**Malware**

**Wat zegt wikipedia** **:**

Malware is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen.

**MalwareBytes :**

**BRON :** [**https://nl.malwarebytes.com/malware/**](https://nl.malwarebytes.com/malware/)



**Alles over malware**

U weet dat artsen een keer per jaar campagne voeren om iedereen een griepprik te geven. Meestal zijn griepuitbraken immers seizoensgebonden: op een bepaalde tijd van het jaar verspreidt de griep zich en begint hij mensen te besmetten.

Pc's, smartphones, tablets en bedrijfsnetwerken zijn echter niet onderhevig aan voorspelbare seizoensinfecties. Voor hen is het griepseizoen nooit voorbij. In plaats van koude rillingen en pijnlijke botten kunnen apparaten van gebruikers hun eigen ziekte oplopen: malware.

Malware-infecties vallen apparaten aan met de kracht van een waterstraal uit een brandslang, elk met een eigen aanvalstactiek: van sluipend en stiekem tot onbehouwen als een voorhamer. Omdat kennis macht is, bieden we u hierna een korte cursus aan over malware, als preventieve prik tegen malwarebesmetting. We leggen u uit wat het is, wat de symptomen ervan zijn, hoe u het krijgt, hoe ermee moet omgaan en hoe u het in de toekomst kunt vermijden.

### Wat is malware?

[Malware](https://blog.malwarebytes.com/glossary/malware/), of "kwaadaardige software", is een overkoepelende term die een kwaadaardig programma of code beschrijft die schadelijk zijn voor computersystemen.

Vijandelijke, opdringerige en opzettelijk boosaardige malware probeert computers, computersystemen, netwerken, tablets en mobiele apparaten binnen te dringen, te beschadigen of uit te schakelen, vaak door gedeeltelijke de controle over te nemen over de werking van een apparaat. Net als griep bij mensen, kan het apparaat niet meer normaal functioneren.

Malware probeert om u op illegale wijze geld afhandig te maken. Hoewel malware de fysieke hardware van systemen of netwerkapparatuur niet kan beschadigen (met één bekende uitzondering: zie de onderstaande rubriek over Google Android), kan het uw gegevens stelen, versleutelen of verwijderen, kan het basisfuncties van uw computer wijzigen of kapen en uw computeractiviteit bespieden, zonder uw medeweten of toestemming.

### Hoe weet ik of ik een malware-infectie heb?

Malware kan aan het licht komen door de vele en uiteenlopende vormen van afwijkend gedrag die het vertoont. Hierna volgen een paar [duidelijke signalen dat uw systeem is besmet met malware](https://blog.malwarebytes.com/101/2016/05/how-to-tell-if-youre-infected-with-malware/):

* Uw computer vertraagt. Een van de belangrijkste effecten van malware is dat het de snelheid van uw besturingssysteem vermindert, of u nu op het internet surft of lokale toepassingen gebruikt.
* Uw scherm wordt overspoeld met een vloedgolf van vervelende advertenties die daar niet thuishoren. Onverwachte pop-upadvertenties zijn een typisch symptoom van een malware-infectie. Ze worden vooral geassocieerd met een vorm van malware die bekend staat als [adware](https://nl.malwarebytes.com/adware/). In deze pop-ups worden meestal ook andere malwarebedreigingen verstopt. Dus als u iets ziet als "GEFELICITEERD, U HEBT NET EEN GRATIS LEZING DOOR EEN HELDERZIENDE GEWONNEN!" in een pop-upvenster, klik er dan niet op. Welke gratis prijs deze advertentie u ook belooft, [hij zal u een aardig centje kosten](https://blog.malwarebytes.com/101/2018/01/how-to-remove-adware-from-your-pc/).
* Uw systeem crasht herhaaldelijk, bevriest of er verschijnt een BSOD (blauw scherm des doods), wat op Windows-systemen soms voorkomt bij een fatale fout.
* U merkt een mysterieus verlies op van schijfruimte, waarschijnlijk als gevolg van een gulzig malwareprogramma dat zich illegaal op uw harde schijf heeft genesteld.
* U merkt een merkwaardige toename op van de internetactiviteit van uw systeem.
* Het gebruik van uw systeembronnen is abnormaal hoog en de ventilator van uw computer begint op volle snelheid te draaien: tekenen van malware-activiteit die op de achtergrond systeembronnen inpalmt.
* De startpagina van uw browser verandert zonder uw toestemming. Of koppelingen waarop u klikt sturen u naar een ongewenst internetadres. Dit betekent meestal dat u op die pop-up met 'felicitaties' hebt geklikt, en dat die op zijn beurt een aantal [ongewenste programma's](https://blog.malwarebytes.com/101/2016/02/how-to-avoid-potentially-unwanted-programs/) heeft gedownload. Ook kan uw browser tergend traag beginnen te werken.
* Nieuwe werkbalken, extensies of plug-ins vullen onverwacht uw browservenster.
* Uw antivirusprogramma werkt niet meer en u kunt het niet bijwerken, waardoor u onbeschermd bent tegen de verborgen malware die uw antivirusprogramma heeft uitgeschakeld.
* En dan is er de pijnlijk voor de hand liggende, opzettelijk onverholen malware-aanval. Dit is het geval met [ransomware](https://nl.malwarebytes.com/ransomware/), die zichzelf aankondigt, meedeelt over uw gegevens te beschikken en losgeld eist om uw bestanden terug te sturen.
* Zelfs als heel uw systeem goed lijkt te werken, wees niet te snel tevreden, want geen nieuws betekent niet altijd goed nieuws. Malware is soms zo krachtig dat hij zich verbergt tot diep in uw computer en zijn vuile zaakjes afhandelt zonder dat er bij u een belletje gaat rinkelen. Ondertussen gaat de malware aan de haal met uw wachtwoorden, steelt uw gevoelige bestanden of gebruikt uw pc om zichzelf te verspreiden op andere computers.

### Hoe loop ik malware op?

Het recept voor een malware-infectie bestaat uit een lange lijst ingrediënten. De belangrijkste zijn de twee meest voorkomende manieren waarop malware toegang krijgt tot uw systeem: het internet en e-mail. Dus eigenlijk altijd wanneer u online bent.

Malware kan uw computer binnendringen (nu even diep ademhalen) als u surft via gehackte websites, klikt op gamedemo's, geïnfecteerde muziekbestanden downloadt, nieuwe werkbalken van een onbekende provider installeert, software van een verdachte bron installeert of een schadelijke e-mailbijlage opent. Vrijwel alles wat u van het internet downloadt op een apparaat dat niet over een goed anti-malwareprogramma beschikt maakt u vatbaar voor malware.

Schadelijke apps kunnen zich verbergen in schijnbaar legitieme applicaties, vooral als ze worden gedownload van websites of uit berichten in plaats van uit een veilige appstore. Het is daarom belangrijk om tijdens de installatie van apps te letten op de waarschuwingen. En u moet extra op uw hoede zijn als die toegang vragen tot uw e-mail of andere persoonlijke informatie.

"Malware-aanvallen kunnen niet werken zonder het belangrijkste ingrediënt: u."

