BODYGUARD.IO

2023 Research Lab Rapport

Blinde vlekken van Microsoft 365

Hoe Goed Bent U Beschermd Tegen Onbekende Malware?

In samenwerking met ethische hacker Saad Ahla (TheD1rkMtr).
Bekende instructeur bij hackersacademie HackTheBox.

liberteq A&H FINANCE it2grow tien MKB IT

KVK Innovatie Top 100 HSD MODERN MSP DAY

11-10-2023

Bodyguard.io
HSD Campus
Wilhelmina van Pruisenweg 104
2595 AN Den Haag Nederland

KVK: 83785574

Inhoudsopgave

Executive summary

Malware, met name ransomware en infostealers, blijft groeien als dreiging. Het gevaar begint vaak met het klikken op een schadelijke bijlage. Eenmaal geïnfecteerd heeft een aanvaller toegang tot een schat aan gevoelige informatie op het apparaat.

Veel organisaties vertrouwen op de beveiliging van Microsoft 365 met Advanced Threat Protection (ATP) e-mailbeveiliging. Om de proef op te som te nemen is ethische hacker Saad Ahla ingeschakeld. Hij is senior instructeur bij de alom bekende hackersacademie HackTheBox en geniet veel bekendheid in de hacker community. Saad heeft tijdens het onderzoek meer dan 20 aanvalsvectoren gevonden om de e-mailbeveiliging te omzeilen. Bijgevolg arriveert de synthetisch gegenereerde malware in de mailbox van eindgebruikers. Slechts één klik van een onoplettende gebruiker kan funest zijn. Dit risico onderstreept de noodzaak voor aanvullende preventieve maatregelen. Als Saad in staat is de Microsoft 365 ATP-beveiliging te omzeilen, dan is het naar ons idee veilig om aan te nemen dat georganiseerde ransomware-groepen dat ook kunnen.

Huidige beveiligingsoplossingen werken op basis van handtekeningen en heuristieken om malware te herkennen. Dit is echter geen effectieve manier om bescherming te bieden tegen onbekende malware en zero-days.

Content Disarm & Reconstruction (CDR) is een nieuwe technologie om beter bewapend te zijn tegen onbekende malware en zero-days. Bijlagen worden door de CDR-software gereconstrueerd met behulp van Positieve Selectie. In het proces wordt alleen vertrouwde bestandsinhoud behouden waardoor onbekende schadelijke elementen verdwijnen.

Bodyguard.io heeft een laagdrempelige oplossing ontwikkeld waarmee CDR-technologie in de basisbeveiliging van Windows werkplekken kan worden opgenomen zonder productiviteitsverlies.

Over Bodyguard.io

Bodyguard.io is een cybersecurity softwarebedrijf opgericht in 2021 met een duidelijke missie, ervoor zorgen dat medewerkers nooit meer een schadelijk bestand openen.

Wij geloven dat cyberveiligheid niet mag afhangen van de alertheid van een individu. De onderneming is gevestigd op de campus van Hague Security Delta (HSD), het Nederlandse veiligheidscluster. Ruim 275 bedrijven, overheidsorganisaties en kennisinstellingen werken sinds 2013 samen om het verschil te maken in het veiligstellen van onze digitaliserende samenleving. Ze delen hun kennis en werken samen aan innovatieve beveiligingsoplossingen, die zowel binnen Nederland als internationaal kunnen worden opgeschaald.

Huidige gevaren Malware

Malware blijft een groot probleem

Het begint allemaal bij een klik...

Bestandsgebaseerde aanvallen vormen een constant en groeiend gevaar voor organisaties van alle soorten en maten. Ondanks het voortdurend evoluerende landschap van cybersecurity, blijft dit type aanval een favoriete tactiek voor cybercriminelen.

