SPECIAAL RAPPORT

# WIE BESPIONEERT U?

## Cyberspionage vormt een bedreiging voor elk bedrijf

With Kaspersky, now you can.
kaspersky.nl/business

Be Ready for What's Next

KASPERSKY lab

“Opzienbarende, doelgerichte aanvallen op ondernemingen komen steeds vaker voor. Duizenden bedrijven zijn al gehackt, waarbij hun vertrouwelijke gegevens werden gestolen - met miljardenverliezen als gevolg. Cyberspionage vormt vandaag de dag een concrete en groeiende internationale bedreiging, en de bestrijding ervan is een van de voornaamste taken die we onszelf hebben gesteld.”

EUGENE KASPERSKY
CEO, KASPERSKY LAB



## INHOUD



“Een groot aantal cyberaanvallen kan met relatief eenvoudige maatregelen worden aangepakt. Helaas verzuimen sommige mensen om de basale voorzorgsmaatregelen te nemen, zoals het gebruik van sterke wachtwoorden, de toepassing van patches en de inzet van een beveiligingsoplossing. In veel gevallen is inbreken in het netwerk van een bedrijf gemakkelijker dan het klinkt.”

COSTIN RAIU
DIRECTOR, GLOBAL RESEARCH & ANALYSIS TEAM
KASPERSKY LAB

# WAAROM ZOU U UW BEDRIJF BESCHERMEN TEGEN CYBER-SPIONAGE?

**IN VOGELVLUCHT**

Cyberspionage klinkt wellicht als een wonderlijke, exotische activiteit uit een film. Maar de wrange werkelijkheid is dat vrijwel elk bedrijf het doelwit kan worden - of beschadigd kan raken in het kruisvuur wanneer cybercriminelen een aanval uitvoeren op een andere organisatie.

Het maakt eigenlijk weinig uit of uw bedrijf rechtstreeks wordt aangevallen of alleen bijkomende schade lijdt als gevolg van onbedoelde betrokkenheid bij de 'strijd' van een andere organisatie. In beide gevallen kunnen de resultaten vernietigend zijn.

In dit rapport bespreken deskundigen van Kaspersky Lab op het gebied van cyberbeveiliging de volgende belangrijke punten:

- Hoe bedrijven schade kunnen lijden van directe - en indirecte - cyberspionage-aanvallen
- Wat u kunt doen om uw bedrijf - en de zorgvuldig opgebouwde reputatie van uw bedrijf - te beschermen
- Hoe specifieke technologieën kunnen helpen uw bedrijfsnetwerk en gegevens te beschermen tegen geraffineerde bedreigingen

De risico's zijn reëel, het aantal groeit en het raffinement neemt toe, maar Kaspersky staat klaar met betrouwbare adviezen ... en innovatieve technologieën.



# SPIONAGE IS NIETS NIEUWS

Spionage, in welke vorm dan ook, bestaat al zo lang als een organisatie of individu voordeel dacht te kunnen behalen door zich illegaal toegang te verschaffen tot vertrouwelijke informatie van een ander. Iedereen kent de pogingen van diverse naties om de geheimen van andere landen te stelen. Op vergelijkbare wijze maakt bedrijfsspionage al heel lang deel uit van het bedrijfsleven. Maar de afgelopen jaren lieten een spectaculaire verandering zien in het niveau en de aard van spionagegevaren die bedrijven van elke omvang kunnen raken.

Het gemak waarmee cyberspionagecampagnes kunnen worden uitgevoerd, verleidt steeds meer bedrijven om zelf spionageactiviteiten te gaan ontplooien - hoewel veel van deze organisaties zich nooit zouden hebben ingelaten met ouderwetse bedrijfsspionage.

### WAT IS ER DAN VERANDERD?

Naarmate het tempo van het internettijdperk versnelde, meer connectiviteit ontstond en mobiele communicatie steeds beter werd, realiseerden bedrijven zich al gauw dat het talloze voordelen met zich meebracht om medewerkers, klanten en leveranciers toegang te bieden tot bedrijfssystemen en essentiële gegevens. Efficiëntie en productiviteit namen aanzienlijk toe en veel bedrijven gooiden het roer om, omdat ze met behulp van internet nieuwe verkoopkanalen konden openen en extra inkomsten konden genereren.

Maar diezelfde 'altijd open verbinding' met bedrijfsinformatie en andere vertrouwelijke gegevens schiep ook kansen voor cybercriminelen. Als bedrijven intellectueel eigendom en vertrouwelijke informatie opslaan op netwerksystemen, kunnen spionageactiviteiten veel eenvoudiger worden geïmplementeerd en veel meer opleveren voor de daders.

### VEREENVOUDIGD SPIONEREN… MET SNELLER VOORDEEL

Inbreken in kantoren of geduldig wachten tot interne contactpersonen informatie verzamelen en geheimen doorgeven - die dagen zijn voorbij. Snuffelen in de prullenbakken van een bedrijf of kantoorpersoneel betalen om informatie te verzamelen was altijd al inefficiënt, tijdrovend en riskant. Nu is het simpelweg onnodig. Met de juiste hackersvaardigheden kunnen personen en organisaties bedrijven bespioneren en zo waardevolle informatie verzamelen, zonder ooit de comfortabele omgeving van hun eigen kantoor te hoeven verlaten.

Bedrijven kunnen worden aangevallen via onveilige elementen op hun eigen website, door zwakke plekken in populaire bedrijfssoftware die ze gebruiken, of omdat medewerkers klikken op e-mails die malware bevatten.

### CYBERAANVALLEN ZIJN VAN GROTE INVLOED OP DE WINST- EN VERLIESCIJFERS VAN EEN BEDRIJF

GEMIDDELDE VERLIEZEN IN HET GEVAL VAN EEN DOELGERICHTE CYBERAANVAL:

**$ 2,4 MILJOEN**

Bron: Global Corporate IT Security Risks 2013, B2B International

### WANNEER BEDRIJVEN GEGEVENS KWIJTRAKEN… … VERLIEZEN ZE VAAK VEEL MEER

GEMIDDELDE KOSTEN VAN EEN GEVAL VAN GEGEVENSVERLIES VOOR EEN GROTE ONDERNEMING:

**$ 649.000**

Bron: Global Corporate IT Security Risks 2013, B2B International



# WAT WINNEN DE DADERS MET CYBERSPIONAGE?

### VERSCHILLENDE SOORTEN AANVALLERS HEBBEN VERSCHILLENDE DOELEN:

- Cybercriminelen begrijpen in een oogwenk de waarde van bedrijfsinformatie. Het biedt ze de mogelijkheid om te gaan afpersen of losgeld te eisen, of om gestolen gegevens te verkopen op de zwarte markt.
- Hacktivisten richten zich op reputatieschade en ontwrichting van organisaties waarmee ze een appeltje te schillen hebben. Ze zijn zich ervan bewust dat het lekken van vertrouwelijke informatie - over klanten, leveranciers of medewerkers - organisaties ernstig in verlegenheid kan brengen en/of kan leiden tot substantiële juridische sancties.
- Cyberhuurlingen laten zich betalen door wie hen maar wil inhuren - denk aan regeringen, protestgroepen of bedrijven - om specifieke informatie te stelen.
- Nationale staten (overheidsinstanties) of hun contractanten richten zich op het verzamelen van strategische informatie of proberen industriële faciliteiten in vijandige landen te ontwrichten.