In de eerste plaats kunt u het beste altijd gebruikmaken van vertrouwde bronnen voor mobiele apps, alleen betrouwbare apps van derden installeren en die apps altijd direct downloaden van de leverancier en nooit van een andere site. Wij leven in [een wereld vol slechte spelers](https://blog.malwarebytes.com/101/2015/10/10-ways-to-protect-against-hackers/), die u proberen lokken met het aas van een internetversneller, een nieuwe downloadmanager, een reinigingsprogramma voor uw harde schijf of een alternatieve webzoekservice.

Malware-aanvallen kunnen niet werken zonder het belangrijkste ingrediënt: **u**. Dat wil zeggen, een goedgelovige versie van uzelf, die bereid is om een ​​e-mailbijlage te openen die hij niet herkent of om op iets te klikken uit een onbetrouwbare bron en dat te installeren. Beschouw dit niet als "click-shaming": zelfs de meest ervaren specialisten worden misleid tot het installeren van malware.

Ook als u iets uit een geloofwaardige bron installeert en geen aandacht schenkt aan het toestemmingsverzoek om tegelijkertijd andere gebundelde software te installeren, installeert u mogelijk ongewenste software. Deze extra software wordt vaak voorgesteld als een noodzakelijk onderdeel, maar vaak is dat niet het geval.

Een ander voorval ging gepaard met [social engineering](https://blog.malwarebytes.com/glossary/social-engineering/) en werd door een Malwarebytes-expert waargenomen in het Verenigd Koninkrijk. De zwendel trof mobiele gebruikers, door misbruik te maken van de veel voorkomende optie om [direct mobiel te betalen](http://www.theregister.co.uk/2015/08/11/direct_to_bill_mobile_payment_scam/). De slachtoffers bezochten mobiele sites en activeerden hierbij onbewust onzichtbare knoppen die bepaalde bedragen aan hun mobiel nummer aanrekenden. Die bedragen werden doorgefactureerd aan de netwerken van de slachtoffers, die deze kosten opnamen in hun rekening.

Om eerlijk te zijn, moeten we ook een onberispelijk malware-infectiescenario aan deze lijst toevoegen. Het is immers zelfs mogelijk dat het bezoeken van een kwaadaardige website en het bekijken van een geïnfecteerde pagina en/of banneradvertentie tot een zogenaamde [driveby-download van malware](https://blog.malwarebytes.com/glossary/drive-by-download/) leidt.

Anderzijds, als u geen adequaat beveiligingsprogramma draait, zijn de malware-infectie en de nasleep ervan nog steeds uw verantwoordelijkheid.

### Wat zijn de meest voorkomende vormen van malware?

Hier zijn de meest voorkomende daders in de zwarte lijst met malwarecriminelen:

* [Adware](https://nl.malwarebytes.com/adware/) is ongewenste software die is ontwikkeld om advertenties op uw scherm te doen verschijnen, meestal in een webbrowser. Gewoonlijk vermomt adware zich stiekem als een legitiem programma of lift het mee met een ander programma, zodat u wordt misleid en het programma installeert op uw pc, tablet of mobiele apparaat.
* [Spyware](https://nl.malwarebytes.com/spyware/) is malware die stiekem en zonder toestemming de activiteiten van de computergebruiker observeert en die rapporteert aan de auteur van de software.
* Een [virus](https://blog.malwarebytes.com/glossary/virus/) is malware die zich hecht aan een ander programma en, wanneer het wordt uitgevoerd (meestal doet de gebruiker dit onbedoeld), zichzelf repliceert door andere computerprogramma's te wijzigen en deze te infecteren met eigen stukjes code.
* [Wormen](https://blog.malwarebytes.com/glossary/worm/) zijn een soort malware die op virussen lijkt en zichzelf vermenigvuldigt om zich via een netwerk naar andere computers te verspreiden. Wormen richten hierbij meestal schade aan door gegevens en bestanden te vernietigen.
* Een [Trojaan](https://blog.malwarebytes.com/glossary/trojan/) of Trojaans paard is een van de gevaarlijkste malwaretypes. Om u te misleiden, doet het zichzelf meestal voor als een nuttig hulpmiddel. Zodra het op uw systeem belandt, krijgen de aanvallers in het Trojaanse paard ongeautoriseerde toegang tot uw getroffen computer. Van daaruit kunnen Trojaanse paarden worden gebruikt om financiële informatie te stelen of om bedreigingen zoals virussen en ransomware te installeren.
* [Ransomware](https://nl.malwarebytes.com/ransomware/) is een vorm van malware die uw apparaat vergrendelt en/of uw bestanden versleutelt en u vervolgens dwingt om losgeld te betalen om ze terug te krijgen. Ransomware wordt het favoriete wapen van cybercriminelen genoemd omdat het een snelle, winstgevende betaling vereist in moeilijk te traceren [cryptovaluta](https://blog.malwarebytes.com/101/2017/11/cryptocurrency-works-cybercriminals-love/). De code achter ransomware is eenvoudig te verkrijgen via online criminele marktplaatsen en het verdedigen ertegen is erg moeilijk.
* [Rootkit](https://blog.malwarebytes.com/glossary/rootkit/) is een vorm van malware die de aanvaller beheerdersrechten geeft op het geïnfecteerde systeem. Gewoonlijk is deze malware ook ontworpen om verborgen te blijven voor de gebruiker, andere software op het systeem en het besturingssysteem zelf.
* Een [keylogger](https://blog.malwarebytes.com/glossary/keylogger/) is malware die alle toetsaanslagen van de gebruiker op het toetsenbord registreert. Hierbij wordt de verzamelde informatie meestal opgeslagen en verzonden naar de aanvaller, die op zoek is naar gevoelige informatie zoals gebruikersnamen, wachtwoorden of creditcardgegevens.
* [Kwaadaardige cryptomining](https://blog.malwarebytes.com/101/2018/02/how-to-protect-your-computer-from-malicious-cryptomining/), ook wel driveby-mining of [cryptojacking](https://nl.malwarebytes.com/cryptojacking/) genoemd, is een steeds vaker voorkomende soort malware, die meestal wordt geïnstalleerd door een Trojaans paard. Hiermee kan iemand anders uw computer gebruiken om cryptovaluta's zoals Bitcoin of Monero te minen. Dus in plaats van dat u zelf de rekenkracht van uw computer verzilvert, sturen cryptominers de verdiende cryptomunten naar hun eigen account en niet de uwe. In wezen steelt een kwaadaardige cryptominer uw middelen om geld te verdienen.
* [Exploits](https://blog.malwarebytes.com/glossary/exploit/) zijn een soort malware die misbruik maakt van bugs en [kwetsbaarheden](https://blog.malwarebytes.com/glossary/software-vulnerability/) in een systeem, zodat de maker van de exploit de controle kan overnemen. Naast andere bedreigingen, worden exploits vaak gekoppeld aan [malvertising](https://blog.malwarebytes.com/101/2016/06/truth-in-malvertising-how-to-beat-bad-ads/), die aanvalt via een legitieme site die onbewust kwaadaardige inhoud van een slechte site haalt. Vervolgens probeert de slechte inhoud zichzelf te installeren op uw computer tijdens een driveby-download. Klikken is hierbij niet nodig. Het enige dat van u wordt verwacht, is dat u op de verkeerde dag een betrouwbare site bezoekt.