Tussenstand 2023: Toename Ransomware en Infostealers

Wederom is er in 2023 een significante toename van ransomware- en infostealer-aanvallen te zien. [1] Het proces van een cyberaanval begint meestal met 'initial access', hetgeen vaak wordt verkregen door het gebruik van malware. Bij het openen van een schadelijke bijlage wordt de malware geactiveerd en krijgt de aanvaller toegang tot het apparaat. Wat kan men allemaal stelen van slechts één gehackt apparaat? [2]

- Wachtwoorden
- Cookies en sessies
- Schermopname
- Documenten
- VPN toegang
- Toetsaanslagen
- Chathistorie
- Netwerktoegang

Een voorbeeld: QakBot netwerk met 700.000 geïnfecteerde apparaten
Door de jaren heen zijn meer dan 700.000 computers geïnfecteerd geraakt. De meeste infecties zijn veroorzaakt door het klikken op schadelijke Office, pdf, html, zip en onenote bestanden. In totaal zijn er 18 unieke bestandsgebaseerde aanvalsmethoden gebruikt. [3] Dit is illustratief voor de snelheid waarmee aanvallers hun technieken aanpassen. Na infectie kon de machine op afstand worden aangestuurd. Het netwerk is in augustus 2023 opgerold.

Menselijke Factoren: De Rol van Social Engineering

De Menselijke Factor

Wanneer technische maatregelen tekortschieten, komt het neer op de alertheid van een individu. Social engineering speelt hierin een cruciale rol; het is de kunst van het manipuleren zodat mensen handelingen uitvoeren of informatie vrijgeven.

Klikactie Uitlokken door Spear-phishing

Bij spear-phishing wordt een plausibele context gepresenteerd om nietsvermoedende medewerkers een schadelijke bijlage te laten openen. Ondanks awareness training, zijn het de alledaagse scenario's waarbij gevaar moeilijk op te merken is:

- CV naar aanleiding van een openstaande vacature
- Bericht van HR-afdeling over personeelszaken
- Vraag van gebruikers aan de servicedesk
- Offerteaanvragen van potentiële klanten

De Rol van AI

De komst van Large Language Models (LLM) zoals Chat-GPT maken het schrijven van valse e-mails eenvoudiger dan ooit.[4] De teksten zijn gepersonaliseerd en bovendien wordt het proces van de cybercriminelen volledig geautomatiseerd. Dit resulteert in nóg meer pogingen om medewerkers in de val te lokken.

Verspreiding via Communicatiekanalen

Medewerkers ontvangen bestanden via talloze applicaties: Outlook, Browsers, Teams, Slack, Zoom en WhatsApp. Niet al deze platformen zijn even goed beveiligd, waardoor het risico op een geslaagde aanval zeer groot is.

Bestandsformaten als Wapens

Honderden Bestandsformaten

In de digitale wereld zijn er honderden verschillende bestandsformaten, van documenten en afbeeldingen tot uitvoerbare bestanden en scripts. Deze rijke verscheidenheid biedt organisaties veel flexibiliteit en functionaliteit, maar het vormt uiteraard ook een groot risico als het gaat om cybersecurity.

Schadelijke documentsoorten

De alom bekende documenten zoals Office en PDF worden terecht vaak geassocieerd met malware-aanvallen.[5] Deze documentsoorten zijn gebaseerd op gedateerde specificaties en bevatten onveilige functionaliteit waarmee code kan worden uitgevoerd bij het openen.

LNK aanvallen

Snelkoppeling-bestanden met extensie LNK, worden steeds vaker ingezet om code uit te voeren bij het openen.[6] De snelkoppeling kan worden voorzien van een icoon zoals Word om gebruikers te misleiden. Bovendien wordt het bestand vaak ook voorzien van een valse extensie zoals bijvoorbeeld “factuur-2023.docx.lnk”.

Containerformaten

Vaak wordt een malafide bestand samengevoegd met legitieme bestanden.[7] Hiermee kunnen beveiligingsmaatregelen worden omzeild en daarnaast is het een slinkse manier om gebruikers te misleiden.

Grote bestanden

Diverse beveiligingsmaatregelen zoals antivirus scannen grote bestanden niet.[8] Door malware bestanden groter te maken, wordt detectie voorkomen en kan een gebruiker het geïnfecteerde bestand openen.

Versleutelde bestanden

Archiefbestanden en documenten kunnen worden voorzien van een wachtwoord, een klassieke manier om detectie te omzeilen. Beveiligingsmaatregelen kunnen de inhoud van dergelijke bestanden namelijk niet inspecteren.

