gevaarlijke bedreiging voor de integriteit van kritieke software-updates.

Geopolitieke gebeurtenissen kunnen de intensiteit en focus van cyberaanvallen direct beïnvloeden.[5] Toegenomen spanningen tussen naties zouden bijvoorbeeld kunnen leiden tot een piek in cyberoperaties gericht op kritieke software en infrastructuur in die naties. Nederland zou, gezien zijn geopolitieke positie, een toename kunnen zien van geavanceerde aanvallen op zijn digitale infrastructuur, waaronder potentiële pogingen om het Microsoft Defender updateproces te compromitteren. Sancties of politieke geschillen zouden ook kunnen leiden tot vergeldingsmaatregelen in cyberspace, waarbij mogelijk wijdverspreide software als doelwit wordt gekozen om verstoring of schade te veroorzaken.

6. Mitigatiestrategieën en Best Practices voor Gebruikers in Nederland

Het inschakelen van automatische updates [10] is cruciaal voor het tijdig ontvangen van beveiligingspatches en intelligence updates voor Microsoft Defender. Hoewel er legitieme zorgen zijn over gecompromitteerde updates tijdens geopolitieke onrust, weegt het risico van het niet patchen van bekende kwetsbaarheden voor de meeste gebruikers vaak zwaarder. Het uitstellen van updates kan systemen kwetsbaar maken voor exploits die door door de staat gesteunde actoren actief kunnen worden misbruikt.

Bij het handmatig downloaden van updates [10] moeten gebruikers uiterst voorzichtig zijn en deze alleen van de officiële Microsoft website betrekken. Het verifiëren van de digitale handtekening van de gedownloade bestanden biedt een extra beveiligingslaag tegen gemanipuleerde updates, wat vooral belangrijk is in een geopolitiek geladen omgeving waarin valse updates kunnen worden gebruikt als een vector voor malware. Gebruikers moeten worden geïnstrueerd over het controleren van digitale handtekeningen om de authenticiteit van de updates te waarborgen.

Organisaties zouden gecentraliseerde update management tools [10] moeten benutten en een gefaseerde uitrolstrategie voor Microsoft Defender updates moeten implementeren. Dit maakt het mogelijk om updates op een subset van systemen te testen voordat ze breed worden geïmplementeerd, waardoor vroege detectie van eventuele problemen mogelijk wordt, of deze nu worden veroorzaakt door defecte updates of potentiële compromitteringen, wat vooral belangrijk is wanneer geopolitieke risico's verhoogd zijn. Een goed beheerd updateproces kan helpen de noodzaak van tijdige patching in evenwicht te brengen met het risico van het implementeren van een gecompromitteerde update over het gehele netwerk.

Robuuste netwerkbeveiligingsmaatregelen [41] zijn essentieel voor het monitoren van netwerkverkeer met betrekking tot Microsoft Defender updates. Firewalls en intrusion detection/prevention systemen kunnen helpen bij het identificeren en blokkeren van pogingen om updateverkeer te onderscheppen of om te leiden naar kwaadaardige servers, wat vaker zou kunnen voorkomen tijdens perioden van geopolitieke instabiliteit. Het monitoren van ongebruikelijke verbindingen van of naar update servers kan vroege waarschuwingen geven voor potentiële aanvallen.

Het up-to-date houden van het besturingssysteem [10] is cruciaal, aangezien de effectiviteit van Microsoft Defender afhankelijk is van een veilig en bijgewerkt onderliggend platform. Verouderde besturingssystemen kunnen kwetsbaarheden bevatten die door aanvallers kunnen worden misbruikt om Defender of het updatemechanisme te compromitteren, vooral in de context van verhoogde geopolitieke cyberdreigingen. Het waarborgen dat het besturingssysteem is gepatcht, vermindert het algehele aanvalsoppervlak en versterkt de basis waarop Defender werkt.

Algemene richtlijnen voor beveiliging [48] blijven van het grootste belang. Aanvallers zouden menselijke kwetsbaarheden kunnen proberen uit te buiten door middel van phishing of social engineering om toegang te krijgen tot systemen en vervolgens update-instellingen te manipuleren of kwaadaardige software te installeren naast of in plaats van legitieme Defender updates, vooral in tijden van geopolitieke onzekerheid waarin gebruikers vatbaarder kunnen zijn voor op angst gebaseerde tactieken. Sterke wachtwoorden en MFA kunnen ongeautoriseerde toegang voorkomen, terwijl waakzaamheid tegen phishing de initiële compromittering kan voorkomen.