### Laatste malwarenieuws

[SamSam ransomware: gecontroleerde verspreiding van een ongrijpbare malware](https://blog.malwarebytes.com/threat-analysis/2018/06/samsam-ransomware-controlled-distribution/)  
[VPNFilter-malware zorgt nog steeds voor problemen](https://blog.malwarebytes.com/cybercrime/2018/06/vpnfilter-malware-still-making-waves/)  
[Malware-analyse: decodering van Emotet, deel 1](https://blog.malwarebytes.com/threat-analysis/2018/05/malware-analysis-decoding-emotet-part-1/)

### Wat is de geschiedenis van malware?

Gelet op de talrijke soorten malware en het enorme aantal varianten dat dagelijks op het internet wordt verspreid, is een volledige lijst van alle malware te lang om hier op te sommen. Maar een overzicht geven van de malwaretrends van de afgelopen decennia is best haalbaar. Hieronder vindt u de belangrijkste trends in de evolutie van malware.

**De jaren tachtig en daarna**: De theoretische basis voor "zichzelf vermenigvuldigende automaten" (d.w.z. virussen) gaat terug naar een artikel dat in 1949 werd gepubliceerd. De eerste computers die werden besmet met vroege vormen van virussen waren pre-personal computerplatformen in de jaren zeventig. De geschiedenis van de moderne virussen begint echter met een programma genaamd Elk Cloner, dat in 1982 Apple II-systemen begon te infecteren. Het virus, dat werd verspreid op geïnfecteerde diskettes, was op zichzelf onschadelijk, maar het verspreidde zich naar alle aan het systeem gekoppelde schijven. Het deed dit zo snel dat dit kan worden beschouwd als de eerste grootschalige virusuitbraak in de geschiedenis. Merk op dat dit gebeurde voordat Windows-pc's onderhevig waren aan malware. Sindsdien zijn virussen en wormen wijdverspreid.

**De jaren negentig**: In dit decennium deed het Microsoft Windows-platform zijn aantrede. Windows-programma's zoals Microsoft Word bevatten een flexibele macrotaal waarin malware-auteurs besmette code konden schrijven. Deze macrovirussen infecteerden documenten en sjablonen in plaats van uitvoerbare applicaties, hoewel strikt genomen Word-documentmacro's een vorm van uitvoerbare code zijn.

**2002 tot 2007:** Instantmessagingwormen: deze zichzelf vermenigvuldigende kwaadaardige code, verspreid via een instantmessagingnetwerk, maakte gebruik van gaten in het netwerk om zichzelf op grote schaal te verspreiden. De wormen infecteerden het AOL AIM-netwerk, MSN Messenger en Yahoo Messenger, evenals zakelijke instantmessagingsystemen.

**2005 tot 2009:** Er gebeurden steeds meer adware-aanvallen, die ongewenste advertenties op computerschermen deden verschijnen, soms in de vorm van een pop-upvenster of een venster dat gebruikers niet konden sluiten. Deze advertenties maakten vaak gebruik van legitieme software om zichzelf te verspreiden, maar rond 2008 begonnen software-uitgevers de adwarebedrijven aan te klagen voor fraude. Dit resulteerde in miljoenen dollars aan boetes. Uiteindelijk werden de adwarebedrijven tot sluiting gedwongen.

**2007 tot 2009:** Malware-oplichters wendden zich tot sociale netwerken zoals MySpace als een kanaal voor het verspreiden van valse advertenties, omleidingen en aanbiedingen van valse antivirus- en beveiligingsprogramma's. Met social engineering-trucs probeerden ze consumenten te misleiden. Nadat MySpace in populariteit was afgenomen, werden Facebook en Twitter de voorkeursplatforms. Gangbare tactieken waren het presenteren van neplinks naar [phishingpagina's](https://blog.malwarebytes.com/glossary/phishing/) en het promoten van Facebook-applicaties met kwaadaardige extensies. Toen deze trend afnam, [gingen oplichters op zoek naar andere manieren om met uw geld aan de haal te gaan](https://blog.malwarebytes.com/tech-support-scams/).

**2013**: Een nieuwe vorm van malware, genaamd ransomware, lanceerde een aanval onder de naam CrytptoLocker, die plaatsvond van begin september 2013 tot eind mei 2014 en gericht was op Windows-pc's. CryptoLocker slaagde erin slachtoffers te dwingen om tegen het laatste kwartaal van 2013 ongeveer 27 miljoen dollar te betalen. Bovendien bracht het succes van de ransomware andere gelijknamige ransomware voort. Eén copycatvariant perste tussen april 2014 en juni 2015 meer dan 18 miljoen USD af van ongeveer 1.000 slachtoffers.

**2013 tot 2017:** Ransomware, afgeleverd door exploits, malvertising en Trojaanse paarden, werd de koning van de malware. Dat culmineerde in enorme uitbraken in 2017, met schadelijke gevolgen voor de meest uiteenlopende bedrijven. Ransomware werkt door de gegevens van het slachtoffer te versleutelen en vervolgens betalingen te eisen om deze vrij te geven.

**2017 tot heden**: Cryptovaluta – en hoe je ze kunt minen – heeft wijdverspreide aandacht getrokken. Dit heeft geleid tot een nieuwe malwaredreiging die cryptojacking wordt genoemd, of het stiekem gebruiken van het apparaat van iemand anders om cryptovaluta te minen met de middelen van de slachtoffers.

### Kunnen Macs malware oplopen?

Veel mensen beweren dat [Macs en iPads immuun zijn voor virussen](https://blog.malwarebytes.com/101/2017/03/mac-security-facts-and-fallacies/) (en geen [antivirusprogramma](https://nl.malwarebytes.com/mac-antivirus/) nodig hebben). Grotendeels is dat waar. Voor een lange tijd is dat inderdaad niet gebeurd.

"Mac-systemen zijn onderhevig aan dezelfde kwetsbaarheden (en daaropvolgende infectiesymptomen) als Windows-machines en kunnen niet als kogelvrij worden beschouwd."

Andere soorten malware zijn een ander verhaal. Mac-systemen zijn onderhevig aan dezelfde kwetsbaarheden (en daaropvolgende infectiesymptomen) als Windows-machines en kunnen niet als kogelvrij worden beschouwd. De ingebouwde bescherming van de Mac tegen malware blokkeert bijvoorbeeld niet alle adware en spyware die is gebundeld in frauduleuze applicatiedownloads. Trojaanse paarden en keyloggers vormen ook een bedreiging. De eerste detectie van ransomware die speciaal werd geschreven voor de Mac vond plaats in maart 2016, toen een Trojaanse aanval meer dan 7.000 Mac-gebruikers trof.

Eigenlijk ontdekte Malwarebytes in 2017 meer malware voor Mac dan in enig voorafgaand jaar. Tegen het einde van 2017 was het aantal nieuwe unieke bedreigingen dat onze professionals telden op het Mac-platform meer dan 270 procent hoger vergeleken met het aantal dat in 2016 werd genoteerd.

Bezoek [hier](https://blog.malwarebytes.com/101/2018/03/the-state-of-mac-malware/) de blog van Malwarebytes voor meer informatie over de stand van zaken rond Mac-malware.

### Kunnen mobiele apparaten malware oplopen?

Malware-criminelen houden van de mobiele markt. Smartphones zijn immers geavanceerde, complexe draagbare computers. Ze bieden ook toegang tot een schat aan persoonlijke informatie, financiële gegevens en allerlei waardevolle gegevens voor diegenen die op een oneerlijke manier een centje willen bijverdienen.

