# Cisco Solution beschermt vóór, tijdens en na een aanval

## Cisco Cloud Web Security Premium helpt een wereldwijd olie- en gasbedrijf een hardnekkige ransomware-infectie te ontdekken en te verwijderen.

### Uitdagingen

De beveiliging van inhoud is nog nooit zo lastig geweest als in dit tijdperk, waarin diefstal of beschadiging van bedrijfsgegevens vaak het hoofddoel van een aanval is. Volgens het Cisco-beveiligingsrapport 2014 ontdekten Cisco-onderzoekers verkeer naar websites met malware bij 100 procent van de bedrijfsnetwerken die ze hadden geanalyseerd.[1] Door observatie van deze activiteiten konden ze ook vaststellen dat wanneer deze netwerken waren geïnfiltreerd, dit waarschijnlijk al een tijdje aan de gang was en dat de hoofdinfiltratie niet was ontdekt.[2]

De volgende factoren maken het voor beveiligingsteams extra moeilijk om bedreigingen te voorkomen en op te sporen:

- **Mobiliteit en de cloud** zorgen er bij het ontbreken van geschikte beveiligingsmaatregelen voor dat de zichtbaarheid afneemt en de beveiligingscomplexiteit toeneemt. Naarmate steeds meer organisaties overgaan op cloudcomputing, virtualisatie, mobiel en extern werken en de BYOD-trend (Bring-Your-Own-Device), raken steeds meer gegevens buiten het bereik van bedrijfscontrole. Het netwerk wordt poreuzer, waardoor er meer aanvalsvectoren ontstaan. En doordat steeds meer bedrijfskritieke services naar de cloud worden verplaatst en worden opengesteld buiten de beveiligingsgrens van het bedrijf, wordt het aanvalsoppervlak alleen maar steeds groter.
- **Geavanceerde tegenstanders** zijn, volgens het *Cisco-beveiligingsrapport 2014*, 'proactief aan het werk om erachter te komen welke soorten beveiliging worden gebruikt, en beginnen minder zichtbare, minder op inhoud detecteerbare gedragspatronen te vertonen, waardoor hun bedreigingen goed verborgen zijn'.[3] Deze strategie betekent dat er minder 'laaghangend fruit' is dat beveiligingsoplossingen en experts kunnen detecteren, en dat organisaties te maken krijgen met 'meer sleutelverkeer, meer codering en meer randomisering door kwaadaardige instanties waardoor command and control-gedrag (C&C) niet te onderscheiden is van echt verkeer'.[4]

### KLANTPROFIEL

**Branche:** Olie en gas

**Werknemers:** ~15.000

**Activiteiten:** Wereldwijd

**Beveiligingspersoneel:** 12

**Andere beveiligingsmaatregelen:** Antivirus, Firewall, Intrusion Detection System (IDS), Security Information and Event Management (SIEM)

**UITDAGING**

- Geavanceerde bedreigingen detecteren die afkomstig zijn van webverkeer, die de bestaande beveiligingsoplossingen kunnen omzeilen en zich in het bedrijfsnetwerk kunnen ingraven
- Werkbare informatie ontwikkelen waarmee het beveiligingsteam bedreigingen kan prioriteren
- Eén oplossing bedenken die in de hele gedistribueerde omgeving kan worden geïmplementeerd, die kan worden geïntegreerd in de bestaande beveiligingsinfrastructuur, en die bescherming biedt in het hele aanvalsspectrum

**OPLOSSING**

- Cisco CWS Premium, dat alle functies van Cisco CWS Essentials bevat
- Cognitive Threat Analytics (CTA) en Advanced Malware Protection (AMP). Dit biedt geautomatiseerd zoeken naar sterk riskante bedreigingen in het webverkeer, en inzicht in geavanceerde aanvallen die actief zijn in het bedrijfsnetwerk