"Informatie is macht, dus wanneer een cybercrimineel informatie steelt, kan de diefstal elk voordeel tenietdoen waarvan de oorspronkelijke eigenaar van de gegevens profiteerde.

Of het doelwit nu een nationale staat is die militaire geheimen bewaart, of een bedrijf met intellectuele eigendommen en commerciële geheimen die concurrentievoordeel opleveren, dit geldt voor elke organisatie."

**SERGEY LOZHKIN**
**SECURITY RESEARCHER**
**GLOBAL RESEARCH & ANALYSIS TEAM**
**KASPERSKY LAB**

"Bedrijven van elke omvang verwerken en bewaren gegevens die van waarde zijn voor de bedrijven zelf, hun klanten en/of hun concurrenten.

Zelfs een simpele database met contactgegevens van klanten is waardevol."

**PETER BEARDMORE**
**SENIOR DIRECTOR OF PRODUCT MARKETING**
**KASPERSKY LAB**

# ZIJN ER BEDRIJVEN WAARVOOR CYBERSPIONAGE GEEN BEDREIGING-VORMT?

Het antwoord is eenvoudig: nee. Zelfs de kleinste bedrijven kunnen rechtstreeks worden aangevallen vanwege de vertrouwelijke of waardevolle informatie die ze bezitten, van bankgegevens van klanten tot leveranciersinformatie of zelfs gegevens die kunnen worden gebruikt om een aanval op een grotere onderneming te organiseren.

Zo wordt bij aanvallen van de aanvoerketen, zoals IceFog (zie Bijlage I), informatie verzameld van diverse andere instanties/leveranciers, om die gegevens vervolgens te gebruiken om doelgerichte aanvallen op specifieke bedrijven of organisaties te ontwikkelen of mogelijk te maken.

"Wanneer u de risico's voor uw bedrijf in kaart brengt, onderschat dan nooit hoe het 'menselijke element' uw verdediging kan verzwakken. Als medewerkers in de val lopen van 'spear-fishing' campagnes of op een 'geïnfecteerde' koppeling in een e-mail klikken, kan uw beveiliging gevaar lopen."

SERGEY LOZHKIN
SECURITY RESEARCHER
GLOBAL RESEARCH & ANALYSIS TEAM
KASPERSKY LAB

"Het maakt niet uit of het gaat om een bedrijf dat in de Fortune 500 staat genoteerd, of om een tweemanszaak die net is gestart in iemands garage. Iedereen heeft iets te verliezen."

CHARLES KOLODGY
RESEARCH VICE PRESIDENT, SECURE PRODUCTS
IDC



## IS UW BEDRIJF EEN BELANGRIJK DOEL?

Het is niet moeilijk om te begrijpen waarom overheidsinstanties en militaire instellingen doelwit zijn van cyberaanvallen. Naast door staten gesponsorde initiatieven, proberen onafhankelijke protestgroepen vaak activiteiten van de overheid te verstoren of vertrouwelijke informatie te stelen. Cyberhuurlingen vallen ook overheidsinstanties aan om geld of gegevens te stelen voor hun opdrachtgever.

Zo zijn grote ondernemingen en multinationals ook een voor de hand liggend doelwit voor tal van verschillende soorten cyberaanvallen, waaronder cyberspionage, vanwege de overvloed aan waardevolle informatie die ze bezitten en de zorgvuldig opgebouwde reputatie die ze willen beschermen.

### GOOGLE, ADOBE EN ANDERE BEDRIJVEN AANGEVALLEN

De Operation Aurora in 2009 waarbij Google, Adobe en meer dan 30 andere bekende bedrijven werden aangevallen, wordt beschouwd als het keerpunt in cyberbeveiliging.

Ondanks pogingen om de zwakke plekken in de software aan te pakken waarvan de aanvallers gebruik maakten, werd in 2012 bekend dat nog steeds op dezelfde manier defensiecontractanten en aanvoerketens van andere bedrijven werden aangevallen.

De aanvallers proberen de controle te krijgen over bedrijfsnetwerken en vertrouwelijke gegevens te stelen. Onveilige websites en phishing via e-mail vormen de kern van wat algemeen wordt beschouwd als door staten gesponsorde cyberspionageaanvallen.

### AANVALLEN OP AMERICAN EXPRESS EN JP MORGAN CHASE

In 2013 werden zowel American Express als JP Morgan Chase het slachtoffer van cyberaanvallen waarvoor een religieuze groepering de verantwoordelijkheid opeiste. Maar deskundigen van de inlichtingendienst en beveiligingsexperts in de VS zijn van mening dat Iran verantwoordelijk was voor de aanvallen.

Door de aanvallen waren beide bedrijven verschillende uren offline.

Begin 2013 waren in een periode van zes weken 15 van de grootste banken in de VS in totaal 249 uur offline als gevolg van cyberaanvallen.

## ELK BEDRIJF KAN HET DOELWIT ZIJN

Middelgrote en kleine bedrijven moeten zich realiseren dat ook zij risico lopen. Het is al te gemakkelijk voor het midden- en kleinbedrijf om de potentiële bedreigingen van cyberspionage en cyberterrorisme weg te wuiven en ten onrechte te denken dat alleen nationale staten en grote multinationals gevaar lopen. Dit valse gevoel van veiligheid kan tot gevolg hebben dat bedrijven een al te relaxte houding aannemen ten aanzien van de bescherming van hun systemen en gegevens, en dat kan het nog eenvoudiger maken voor cyberspionnen om de aanval in te zetten.

Verder zien cybercriminelen kleine en middelgrote bedrijven vaak als springplank voor aanvallen op grotere bedrijven. Veel kleinere bedrijven genieten de status van 'vertrouwde partner' van bekende bedrijven, en criminelen profiteren maar al te graag van die relaties.

## KAN UW BEDRIJF ALS 'OPSTAPJE' FUNGEREN VOOR EEN AANVAL OP ANDERE ORGANISATIES?

Overheidsinstanties, departementen van defensie, eigenaars van cruciale infrastructuren, zoals energiecentrales, gasleveranciers, netwerken voor energiedistributie en waterleidingbedrijven, en grote bedrijven in vrijwel elke marktsector, erkennen dat ze een belangrijk doelwit kunnen vormen voor cyberaanvallen. Dus al deze organisaties hebben waarschijnlijk geïnvesteerd in robuuste veiligheidsmaatregelen tegen cybercriminaliteit.

Maar veel van de bedrijven die samenwerken met deze organisaties, als leverancier of als contractant, hebben mogelijk niet voldoende inzicht in de bedreigingen van vandaag, of wat er nodig is om ervoor te zorgen dat ze cyberaanvallers een stap voor blijven. Dit biedt aanvallers een prachtige gelegenheid om toegang te krijgen tot hun hoofddoelwit: via zwakke plekken in de beveiliging van systemen van leveranciers of contractanten.