Organisaties, met name in kritieke infrastructuursectoren in Nederland, zouden hun netwerkbeveiliging en monitoring moeten verbeteren [5] vanwege het verhoogde risico op gerichte aanvallen van door de staat gesteunde actoren tijdens geopolitieke onrust. Dit omvat rigoureuze monitoring van updateverkeer, implementatie van strengere toegangscontroles en mogelijk het gebruik van gespecialiseerde beveiligingsapparaten om updatepakketten te inspecteren. De potentiële gevolgen van een succesvolle aanval op kritieke infrastructuur zijn ernstig, wat een verhoogde beveiligingshouding noodzakelijk maakt.

Organisaties, met name die met verhoogde beveiligingszorgen vanwege het geopolitieke klimaat, zouden kunnen overwegen om Endpoint Detection and Response (EDR) oplossingen van derden [78] in te zetten als aanvulling op Microsoft Defender. EDR-oplossingen bieden vaak geavanceerdere mogelijkheden voor dreigingsdetectie, analyse en respons die een extra beveiligings- en monitoringlaag kunnen bieden bovenop het updateproces en het algehele endpointgedrag. Een gelaagde beveiligingsaanpak kan de kans op het detecteren en beperken van geavanceerde aanvallen vergroten die de standaard antivirusbescherming zouden kunnen ontwijken.

7. Conclusie

De analyse heeft potentiële kwetsbaarheden in het Microsoft Defender updateproces blootgelegd, waaronder de inherente risico's van software-updates, historische incidenten van compromittering en het versterkte dreigingslandschap als gevolg van geopolitieke onrust. Hoewel Microsoft aanzienlijke beveiligingsmaatregelen implementeert, waaronder digitale handtekeningen en veilige implementatiepraktijken, vormen de toenemende verfijning en motivatie van door de staat gesteunde actoren een persistente bedreiging die mogelijk zelfs deze robuuste mechanismen kan targeten.

Er is een voortdurende noodzaak tot waakzaamheid en proactieve beveiligingsmaatregelen door individuen en organisaties in Nederland om hun systemen te beschermen tegen evoluerende geopolitieke cyberdreigingen. Dit omvat het nauwgezet toepassen van updates, waar mogelijk de authenticiteit ervan verifiëren en het implementeren van een gelaagde beveiligingsaanpak die de sterke punten van Microsoft Defender combineert met andere best practices op het gebied van beveiliging en potentieel aanvullende oplossingen.

eRemote

Geciteerd werk

1. Desktop Operating System Market Share Netherlands | Statcounter Global Stats, geopend op mei 7, 2025, https://gs.statcounter.com/os-market-share/desktop/netherlands/vjhtxqmkl.lol
2. Desktop Operating System Market Share Netherlands | Statcounter ..., geopend op mei 7, 2025, https://gs.statcounter.com/os-market-share/desktop/netherlands/679uv.us
3. Desktop Operating System Market Share Netherlands | Statcounter Global Stats, geopend op mei 7, 2025, https://gs.statcounter.com/os-market-share/desktop/netherlands
4. Desktop Operating System Market Share Netherlands | Statcounter, geopend op mei 7, 2025, https://gs.statcounter.com/os-market-share/desktop/netherlands/maowr.bartikus.site
5. Cybersecurity Risks from Political Instability: Are Businesses More Vulnerable? - Managed IT Services & Technology Consulting | OSIbeyond, geopend op mei 7, 2025, https://www.osibeyond.com/blog/cybersecurity-risks-from-political-instability-are-businesses-more-vulnerable/
6. March 25 - Impact of Geopolitical Conflicts on Cybersecurity Risks, geopend op mei 7, 2025, https://www.iseoblue.com/post/impact-of-geopolitical-conflicts-on-cybersecurity-risks
7. WEF Global Cybersecurity Outlook 2025 report addresses geopolitical tensions, emerging threats to boost resilience - Industrial Cyber, geopend op mei 7, 2025, https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2025-report-addresses-geopolitical-tensions-emerging-threats-to-boost-resilience/
8. Geopolitical Factors Shaping the Future of the Cyber Domain - Critical Start, geopend op mei 7, 2025, https://www.criticalstart.com/geopolitical-factors-shaping-the-future-of-the-cyber-domain/
9. Growing convergence of geopolitics and cyber warfare continue to threaten OT and ICS environments in 2024, geopend op mei 7, 2025, https://industrialcyber.co/features/growing-convergence-of-geopolitics-and-cyber-warfare-continue-to-threaten-ot-and-ics-environments-in-2024/
10. Latest security intelligence updates for Microsoft Defender Antivirus and other Microsoft antimalware, geopend op mei 7, 2025, https://www.microsoft.com/wdsi/definitions
11. Manage how and where Microsoft Defender Antivirus receives ..., geopend op mei 7, 2025, https://learn.microsoft.com/en-us/defender-endpoint/manage-protection-updates-microsoft-defender-antivirus
12. Microsoft Defender Antivirus security intelligence and product updates, geopend op mei 7, 2025, https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-antivirus-updates