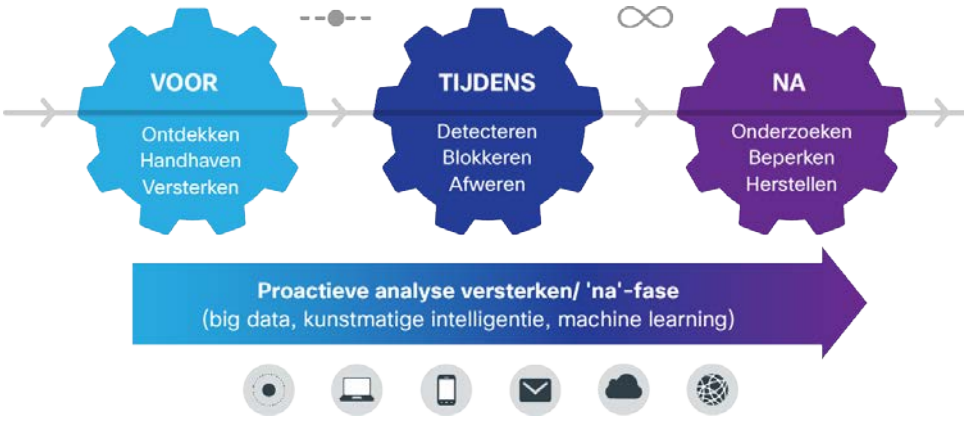
**RESULTATEN**

- Hardnekkige en niet eerder ontdekte malware-infectie is opgespoord en opgelost
- Er is nu bescherming tegen bedreigingen in het hele aanvalsspectrum
- Het beveiligingsteam van de klant kan zich nu richten op de belangrijkste bedreigingen

[1] *Cisco-beveiligingsrapport 2014*: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
[2] Ibid.
[3] Ibid.
[4] Ibid.

Het complexe en zich voortdurend ontwikkelende landschap van bedreigingen maakt dat ontdekking belangrijker is dan verdediging bij de moderne beveiliging van inhoud. Ondernemingen van vandaag moeten zich richten op inspectie van inhoud, detectie van afwijkend gedrag en geavanceerd forensisch onderzoek om zicht te krijgen op bedreigingen die al in hun netwerken aanwezig zijn: de 'na'-fase van een aanval.

**Afbeelding 1.** Nieuw beveiligingsmodel: doorlopende beveiliging na een aanval




Cisco® Cloud Web Security (CWS) Premium helpt organisaties bij het handhaven van een doorlopende beveiliging op het uitgebreide netwerk. Het Cisco CWS-platform is een cloudversie van Cisco Web Security dat de webbeveiliging uitbreidt naar mobiele apparaten en gedistribueerde omgevingen. Het beschermt alle gebruikers via de informatie over bedreigingen wereldwijd, geavanceerde verdedigingsmogelijkheden en bescherming voor mobiele gebruikers. Het omvat alle functies van Cisco CWS Essentials, en combineert ook twee innovatieve malwaredetectiesystemen om het zoeken naar sterk riskante bedreigingen in het webverkeer te automatiseren:

- **Cognitive Threat Analytics (CTA)** is een near-realtimeanalysesysteem voor netwerkgedrag, dat gebruikmaakt van machine learning en geavanceerde statistieken om ongewone activiteiten in een netwerk te detecteren—aanwijzingen voor een probleem (IOC, Indicator Of Compromise). CTA ontdekt afwijkingen en stuurt beveiligingsanalisten naar potentiële problemen. Dat vermindert hun werklast en helpt bij de prioritering van bedreigingen.
- **Advanced Malware Protection (AMP)** maakt gebruik van een combinatie van bestandsreputatie, bestandssandboxing en retrospectieve bestandsanalyse om bedreigingen in het hele aanvalsspectrum te vinden en stop te zetten.

Door de combinatie van deze oplossingen kan CWS Premium nieuwe command and control-kanalen opsporen die niet eerder door de beveiligingsindustrie zijn ontdekt.

In deze casestudy wordt bekeken hoe CWS Premium een wereldwijd olie- en gasbedrijf hielp bij het volgende:

- Meer zicht krijgen op een groot en steeds toenemend volume aan webverkeer (meer dan 35 miljoen HTTP/HTTPS-verzoeken per dag).
- Werkbare informatie over bedreigingen genereren waardoor het beveiligingsteam zijn reacties op bedreigingen makkelijker kan prioriteren.
- Eén oplossing implementeren die wordt geïntegreerd met de bestaande beveiligingsinfrastructuur en die bescherming biedt in het hele aanvalsspectrum—vóór, tijdens en na een aanval.

## Oplossing

Cisco adviseerde de klant om te upgraden naar CWS Premium, dat CTA en AMP omvat, om meer zicht te krijgen op het netwerk en het beveiligingsteam te helpen bij het prioriteren van reacties op bedreigingen.