Helaas heeft dit geleid tot een exponentiële toename van kwaadaardige pogingen om gebruik te maken van de kwetsbaarheden van smartphones. Van adware, Trojaanse paarden, spyware, wormen tot ransomware: malware vindt op verschillende manieren de weg naar uw telefoon. Klikken op een verdachte link of een onbetrouwbare app downloaden zijn enkele voor de hand liggende boosdoeners, maar je kunt ook geïnfecteerd raken via e-mails, sms-berichten en zelfs je Bluetooth-verbinding. Bovendien kunnen malware zoals wormen zich van de ene geïnfecteerde telefoon naar de andere verspreiden.

Smartphones zijn een enorme markt (lees: doelwit). Eén [bron van statistieken](http://www.itnewsafrica.com/2018/03/meet-the-hackers-a-series-on-mobile-malware/) schat het aantal gebruikers van mobiele apparaten wereldwijd op 2,1 miljard, met een verwachte groei tot 2,5 miljard gebruikers in 2019. Een kwart van deze gebruikers heeft meer dan één apparaat. Fraudeurs vinden de mobiele markt erg aantrekkelijk en maken gebruik van deze gigantische economie om een maximaal voordeel te halen uit hun inspanningen.

Mobiele gebruikers zijn vaak ook een eenvoudiger doelwit. De meesten [beschermen hun telefoons niet](https://blog.malwarebytes.com/101/2016/09/top-10-ways-to-secure-your-mobile-phone/) zo ijverig als hun pc, installeren geen beveiligingssoftware of houden hun besturingssystemen niet up-to-date. Dit maakt hen zelfs kwetsbaar voor primitieve malware. Omdat de schermen van mobiele apparaten klein zijn en gebruikers activiteiten niet gemakkelijk opmerken, kan het gebruikelijke alarmerende gedrag dat u op een pc meteen duidelijk maakt dat u geïnfecteerd bent, in stealth-modus achter de schermen worden uitgevoerd. Dat is bijvoorbeeld het geval met spyware.

Geïnfecteerde mobiele apparaten kunnen bijzonder verraderlijk zijn, zeker in vergelijking met geïnfecteerde pc's. Een gehackte microfoon en camera kunnen elke beweging en elk gesprek volgen. Erger nog, malware voor mobiel bankieren onderschept inkomende oproepen en sms-berichten om de tweestapsverificatie die veel bank-apps gebruiken te omzeilen.

"Het populairdere Android-platform trekt meer malware aan dan de iPhone."

Houd er rekening mee dat op goedkope telefoons vooraf geïnstalleerde malware kan worden geïnstalleerd, die bijna niet kan worden verwijderd. ([Malwarebytes for Android](https://nl.malwarebytes.com/mobile/) waarschuwt u voor dergelijke vooraf geïnstalleerde malware en geeft instructies voor het verwijderen ervan.)

Wat het mobiele malware-ecosysteem betreft, zijn de twee meest voorkomende besturingssystemen voor smartphones Android van Google en iOS van Apple. Android is marktleider met 80 procent van alle smartphoneverkopen, gevolgd door iOS met 15 procent van alle verkochte smartphones. Het is dus geen grote verrassing dat het meer populaire Android-platform meer malware aantrekt dan de iPhone. Laten we ze elk afzonderlijk bekijken.

### Hoe weet ik of mijn Android-apparaat malware bevat?

Gelukkig zijn er een paar onmiskenbare alarmsignalen die u kunt detecteren als uw Android-telefoon is geïnfecteerd. Als u een van de volgende dingen ziet, bent u mogelijk geïnfecteerd:

* Plots verschijnen er pop-upvensters met opdringerige advertenties. Als ze uit het niets verschijnen en u naar verdachte websites sturen, hebt u waarschijnlijk iets geïnstalleerd waarin adware zit verborgen. Klik dus niet op de advertentie.
* Een raadselachtige toename in datagebruik. Malware gebruikt uw mobiele data om advertenties weer te geven en de uit uw telefoon gestolen gegevens te verzenden.
* Vreemde kosten op uw telefoonrekening. Dit gebeurt wanneer kwaadaardige software oproepen maakt en sms-berichten verstuurt naar betalende nummers.
* De batterij van uw smartphone is te snel leeg. Malware gebruikt veel rekenkracht, waardoor uw batterij sneller leegloopt dan normaal.
* Mensen op uw contactlijst melden vreemde oproepen en sms-berichten vanaf uw telefoon. Malware verspreidt zich via e-mails en sms-berichten van het ene apparaat naar het andere, met het verzoek om op de geïnfecteerde link te klikken die de malware weergeeft.
* De telefoon wordt warm, maar de prestaties blijven traag. Zo is er zelfs een Trojaan die Android-telefoons binnendringt met een misdadig installatieprogramma dat de processor zodanig belast dat hij oververhit raakt, waardoor de batterij opzwelt en [uw Android het begeeft](https://blog.malwarebytes.com/cybercrime/2017/12/lo-lo-lo-lo-loapi-we-have-you-protected/).
* Onverwachte apps op uw scherm. Soms download u apps die malware bevatten die ongemerkt wordt geïnstalleerd. Dat komt omdat Android gebruikers rechtstreeks van Google Play naar andere marktplaatsen zoals Amazon verwijst. Het is mogelijk dat deze markplaatsen een malwaremaker door de mazen van het net hebben laten glippen.
* Uw telefoon schakelt zelf wifi- en internetverbindingen in. Dat is nog een manier waarop malware zich verspreidt, door uw voorkeuren te negeren en infectiekanalen te openen.
* Hieronder bespreken we wat u moet doen als [uw Android is geïnfecteerd](https://blog.malwarebytes.com/101/2018/03/10-ways-to-protect-your-android-phone/). Bovendien vindt u hier een blogartikel van Malwarebytes over het [beveiligen van uw privacy op een Android-apparaat](https://blog.malwarebytes.com/cybercrime/2017/04/mobile-menace-monday-securing-your-privacy-on-android/).

### Hoe weet ik of mijn iPhone of iPad malware bevat?

Als de naam van uw smartphone begint met een kleine letter "i", dan kunt u uzelf een schouderklopje geven: malware is geen belangrijk probleem op de iPhone. Dat wil niet zeggen dat het niet bestaat, maar het is uiterst zeldzaam. In feite kan een malware-infectie op een iPhone meestal alleen plaatsvinden in twee uitzonderlijke omstandigheden.

"Hoewel het onwaarschijnlijk is dat u het slachtoffer wordt van regelrechte malware-infecties, beschermt een iPhone je helemaal niet tegen scam-telefoontjes of scam-tekstberichten."

Het eerste is een gerichte aanval door een tegenstander op nationaal niveau – een regering die voor een bedrag van miljoenen dollars een stukje malware heeft gemaakt of gekocht om misbruik te maken van een obscuur beveiligingslek in iOS. Wees niet verwonderd: alle apparaten hebben hun kwetsbare plekken. Om zeker te zijn, heeft Apple iOS goed beveiligd. iOs voorkomt zelfs dat apps (inclusief beveiligingssoftware) de telefoon of andere apps op het systeem van het apparaat kunnen scannen. Daarom is het zo duur om malware te ontwikkelen die zijn eigen code installeert om de misdadige natie of staat op afstand de gewenste activiteiten te laten uitvoeren.