eRemote

13. How does the Security intelligence updates for Microsoft Defender Antivirus and other Microsoft Antimalware - KB2267602 work? - MetaDefender IT Access - OPSWAT, geopend op mei 7, 2025, https://www.opswat.com/docs/macloud-sdp/kb/how-does-the-security-intelligence-updates-for-microsoft-defende
14. Are Microsoft Defender monthly Security Intelligence updates cumulative?, geopend op mei 7, 2025, https://answers.microsoft.com/en-us/windows/forum/all/are-microsoft-defender-monthly-security/7cdab566-07aa-4c60-af27-6f364f9bc4ab
15. Microsoft Defender Definition download, geopend op mei 7, 2025, https://answers.microsoft.com/en-us/windows/forum/all/microsoft-defender-definition-download/0a91f326-2709-4422-bb07-ff63018376d9
16. Signature/Definition update - Microsoft Q&A, geopend op mei 7, 2025, https://learn.microsoft.com/en-us/answers/questions/286500/signature-definition-update
17. Defender updates : r/DefenderATP - Reddit, geopend op mei 7, 2025, https://www.reddit.com/r/DefenderATP/comments/165gfc7/defender_updates/
18. A strange thing I've noticed about windows defender updates, geopend op mei 7, 2025, https://www.tenforums.com/antivirus-firewalls-system-security/215031-strange-thing-ive-noticed-about-windows-defender-updates.html
19. Why so many Security Intelligence updates? - Microsoft Community, geopend op mei 7, 2025, https://answers.microsoft.com/en-us/windows/forum/all/why-so-many-security-intelligence-updates/5b118568-3aac-4640-bdc0-e65cacd9e777
20. Definition Updates everyday? : r/windows - Reddit, geopend op mei 7, 2025, https://www.reddit.com/r/windows/comments/onufbj/definition_updates_everyday/
21. Onboard servers through Microsoft Defender for Endpoint's ..., geopend op mei 7, 2025, https://learn.microsoft.com/en-us/defender-endpoint/configure-server-endpoints
22. Minimum requirements for Microsoft Defender for Endpoint, geopend op mei 7, 2025, https://learn.microsoft.com/en-us/defender-endpoint/minimum-requirements
23. Plan Defender for Servers data residency - Microsoft Defender for Cloud | Microsoft Learn, geopend op mei 7, 2025, https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace
24. Windows Defender Security Risk: Defender Pretender - SafeBreach, geopend op mei 7, 2025, https://www.safebreach.com/blog/defender-pretender-when-windows-defender-updates-become-a-security-risk/
25. Microsoft Defender Security Feature Bypass Vulnerability (CVE-2023-24934) - Rapid7, geopend op mei 7, 2025, https://www.rapid7.com/db/vulnerabilities/windows-defender-cve-2023-24934/
26. CVE-2023-24934 : Microsoft Defender Security Feature Bypass Vulnerability, geopend op mei 7, 2025, https://www.cvedetails.com/cve/CVE-2023-24934/