Onbekende Virussen en Antivirus Tekortkomingen

De Aard van Antivirusbescherming

Traditionele antivirussoftware werkt veelal op basis van een database met bekende malware handtekeningen. Hoewel dit een effectieve methode is voor het identificeren van bekende virussen, schiet het tekort bij het detecteren van onbekende malware.

Het Probleem van Onbekende Malware

Nieuwe en onbekende malware varianten verschijnen dagelijks, en antivirusbedrijven hebben tijd nodig om deze te identificeren, analyseren en toe te voegen aan hun databases. Tijdens deze 'grijze periode' zijn systemen kwetsbaar voor infectie.

Onderlinge Verschillen tussen Aanbieders

Interessant is dat verschillende antivirusaanbieders uiteenlopende conclusies trekken of een bestand wel of geen malware betreft. Onderzoek toont aan dat de detectiepercentages tussen toonaangevende antivirusprogramma's aanzienlijk kunnen verschillen, wat de kans vergroot dat een potentieel schadelijk bestand onopgemerkt blijft.[9]

Het Gevaar van Zero-Day Aanvallen

Wat Zijn Zero-Day Kwetsbaarheden?

Zero-day kwetsbaarheden zijn beveiligingslekken in software die nog niet bekend zijn bij de ontwikkelaar of het grote publiek, en daardoor ook nog niet zijn gepatcht. Aanvallers kunnen deze kwetsbaarheden misbruiken om toegang te krijgen tot system.

Waarom Zero-Days Gevaarlijk Zijn

Het gevaarlijke aan zero-day kwetsbaarheden is dat deze, per definitie, onbekend zijn. Dit betekent dat ze niet kunnen worden gedetecteerd door traditionele beveiligingstools, waaronder antivirusprogramma's. Omdat er nog geen patch of fix beschikbaar is, zijn organisaties bijzonder kwetsbaar voor aanvallen die van deze lekken gebruik maken.

Recente Voorbeelden van Zero-Day Aanvallen

- CVE-2023-36884 – Microsoft Office [10]
- CVE-2023-38831 – WinRar [11]
- CVE-2023-26369 – Adobe Reader [12]

Microsoft is koploper in de lijst van meeste zero-day kwetsbaarheden.

De Blinde Vlek van Traditionele Beveiligingsmaatregelen

Omdat zero-day kwetsbaarheden nog niet zijn geïdentificeerd, worden deze niet gedekt door de handtekeningendatabases van antivirusprogramma's. Zelfs geavanceerdere technieken zoals heuristische analyse schieten tekort, omdat ze vaak zijn gericht op gedragspatronen die bekend zijn bij eerdere malwareaanvallen: onbekend maakt onherkenbaar.

Gevolgen van Anti-detectie Malware

Over Microsoft Defender

Microsoft Defender is een ander ingebouwd beveiligingsinstrument binnen de Microsoft 365-suite, gericht op endpoint-beveiliging. Hoewel het goed is geïntegreerd en gemakkelijk te beheren, rijst de vraag hoe effectief deze vorm van traditionele beveiliging is.

Malware met Anti-detectie Capaciteiten

Virusbestanden worden steeds vaker uitgerust met de technische capaciteit om detectie te omzeilen.[13]

98%	32%	27%
Malware gebruikt tenminste één tactiek om detectie te omzeilen	Malware gebruikt 6 of meer tactieken om detectie te omzeilen	Malware omzeilt de detectie van een enkele sandbox

De Gevolgen van Onopgemerkte Malware

Wat kan de impact zijn van één gehackt apparaat? De gevolgen kunnen variëren van infostealers die gevoelige data verzamelen tot ransomware die het hele netwerk kan vergrendelen.

Infostealers: Veel waardevols op één apparaat

Infostealer malware kan wachtwoorden, financiële gegevens en andere gevoelige informatie verzamelen zonder merkbare symptomen. Dit soort malware kan lang actief blijven en een schat aan data doorsturen naar cybercriminelen.

Ransomware: Lateraal bewegen in het netwerk

De gehackte machine geeft de cybercrimineel mogelijkheid om lateraal te bewegen naar andere systemen. In het ergste geval kan onopgemerkte malware, na verdere penetratie in het bedrijfsnetwerk, leiden tot een volledige ransomware-aanval.

