TRUST IN GERMAN SICHERHEIT

G DATA Whitepaper

DeepRay®

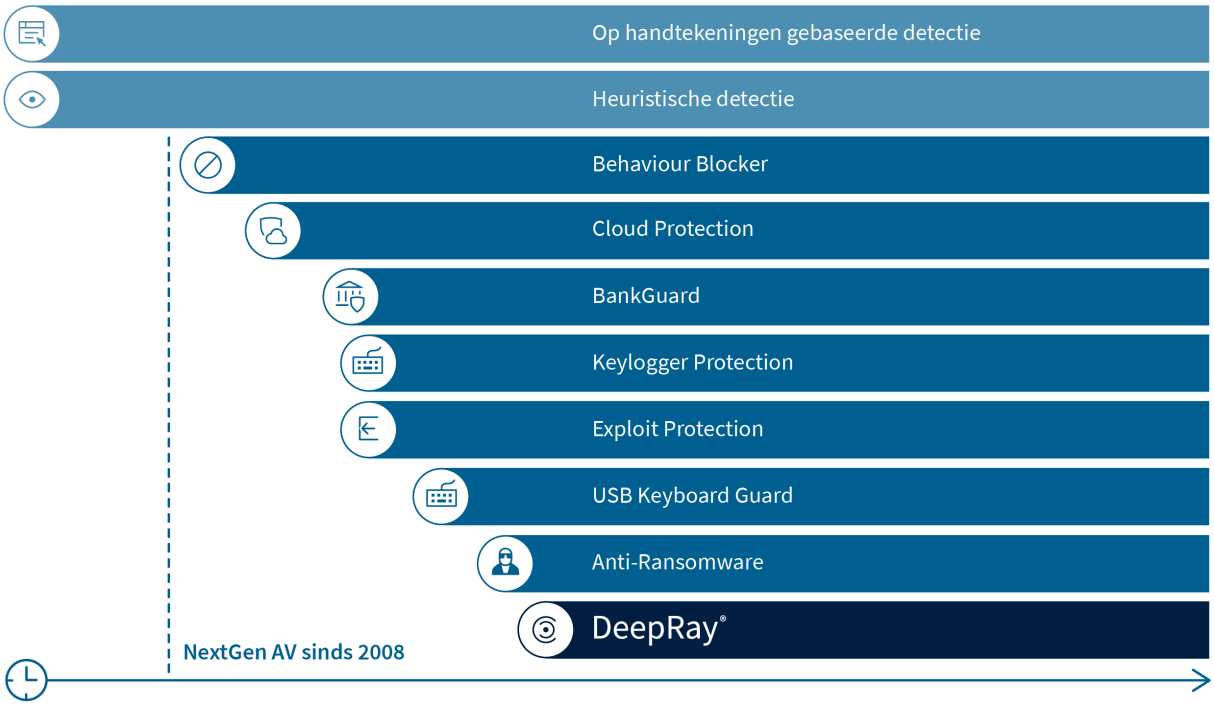
G DATA Software AG

Contents

IT-beveiliging maakt gebruik van kunstmatige intelligentie en Machine Learning

Cybercriminelen en aanbieders van IT-beveiligingsoplossingen spelen al heel lang een kat-en-muis-spelletje met elkaar. Aanvallen met bekende tactieken kunnen sneller en eenvoudiger worden afgeslagen dan aanvallen met nieuwe malware. Daarom bedenken hackers telkens weer nieuwe tactieken om het door beveiligingsoplossingen gevormde bolwerk te slechten. Traditionele benaderingen, zoals op handtekeningen gebaseerde detectietechnieken, kunnen alleen reactief ageren.

Al sinds 2008 omvat ons aanbod Next Generation-technologieën die veranderde en nieuwe dreigingen onmiddellijk kunnen uitschakelen. DeepRay® beschermt gebruikers tegen de geavanceerde tactieken van criminele hackers. Technologische innovaties met kunstmatige intelligentie, Machine Learning en neurale netwerken helpen ons om bedreigingen het hoofd te bieden.