De retrospectieve analyse van AMP kan duidelijk maken dat bestanden die als 'schoon' werden bestempeld tijdens het passeren van een verdediging aan de rand, in werkelijkheid toch goed vermomde, geavanceerde malware zijn. AMP waarschuwt onmiddellijk de beveiligingsbeheerder en maakt zichtbaar welke netwerkgebruiker misschien is geïnfecteerd en wanneer.

CTA detecteert intussen nog onopvallender bedreigingen die verdedigingen zijn gepasseerd en actief aan het werk zijn in het bedrijfsnetwerk. Het is een innovatief malwaredetectiesysteem dat gebruikmaakt van gedragsanalyse en detectie van afwijkingen om vast te stellen welke apparaten zijn besmet. CTA maakt gebruik van geavanceerde statistische modellering en machine learning om nieuwe bedreigingen onafhankelijk op te sporen. Het systeem leert van wat het tegenkomt en past zich in de loop van de tijd aan, zonder dat het hoeft te worden aangepast of geconfigureerd.

CTA identificeerde bewijzen van malwareactiviteit in het netwerk van de klant en rapporteerde deze. De malware bestond uit een reeks modules die door één malware-entiteit werden beheerd. In dit geval betrof het de payload Cryptolocker-ransomware, een type malware dat bestanden op de computers van slachtoffers versleutelt en hun apparaat 'vergrendelt' totdat ze een 'losprijs' betalen.[5]

Zoals u kunt zien in afbeelding 2, gebruikte de tegenstander een command and control-infrastructuur om de aanval uit te voeren. Deze campagne bestond uit vier belangrijke stappen:

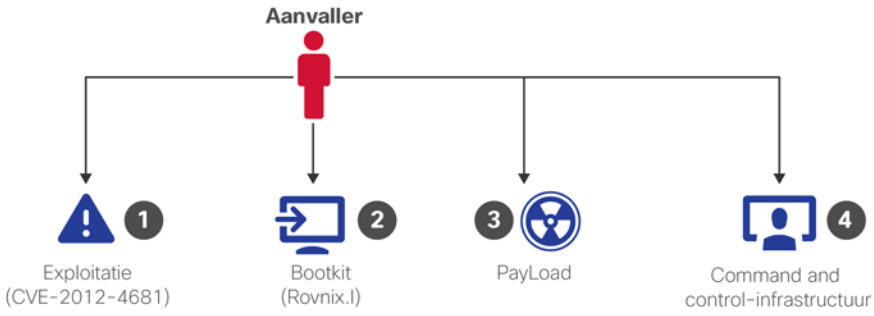
Stap 1. De aanvaller gebruikte een exploit (CVE-2012-4681) om te profiteren van een zwakke plek in het JRE-onderdeel (Java Runtime Environment) in Oracle Java SE 7 Update 6. Hierdoor kon de aanvaller op afstand code uitvoeren en de beveiligingsmanager omzeilen.

Stap 2. Daarnaast werd de bootkit (Rovnix.I) geïnstalleerd om te zorgen dat de malware op de machine actief bleef.

Stap 3. Vervolgens werd de payload geleverd om de malware volledig operationeel te maken. (In dit geval ging het om Cryptolocker-ransomware.)

Stap 4. De aanval stelde command and control-kanalen in om de functie actief te houden.