Detection and Response Producten Omzeilen

EDR, MDR en XDR berusten op zichtbaarheid om te functioneren. Geavanceerde malware is in staat om systeemacties uit te voeren zonder sporen achter te laten, bijvoorbeeld door de inzet van direct system calls en system API unhooking.[14]

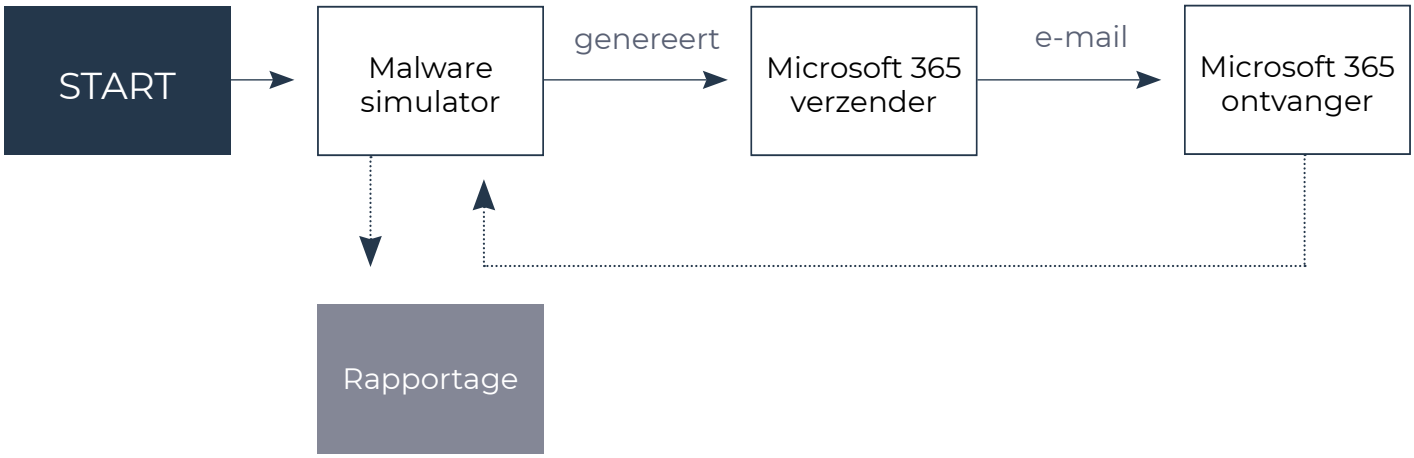
Evaluatie Microsoft 365 ATP E-mailbeveiliging

Over Microsoft ATP

Microsoft Advanced Threat Protection (ATP) is de meest uitgebreide beveiligingsmodule in de Microsoft 365-suite, ontworpen de mailbox te beschermen tegen geavanceerde cyberdreigingen. ATP is alleen inbegrepen bij Microsoft Business Premium, E3 en E5 licenties. De service omvat e-mailfiltering, beveiligingsanalyses en dreigingsintelligentie, maar hoe effectief is het tegen onbekende virussen? Bodyguard.io heeft een extern onderzoek laten verrichten.

Methodologie

Ethisch hacker Saad Ahla heeft eerdergenoemde risicovolle bestandsformaten getest met Microsoft 365 Advanced Threat Protection om vast te stellen wat wordt geblokkeerd of gedetecteerd. De malware is synthetisch gegenereerd door de inzet van de malware simulator, welke bestaat uit commerciële red-team tools en zelfontwikkelde scripts. Geproduceerde bestanden zijn altijd uniek en worden door de simulator naar een gemonitorde Microsoft 365 omgeving gemaild. Wanneer de ATP-beveiliging is omzeild zal de malware arriveren in de mailbox. De doelstelling is het vinden van meerdere aanvalsmethoden, ofwel ‘aanvalsvector’, waarmee malware succesvol in de mailbox van eindgebruikers terechtkomt.