Hoe wordt malware verspreid naar endpoints?

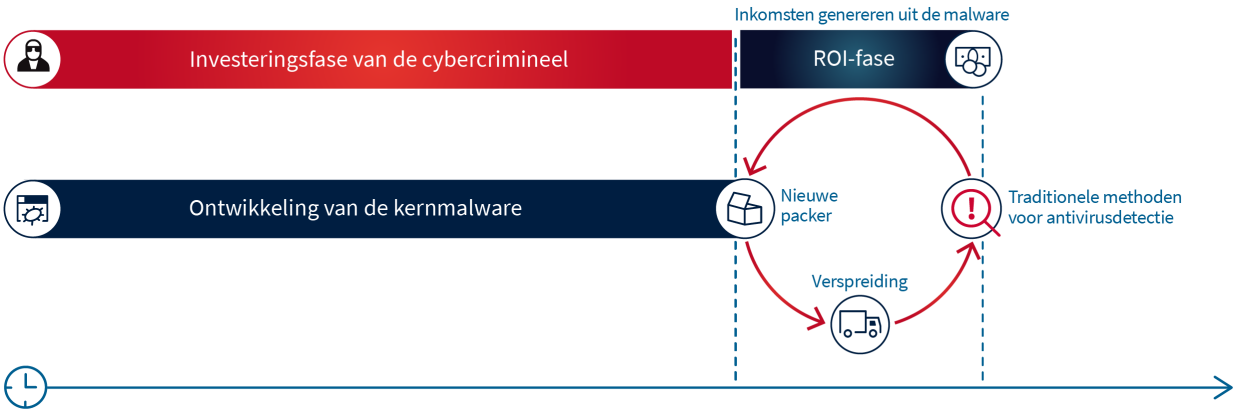
Criminele malwareontwikkelaars opereren in een markt die de traditionele bedrijfslogica volgt. Het produceren van malware gaat gepaard met hoge kosten. Daarom moet deze investering een voldoende rendement genereren. Om dit rendement te bereiken, moet de malware zoveel mogelijk endpoints infecteren. Eenmaal geïdentificeerd, wordt de malware echter gedetecteerd door antivirusprogramma's en kan geen schade meer aanrichten. De malware is dan niet langer rendabel.

Om niet telkens weer met veel moeite nieuwe malware te hoeven schrijven, wordt de malware gecamoufleerd. Camouflage is veel eenvoudiger, lees goedkoper, en daarom efficiënter dan het programmeren van nieuwe malware. De programmeurs van de malware zijn vaak niet meer de enigen die deze versluiering en de verspreiding voor hun rekening nemen. Ze verkopen de malware aan een groot aantal verschillende aanvallers. De aanvallers zorgen voor het verpakken en verspreiden hun pakketten in een nieuw jasje op de meest uiteenlopende manieren onder nietsvermoedende gebruikers. De programmeur profiteert hiervan door bijvoorbeeld een deel van het losgeld te ontvangen dat via de ransomware wordt afgeperst. Dit bedrijfsmodel, 'Ransomware as a service', wordt bijvoorbeeld toegepast bij de kwaadaardige software Gandcrab die momenteel wordt verspreid. Via relevante discussieforums is bekend geworden dat de programmeur en de malwareklanten de afgeperste sommen delen op 60/40-basis..

Malware gebruikt camouflage als tactiek

De hoeveelheid packers is inmiddels niet meer te overzien en groeit nog steeds gestaag. Daar komt nog bij dat elke packer snel en eenvoudig kan worden gewijzigd. Via deze aanpak moeten de antivirusprogramma's om de tuin worden geleid en uiteindelijk worden overwonnen. Dit is de reden waarom de traditionele malwaredetectie op belemmeringen stuit.

Soms worden packers ook in meerdere lagen toegepast. De kwaadaardige software die de kern van het uitvoerbare bestand vormt, wordt daarbij echter niet gewijzigd. Dit is de meest rendabele manier om de levensduur van malware te verlengen en de winstgevendheid te maximaliseren.