Elk bedrijf, waaronder:

- serviceproviders
- hardwareleveranciers
- bedrijven voor outsourced services
- kleine of 'eenmans'-adviesbureaus
- tijdelijke medewerkers/ uitzendkrachten

… kan worden gebruikt als eerste fase in een aanval op een multinational of een organisatie in de publieke sector.



"De afgelopen tijd ontdekten aanvallers dat het steeds lastiger werd om in te breken op de netwerken van grote bedrijven. In plaats daarvan concentreren ze zich nu op de aanvoerketen. Door netwerken van kleinere bedrijven te hacken, profiteren de aanvallers van de kennis en identiteit van het kleine bedrijf om in te breken bij grotere bedrijven."

**COSTIN RAIU**
**DIRECTOR, GLOBAL RESEARCH & ANALYSIS TEAM**
**KASPERSKY LAB**

## AANVAL OP LEVERANCIERS HELPT DOELGERICHTE AANVAL OP GROTE AMERIKAANSE FABRIKANT MOGELIJK TE MAKEN

In 2011 werd het Amerikaanse defensiebedrijf Lockheed Martin slachtoffer van een grote cyberaanval.

De dader had daarvoor twee leveranciers aangevallen van Lockheed Martin, waaronder RSA, een beveiligingsbedrijf. De informatie die de dader bij deze twee aanvallen verzamelde, heeft naar verluidt geholpen om de aanval op Lockheed Martin te organiseren.

Lockheed Martin ontdekte de aanval snel en beschermde hun systemen en gegevens. Maar de aanval laat zien hoe andere bedrijven als springplank kunnen worden gebruikt bij een poging om de beveiliging van grotere bedrijven aan te tasten.

## REPUTATIEVERLIES

Natuurlijk, als uw bedrijf vooral wordt gebruikt als middel om een andere organisatie aan te vallen, lijdt u mogelijk geen directe schade. Maar de kans dat uw bedrijf indirecte schade lijdt, is groot. Het is de moeite waard om de mogelijke consequenties te overzien als uw bedrijf wordt gebruikt als de 'zwakste schakel' die een cyberspionageaanval mogelijk maakt op een van uw klanten of partners:

- Welke invloed heeft de aanval op de lopende relatie met de klant/partner?
- Zijn er mogelijk juridische gevolgen voor uw bedrijf?
- Hoe beïnvloedt mogelijke negatieve publiciteit uw reputatie op de markt?
- Kunt u bewijzen dat u alle mogelijke voorzorgsmaatregelen hebt genomen om de aanval te voorkomen?

Het is zonneklaar dat u het beste al het mogelijke kunt doen om het onbehagen en het reputatieverlies te voorkomen dat een indirecte aanval met zich mee kan brengen.

"Het opbouwen van een sterke reputatie als bedrijf vereist standvastigheid en consistentie over een langere periode. Een zorgvuldig opgebouwde reputatie kwijtraken kan in een oogwenk zijn gebeurd."

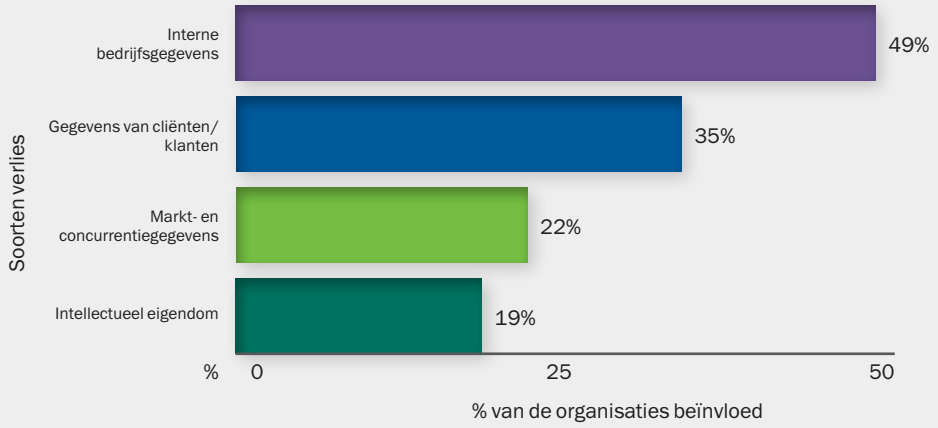
**DAVID EMM**
**SENIOR REGIONAL RESEARCHER**
**GLOBAL RESEARCH & ANALYSIS TEAM**
**KASPERSKY LAB**

## DIRECT VERLIES VAN WAARDEVOLLE INFORMATIE

Het is bovendien de moeite waard om te bepalen welk soort informatie gevaar loopt als uw bedrijf het belangrijkste doelwit vormt van een cyberspionageaanval. Wat is de invloed op uw bedrijfsvoering als de volgende gegevens worden gestolen:

- Marktgegevens, waaronder 'inside information' over de sterke en zwakke punten en de concurrentiepositie van uw bedrijf?
- Productontwerpen, informatie over innovatieve processen, know-how en ander intellectueel eigendom?
- Persoonlijke informatie over uw medewerkers?
- Klantenbestanden en vertrouwelijke informatie over klanten/cliënten?
- Informatie over uw partners of vertrouwelijke partnergegevens?

**Recent onderzoek wees uit dat organisaties die werden getroffen door gegevenslekken, de volgende verliezen leden:**




Bron: Global Corporate IT Security Risks 2013, B2B International

# METHODEN VOOR VERSPREIDING VAN MALWARE VOOR CYBERSPIONAGE

Om cyberspionageprogramma's te verspreiden, gebruiken cybercriminelen veel van dezelfde methoden die ze toepassen om andere vormen van malware te verspreiden, waaronder:

- Uitbuiting van de zwakke plekken in besturingssystemen of applicaties, met inbegrip van enkele veelgebruikte softwareproducten, zoals:
  - Java
  - Adobe Reader
  - Microsoft Office
  - Internet Explorer
  - Adobe Flash… en nog veel meer
- Social-engineeringtechnieken, waaronder 'spear-phishing' campagnes
- Drive-by downloads, waarbij een bezoek aan een website met gaten in de beveiliging al genoeg is om de computer van de gebruiker te infecteren

### HET BOEMERANGEFFECT

Nadat een nieuw cyberspionageprogramma is ontdekt en geïdentificeerd, denkt u misschien dat de wereld weer een beetje veiliger is geworden. Helaas is dat niet het geval! De risico's kunnen groter worden en de kwalijke effecten van de aanval kunnen zelfs als een boemerang terugkeren naar de daders die de bedreiging als eerste hebben gelanceerd.

In sommige gevallen worden aanvalsmethoden door andere cybercriminelen gekopieerd en worden nieuwe aanvallen uitgevoerd op de oorspronkelijke aanvaller.

"Ons inzicht in cyberaanvallen is de afgelopen jaren veranderd. Wat op zichzelf staande incidenten leken, zoals Stuxnet en Duqu, vormden slechts het topje van de ijsberg. In werkelijkheid worden er elk moment honderden, zo niet duizenden aanvallen uitgevoerd… zelfs als er maar een paar worden gesignaleerd."