Een [bijzonder opmerkelijk geval](http://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/) vond plaats in 2016 toen een internationaal erkende mensenrechtenverdediger, gevestigd in de Verenigde Arabische Emiraten (VAE), sms-berichten ontving op zijn iPhone die "nieuwe geheimen" beloofde over gedetineerden die werden gemarteld in gevangenissen in de Verenigde Arabische Emiraten. De getargete ontvanger werd uitgenodigd om op een bijgevoegde link te klikken. Hij deed dat niet, maar stuurde de boodschap in plaats daarvan naar experts in computerbeveiliging, die het identificeerden als een exploit die de telefoon van de activist in een digitale spion zou veranderen.

Het tweede voorbeeld is wanneer een gebruiker zijn iPhone kwetsbaar maakt door deze te jailbreaken, waardoor de beperkingen die Apple oplegt worden opgeheven. Deze beperkingen zijn er voornamelijk op gericht dat apps alleen kunnen worden geïnstalleerd vanuit de App Store. Apple controleert immers zorgvuldig de ontwikkelaars waarvan het de apps aanbiedt, ook al is het al gebeurd dat samen met een legitieme app tevens malware werd geïnstalleerd.

Nog een punt. Hoewel het onwaarschijnlijk is dat u het slachtoffer wordt van regelrechte malware-infecties, beschermt een iPhone je helemaal niet tegen scam-telefoontjes of scam-tekstberichten. Als u op een link tikt in een bericht van een onbekende bron (of van iemand die zich uitgeeft voor een bekende en diens identiteit heeft gekaapt), kan deze u naar een site sturen die uw inloggegevens en andere persoonlijke gegevens vraagt. Er zijn dus nog steeds voldoende manieren waarop u een slachtoffer kunt worden. Wees altijd voorzichtig.

### Op wie is malware gericht?

Het antwoord is: maak zelf uw keuze. Consumenten zijn in het bezit van miljarden apparaten. Deze apparaten zijn verbonden met banken, winkelaccounts en alles wat de moeite loont om te stelen. Daarom is het werkgebied van adware, spyware, keyloggers en malvertising heel omvangrijk en vergt het luie criminelen relatief weinig inspanning om malware te maken en die te verspreiden naar zoveel mogelijk doelwitten.

"Als u uw smartphone of tablet op de werkplek gebruikt, kunnen hackers hun aanval op uw werkgever richten."

Cyptominers en ransomwareleveranciers lijken niet te discrimineren wat hun doelen betreft. Zowel individuen als bedrijven, ziekenhuizen, gemeenten en winkelsystemen zijn hun slachtoffers.

De makers van mobiele spyware hebben het echter niet alleen op consumenten gemunt. Als u uw smartphone of tablet op de werkplek gebruikt, kunnen hackers hun aanval op uw werkgever inzetten via kwetsbaarheden in mobiele apparaten. Bovendien is het mogelijk dat het responsteam van uw bedrijf geen inbreuken kan opsporen die ontstaan ​​door het gebruik van zakelijke e-mail via een mobiel apparaat.

Nogmaals: niet alle apps die beschikbaar zijn via App Store en Google Play zijn wenselijk, en het probleem is nog groter in appstores van derden. Hoewel de eigenaars van appstores proberen te voorkomen dat kwaadaardige apps hun site binnendringen, is het onvermijdelijk dat er een aantal door de mazen van het net glippen. Deze apps kunnen gebruikersinformatie stelen, geld proberen af te persen van gebruikers, toegang proberen te krijgen tot bedrijfsnetwerken waarmee het apparaat is verbonden en gebruikers dwingen ongewenste advertenties te bekijken of zich in te laten met andere vormen van ongewenst gedrag.

### Hoe kan ik malware verwijderen?

Als u denkt het slachtoffer van malware te zijn of als u gewoon voorzichtig wilt zijn, moet u de volgende stappen ondernemen.

Als u dit nog niet hebt gedaan, moet u allereerst een legitiem [antimalwareprogramma downloaden](https://nl.malwarebytes.com/), zoals [Malwarebytes for Windows](https://nl.malwarebytes.com/premium/), [Malwarebytes for Mac](https://nl.malwarebytes.com/mac/), [Malwarebytes for Android](https://nl.malwarebytes.com/mobile/) of [een van onze producten voor bedrijven](https://nl.malwarebytes.com/business/). Vervolgens installeert u het en voert u een scan uit. Deze programma's zijn ontworpen om malware op uw apparaat op te sporen en te elimineren.

Zodra het apparaat schoon is, is het een goed idee om uw wachtwoorden te wijzigen, niet alleen van uw pc of mobiel apparaat, maar ook van uw e-mail, uw accounts op sociale media, uw favoriete online winkels en uw bank- en factureringsapps.

Als uw iPhone op de een of andere manier is geïnfecteerd met hardnekkige malware, maakt dat de zaken iets lastiger. Apple staat scans van het iPhone-systeem of andere bestanden niet toe. Uw enige optie is de gegevens van uw telefoon te wissen met een fabrieksreset en ze vervolgens te herstellen vanaf uw back-up (want die hebt u, toch?). U kunt ook overwegen beveiligingssoftware te gebruiken die scam-telefoontjes en scam-berichten, zoals Malwarebytes for iOS (binnenkort beschikbaar), kan screenen en blokkeren.  
(Lees voor meer informatie "[10 eenvoudige stappen om uw geïnfecteerde computer schoon te maken](https://blog.malwarebytes.com/101/2015/06/10-easy-steps-to-clean-your-infected-computer/)" door Wendy Zamora.)

### Hoe kan ik mezelf beschermen tegen malware?

Blijf waakzaam. Let goed op als u een domeinnaam tegenkomt die eindigt in een oneven aantal letters, dat wil zeggen iets anders dan com, org, edu of biz, om er maar een paar te noemen, omdat deze een indicator kunnen zijn voor verdachte websites.

"Zorg ervoor dat uw besturingssysteem, browsers en plug-ins altijd up-to-date zijn."

Let op al uw apparaten goed op de voortekenen van een malware-infectie, om te voorkomen dat de malware zich in uw systeem ingraaft.

Vermijd het te klikken op pop-upadvertenties wanneer u surft op het internet. Open geen ongevraagde e-mailbijlagen en download geen software van onbetrouwbare websites of peer-to-peer bestandsoverdrachtsnetwerken.

Zorg ervoor dat uw besturingssysteem, browsers en plug-ins altijd up-to-date zijn, omdat bijgewerkte software criminelen op afstand kan houden.

Mobiele gebruikers: download alleen apps uit de Google Play Store (met de iPhone bent u sowieso beperkt tot de App Store). Controleer telkens wanneer u een app downloadt eerst de score en de beoordelingen. Als de app een lage score en een laag aantal downloads heeft, kunt u deze het beste vermijden.

Download geen apps van externe bronnen. De beste manier om hier zeker van te zijn, is om deze functie op uw Android-telefoon uit te schakelen. Ga naar Instellingen op uw Android-apparaat en open het gedeelte Beveiliging. Zorg ervoor dat Onbekende bronnen is uitgeschakeld, om te voorkomen dat apps van andere marktplaatsen dan de Play Store worden geïnstalleerd.

Klik niet op vreemde, niet-geverifieerde links in e-mails, sms-berichten en WhatsApp-berichten van onbekende oorsprong. Vreemde links van vrienden en contacten moeten ook worden vermeden, tenzij je hebt gecontroleerd of ze veilig zijn.