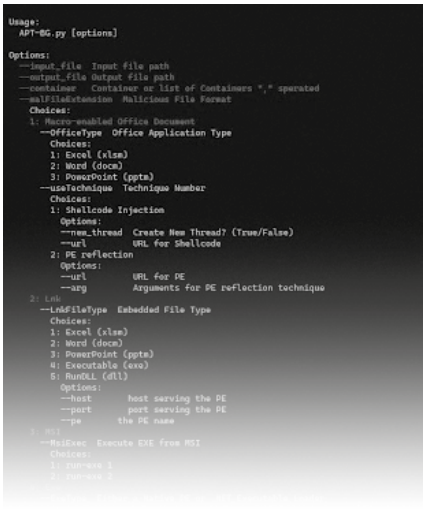


Wie is Saad Ahla

Saad is senior instructeur voor de alom bekende online hackersacademie HackTheBox. Door zijn openbare werk is hij erg geliefd in de red teaming community. Op zijn Github profiel wordt hij door meer dan 1100 mensen gevolgd, waarvan de meeste security professionals zijn.[15]

Geavanceerde Red Team Tooling: Azrael

De red team toolset Azrael is een geavanceerde suite ontworpen voor moderne initial access assessments, gebaseerd op het Red Macro Framework van Binary Offensive en aangevuld met zelfontwikkelde tooling. Uniek aan Azreal is het vermogen om complexe infectieketens te genereren. Dit wordt gedaan door verschillende aanvalsvectoren te combineren, zoals diverse containerformaten en documentsoorten, met synthetische, polymorfe malwarebestanden. Bovendien worden misleidende bestandsnamen en snelkoppelingen ingezet, alsook zeldzame bestandsformaten die vaak onopgemerkt blijven door standaardbeveiliging.



Resultaten van het Onderzoek

Meerdere aanvalsvectoren zijn ontdekt waarmee ATP kan worden omzeild. Deze kunnen worden onderverdeeld in meerdere technieken.

6	5	4	2	2
Document	Snelkoppeling	Container	Installer	Overig

Malware Arriveert in de Mailbox

E-mail gebaseerde aanvallen vormen een aanhoudende dreiging die organisaties effectief moeten afwenden. Onze bevindingen laten zien dat zelfs robuuste verdedigingen zoals ATP ruimte laten voor onbekende malware om binnen te dringen. De noodzaak voor gelaagde beveiliging wordt hiermee onderstreept.

CDR
Waarom Preventie Beter is dan Detectie

De Beperkingen van Detectieoplossingen
Detectiegebaseerde oplossingen zoals Managed Detection and Response (MDR), Extended Detection and Response (XDR), Network Detection and Response (NDR), en Endpoint Detection and Response (EDR) zijn belangrijke componenten in het cybersecurity-ecosysteem. Echter, ze zijn voornamelijk gericht op het identificeren en mitigeren van aanvallen nádat ze zijn uitgevoerd. In veel gevallen is dit te laat om schade te voorkomen.[16

Waarom Preventie Cruciaal Is
In het ideale geval zou een aanval moeten worden gestopt voordat hij enige schade kan aanrichten. Preventie is de sleutel tot het minimaliseren van het risico en de impact van een cyberaanval. Het is het digitale equivalent van een goed slot op de deur in plaats van een alarmsysteem dat afgaat als de inbreker al binnen is.

De Kosten van Reactieve Beveiliging
De kosten van het reageren op een cyberaanval kunnen astronomisch zijn, inclusief downtime, verlies van gegevens, herstelkosten, en reputatieschade. Proactieve maatregelen om aanvallen te voorkomen zijn over het algemeen veel goedkoper en effectiever op de lange termijn.

Een Holistische Aanpak
Preventieve oplossingen moeten worden geïntegreerd in een breder beveiligingsbeleid dat ook detectie- en responsmechanismen omvat. Maar zonder een solide basis van preventieve maatregelen zijn deze aanvullende lagen veel minder effectief.

Introductie van Content, Disarm and Reconstruction (CDR)

CDR is een Nieuwe Preventie Beveiligingslaag
Content, Disarm and Reconstruction (CDR) is een geavanceerde beveiligingstechnologie die een nieuwe laag van bescherming introduceert tegen malware en andere cyberdreigingen. In tegenstelling tot traditionele beveiligingsmaatregelen die vooral gericht zijn op detectie, is CDR ontworpen

om actief bestanden te ontmantelen en te herbouwen, waardoor alle mogelijke schadelijke elementen worden verwijderd.

