**PERSBERICHT**

**SophosLabs ziet ‘designer’ cyberdreigingen toenemen**

* *Regionale cyberdreigingen met lokale talen, merken en betaalmethoden*
* *Ransomware slim verborgen in persoonlijke, ‘klikbare’ spam*
* *Lokale witwasserij en cyberbank-overvaltechnieken op wereldwijde schaal*
* *Cybercriminelen filteren slachtoffers op locatie*

Oosterhout, 9 mei 2016 - **Sophos heeft de onderzoeksresultaten van SophosLabs bekendgemaakt waarin een groei wordt bespeurd van cybercriminelen die specifieke landen selecteren of filteren wanneer zij ransomware en andere kwaadwillende cyberaanvallen voorbereiden. Het onderzoek omvat onder meer informatie van miljoenen eindgebruikers wereldwijd en zijn geanalyseerd door het team van** [**SophosLabs**](https://www.sophos.com/en-us/threat-center/threat-analyses.aspx)**.**

Om meer mensen in hun aanvallen mee te slepen, leggen cybercriminelen zich toe op aangepaste spamtechnieken waarbij lokale talen, merken en betaalmethoden worden ingezet. Ransomware, vermomd als een heuse mailnotificatie en voorzien van vervalste lokale logo’s, komen geloofwaardig over. Hierdoor zijn nietsvermoedende individuen eerder geneigd dit aan te klikken en is het de crimineel die hierdoor aan het langste eind trekt. Om zo effectief mogelijk te zijn, doen deze mails zich voor als een lokaal postorderbedrijf, een belastingkantoor of juridische instelling. Deze mails worden vaak voorzien van nagemaakte verschepingsbonnen, terugstortingen, boetes voor te snel rijden of elektriciteitsrekeningen. SophosLabs constateert een toename in spam waarbij zinnen perfect zijn opgeschreven en geen grammaticale fouten bevatten.

“Je moet nu twee keer zo goed kijken om een namaak e-mail van een echte te onderscheiden”, zegt Chester Wisniewski, senior security advisor bij Sophos. “Behoedzaam zijn voor deze technieken in je eigen land is een belangrijk aspect van beveiliging.”

De onderzoekers zijn ook belangrijke trends op het gebied van ransomware tegengekomen waarbij specifieke locaties worden aangevallen. Versies van *CryptoWall* hebben voornamelijk toegeslagen in de VS, het Verenigd Koninkrijk, Canada, Australië, Duitsland en Frankrijk. *TorrentLocker* heeft voornamelijk schade aangericht in het Verenigd Koninkrijk, Italië, Australië en Spanje, terwijl *TeslaCrypt* zijn slag probeerde te slaan in het Verenigd Koninkrijk, de VS, Singapore en Thailand.

De analyses gaven ook de Threat Exposure Rates (TER)\* aan voor landen in de eerste drie maanden van 2016. Ook al werden Westerse landen meer onder vuur genomen, toch hadden zij een lagere TER. Landen met de laagste TER: Frankrijk (5,2 procent), Canada (4,6 procent), Australië (4,1 procent), de VS (3 procent) en het Verenigd Koninkrijk (2,8 procent). Algerije (30,7 procent), Bolivia (20,3 procent), Pakistan (19,9 procent), China (18,5 procent) en India (16,9 procent) telden het hoogste percentage eindgebruikers dat door een malware-aanval werd bestookt. De Benelux scoort hierin nog relatief hoog: Luxemburg (4,2 procent), België (4 procent) en Nederland (3,9 procent).

“Zelfs witwassen wordt lokaal toegepast en wordt zo lucratief. Afhandeling via kredietkaarten kan voor criminelen riskant zijn, dus het is niet verwonderlijk dat zij nu anonieme betalingsmethodieken op het internet gebruiken om ransomware-slachtoffers te laten betalen,” vervolgt Wisniewski. “We hebben gezien dat cybercriminelen lokale, online kaarten gebruiken die gelijk staan aan contant geld. Maar ook maken ze gebruik van aankooplocaties zoals prepaid Green Dot MoneyPak-cards van Walgreens in de VS en Ukash vanuit verschillende retailwinkels in het Verenigd Koninkrijk.”