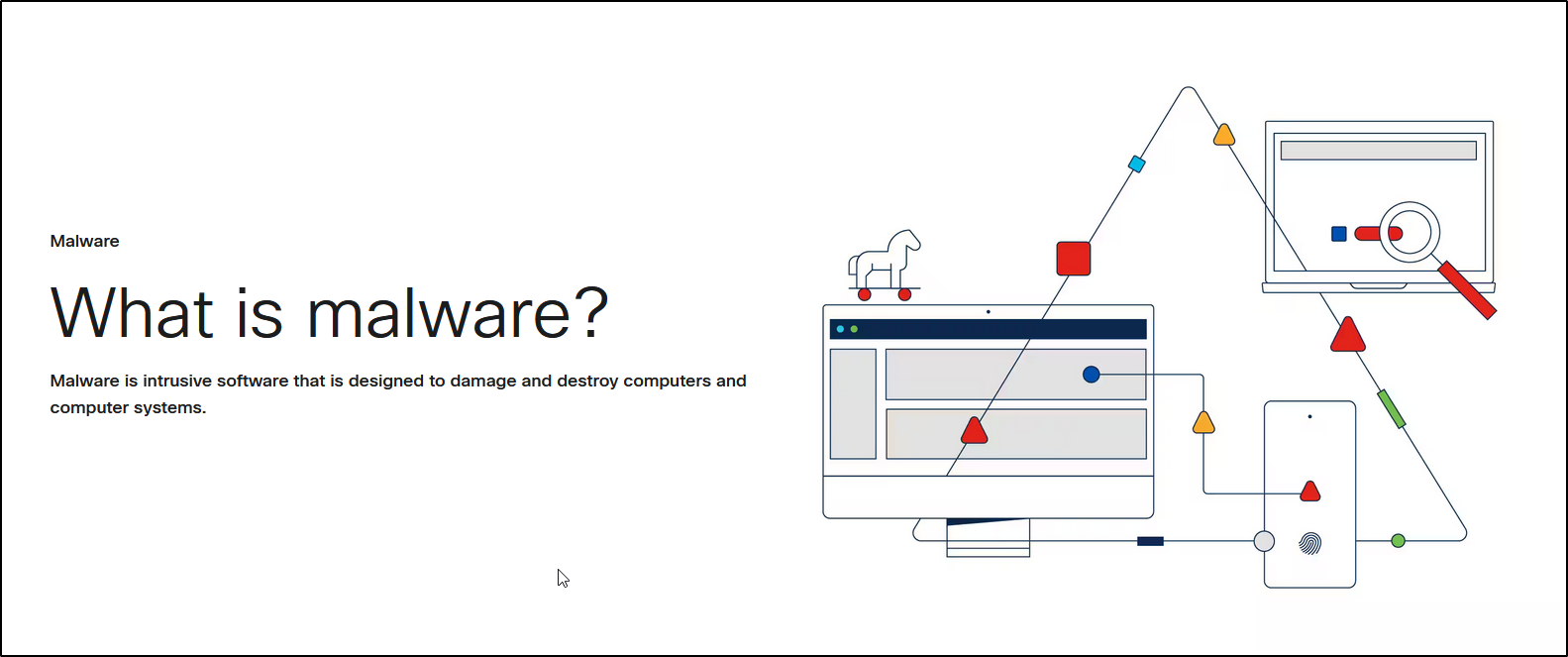
Om hun bedrijven veilig te houden, kunnen organisaties voorkomen dat kwaadaardige apps hun netwerken bedreigen door een sterk mobiel beveiligingsbeleid te ontwikkelen en door een mobiele beveiligingsoplossing te implementeren die dit beleid kan afdwingen. Dit is van vitaal belang in de huidige zakelijke omgeving, waarin meerdere besturingssystemen in meerdere vestigingen aan het werk zijn.

Zorg tot slot voor een goed anti-malwareprogramma. Het moet gelaagde bescherming bieden (de mogelijkheid om malware zoals adware en spyware [te scannen en te detecteren](https://nl.malwarebytes.com/mwb-download/) en tegelijk een proactieve realtime verdediging bieden om bedreigingen zoals ransomware te kunnen blokkeren). Uw beveiligingsprogramma moet ook de mogelijkheid bieden om alle eventueel door de malware aangebrachte systeemwijzigingen terug te draaien, zodat uw systeem weer normaal functioneert.

Dus om te vermijden dat uw pc, smartphone of bedrijfsnetwerk een slachtoffer wordt, moet u in tegenaanval gaan door een [computerbeveiligings- en antivirusprogramma](https://nl.malwarebytes.com/) van hoge kwaliteit te downloaden, zoals [Malwarebytes for Windows](https://nl.malwarebytes.com/premium/), [Malwarebytes for Mac](https://nl.malwarebytes.com/mac/), [Malwarebytes for Android](https://nl.malwarebytes.com/mobile/), [Malwarebytes Portable](https://nl.malwarebytes.com/techbench/) of een van [Malwarebytes' zakelijke producten](https://nl.malwarebytes.com/business/). . (Net zoals het een goed idee is om die griepprik te krijgen!)

**Cisco:**

**BRON**: <https://www.cisco.com/site/us/en/products/security/what-is-malware.html>



## Introduction

Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.

## What is the intent of malware?

Malware is developed as harmful software that invades or corrupts your computer network. The goal of malware is to cause havoc and steal information or resources for monetary gain or sheer sabotage intent.

### Intelligence and intrusion

Exfiltrates data such as emails, plans, and especially sensitive information like passwords.

### Disruption and extortion

Locks up networks and PCs, making them unusable. If it holds your computer hostage for financial gain, it's called ransomware.

### Destruction or vandalism

Destroys computer systems to damage your network infrastructure.

### Steal computer resources

Uses your computing power to run botnets, cryptomining programs (cryptojacking), or send spam emails.

### Monetary gain

Sells your organization's intellectual property on the dark web.

## How do I protect my network against malware?

Typically, businesses focus on preventative tools to stop breaches. By securing the perimeter, businesses assume they are safe. However, some advanced malware will eventually make their way into your network. As a result, it is crucial to deploy technologies that continually monitor and detect malware that has evaded perimeter defenses. Sufficient advanced malware protection requires multiple layers of safeguards along with high-level network visibility and intelligence.

## How do I detect and respond to malware?

Malware will inevitably penetrate your network. You must have defenses that provide significant visibility and breach detection. To remove malware, you must be able to identify malicious actors quickly. This requires constant network scanning. Once the threat is identified, you must remove the malware from your network. Today's antivirus products are not enough to protect against advanced cyberthreats.

## 7 types of malware

### Virus

Viruses are a subgroup of malware. A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lie dormant until the file is opened and in use. Viruses are designed to disrupt a system's ability to operate. As a result, viruses can cause significant operational issues and data loss.

### Worms

A worm is a type of malicious software that rapidly replicates and spreads to any device within the network. Unlike viruses, worms do not need host programs to disseminate. A worm infects a device through a downloaded file or a network connection before it multiplies and disperses at an exponential rate. Like viruses, worms can severely disrupt the operations of a device and cause data loss.

### Trojan virus

Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data. This can be extremely harmful to the performance of the device. Unlike normal viruses and worms, Trojan viruses are not designed to self-replicate.