**COSTIN RAIU**
**DIRECTOR, GLOBAL RESEARCH & ANALYSIS TEAM**
**KASPERSKY LAB**

# VERDER DAN CYBERSPIONAGE. CYBEROORLOG EN HET RISICO OP 'BIJKOMENDE SCHADE'

Cyberoorlogshandelingen, waarbij een nationale staat een cyberaanval uitvoert op een ander land, komen steeds vaker voor en kunnen ook consequenties hebben voor bedrijven.

In conventionele oorlogen is bijkomende schade een eufemistische term die wordt gebruikt om infrastructuur en burgers aan te duiden die onbedoeld zijn getroffen bij militaire acties. In de wereld van de cyberoorlog kunnen onschuldige bedrijven en personen onderdeel worden van de bijkomende schade die het gevolg is van een aanval op een ander doelwit.

Wanneer in het kader van een cyberoorlog op internet een cyberaanval op een nationale staat in gang is gezet, kan dit talloze onbedoelde en onwenselijke consequenties hebben die veel verder strekken dan oorspronkelijk is bedoeld. Nationale staten, strijdkrachten en uw bedrijf maken allemaal gebruik van internet, dus als er een aanval in een cyberoorlog wordt uitgevoerd, is het mogelijk dat onschuldige bedrijven daarin worden meegesleept… met malware op de IT-bedrijfsnetwerken tot gevolg.

Als een of meer van uw systemen zijn verbonden met internet, lopen ze altijd risico op bijkomende schade. Zo simpel is het.

Verder kunt u in het geval van een aanval op essentiële infrastructuur van een land - zelfs als de systemen van uw eigen bedrijf niet direct worden geraakt - schade lijden als gevolg van:

- Geen toegang tot services en gegevensopslag in de cloud
- Onvermogen om financiële transacties te verwerken, zoals betaling aan leveranciers en medewerkers of het plaatsen van orders door klanten
- Problemen met de aanvoerketen, zoals te late leveringen en vertragingen in de verwerking van import/export
- Uitval van telecomsystemen, met inbegrip van communicatie via VoIP of LAN
- Storing in andere sectoren van de cruciale infrastructuur van een land, zoals de opwekking en distributie van elektriciteit
- Verlies van gegevens die nodig zijn voor naleving van wet- en regelgeving



# HOE KUNT U UW BEDRIJF BESCHERMEN TEGEN CYBERSPIONAGE?

Hoewel sommige aanvallen rechtstreeks uit een sciencefictionroman lijken te komen, is helaas niets minder waar. Ze vormen de realiteit van vandaag en u moet zich ertegen beschermen.

"Cybercriminelen hebben een levendige belangstelling voor nieuwe technieken die hun eigen aanvallen effectiever kunnen maken. Ze steken veel tijd en energie in het terugvolgen van het ontwikkelingsproces van de meest geraffineerde aanvallen, zelfs als deze aanvallen door landen zijn ontwikkeld.

Zodra de 'geest uit de fles' is en nieuwe malwaremethoden 'in het wild' worden toegepast, kunt u alleen nog maar hopen dat uw beveiligingsleverancier hen de baas is."

SERGEY LOZHKIN
SECURITY RESEARCHER
GLOBAL RESEARCH & ANALYSIS TEAM
KASPERSKY LAB

## DE RISICO'S INSCHATTEN… EN EEN BEVEILIGINGSBELEID VASTSTELLEN

Het is belangrijk dat alle bedrijven de risico's beoordelen die ze kunnen lopen, en vervolgens hun eigen beveiligingsbeleid vaststellen.

Veel bedrijven lopen in de val en baseren hun beveiligingsstrategie op een verouderde perceptie van risico's die 10 jaar geleden bestonden. Zorg er dus voor dat uw beleid relevant is voor de bedreigingen van vandaag en dat het is gebaseerd op een helder inzicht in de actuele risico's. Uw beleid moet:

- Dagelijkse beveiligingsprocedures beschrijven
- Een plan bevatten voor de reactie op een aanval
- Een mechanisme omvatten voor het bijwerken van procedures, zodat deze gelijke tred houden met de zich ontwikkelende aard van de bedreigingen
- Een routine beschrijven voor regelmatige controle van de IT-veiligheidsvoorzieningen

## UW PERSONEEL INFORMEREN OVER DE RISICO'S

Dit is absoluut noodzakelijk. Bij veel cyberspionage en andere cybercrimeaanvallen rekenen de daders op menselijke vergissingen of naïviteit om de omstandigheden te scheppen waarin systemen en gegevens van bedrijven voor hen toegankelijk zijn. Als het gaat om verdediging tegen aanvallen, dan geldt: een gewaarschuwd mens telt voor twee. Zorg er dus voor dat uw personeel op de hoogte is van:

- De veiligheidsrisico's en de wijze waarop cybercriminelen informatie en wachtwoorden proberen te stelen
- De potentiële kosten voor het bedrijf wanneer het wordt aangevallen
- Eenvoudige voorzorgsmaatregelen die medewerkers kunnen nemen om de beveiliging te verbeteren
- Het beveiligingsbeleid van uw bedrijf en wat medewerkers moeten doen om zich aan de richtlijnen te houden

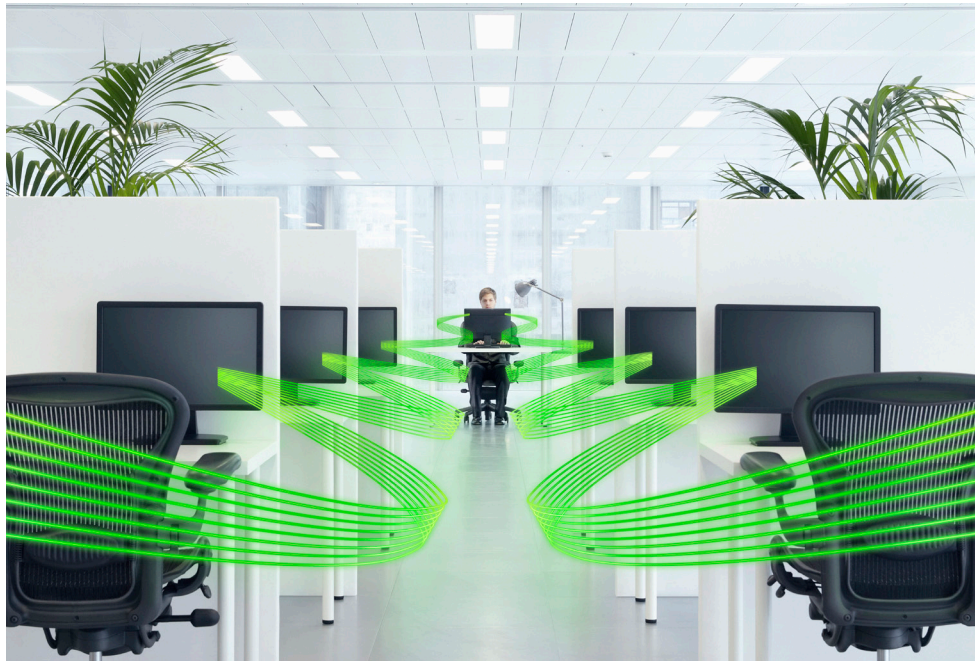


## UW BESTURINGSSYSTEMEN ONDER DE LOEP

Vergeet niet dat recente besturingssystemen, zoals Windows 7, Windows 8 of Mac OS X, vaak veiliger zijn dan hun voorgangers. Het is de moeite waard om hiermee rekening te houden als u uw IT-upgradestrategie bepaalt.