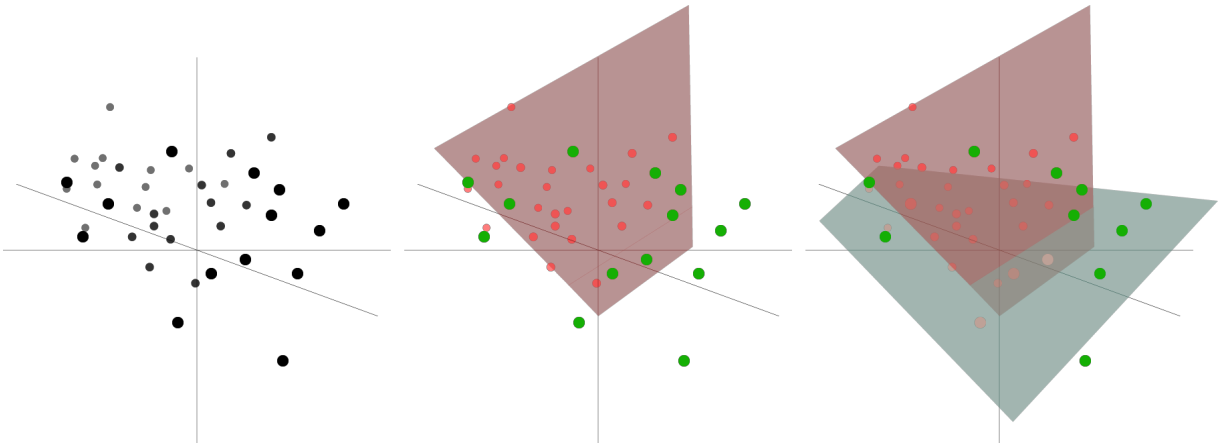
DeepRay® verandert de spelregels

Met DeepRay® hebben we een technologie op basis van Machine Learning ontwikkeld die in staat is G DATA een beslissend voordeel in de strijd tegen criminelen te verschaffen. Nadat de in een packer gecamoufleerde kwaadaardige software is gestart, wordt de oorspronkelijke inhoud van de malware opnieuw uitgepakt in het geheugen. Omdat het echter niet mogelijk is voortdurend de inhoud van elk proces te analyseren en te evalueren, hebben we een andere aanpak gevolgd.
De door ons ontwikkelde zelflerende technologie is in staat om te detecteren of een bestand al dan niet is gecamoufleerd. Daarbij speelt niet langer een rol welke camouflagemethode, oftewel welke

packer, is gebruikt en of de methode bekend is. Aanvallers hebben dan ook geen andere optie dan de malware te herschrijven, wat veel moeite kost. Een goede camouflagevariant is niet genoeg om DeepRay® in het stof te laten bijten.

Hoe werkt DeepRay®?

Voor de eerste detectiestap maakt G DATA gebruik van een neuraal netwerk dat bestaat uit meerdere perceptrons. Op basis van enkele honderden criteria bepaalt dit netwerk al voordat de malware is uitgepakt en de kern is onthuld of een bestand verdacht is gecamoufleerd. Voorbeelden van deze criteria zijn de verhouding tussen bestandsgrootte en uitvoerbare code, de gebruikte compilerversie of het aantal geïmporteerde systeemfuncties.