### Spyware

Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information.

### Adware

Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous, in some cases adware can cause issues for your system. Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware. Additionally, significant levels of adware can slow down your system noticeably. Because not all adware is malicious, it is important to have protection that constantly and intelligently scans these programs.

### Ransomware

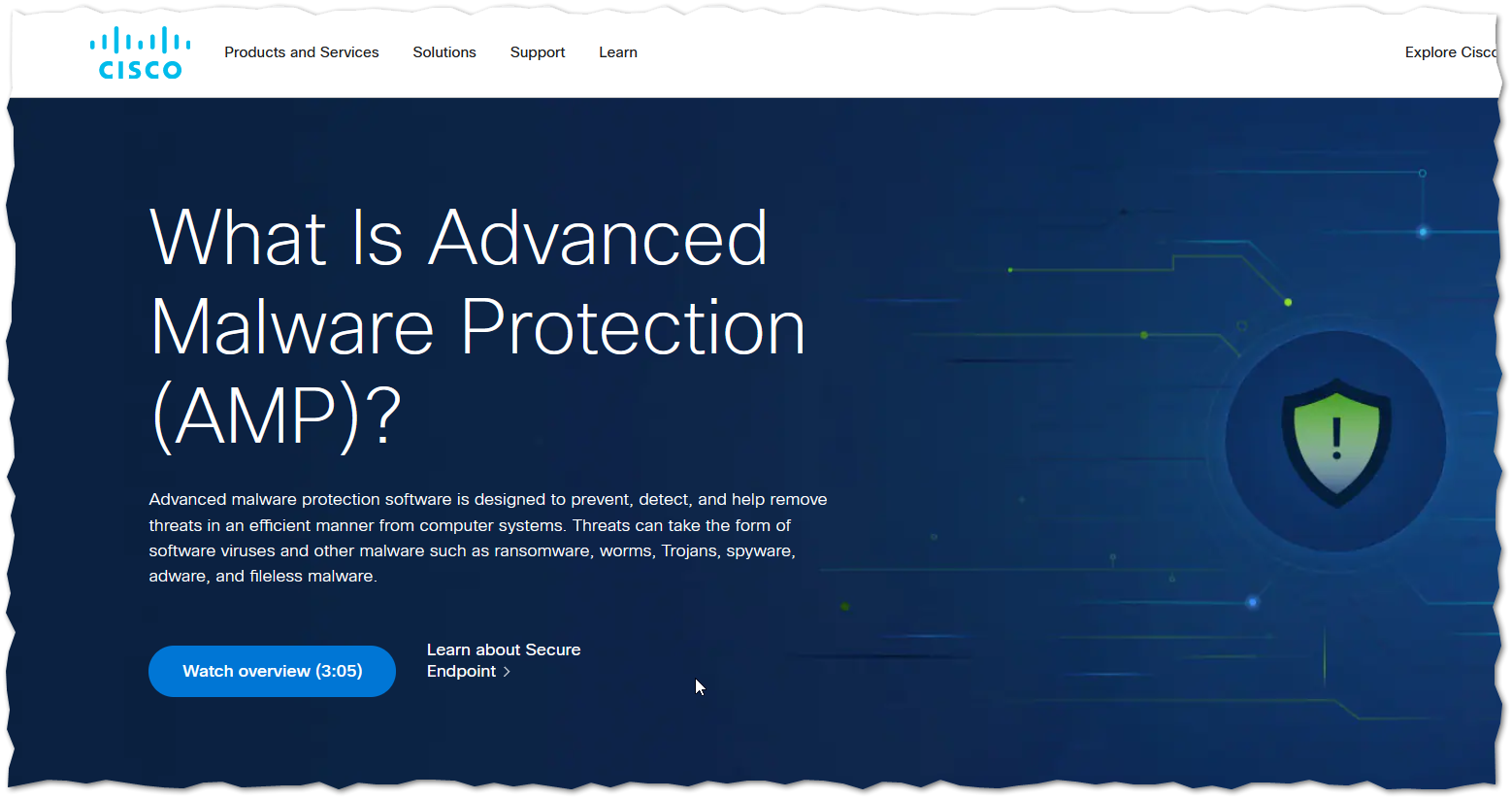
Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released. Ransomware is commonly part of a phishing scam. By clicking a disguised link, the user downloads the ransomware. The attacker proceeds to encrypt specific information that can only be opened by a mathematical key they know. When the attacker receives payment, the data is unlocked.

### Fileless malware

Fileless malware is a type of memory-resident malware. As the term suggests, it is malware that operates from a victim's computer's memory, not from files on the hard drive. Because there are no files to scan, it is harder to detect than traditional malware. It also makes forensics more difficult because the malware disappears when the victim computer is rebooted. [In late 2017, the Cisco Talos threat intelligence team posted an example of fileless malware that they called DNSMessenger.](https://blog.talosintelligence.com/dnsmessenger/)

## What are the benefits of advanced malware protection?

Advanced malware can take the form of common malware that has been modified to increase its capability to infect. It can also test for conditions of a sandbox meant to block malicious files and attempt to fool security software into signaling that it is not malware. Advanced malware protection software is designed to prevent, detect, and help remove threats in an efficient manner from computer system.



## What is advanced malware?

Advanced malware's goal, in general, is to penetrate a system and avoid detection. It usually has a specific target—most often an organization or enterprise—with the objective of financial gain. It might also target similar organizations within the same industry, such as several companies in field of insurance or finance. Advanced malware can take the form of common malware that has been modified to increase its capability to infect.

## How does advanced malware work?

Once loaded onto a computer system, advanced malware can self-replicate and insert itself into other programs or files, infecting them in the process. It can even lay dormant for a time. Advanced malware can also test for conditions of a sandbox meant to block malicious files and attempt to fool security software into signaling that it is not malware.

## Why is advanced malware protection important?

Advanced malware protection is primarily designed to help organizations prevent breaches caused by advanced malware. The damage from such breaches can range from losing a single endpoint to incapacitating an entire IT infrastructure, causing loss of productivity to employees and potentially interrupting customer services and product sales and support.

## Types of advanced malware protection

### Prevention

Traditional antivirus (AV) software relies heavily upon detecting the signature, or binary pattern, of a virus to identify and prevent damage from malware. But most malware authors stay a step ahead of such software by writing oligomorphic, polymorphic, and more recently metamorphic viruses, which use obfuscation techniques such as encrypting parts of themselves or otherwise modify themselves so as to not match virus signatures in the antivirus database.

Endpoint security that employs advanced malware protection blocks known malware exploits accurately and efficiently without being solely dependent on signatures. Conversely, legacy AV solutions can be blind to malware in zip and other formats, as well as fileless malware, and fail to catch advanced threats.

### Detection

Around 2013, the security industry's focus began to shift toward signature-less approaches to antivirus protection. Traditional antivirus solutions may struggle to accurately detect low-prevalence threats. But endpoint security that employs continuous monitoring of all file activity results in faster detection of new threats.

New antivirus capabilities were developed to detect and mitigate zero-day attacks and other, more sophisticated malware. Some of these next-generation capabilities include:

* Behavior-based malware detection, which builds a full context around every process execution path in real time
* Machine learning models, which identify patterns that match known malware characteristics and other various forms of artificial intelligence

### Response

More effective response methods are now found in advanced malware protection solutions, such as endpoint detection and response (EDR) and—more recently—extended detection and response (XDR) tools. Unlike traditional endpoint security, advanced malware protection solutions also provide retrospective security that rapidly contains the threat at the first sign of malicious behavior.