Daarnaast zijn de 64-bits versies van de meeste computerbesturingssystemen meestal beter bestand tegen cyberaanvallen.

"Eén van de nieuwe trends die we hebben gesignaleerd, is de opkomst van destructieve malware. Een voorbeeld hiervan is Shamoon, waarmee in 2012 Saudi Aramco en Rasgas werden aangevallen. Destructieve malware is gericht op brede beschadiging van het netwerk van het slachtoffer, tijdelijke uitschakeling van de bedrijfsvoering of het toebrengen van onherstelbare schade. Dit is een totaal andere opzet dan financieel gemotiveerde aanvallen, zoals Trojaanse paarden binnen banken - en het is misschien zelfs gevaarlijker."



## EEN ALLESOMVATTENDE OPLOSSING VOOR IT-BEVEILIGING

Bescherming tegen malware is van cruciaal belang, maar is op zich niet voldoende. Kies een beveiligingsoplossing die ook de volgende beveiligingstechnologieën omvat:

- Risico-evaluatie
- Patch management
- Applicatiecontrole, met inbegrip van een whitelist en default-deny functionaliteit
- Apparaatcontrole, zodat u kunt bepalen welke apparaten met uw systemen/netwerk mogen worden verbonden
- Internetcontrole, zodat u op eenvoudige wijze de toegang tot internetbronnen kunt beheren, beperken en controleren
- Bescherming tegen zero-dayaanvallen
- Data encryptie
- Mobiele veiligheid met mobile device management (MDM)

## HET BELANG VAN MOBIELE BEVEILIGING

De smartphones van vandaag zijn veel meer dan louter een telefoon. Het zijn krachtige computers waarop veel bedrijfsgegevens - en wachtwoorden - kunnen worden opgeslagen die waardevol kunnen zijn voor cyberspionnen. Het is dan ook belangrijk om mobiele apparatuur, waaronder tablets en smartphones, even zorgvuldig te beschermen als uw IT-systemen.

Met het toenemende risico op verlies of diefstal zou je zelfs kunnen pleiten voor een nog hoger beveiligingsniveau, om de gegevens op kwijtgeraakte apparaten te beveiligen.

Als uw bedrijf de strategie Bring Your Own Device (BYOD) in praktijk brengt, kan dat de beveiliging van mobiele apparatuur nog veel lastiger maken. Met de vrijwel ontelbare platforms en modellen die moeten worden beveiligd, is het van belang dat u hiermee rekening houdt in uw beveiligingsbeleid.

Zelfs als u geen formeel BYOD-beleid volgt, moet u eraan denken dat medewerkers vaak hun eigen smartphone meenemen naar hun werk.

### APPLICATION CONTROL MET DEFAULT DENY

Met Default Deny kunt u op eenvoudige wijze bepalen welke applicaties op uw systemen zijn toegestaan.

Alleen software die op uw whitelist van veilige applicaties voorkomt, mag worden gestart. Alle andere software wordt automatisch geblokkeerd.



## UW VIRTUELE OMGEVING BEVEILIGEN

Sommige bedrijven blijven ten onrechte denken dat een gevirtualiseerde IT-omgeving veel veiliger is. Dat is niet het geval. Virtuele computers draaien op fysieke servers en die fysieke servers zijn nog steeds gevoelig voor een aanval met malware.

Het is duidelijk dat ook virtuele computers bescherming nodig hebben. Maar om het rendement van uw investeringen te verbeteren, is het de moeite waard om beveiligingsoplossingen te overwegen die speciale voorzieningen omvatten voor virtuele omgevingen. Als u bijvoorbeeld een agentless beveiligingsoplossing kiest in plaats van een traditioneel agent-based beveiligingspakket, kunt u waarschijnlijk de consolidatieratio van uw server verbeteren.

## BEVEILIGING COMBINEREN MET SYSTEEMBEHEER VOOR MEER TRANSPARANTIE EN MINDER COMPLEXITEIT

Overweeg een oplossing waarin beveiliging wordt gecombineerd met een uitgebreide reeks algemene functies voor het beheer van IT-systemen. Dit helpt u beter zicht te houden op uw netwerk en, als u alles op uw netwerk kunt zien, is het eenvoudiger om passende veiligheidsmaatregelen toe te passen.

"Virtualisatie is erop gericht om meer uit uw IT-infrastructuur te halen. Als u conventionele anti-malwaresoftware op uw gevirtualiseerde servers laat draaien, verspilt u mogelijk veel verwerkingsvermogen en opslagcapaciteit.

Dit kan het doel van uw virtualisatieprogramma tenietdoen en het rendement van uw investeringen aanzienlijk reduceren."

**DAVID EMM**
**SENIOR REGIONAL RESEARCHER**
**GLOBAL RESEARCH & ANALYSIS TEAM**
**KASPERSKY LAB**

# HOE DE BEVEILIGINGSTECHNOLOGIEËN VAN KASPERSKY LAB KUNNEN HELPEN OM UW BEDRIJF TE BESCHERMEN

Cybercriminelen gebruiken steeds geraffineerdere methoden om cyberaanvallen uit te voeren. Het is dan ook van cruciaal belang dat bedrijven een beveiligingsoplossing kiezen die de allerlaatste bedreigingen bij kan houden.

## INNOVATIEVE TECHNOLOGIEËN DIE MEERLAAGSE VERDEDIGING BIEDEN

Naast de bekroonde anti-malwarecapaciteiten van het bedrijf blijft Kaspersky innovatieve technologieën ontwikkelen die bedrijven meer beschermlagen bieden:

### Automatische scans naar beveiligingslekken en patch management

Veel beveiligingsoplossingen van Kaspersky scannen automatisch uw bedrijfsnetwerk op de aanwezigheid van zwakke plekken binnen besturingssystemen of applicaties waarvoor geen patch is toegepast.

Met behulp van de Microsoft WSUS-database, de Secunia Vulnerability Database en Kaspersky's eigen unieke database van vulnerabilities (geleverd via het Kaspersky Security Network in de cloud), kunnen de oplossingen van Kaspersky regelmatig gegevens van Microsoft-hotfixes en -updates synchroniseren en ze vervolgens automatisch verspreiden over uw netwerk. Voor veel niet-Microsoft-applicaties kan bovendien informatie over patches rechtstreeks van de servers van Kaspersky worden gedownload.

### Automatic Exploit Prevention (AEP)

De Automatic Exploit Prevention-technologie van Kaspersky beschermt tegen malware-infecties die zich kunnen voordoen door beveiligingslekken binnen besturingssystemen of applicaties op uw computers.