**Afbeelding 2.** Vier belangrijke stappen in de aanval

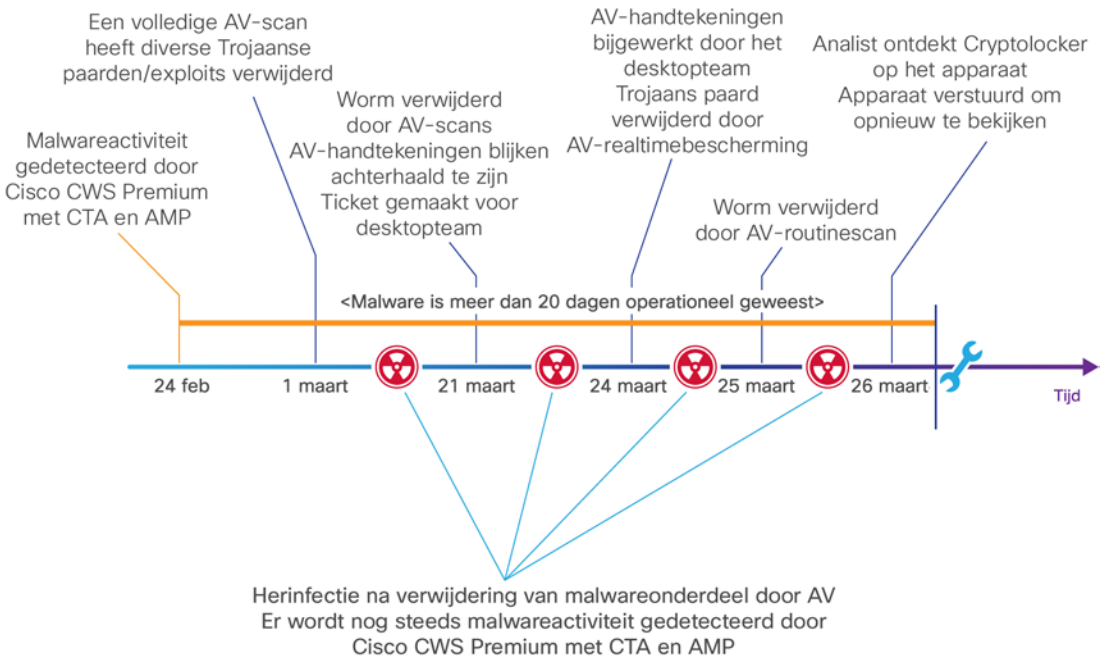



[5] Malvertising, online adverteren dat wordt gebruikt om malware te verspreiden, speelde een hoofdrol bij de distributie van Cryptolocker, dat sindsdien is uitgeschakeld. Maar malvertising en ransomware zijn nog steeds actuele bedreigingen, en ze worden door tegenstanders gebruikt om zeer gerichte campagnes te starten via internet. Ga voor meer details naar het Cisco 2014 Midyear Security Report: http://www.cisco.com/web/offer/grs/190720/SecurityReport_Cisco_v4.pdf.

Het beveiligingsteam van de klant probeerde de bedreiging op te lossen met AV-tools. Maar aangezien dit een rootkitinfectie was, zat de malware diep verankerd in het geïnfecteerde systeem. De AV-oplossing kon alleen maar een aantal malwareonderdelen onschadelijk maken. Totdat de infectie volledig was verwijderd, bleef CTA het beveiligingsteam waarschuwen voor de aanwezigheid van voortdurende, schadelijke activiteit.

In afbeelding 3 ziet u de volledige tijdslijn vanaf de detectie van de malwareactiviteit tot aan de oplossing van de bedreiging.

**Afbeelding 3.** Tijdslijn van malwareactiviteit: detectie tot oplossing




De situatie van de klant laat zien hoe waardevol CWS Premium is in de 'na'-fase van een aanval. Dit maakt ook duidelijk waarom het moeilijk is om geavanceerde aanvallen te pareren met AV-producten. Het CTA-systeem leverde bewijs van de doorlopende actieve command and control-kanalen. Daarnaast werden diverse andere domeinen opgespoord die werden gebruikt voor de doorsluizing van gegevens. Dergelijke infecties zijn inbreuken op lange termijn die diep verborgen zijn in de infrastructuur van de klant.

## Resultaten

In de wereld van vandaag, waarin beveiligingsteams dagelijks een groot aantal incidenten moeten behandelen, is er geen tijd om te zoeken naar een naald in een hooiberg. Beveiligingsteams hebben hulp nodig om zich te kunnen richten op de meest geavanceerde aanvallen, en het CTA-systeem is ontworpen om dergelijke aanvallen te detecteren en te categoriseren.

In het geval van de Cryptolocker-ransomware-infectie bij de klant detecteerde CWS Premium malwareactiviteit en paste bestaande beveiligingsinformatie toe om een aantal van de command and control-kanalen te blokkeren die het geïnfecteerde apparaat probeerde in te stellen. Maar toen ging de aanvaller een extra IP-adres gebruiken met onbekende reputatie; dit nieuwe kanaal bleef tijdens de hele infectie operationeel. Dit voorbeeld laat zien wat de sterke (automatisch blokkeren) en zwakke (nieuwe kanalen worden niet geblokkeerd) kanten zijn van detectie die

alleen op handtekeningen en webreputatie is gebaseerd, en waarom een doorlopende bescherming na een aanval noodzakelijk is.