27. CVE-2023-24934, geopend op mei 7, 2025, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24934
28. Windows Defender bypass - ThreatLocker, geopend op mei 7, 2025, https://www.threatlocker.com/blog/windows-defender-bypass?5f288fb5_page=3
29. CVE-2023-24934 | Tenable®, geopend op mei 7, 2025, https://www.tenable.com/cve/CVE-2023-24934
30. CVE-2023-24934 | INCIBE-CERT, geopend op mei 7, 2025, https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-24934
31. CVE-2023-24934 Detail - NVD, geopend op mei 7, 2025, https://nvd.nist.gov/vuln/detail/CVE-2023-24934
32. CVE-2023-24934 - Security Update Guide - Microsoft Security Response Center, geopend op mei 7, 2025, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24934
33. CVE-2023-24934 - CVE: Common Vulnerabilities and Exposures, geopend op mei 7, 2025, https://www.cve.org/CVERecord?id=CVE-2023-24934
34. CVE-2023-24934: Microsoft Defender Security Bypass - CloudDefense.AI, geopend op mei 7, 2025, https://www.clouddefense.ai/cve/2023/CVE-2023-24934
35. How do I patch the Microsoft Malware Protection Engine? : r/DefenderATP - Reddit, geopend op mei 7, 2025, https://www.reddit.com/r/DefenderATP/comments/12qraqf/how_do_i_patch_the_microsoft_malware_protection/
36. Update for Microsoft Defender Antivirus Antimalware Platform v 1.0.2303.27001, geopend op mei 7, 2025, https://answers.microsoft.com/en-us/insider/forum/all/update-for-microsoft-defender-antivirus/27f82e1d-4ba9-43c4-b201-2d16356d7bac
37. Microsoft Malware Protection Platform versions and number of CVEs, vulnerabilities, geopend op mei 7, 2025, https://www.cvedetails.com/version-list/26/166514/1/Microsoft-Malware-Protection-Platform.html?order=0
38. Microsoft Malware Protection Platform 4.18.2303.8 security, geopend op mei 7, 2025, https://www.cvedetails.com/version/1727210/Microsoft-Malware-Protection-Platform-4.18.2303.8.html
39. Use safe deployment practices to safeguard your environment ..., geopend op mei 7, 2025, https://learn.microsoft.com/en-us/defender-endpoint/mde-sdp-strategy
40. Manage the gradual rollout process for Microsoft Defender updates, geopend op mei 7, 2025, https://learn.microsoft.com/en-us/defender-endpoint/manage-gradual-rollout
41. Configure and validate Microsoft Defender Antivirus network connections, geopend op mei 7, 2025, https://learn.microsoft.com/en-us/defender-endpoint/configure-network-connections-microsoft-defender-antivirus

42. Why Software Updates Can Lead to Cyberattacks — and What to Do | HackerNoon, geopend op mei 7, 2025, https://hackernoon.com/why-software-updates-can-lead-to-cyberattacks-and-what-to-do

43. How Software Updates Can Lead to Cyber Attacks - Cybersecurity Insiders, geopend op mei 7, 2025, https://www.cybersecurity-insiders.com/how-software-updates-can-lead-to-cyber-attacks/

44. Nation-State-Sponsored Attacks: Not Your Grandfather's Cyber Attacks - Data Matters, geopend op mei 7, 2025, https://datamatters.sidley.com/2022/05/17/nation-state-sponsored-attacks-not-your-grandfathers-cyber-attacks/

45. Destructive Code: The Most Infamous Malware Attacks in History - Private Internet Access, geopend op mei 7, 2025, https://www.privateinternetaccess.com/blog/worst-malware-in-history/

46. Are Windows Updates susceptible to tampering, eg. using a MiTM attack., geopend op mei 7, 2025, https://security.stackexchange.com/questions/19979/are-windows-updates-susceptible-to-tampering-eg-using-a-mitm-attack

47. New OpenSSH Flaws Enable Man-in-the-Middle and DoS Attacks — Patch Now, geopend op mei 7, 2025, https://thehackernews.com/2025/02/new-openssh-flaws-enable-man-in-middle.html

48. The Critical Role of Real-Time Personal Cybersecurity in Thwarting Man-in-the-Middle Attacks - BlackCloak, geopend op mei 7, 2025, https://blackcloak.io/the-critical-role-of-real-time-personal-cybersecurity-in-thwarting-man-in-the-middle-attacks/

49. Man in the Middle (MITM) Attack - CrowdStrike, geopend op mei 7, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/man-in-the-middle-mitm-attack/

50. Windows 10 Update - Man In The Middle Attack - Tamper Update - ESET Forum, geopend op mei 7, 2025, https://forum.eset.com/topic/35501-windows-10-update-man-in-the-middle-attack-tamper-update/

51. Man in the Middle Attack Tools - Comprehensive Guide - Sepio Cyber, geopend op mei 7, 2025, https://sepiocyber.com/blog/man-in-the-middle-attack/

52. Man In The Middle Attacks and How to Prevent Them - Veracode, geopend op mei 7, 2025, https://www.veracode.com/security/man-middle-attack/

53. Man-in-the-middle attack - Wikipedia, geopend op mei 7, 2025, https://en.wikipedia.org/wiki/Man-in-the-middle_attack

54. Hackers hijacked the eScan Antivirus update mechanism in malware campaign, geopend op mei 7, 2025, https://securityaffairs.com/162228/breaking-news/escan-antivirus-mitm-attack.html