### Kaspersky Security Network

Miljoenen leden van de internationale gebruikerscommunity van Kaspersky hebben vrijwillig meegewerkt om het Kaspersky Security Network (KSN) in de cloud te voorzien van gegevens over verdachte activiteiten en pogingen tot infectie met malware die op hun computers plaatsvonden. Ook als u geen gegevens wilt leveren aan het KSN, profiteert uw bedrijf van deze realtime-instroom van gegevens over bedreigingen uit het veld.

Het KSN helpt om veel sneller te kunnen reageren op nieuwe bedreigingen. Bovendien kan het optreden van 'vals-positieven' worden verminderd om de productiviteit van uw bedrijf te helpen verbeteren.

### Application Control

Met de functies van Kaspersky's Application kunt u bepalen hoe applicaties worden uitgevoerd op uw bedrijfsnetwerk. Het is eenvoudig om een Default Allow-beleid op te zetten, waarmee het openen van een applicatie die op de zwarte lijst staat, wordt geblokkeerd, of om een Default Deny-beleid toe te passen, waardoor alleen applicaties kunnen worden gestart die op de whitelist staan.

### Whitelist Lab

Kaspersky is de enige leverancier van beveiligingsproducten die heeft geïnvesteerd in een eigen Whitelist Lab. Het lab is verantwoordelijk voor de beoordeling van de beveiliging van veelgebruikte applicaties en het brengt voortdurend updates uit voor Kaspersky's whitelistdatabase met applicaties die veilig kunnen worden uitgevoerd.

De updates voor de whitelist komen uit het Kaspersky Security Network in de cloud, om ervoor te zorgen dat klanten van Kaspersky profiteren van de nieuwste whitelistgegevens.

### ZetaShield

Kaspersky's ZetaShield (Zero-Day Exploit and Targeted Attack Shield) is een technologie die bescherming biedt tegen onbekende malware en aanvallen, om u te verdedigen tegen zero-day- en zero-hour-aanvallen, en tegen advanced persistent threats (APT's). De combinatie van Kaspersky's krachtige anti-virusengine en innovatieve ZetaShield-technologie heeft de kans op ontdekking van malware aanzienlijk vergroot en daarmee het beschermingsniveau nog eens opgeschroefd.

### Mobiele beveiliging en MDM

De technologieën voor mobiele beveiliging van Kaspersky leveren

meerlaagse beveiliging voor mobiele apparatuur, met inbegrip van speciale voorzieningen om gegevens op verloren of gestolen apparaten te beschermen. Daarnaast biedt Kaspersky een reeks functies voor het beheer van mobiele apparaten (MDM) die bedrijven helpen om de tijd te minimaliseren die ze moeten besteden aan het beheer van mobiele eindpunten.

### Beveiliging van gevirtualiseerde omgevingen

Kaspersky biedt bescherming die speciaal is ontwikkeld om te voldoen aan de unieke eisen van gevirtualiseerde IT-omgevingen, zoals gevirtualiseerde servers, desktops en datacenters.

Met een agentless anti-malwareoplossing biedt Kaspersky een efficiëntere manier om een gevirtualiseerde infrastructuur te beschermen, om zo de prestaties te behouden, de impact op virtualiteitsdichtheid te minimaliseren en het algemene rendement te verhogen.

### Verstrekkende mogelijkheden voor systeembeheer

Door een groot aantal gangbare IT-beheertaken te automatiseren, biedt Kaspersky Systems Management bedrijven meer zicht op en controle over hun IT-assets, terwijl IT-beheerders meer tijd hebben voor andere taken.

## INTERNATIONALE AUTORITEIT OP CYBERBEVEILIGINGSGEBIED

Als particulier bedrijf is Kaspersky volkomen onafhankelijk. Hoewel Kaspersky talloze overheidsinstanties adviseert, bestaan er geen politieke banden met welke overheid dan ook. Experts van Kaspersky werken nauw samen met de internationale community voor IT-beveiliging, waaronder Computer Emergency Response Teams (CERT's) overal ter wereld, en neemt deel aan gezamenlijke onderzoeken naar cyberspionage, cybersabotage en cyberoorlogvoering.

### Kies de kant van GReAT

Het Global Research & Analysis Team (GReAT) is een van de belangrijkste technologische assets van Kaspersky. Met wereldwijd toonaangevende researchers op het gebied van beveiliging analyseert GReAT voortdurend nieuwe cyberbedreigingen en ontwikkelt het bescherming.



"Kaspersky Lab's Global Research & Analysis Team (GReAT) is opgericht in 2008 en is inmiddels een begrip op het gebied van anti-malware, onderzoek naar cyberspionage en innovatie, zowel intern als extern. De beveiligingsanalisten van het team bevinden zich overal ter wereld. Elke analist beschikt over een unieke expertise en reeks vaardigheden die een bijdrage leveren aan het onderzoek en de ontwikkeling van oplossingen om de steeds complexere malwarecode te bestrijden.

GReAT voert incident response uit bij scenario's die met malware te maken hebben. De voornaamste verantwoordelijkheden van het team zijn onder meer leiderschap in ideeën op het gebied van beveiliging tegen bedreigingen, initiatieven bevorderen en uitvoeren om het aantal accurate ontdekkingen van malware te vergroten en de procedures hiervoor efficiënter te laten verlopen, evenals pre- en post-sales ondersteuning van belangrijke klantaccounts ten aanzien van expertise op het terrein van beveiliging tegen malware.

De afgelopen jaren heeft de combinatie van expertise, passie en nieuwsgierigheid van GReAT geleid tot de ontdekking van diverse cyberspionagecampagnes, waaronder Flame, Gauss, Red October, NetTraveler en Icefog."

**COSTIN RAIU**
**DIRECTOR, GLOBAL RESEARCH & ANALYSIS TEAM**
**KASPERSKY LAB**

“Met de opkomst van advanced persistent threats (APTs) is het internationale cyberbedreigingslandschap getransformeerd. Cruciale infrastructuur, financiën, telecommunicatie, onderzoeksinstituten, militaire contractanten en de cybernetwerkinfrastructuur van overheden lopen een enorm risico.

Deze bedreigingen zijn veel complexer en sluipender dan de gemiddelde malware. Daarom blijven we investeren in GReAT – als een geavanceerde, elitaire groep cyberbeveiligingsexperts.”

**EUGENE KASPERSKY**
**CEO**
**KASPERSKY LAB**

**COSTIN RAIU**
**DIRECTOR, GLOBAL RESEARCH & ANALYSIS TEAM**
**KASPERSKY LAB**

Costin Raiu kwam in 2000 bij Kaspersky en leidt GReAT sinds 2010. Hij is gespecialiseerd in de analyse van advanced persistent threats en malwareaanvallen van hoog niveau. Zijn werkzaamheden omvatten onder meer de analyse van kwaadaardige websites, aanvallen en online malware die op banken is gericht.