Het Principe van Positieve Selectie

In plaats van te jagen op kwaadaardige kenmerken in een bestand—een benadering die altijd het risico van overzien of misidentificatie met zich meebrengt—maakt CDR gebruik van positieve selectie. Dit betekent dat alleen bekende, goedaardige elementen van een bestand worden toegelaten, terwijl alle andere elementen worden verwijderd of vervangen.

Brede Ondersteuning Bestandsformaten

CDR kan worden toegepast op een breed scala aan bestandsformaten: van documenten en spreadsheets tot afbeeldingen en gecomprimeerde bestanden. Dit maakt het een bijzonder veelzijdige oplossing die in veel verschillende gebruiksscenario's kan worden ingezet.

Gebruikers Merken Geen Vertraging

Het CDR-proces is meestal naadloos en onopvallend, met minimale impact op de gebruikerservaring. Bestanden worden in real-time ontmanteld en gereconstrueerd, waardoor de workflow niet wordt onderbroken maar de veiligheid wel aanzienlijk wordt verbeterd.

CDR als Onderdeel van de Basisbeveiliging

Het Belang van Gelaagde Beveiliging

In de moderne cybersecurity-omgeving is het cruciaal om een gelaagde beveiligingsaanpak te hanteren. Dit betekent het implementeren van verschillende verdedigingsmechanismen die elkaar aanvullen en versterken. CDR vormt een kernonderdeel van deze gelaagde strategie, vooral als het gaat om bestandsgebaseerde dreigingen.

CIS Controls en CDR

CDR heeft impact op verschillende CIS Controls om het securitybeleid te versterken.

- Control 8: Malware Defenses.
- Control 7: Email and Web Browser Protections.
- Control 13: Data Protection
- Control 18: Application Software Security

Complementair aan Bestaande Tools

CDR is een nieuwe beveiligingslaag en heeft geen overlap met overige security producten. De technologie is eenvoudig toe te voegen aan de Microsoft werkplek.

Return on Investment (ROI)

Hoewel de initiële investering in CDR mogelijk hoger kan zijn dan simpelweg vertrouwen op ingebouwde Microsoft 365-beveiliging, biedt de technologie een uitstekende ROI. Het is een voordelige preventieve beveiligingslaag ten opzichte van de hoge kosten van premium detectieoplossingen. Voorkomen is altijd beter dan genezen. Het hebben van minder cyberincidenten om op te acteren betaalt zich al snel terug.

Voordelen van Bodyguard CDR

’s Werelds eerste CDR voor Desktops

Dankzij een diepe integratie met het besturingssysteem wordt bescherming geboden tegen onbekende malware uit elke bron (web, mail, Teams, Zoom en meer).