Het concept van het filteren van specifieke landen is ook als trend toegenomen.

“Cybercriminelen programmeren aanvallen in een bepaalde taal om zo bepaalde landen te omzeilen”, zegt Wisniewski. “Dit kan om verschillende redenen gebeuren. Misschien willen deze criminelen geen aanvallen rondom het punt van lancering om zo opsporing te voorkomen. Het kan te maken hebben met nationale trots, of wellicht een samenzwerende ondertoon om zo een vermoeden over een land te creëren door het bij de aanval bewust weg te laten.”

Banking is een voorbeeld van hoe cybercriminelen locatiegebaseerde malware inzetten om het nog meer te laten floreren. Het onderzoek van Sophos toont aan hoe *Trojans* en malware worden gebruikt om banken en financiële instellingen in specifieke regio’s te infiltreren:

* Braziliaanse bank trojans en varianten richten zich op Brazilië
* Dridex is zeer aanwezig in de VS en in Duitsland
* Trustezeb is dominant in Duits sprekende landen
* Yebot is populair in Hong Kong en Japen
* Zbot wordt vrij breed verspreid, maar voornamelijk in de VS, het Verenigd Koninkrijk, Canada, Duitsland, Australië, Italië, Spanje en Japan

“Er is een volledige *cottage industry* van unieke Trojans die zich slechts en alleen op Braziliaanse banken richten”, vertelt Wisniewski.

Omdat de cybercriminelen dreigingen creëren die er echt uitzien en die heel specifiek worden ingezet, wordt het alleen maar lastiger om kwaadwillende spam te herkennen. Gebruikers van thuiscomputers zijn veelal het doel van deze aanvallen en zouden hun systemen tegen deze verfijnde malware-aanvallen dienen te beschermen. Gratis software die deze dreigingen kan opsporen en zowel Mac- als PC-gebruikers kan beschermen is beschikbaar via [Sophos Home](https://www.sophos.com/en-us/lp/sophos-home.aspx).

Dit onderzoek en de analyses zijn afkomstig van SophosLabs, een netwerk van beveiligingsexperts wereldwijd die 24 uur per dag, 7 dagen per week allerlei internet-gerelateerde malafide praktijken opsporen. Hieronder vallen onder meer computervirussen, geavanceerde malware en Trojans, spam, webdreigingen, hackaanvallen en nog veel meer. SophosLabs ontvangt en onderzoekt dagelijks miljoenen e-mails, URL’s, bestanden en andere datapunten en gebruikt haar uitgebreide expertise binnen deze groep om nieuwe definities te ontwikkelen die complete groepen dreigingen en nieuwe varianten kunnen blootleggen. Met faciliteiten die strategisch in Australië, Hongarije, het Verenigd Koninkrijk en Canada zijn opgesteld, kijken de experts van SophosLabs ook naar trends op het gebied van dreigingen en onderhouden zij een [real time dashboard](https://www.sophos.com/en-us/threat-center/threat-monitoring/threatdashboard.aspx#malware-threats) waarop alle malware en nieuwe web-dreigingen op terug te vinden zijn. Voor meer informatie: [Sophos News Blog](https://blogs.sophos.com).

Voor de laatste ontwikkelingen, bezoek ook [Naked Security News](https://nakedsecurity.sophos.com) of lees meer via [Sophos News](http://blogs.sophos.com/).

*\*TER-data vertegenwoordigt de malware-infecties en aanvallen per 1.000 Sophos-eindgebruikers in elk land (1 januari 2016 tot 8 april 2016).*

**Connect with Sophos**

[Twitter](http://soph.so/CfuKd)

[LinkedIn](http://soph.so/Cfv36)

[Facebook](http://soph.so/CfvaA)

[Google+](https://plus.google.com/%2Bsophos)

[Spiceworks](http://soph.so/Cgbwa%20)

[YouTube](http://www.youtube.com/user/sophoslabs)

[Sophos Blog](http://blogs.sophos.com/)

[Naked Security News](http://nakedsecurity.sophos.com/)

**Over Sophos**

Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com/).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**

Square Egg, Sandra Van Hauwaert, Sandra@square-egg.be, 0032 497 251816