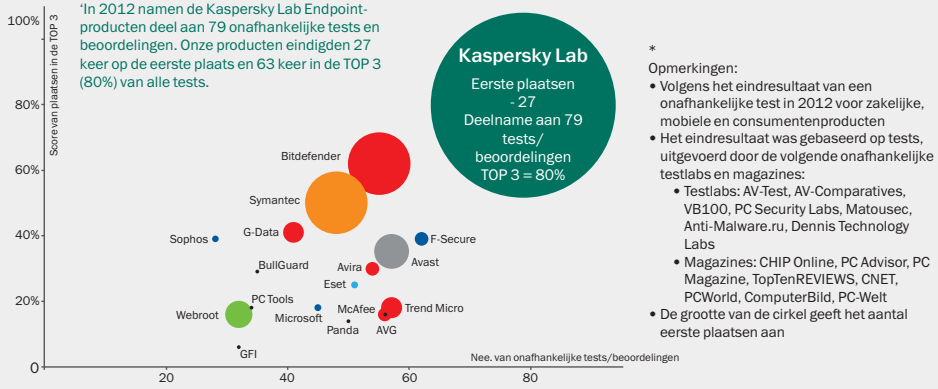
Costin heeft meer dan 19 jaar ervaring in anti-virustechnologieën en beveiligingsonderzoek, en is lid van de Virus Bulletin Technical Advisory Board, lid van de Computer Antivirus Researchers’ Organization (CARO) en verslaggever voor de WildList Organization International. Voordat hij bij Kaspersky kwam, werkte Costin als Chief Researcher voor GeCad en als Data Security Expert bij de RAV-groep van anti-virusontwikkelaars.

## ONAFHANKELIJKE PRIJZEN EN SUCCESSEN

Kaspersky is uiteraard trots op het aantal prijzen en lofbetuigingen die de eigen technologieën ten deel vielen:

- ‘Information Security Vendor of the Year’ – SC Magazine Awards Europe 2013
- ‘Information Security Team of the Year’ – SC Magazine Awards Europe 2013
- Winnaar Excellence Award – SC Magazine Awards 2013
- Kaspersky Endpoint Security for Windows werd bekroond met de eerste plaats in de test Enterprise Antivirus Protection april – juni 2013 door Dennis Technology Labs
- Het grootste aantal gouden en platina awards, in alle testcategorieën, toegekend door het externe Anti-Malware Test Lab sinds 2004
- Meer dan 50 maal geslaagd voor de zware VB100-test sinds 2000
- De Checkmark Platinum Product-award van West Coast Labs
- Product van het jaar – AV Comparatives 2011

## KASPERSKY LAB PRESTEERT HET BESTE IN DE SECTOR BEVEILIGING*:




*
Opmerkingen:
- Volgens het eindresultaat van een onafhankelijke test in 2012 voor zakelijke, mobiele en consumentenproducten
- Het eindresultaat was gebaseerd op tests, uitgevoerd door de volgende onafhankelijke testlabs en magazines:
  - Testlabs: AV-Test, AV-Comparatives, VB100, PC Security Labs, Matousec, Anti-Malware.ru, Dennis Technology Labs
  - Magazines: CHIP Online, PC Advisor, PC Magazine, TopTenREVIEWS, CNET, PCWorld, ComputerBild, PC-Welt
- De grootte van de cirkel geeft het aantal eerste plaatsen aan

‘In 2012 namen de producten van Kaspersky Lab deel aan 79 onafhankelijke tests en beoordelingen. Onze producten eindigden 27 keer op de eerste plaats en 63 keer in de top 3’

BIJLAGE 1

# EEN OVERZICHT VAN ENKELE BELANGRIJKE CYBERBEDREIGINGEN

## CYBERSPIONAGEBEDREIGINGEN

### Icefog

Dit is een advanced persistent threat (APT) die in 2011 startte en die zowel op industriële bedrijven als op overheidsinstellingen en militaire contractanten was gericht. De meeste doelwitten bevinden zich in Japan of Zuid-Korea, maar internationale bedrijven ondervinden problemen in de aanvoerketen. De aanvallers lijken het te hebben voorzien op telecombedrijven, satellietbedrijven, massamedia en televisiediensten, evenals op militaire operaties, scheepsbouw/maritieme operaties, computer- en softwareontwikkeling, en bedrijven voor wetenschappelijk onderzoek.

Doorgaans worden spear-phishing e-mails gebruikt om malware over te brengen die profiteert van de zwakke plekken in veelgebruikte applicaties, zoals Java en Microsoft Office. Hoewel de zwakke plekken bekend zijn en er patches beschikbaar zijn, rekenen de cybercriminelen erop dat veel slachtoffers traag zijn met het verspreiden van patches in hun IT-infrastructuur. Naar verluidt zijn de aanvallers cyberhuurlingen die worden betaald om aanvallen uit te voeren.

### Kimsuky

Een groep Noord-Koreaanse hackers wordt ervan verdacht de cyberspionagecampagne Kimsuky te hebben opgezet om defensie- en beveiligingsgegevens te stelen van doelwitten in Zuid-Korea. Onderzoekers van Kaspersky Lab ontdekten de campagne, waarbij gebruik wordt gemaakt van spear-phishing technieken om gebruikerswachtwoorden en andere informatie te stelen. De hackers namen ook de controle over van de geïnfecteerde computers.

### Red October

Hoewel al daterend van 2007, bleef Operation Red October ook in 2013 actief. Deze geavanceerde cyberspionagecampagne is gericht op diplomatieke en overheidsinstellingen over de hele wereld. Daarnaast waren onderzoeksinstellingen, olie- en gasbedrijven en andere commerciële organisaties doelwit. Red October steelt gegevens uit computersystemen, mobiele telefoons en bedrijfsnetwerken. De aanvallen omvatten acties waarbij gebruik wordt gemaakt van zwakke plekken in de beveiliging van Microsoft Office en Microsoft Excel.

### NetTraveler

Dit is een cyberspionagecampagne die erin is geslaagd om meer dan 350 bekende slachtoffers in 40 landen te compromitteren. ontwikkelt het bescherming de cybercriminelen tijdens deze aanvallen gebruikten, is NetTraveler, een kwaadaardig programma voor heimelijke computerbewaking. Het is ontwikkeld om vertrouwelijke gegevens te stelen, om toetsaanslagen te registreren en om lijsten van bestandssystemen en diverse Office- of PDF-documenten op te halen.

NetTraveler is sinds 2004 actief en heeft aanvallen uitgevoerd op Tibetaanse en Oeigoerse activisten, bedrijven in de olie-industrie, centra en instellingen voor wetenschappelijk onderzoek, universiteiten, particuliere bedrijven, regeringen en overheidsinstellingen, ambassades en militaire contractanten.

### Shamoon

Wanneer een computer wordt geïnfecteerd met Shamoon, kan het virus gebruik maken van de aanwezigheid van gedeelde harde schijven om zich te verspreiden naar andere computers op het netwerk van de organisatie die doelwit is. Shamoon verzendt niet alleen gegevens naar de aanvaller, maar verwijdert ook bestanden van de computers van het slachtoffer.

## GEGEVENS GEWIST VAN COMPUTERS VAN GROTE OLIEPRODUCENT

Naar verluidt zijn met een Shamoon-aanval gegevens vernietigd op 30.000 computers van Saudi Aramco.