Hier volgt een analyse van de command and control-kanalen die werden opgespoord door het CTA-systeem in CWS Premium, samen met voorbeelden van webverkeerverzoeken en statistieken:

**Tabel 1.** Aanval op infrastructuur

| Order | Remote server | Doel-IP | Beoogd land | Aantal verzoeken | Activiteitsstatus |
|---|---|---|---|---|---|
| 1 | C&C-server 1 | 109.XXX.XXX.XXX | Nederland | 17 (pogingen) | GEBLOKKEERD door webreputatie |
| **2** | **C&C-server 2** | **94.XXX.XXX.XXX** | **Luxemburg** | **75** | **ACTIEF KANAAL** |
| 3 | C&C-server 3 | fistristy.com | Luxemburg | 175 (pogingen) | GEBLOKKEERD door webreputatie |
| 4 | C&C-server 4 | ffeed5.com | Rusland | 7 (pogingen) | GEBLOKKEERD door webreputatie |

**Tabel 2.** Door CTA geïdentificeerde bedreigingen die vervolgens van het apparaat zijn verwijderd

| Naam van bedreiging | Verwijderd |
|---|---|
| Cridex-worm | 19 maart |
| Cridex.E-worm | 19 maart |
| Trojaans paard Tesch.B | 19 maart |
| Java Exploit/CVE-2012-4681 | 19 maart |
| Trojaanse downloader Win32/Upatre | 19 maart |
| Cridex-worm | 21 maart |
| Trojaans paard Win32/Viknok.C | 24 maart |
| Cridex-worm | 24 maart |
| CryptoDefense | 26 maart |

## Communicatie met C&C-server 1 (109.XXX.XXX.XXX)

Communicatie-eigenschappen:

- Het totale aantal pogingen tot verzoeken aan de server was 17; het waren allemaal gevallen van C&C-communicatie en ze werden geblokkeerd door reputatie.
- De verzoeken werden gedetecteerd door CTA als pogingen om een URL-string als Communication Channel (C&C) te gebruiken. De URL (hieronder weergegeven in 'Voorbeeld van HTTP-verzoek') staat voor een gecodeerd bericht. Een vergelijkbare structuur van de URL-string (IP-adres/m/IbQ.*) was te vinden in meerdere URL's die bij deze aanval werden gebruikt. Het feit dat de communicatie door het reputatiesysteem werd geblokkeerd, voegt nog meer indirect bewijs toe.
- De aanvaller stelde ook een tweede C&C-kanaal in op een server die nog geen deel uitmaakte van de reputatiefeeds om ervoor te zorgen dat de malware actief bleef. De URL zelf is een gecodeerd bericht.

### Voorbeeld van HTTP-verzoek (geanonimiseerd en ingekort)

http://109.XXX.XX.XXX/m/IbQXXXVjjpcE6+54HXXXdmmGcNZxtMZdvqyB5EkJAUmL/1sOXXXvq5zzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXX.g+fq4XXXOTYke6uhGHDOEeqje76v7z7i+wgqXXXFBuMz5k08yocxOH63bwQ9JMfwy8uNRM…


### Communicatie met C&C-server 2 (94.XXX.XXX.XXX)

Communicatie-eigenschappen:

- Het totale aantal verzoeken aan deze server was 75; het waren allemaal C&C-verzoeken.
- Er werden twee C&C-pogingen gedetecteerd door CTA als **HTTP-verkeer naar IP-adres (geen domein opgegeven)**. Deze gedragscategorie detecteert afwijkende verzoeken die bestaan in een communicatie buiten de normale volgorde aan een puur IP-adres. Zo'n activiteit kan door malware worden uitgevoerd als 'keep-alive'-controle om te zien of de malware nog actief is, of gewoon om gegevens door te sluizen en aanvullende instructies te ontvangen van de kwaadaardige infrastructuur (C&C). Dit type verkeer wordt niet geproduceerd door normaal surfen op internet.
- Deze 75 C&C-verzoeken werden geen van allen gedetecteerd door technologieën op basis van handtekeningen of reputatie.

### Voorbeeld van HTTP-verzoek (geanonimiseerd en ingekort)

http://94.XXX.XXX.XXX/m/IbQXXXVjj7iA+O54XXXodmmGcNZxtMZdvqyB5EkJAUmLb3pvGIRvqizzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXXog+fq4XXXaE0qfJf1FwalZJKnDc7U0H30+XkiXXXIApkslTo5yvM0TkHrZncwIvumxLCQ+fq4XXXOT…

## Communicatie met C&C-server 3 (fistristy.com)

Communicatie-eigenschappen:

- Het totale aantal verzoeken aan het domein fistristy.com was 175. Het waren allemaal gevallen van C&C-communicatie.
- De technologieën op basis van webhandtekeningen en reputatie blokkeerden alle verzoeken.