### Efficiency

Legacy antivirus deployments often require complex configuration and management. Advanced malware protection solutions provide prevention, detection, and response all in one solution and are generally highly automated. Their built-in, open platforms enable much simpler and more efficient workflows.

**DATABASE maleware:**

**BRON**: <https://resources.infosecinstitute.com/topic/top-7-malware-sample-databases-and-datasets-for-research-and-training/>

Afbeelding met tekst

Automatisch gegenereerde beschrijving

## 7. SoReL-20M

In response to the lack of large-scale, standardized and realistic data for those needing to research malware, researchers at Sophos and ReversingLabs have released SoReL-20M, which is a database containing 20 million malware samples, including 10 million disabled malware samples.

Samples in SoReL-20M have adopted features from the Ember 2.0 dataset, such as detection metadata, labels and complete binaries. It is still young, and mostly contains executable and Windows files, so it still has some room to grow. That being said, researchers can already make use of the vastness of the malware samples it contains, which can be found [here](https://github.com/sophos-ai/SOREL-20M).

## 6. VirusShare

A longtime staple of malware sample datasets, [VirusShare](https://virusshare.com/) deserves to be in the top seven. After registering for an account (by emailing admin@virusshare.com and asking for one), you can search for samples, grab some hashes, research specific malware families and other key details about any of the over 37 million malware samples that VirusShare contains.

Don’t let the barebones aesthetics of VirusShare fool you — it is one of the most useful sources for malware research and training out there.

## 5. InQuestLabs

Earning its spot on the list due to usability (not to mention offering features that the others don’t) is [InQuestLabs](https://labs.inquest.net/). This malware database offers a solid list of features:

* Deep file inspection (DFI)
* Aggregate reputation database
* Indicators of compromise (IOC)
* Base64 regular expression generator
* Mixed hex case generator
* UInt() trigger generator

## 4. MalwareBazaar

While it may not have the sheer number of malware samples that others have, it offers great insights for researching and malware training. One of the most useful things about the [MalwareBazaar](https://bazaar.abuse.ch/) is the information available. The dashboard is referred to as “browse” and at first glance, it tells you how many samples were uploaded to the database in the last 24 hours, the most seen malware family in the last 24 hours, the number of malware samples currently in the database, a syntax search field and a running list of the most recent uploaded samples, in descending order based on upload date.

MalwareBazaar organizes samples based upon date, SHA256 hash, file type, signature, tags and reporter of the malware. Once you have found your sample, downloading it in a zip file is as simple as using the file password that MalwareBazaar provides for the malware sample.

## 3. Hybrid Analysis

[Hybrid Analysis](https://www.hybrid-analysis.com/) offers a database of malware samples but what sets it apart is two things. The first is a free malware analysis service open to all. And all you have to do to get the file analyzed is drag and drop the file you think is suspicious and you are off to the races. The second thing that distinguishes this malware sample database is the aptly named Hybrid Analysis technology that the search uses to compare the sample. It checks multiple databases and file collections to detect some of the rarer malware samples.

It should be noted that for full use of Hybrid Analysis, you will want to use one of the paid versions for full access to all malware samples.

## 2. URLhaus

Let’s face it — sometimes all you have to go on is a URL. If you thought it may be suspicious, the last thing you would want to do is paste the URL into your browser and go to it. For those situations, [URLhaus](https://urlhaus.abuse.ch/) is just what you are looking for. This malware database stores URLs for known malware, lets users propose new malware URLs, and offers the dataset as a parsable list of the URLs via the URLhause API.

Offering statistics for a malware sample database is fairly common, but what is not common is what URLhaus provides:

* Most delivered payload
* Average takedown time
* Top malware-hosting network
* Blocklist comparison
* Average reaction time

## 1. VirusBay

[VirusBay](https://beta.virusbay.io/) offers what virtually no one else can — a collaborative support system that connects SOC professionals, learners and novices with high-end malware researchers. This heightened collaboration within cybersecurity intends to help organizations’ response and recovery to information security incidents when it would not be possible for external experts to come out to the site or facility.

VirusBay offers the following features:

* Secure (and free) malware sample exchange
* Security incident report generator
* Indicators of compromise (IOC) Q&A
* One-click call for papers (CFP)
* A credits-based community where your skills are noticeable immediately. Each user’s skill is measured separately, and actions taken by users can earn credits.

**Sophos:**

**BRON:** [**https://www.securityweek.com/sophos-reversinglabs-release-20-million-sample-dataset-malware-research/**](https://www.securityweek.com/sophos-reversinglabs-release-20-million-sample-dataset-malware-research/)

Afbeelding met tekst, schermafbeelding, monitor

Automatisch gegenereerde beschrijving

**Sophos and ReversingLabs on Monday announced SoReL-20M, a database of 20 million Windows Portable Executable files, including 10 million malware samples.**

Aimed at driving security improvements across the industry, the database provides metadata, labels, and features for the files within, and enables interested parties to download the available malware samples for further research.

Containing a curated and labeled set of samples and relevant metadata, the [publicly-accessible dataset](https://github.com/sophos-ai/SOREL-20M) is expected to help accelerate machine learning research for malware detection.

Although machine learning models are built on data, the field of security lacks a standard, large-scale dataset that all types of users (ranging from independent researchers to laboratories and corporations) can easily access, which has so far slowed down advancement, Sophos argues.

“Obtaining a large number of curated, labeled samples is both expensive and challenging, and sharing data sets is often difficult due to issues around intellectual property and the risk of providing malicious software to unknown third parties. As a consequence, most published papers on malware detection work on private, internal datasets, with results that cannot be directly compared to each other,” the company says.

A production-scale dataset covering 20 million samples, including 10 million disarmed pieces of malware, the SoReL-20M dataset aims to address the problem.

For each sample, the dataset includes features that have been extracted based on the EMBER 2.0 dataset, labels, detection metadata, and complete binaries for the included malware samples.

Additionally, PyTorch and LightGBM models that have already been trained on this data as baselines are provided, along with scripts needed to load and iterate over the data, as well as to load, train, and test the models.

Given that the malware being released has been disarmed, it would require “knowledge, skill, and time to reconstitute” and run, Sophos [says](https://ai.sophos.com/2020/12/14/sophos-reversinglabs-sorel-20-million-sample-malware-dataset/).

The company does admit that there is a chance that skilled attackers would learn from these samples or use them to create attack tools, but argues that there “are already many other sources attackers could leverage to gain access to malware information and samples that are easier, faster and more cost effective to use.”

Thus, the company believes that the disarmed samples are more valuable to security researchers looking to advance their independent defenses.

The disabled malware samples, which have been in the wild for a while, are expected to call back to dismantled infrastructure. Moreover, they should be detected by most anti-virus vendors. With metadata released alongside the samples, detection is expected to improve.

“As an industry, we know malware isn’t limited to Windows or even executable files, which is why researchers and security teams will always need more data,” ReversingLabs, which claims to be providing a reputation database of more than 12 billion goodware and malware files, [said](https://blog.reversinglabs.com/blog/advancing-the-cybersecurity-industry-with-the-sorel-20m-initiative).