*Of uw bedrijf nu 10 of 10.000 computers heeft… als van alle computers gegevens verdwijnen, komt uw bedrijf daar weer bovenop?*

## BEDREIGINGEN DIE NAAR VERLUIDT WORDEN GESTEUND DOOR NATIONALE STATEN, WAARONDER CYBEROORLOGVOERING, CYBERSABOTAGE EN CYBERSPIONAGE

### Stuxnet (geschatte aantal slachtoffers: meer dan 300.000)

Stuxnet wordt vaak gezien als een voorbeeld van cyberoorlogvoering. Het was het eerste kwaadaardige programma dat industriële controlesystemen als doelwit had. Het doel achter Stuxnet was om de werkzaamheden in een kernreactor te verstoren en te saboteren door de controle over te nemen van de bediening van centrifuges voor uraniumverrijking. Tot op de dag van vandaag is het de enige bekende malware die fysieke schade heeft veroorzaakt aan industriële systemen.

Maar in weerwil van het oorspronkelijke doel verspreidde Stuxnet zich op een onstabiele manier en infecteerde honderdduizenden pc's in duizenden verschillende organisaties.

### Duqu (geschatte aantal slachtoffers: 50 - 60)

Dit geraffineerde Trojaanse paard is sinds 2007 actief. Het is afkomstig van hetzelfde aanvalsplatform als Stuxnet. Nadat een computer met Duqu is geïnfecteerd, worden extra componenten gedownload om vertrouwelijke informatie te kunnen stelen. Bovendien kan het alle sporen van de eigen activiteit vernietigen.

### STUXNET INFECTEERT OLIEREUS

In oktober 2012 was Chevron, een internationale reus in de olie-industrie, het eerste Amerikaanse bedrijf dat melding deed van infectie door Stuxnet.

### Flame (geschatte aantal slachtoffers: 5000 - 6000)

Flame onderschept updateverzoeken van Microsoft Windows en vervangt ze door een eigen malwaremodule. De module bevat een vals Microsoft-certificaat dat door cybercriminelen is ontwikkeld.

Flame is actief sinds 2008 en kan het netwerkverkeer van slachtoffers analyseren, screenshots van hun computers maken, gesproken communicatie opnemen en de toetsaanslagen van gebruikers vastleggen.

### Gauss (geschatte aantal slachtoffers: 10.000)

Gauss is een cyberspionageprogramma dat sinds 2011 actief is en dat is geïmplementeerd door dezelfde groep die het Flame-platform heeft opgezet. De modules van Gauss kunnen diverse kwaadaardige acties uitvoeren, waaronder:

- Cookiebestanden en wachtwoorden in de internetbrowser van het slachtoffer onderscheppen
- USB-opslagapparatuur infecteren om gegevens te kunnen stelen
- Accountgegevens voor e-mailsystemen en websites van sociale netwerken onderscheppen

Gauss is gebruikt om toegang te verkrijgen tot banksystemen in het Midden-Oosten.

# EEN CYBERWOORDENLIJST

**Cyberaanval** – een aanval, uitgevoerd door een hacker of crimineel, op een computer, smartphone, tablet of IT-netwerk.

**Cybercrime** – verwijst naar een scala aan illegale activiteiten die worden geïmplementeerd via IT-systemen, waaronder mobiele apparaten.

**Cybercrimineel** – een individu dat criminele activiteiten uitvoert via IT-systemen en/of mobiele apparaten. Cybercriminelen kunnen variëren van individuele, opportunistische criminelen tot uiterst deskundige en professionele groepen computerhackers. Cybercriminelen kunnen zijn gespecialiseerd in:

- Ontwikkelen van malware en dit verkopen aan anderen die daarmee aanvallen uitvoeren
- Verzamelen van gegevens, zoals creditcardnummers, en deze verkopen aan andere criminelen… of elke fase van een aanval ondernemen, van ontwikkeling van de malware tot het stelen van geld van het slachtoffer.

**Cyberspionage** – spioneren en illegaal toegang verkrijgen tot informatie via IT-systemen en/of internet.

**Cyberhooligan** – een individu dat voor de lol malware ontwikkelt en aanvallen in gang zet. Cyberhooligans kwamen veel voor in de jaren tachtig en negentig, maar nu niet meer. Cybercriminelen en cyberterroristen vormen nu een veel grotere bedreiging.

**Cyberhuurlingen** – zijn in feite hackers die te huur zijn. Eigenlijk op vrijwel dezelfde manier als waarop professionele huursoldaten hun diensten aanbieden in een conventionele oorlog, zijn cyberhuurlingen cybercriminelen en hackers die hun diensten verkopen aan anderen, waaronder nationale staten en andere organisaties.

**Cybersabotage** – activiteiten die door cybersaboteurs worden uitgevoerd om legitieme processen of bedrijven te ontwrichten.

**Cyberbeveiliging** – maatregelen die worden genomen om IT-systemen en apparaten te verdedigen tegen cyberaanvallen.

**Cyberspace** – het immateriële gebied of de immateriële omgeving waarin computernetwerken over de hele wereld met elkaar communiceren.

**Cyberterrorist** – individuen of groepen die geruggensteund door een staat of als onderdeel van een onafhankelijke terroristische organisatie cyberaanvallen uitvoeren.

**Cyberoorlog/Cyberoorlogvoering** – beide termen verwijzen naar cyberaanvallen die door nationale staten worden uitgevoerd op andere nationale staten. Doorgaans is cyberoorlogvoering erop gericht om infrastructuur in staatseigendom te beschadigen of schade toe te brengen door vertrouwelijke gegevens te stelen - in plaats van te proberen geld te stelen. Veelvoorkomende doelwitten zijn onder meer militaire faciliteiten en cruciale infrastructuren, zoals vervoersnetwerken, regeling van het luchtvaartverkeer, elektriciteitsnetwerken, telecommunicatie, de voedselketen… en meer.

**Cyberwapens** – malware (kwaadaardige software) die is ontwikkeld om anderen schade toe te brengen. Cyberwapens worden gebruikt om cyberspionage- en cybersabotageaanvallen uit te voeren. In tegenstelling tot conventionele wapens zijn cyberwapens eenvoudig te klonen en te herprogrammeren.

**Hacktivisten** – ondanks de afwezigheid van 'cyber' in de naam verdienen deze hackeractivisten een plaats in onze verklarende woordenlijst. Hacktivisten zijn computerhackers die zich betrokken voelen bij een specifieke protestorganisatie of groep activisten. Hun activiteiten kunnen vergelijkbaar zijn met die van cyberterroristen of cybersaboteurs.

# OVER KASPERSKY

Kaspersky Lab is een van de snelst groeiende aanbieders van IT-beveiliging ter wereld. Het bedrijf zit stevig in het zadel als een van de vier beste beveiligingsbedrijven. Als internationale groep zijn we actief in bijna 200 landen en territoria over de hele wereld. We bieden beveiliging aan ruim 300 miljoen gebruikers en ruim 200.000 bedrijven, van het midden- en kleinbedrijf tot grote overheidsorganisaties en commerciële concerns.

We bieden geavanceerde, geïntegreerde beveiligingsoplossingen die bedrijven ongekende mogelijkheden bieden om greep te houden op het gebruik van toepassingen, het web en apparaten: u stelt de regels in en onze oplossingen helpen die regels uit te voeren.

Meer informatie vindt u op kaspersky.com/business