55. Antivirus updates hijacked to drop dangerous malware - TechRadar, geopend op mei 7, 2025, https://www.techradar.com/pro/security/antivirus-updates-hijacked-to-drop-dangerous-malware
56. What are state-sponsored cyber attacks? - F-Secure, geopend op mei 7, 2025, https://www.f-secure.com/en/articles/what-are-state-sponsored-cyber-attacks
57. Recent State-Sponsored Activity Impacting the Cyber Threat Landscape | Latest Alerts and Advisories | NJCCIC, geopend op mei 7, 2025, https://www.cyber.nj.gov/Home/Components/News/News/1402/214
58. Top 10 Signs That Your System Has Been Compromised - Lepide, geopend op mei 7, 2025, https://www.lepide.com/blog/top-10-signs-that-your-system-has-been-compromised/
59. The challenges of detecting compromised public Web servers - Cybereason, geopend op mei 7, 2025, https://www.cybereason.com/blog/the-challenges-of-detecting-compromised-public-web-servers
60. Strategies for Handling a Compromised Server: Expert Tips & Best Practices, geopend op mei 7, 2025, https://www.mobitsolutions.com/strategies-for-handling-a-compromised-server/
61. Weekly Recap: Nation-State Hacks, Spyware Alerts, Deepfake Malware, Supply Chain Backdoors - The Hacker News, geopend op mei 7, 2025, https://thehackernews.com/2025/05/weekly-recap-nation-state-hacks-spyware.html
62. Chinese Hackers Exploit MAVInject.exe to Evade Detection in Targeted Cyber Attacks, geopend op mei 7, 2025, https://thehackernews.com/2025/02/chinese-hackers-exploit-mavinjectexe-to.html
63. Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations - CISA, geopend op mei 7, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
64. 16 Types of Endpoint Security Risks To Watch Out For - Teramind, geopend op mei 7, 2025, https://www.teramind.co/blog/endpoint-security-risks/
65. How Malicious Software Updates Endanger Everyone | American Civil Liberties Union, geopend op mei 7, 2025, https://www.aclu.org/how-malicious-software-updates-endanger-everyone
66. Everything you should know about the recent ban on Kaspersky Antivirus in the US, geopend op mei 7, 2025, https://dmarcreport.com/blog/everything-you-need-to-know-about-the-us-ban-on-kaspersky-antivirus/
67. Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks, geopend op mei 7, 2025, https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/

68. Significant Cyber Incidents | Strategic Technologies Program - CSIS, geopend op mei 7, 2025, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

69. State-Sponsored Cyber Attacks: A 20-Year Evolution and National Security Realities, geopend op mei 7, 2025, https://nationalsecuritynews.com/2023/12/state-sponsored-cyber-attacks-a-20-year-evolution-and-national-security-realities/

70. Keeping devices and software up to date - NCSC.GOV.UK, geopend op mei 7, 2025, https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date

71. Mitigating malware and ransomware attacks - NCSC.GOV.UK, geopend op mei 7, 2025, https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

72. memory integrity - Microsoft Community, geopend op mei 7, 2025, https://answers.microsoft.com/en-us/windows/forum/all/memory-integrity/d00368a8-4c29-4527-9381-6081ca044888

73. What is Windows Defender integrity service? - Microsoft Community, geopend op mei 7, 2025, https://answers.microsoft.com/en-us/windows/forum/all/what-is-windows-defender-integrity-service/965c0f2b-6521-4df9-a23d-763121d716ae

74. Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.613.0) - Current Channel (Broad) turned off my memory integrity, geopend op mei 7, 2025, https://answers.microsoft.com/en-us/windows/forum/all/security-intelligence-update-for-microsoft/8aa6de67-0f6b-4b64-81a3-292853410487

75. I am receiving a warning from windows defender security center with a help support #1-844-622-4430. - Microsoft Community, geopend op mei 7, 2025, https://answers.microsoft.com/en-us/msoffice/forum/all/i-am-receiving-a-warning-from-windows-defender/997694f2-4f6b-46c4-8a27-ec2a6ad112b2

76. Updating Windows Defender - Microsoft Q&A, geopend op mei 7, 2025, https://learn.microsoft.com/en-us/answers/questions/2006060/updating-windows-defender

77. The Endpoint Security Risks You Need to Know About - Impact Networking, geopend op mei 7, 2025, https://www.impactmybiz.com/blog/endpoint-security-risks/

78. CrowdStrike: We Stop Breaches with AI-native Cybersecurity, geopend op mei 7, 2025, https://www.crowdstrike.com/en-us/

79. 20 Best Cybersecurity Software Reviewed for 2025 - The CTO Club, geopend op mei 7, 2025, https://thectoclub.com/tools/best-cybersecurity-software/

80. Cybereason - AI-Driven XDR Platform | MDR | Retainers, geopend op mei 7, 2025, https://www.cybereason.com/

81. CrowdStrike: Worst Update in History takes down Computers - YouTube, geopend op mei 7, 2025, https://www.youtube.com/watch?v=XMv35syos3M