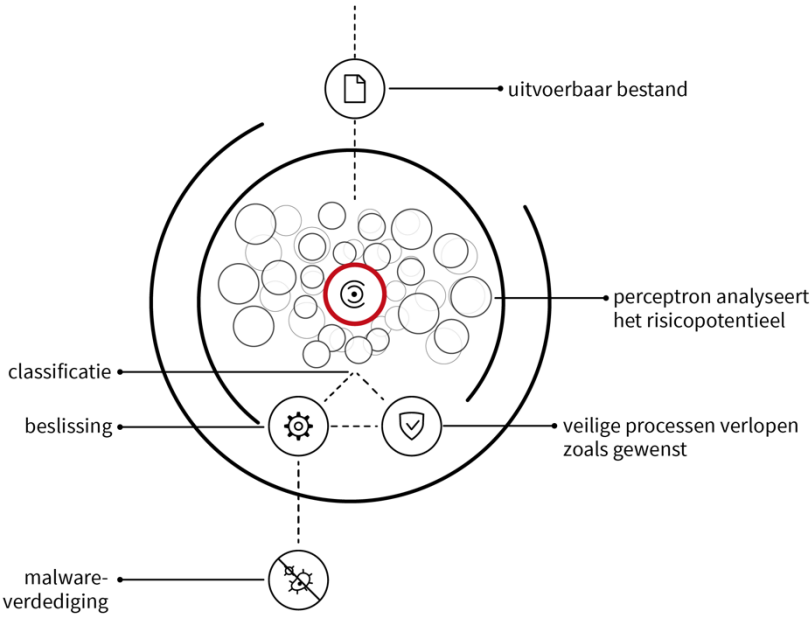


Zoals de grafiek weergeeft, categoriseren perceptrons objecten in een kenmerkende ruimte, waarbij het in het geval van DeepRay® gaat om ingepakt of niet-ingepakt, oftewel bedreigend of onschadelijk. In werkelijkheid worden hierbij wezenlijk meer dan de getoonde twee niveaus in drie dimensies gebruikt. Omdat elk van de honderden criteria overeenkomt met een bepaald niveau, loopt ook de scheidslijn van elke perceptron langs honderden niveaus. Dit hoge aantal niveaus is echter vereist om een betrouwbare scheidslijn te kunnen trekken. Het optimale verloop wordt door de perceptron ingeleerd met behulp van een vooraf geclassificeerde trainingsset. Deze sets worden continu bijgewerkt om een ideaal leerresultaat mogelijk te maken. Om de nauwkeurigheid van het proces in DeepRay® te optimaliseren, worden meerdere perceptrons gekoppeld aan een neuraal netwerk.

Snelle verdediging tegen elke vorm van bedreiging

Wanneer het neurale netwerk van DeepRay® besluit dat een bestand verdacht is, wordt een diepteanalyse uitgevoerd. Deze analyse vindt plaats in het geheugen van het proces en in dat van de andere mogelijk geïnfecteerde processen. Het is belangrijk dat deze processen worden geïdentificeerd, omdat malware vaak probeert om kwaadaardig gedrag uit te besteden aan schijnbaar onschadelijke systeemprocessen.

Deze detectiemethode wordt 'Taint tracking' genoemd. Om mogelijke infecties te detecteren, worden systeemfuncties bewaakt die toegang vanuit het ene proces naar het andere mogelijk maken. Als een dergelijke toegang wordt geregistreerd, wordt het betreffende proces voortaan beschouwd als kwetsbaar ('taint', de Engelse term voor 'besmetting'). Deze 'taint' kan op elke diepte worden overgedragen naar andere processen. Ook deze processen worden vervolgens onderworpen aan een analyse. Zelfs 'fileless malware', die niet in het bestandssysteem wordt opgeslagen, kan op deze wijze worden gedetecteerd.



Tijdens de diepteanalyse worden patronen geïdentificeerd die passen bij de kern van bekende malwarefamilies of bij algemeen schadelijk gedrag..

Optimaal beschermingsniveau vanaf het begin

Om direct een ideaal beveiligingsniveau mogelijk te maken, hebben we het neurale netwerk getraind met gegevens uit meer dan dertig jaar malwaredetectie. Dankzij de analyse van nieuwe bedreigingen en de informatie van de G DATA SecurityLabs zal de performance voortdurend toenemen en DeepRay® altijd up-to-date zijn.

Bovendien wordt elke succesvolle detectie van de algehele component gebruikt om het neurale netwerk te trainen. Dit resulteert in een adaptief leerproces van het kunstmatige intelligentie-systeem.

Veilige bestanden werken zoals bedoeld, zodat gebruikers altijd kunnen beschikken over de beste prestaties op hun werkstation.

DeepRay® is de nieuwste Next Generation-functie voor G DATA beveiligingsoplossingen die dreigingen proactief detecteert en schade voor de gebruiker voorkomt.