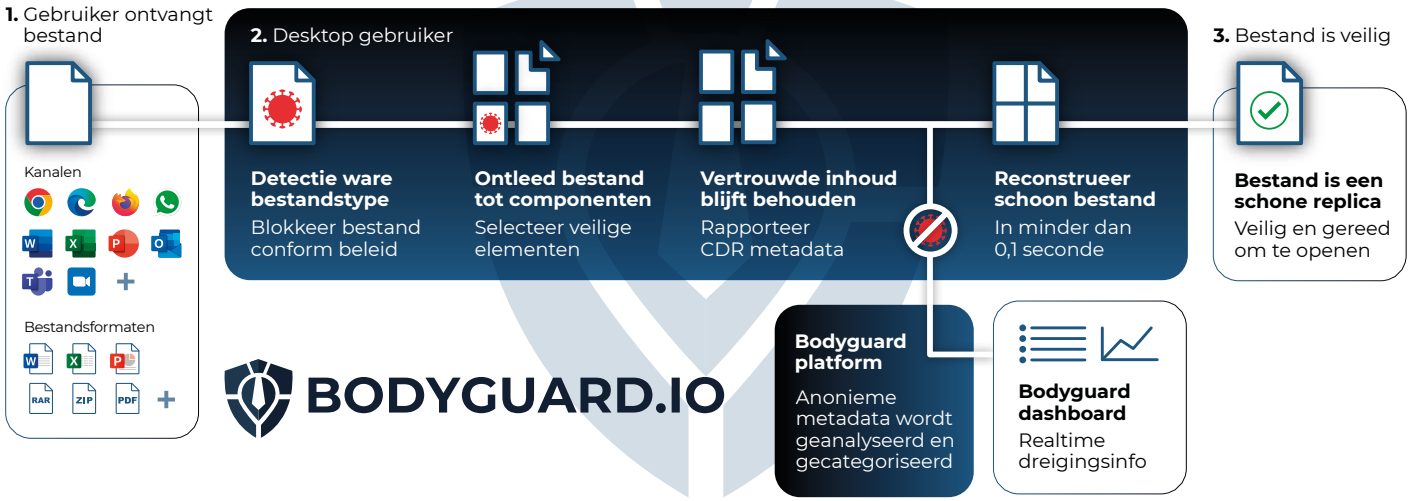
Voordelen

- Voorkom nieuwe malware die niet wordt herkend door antivirus
- “Peace of mind” – medewerkers awareless bestanden laten openen
- Medewerker merkt geen vertraging en behoud functionaliteit
- Bestanden worden op het apparaat verwerkt

Techniek

- Middels positieve selectie krijgen zero-days geen kans
- Lichte footprint op het apparaat van de medewerker
- Brede ondersteuning van bestandsformaten en archieven
- Management dashboard voorziet in dreigingsinformatie

Hoe het werkt



Probeer het uit

Dat kan geheel vrijblijvend. Ga naar **www.bodyguard.io** en druk op “nu uitproberen”.

Liever persoonlijk contact?

Bel met **Vincent van Sas: 06 - 25 01 66 73**
of plan een gesprek in op **www.bodyguard.io**.

Bronvermelding

1 "Infostealer incidents more than doubled in q1 2023," SC Media, 26-7-2023. [Online]. Available: **https://www.scmagazine.com/news/infostealer-incidents-more-than-doubled-in-q1-2023**.

2 "The growing threat from infostealers," Secureworks, 16-5-2023. [Online]. Available: **https://www.secureworks.com/research/the-growing-threat-from-infostealers**.

3 "FBI dismantles qakbot malware," thehackernews, 8-2023. [Online]. Available: **https://thehackernews.com/2023/08/fbi-dismantles-qakbot-malware-frees.html**.

4 "AI chatbots making it harder to spot phishing emails, say experts," The Guardian, 29-3-2023. [Online]. Available: **https://www.theguardian.com/technology/2023/mar/29/ai-chatbots-making-it-harder-to-spot-phishing-emails-say-experts**.

5 P. Schläpfer, "PDF Malware Is Not Yet Dead," HP, 20-5-2022. [Online]. Available: **https://threatresearch.ext.hp.com/pdf-malware-is-not-yet-dead/**.

6 "Rise of LNK (Shortcut files) Malware," McAfee, 21-6-2022. [Online]. Available: **https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/**.

7 "Threat Insights Report Q2 2023," HP Wolf Security, 2023.

8 "Obfuscated Files or Information: Binary Padding," The MITRE Corporation, [Online]. Available: **https://attack.mitre.org/techniques/T1027/001/**.

9 "Detection Efficacy Overview," OPSWAT, [Online]. Available: **https://metadefender.opswat.com/reports/statistics**.

10 "CVE-2023-36884: A Detailed Look at The Recent Microsoft Vulnerability," Picus Security, [Online]. Available: **https://www.picussecurity.com/resource/blog/cve-2023-36884-a-detailed-look-at-the-recent-microsoft-vulnerability**.

11 "Traders' Dollars in Danger: CVE-2023-38831 zero-Day vulnerability in WinRAR exploited by cybercriminals to target traders," Group-IB, 2023. [Online]. Available: **https://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/**.

12 "Adobe warns of critical Acrobat and Reader zero-day exploited in attacks," Bleeping Computer, 12-9-2023. [Online]. Available: **https://www.bleepingcomputer.com/news/security/adobe-warns-of-critical-acrobat-and-reader-zero-day-exploited-in-attacks/**.

13 “CDR Technology Guide,” OPSWAT, 2020.

14 J. Heibrink, “Antivirus and EDR bypasses for initial access,” Radboud University, 2023.

15 “TheD1rkMtr Github profiel,” Github, [Online]. Available: **https://github.com/TheD1rkMtr**.

16 “8 Reasons Why EDR is Not Enough,” Deep Instinct.