### Voorbeeld van een HTTP-verzoek

hXXp://fistristy.com/aa/


## Communicatie met C&C-server 4 (ffeed5.com)

Communicatie-eigenschappen:

- Het totale aantal verzoeken aan ffeed5.com was 7. Het waren allemaal gevallen van C&C-communicatie, geblokkeerd door CWS Premium.
- CTA heeft 6 verzoeken gedetecteerd in de categorie **Afwijkend HTTP-verkeer**. Deze gedragscategorie omvat malwaregedrag dat meestal niet past in het 'basislijn'-gedrag dat is vastgesteld met de doorlopende CTA-analyse. De term 'basislijn' wijst op de status van de statistische modellen die zijn gebouwd door het CTA- systeem, dat de trends en kenmerken van geanalyseerd webverkeer 'leert'. CTA past automatisch de basislijn aan wanneer het netwerk verandert (bijvoorbeeld overdag of 's nachts) voor de best mogelijke detectieresultaten.
- CTA gebruikt langetermijnmodellering van netwerkgedrag om ogenschijnlijk ongerelateerde activiteiten te correleren. Vervolgens worden deze gegevens vergeleken met het gedrag van individuele gebruikers in het klantnetwerk voor een betere detectie van steelse en hardnekkige bedreigingen.

### Voorbeeld van een HTTP-verzoek

hXXp://ffeed5.com/cmd?version=1,5&aid=555&id=24c6b407-5010-4d8d-a266-ffdac7d6f901&os=6,1.7601_1,0_64

## Conclusie

Het beveiligingsteam van de klant had een eenvoudiger manier nodig om activiteiten te bewaken en om beveiligingsincidenten te prioriteren in een netwerk met meer dan 15.000 gebruikers en gemiddeld meer dan 35 miljoen webtransacties per dag. De klant had tevens een oplossing nodig die niet alleen bedreigingen kan blokkeren, maar ook snel bedreigingen kan detecteren die onvermijdelijk aan andere verdedigingen ontsnappen. De klant had een technologie nodig die is ontworpen om beveiligingspersoneel te waarschuwen voor hardnekkige, verdachte activiteiten totdat de bedreiging geheel is opgelost.

Door CTA te implementeren als onderdeel van Cisco CWS Premium heeft de klant nu een near-realtimeanalysesysteem voor netwerkgedrag, dat gebruikmaakt van machine learning en geavanceerde statistieken om IOC's in het netwerk te detecteren. In het voorbeeld van de ransomware-infectie met Cryptolocker bleef CTA waarschuwingen geven over kwaadaardige activiteit totdat het beveiligingsteam de infectie volledig had opgelost. Door het inzicht dat CTA geeft in het gedrag van malware, kan het beveiligingsteam van de klant hun aandacht nu richten op uitsluitend de belangrijkste bedreigingen vóór, tijdens en na een aanval.

## Meer informatie

Cisco CWS Premium, dat CTA en AMP omvat, is in lijn met de strategie van Cisco om organisaties te helpen bij de aanpak van bekende en nieuwe beveiligingsproblemen. Dat doen ze door te helpen bij het detecteren, begrijpen en stopzetten van bedreigingen aan de hand van doorlopende analyse en realtimebeveiligingsinformatie van de cloud, die wordt gedeeld met alle beveiligingsoplossingen om de effectiviteit te vergroten. Dankzij de combinatie van deze drie oplossingen kan CWS Premium nieuwe command and control-kanalen identificeren die niet eerder door de beveiligingsindustrie zijn ontdekt, en kan organisaties helpen bij de aanpak van beveiligingsproblemen in het hele aanvalsspectrum.

Ga voor meer informatie over CWS Premium naar http://www.cisco.com/go/cws.

Ga voor meer informatie over CTA naar http://www.cisco.com/go/cognitive.

Ga voor meer informatie over AMP naar http://www.cisco.com/go/amp.

**Hoofdkantoor Amerika**
Cisco Systems, Inc.
San Jose, CA

**Hoofdkantoor Zuidoost-Azië**
Cisco Systems (USA) Pte, Ltd.
Singapore

**Hoofdkantoor Europa**
Cisco Systems International BV Amsterdam,
Nederland

Cisco beschikt wereldwijd over meer dan 200 kantoren. Adressen, telefoonnummers en faxnummers vindt u op de Cisco-website op **www.cisco.com/go/offices**.



Gedrukt in de VS C36-733153-00 10/14