**Media Alert**

**SophosLabs:**

**“*Sextortion* Money Trail leidt tot onderbuik van cybercriminaliteit”**

*SophosLabs Report is de eerste die Sextortion Bitcoin Haul opspoort*

**OXFORD, U.K.** – 23 april 2020 – **Sophos heeft het rapport** [***Follow the Money in a Massive "Sextortion" Spam Scheme***](https://news.sophos.com/en-us/2020/04/22/following-the-sextortion-money/) **gepubliceerd, dat aantoont hoe geld van slachtoffers leidde tot de onderbuik van cybercriminaliteit. Onderzoekers ontdekten de oorsprong van miljoenen *sextortion*-spammails die tussen september 2019 en februari 2020 werden verspreid en analyseerden vervolgens wat er met het geld gebeurde dat via slachtoffers in bitcoin-portemonnees van aanvallers terechtkwam. De afpersing bedroeg in totaal ongeveer $ 500.000. Volgens SophosLabs is dit het eerste rapport dat een bitcoin-afstand van *sextortion* traceert.**

*Sextortion* is een veel gebruikte vorm van spamaanval die de ontvanger ervan beschuldigt een pornografische website te bezoeken. Vervolgens wordt gedreigd videobewijs te delen met vrienden en familie, tenzij de ontvanger losgeld betaalt. In de geanalyseerde voorbeelden werd de ontvangers gevraagd om tot $ 800 aan bitcoins te betalen.

SophosLabs-onderzoekers werkten samen met CipherTrace Inc. om de geldstroom uit deze bitcoinportefeuilles te volgen. Ze ontdekten dat de inkomsten door afpersing werden gebruikt voor ondersteuning van onder meer transacties op darkweb-marktplaatsen en het aanschaffen van gestolen creditcardgegevens. Andere gelden werden snel door een reeks portefeuilleadressen verplaatst om te worden geconsolideerd, door 'mixers' geleid in een poging de transacties wit te wassen of in contanten om te zetten.

“De cybercriminele onderwereld is ingewikkeld en het onderzoek van SophosLabs laat zien hoe aanvallers het verkregen losgeld gebruiken om in andere operaties te investeren”, aldus Tamás Kocsír, security researcher bij SophosLabs die het onderzoek leidde. “*Sextortion*-zwendel jaagt op angst en dit maakt het een effectieve manier om snel geld te verdienen. Gedurende de vijf maanden van ons onderzoek zagen we golf na golf van aanvallen, die vaak in het weekend plaatsvonden en soms goed waren tot een vijfde van alle spam die bij SophosLabs werd bijgehouden. En hoewel de meeste ontvangers e-mails niet hebben geopend of niet hebben voldaan, hebben velen van hen de aanvallers rond de 50,9 aan bitcoins betaald. Dit komt overeen met ongeveer $ 500.000.”

De oplichters maken gebruik van wereldwijde botnets op besmette pc's om miljoenen spam-e-mails de wereld in te sturen. Vietnam, Brazilië, Argentinië, Zuid-Korea, India, Italië, Mexico, Polen, Colombia en Peru waren de top-10 landen waar besmette computers spamberichten verstuurden: 81% in het Engels, 10% in het Italiaans, 4% in het Duits, 3,5% in het Frans en 1,2% in het Chinees.

“Spamcampagnes zijn relatief goedkoop en gemakkelijk te implementeren. Maar de veronderstelling dat dit betekent dat ze alleen door laaggeschoolde aanvallers worden gelanceerd, hoeft niet waar te zijn”, aldus Kocsír. “Uit ons onderzoek blijkt dat innovatieve verduisteringstechnieken worden toegepast die zijn ontworpen om antispamfilters te omzeilen. Voorbeelden hiervan zijn het opsplitsen van de woorden met onzichtbare willekeurige tekenreeksen, het invoegen van blokken witte afvaltekst of het toevoegen van woorden uit het Cyrillische alfabet om het scannen van machines te verwarren. Dit zijn geen technieken voor beginners, en ze zijn een goede herinnering dat spamaanvallen van welke aard dan ook serieus moeten worden genomen. Een robuuste aanpak van cyberbeveiliging is essentieel. Als je bang bent dat je het doelwit wordt van een sextortion-zwendel, schakel dan de camera op je computer uit of dek hem af”, aldus Kocsír.

**Over Sophos**

Als wereldwijde leider in *next-gen* cybersecurity beschermt Sophos meer dan 400.000 organisaties in meer dan 150 landen tegen de meest geavanceerde cyberdreigingen. Aangedreven door SophosLabs, een wereldwijd team voor *threat intelligence* en *data science*, beschermen de cloudgebaseerde en AI-aangedreven oplossingen laptops, servers, mobiele devices en netwerken tegen immer evoluerende cyberaanvaltechnieken waaronder ransomware, malware, exploits en phishing.

Het cloudgebaseerde beheerplatform Sophos Central integreert het volledige portfolio van Sophos’ *next-gen* oplossingen (waaronder de endpointoplossing Intercept X en XG next-gen firewall) in een enkel ‘gesynchroniseerd beveiligingssysteem’ dat via een set API's toegankelijk is. Sophos verkoopt zijn oplossingen en diensten via een wereldwijd kanaal van meer dan 47.000 partners en Managed Service Providers. Sophos stelt zijn innovatieve commerciële technologieën via Sophos Home ook beschikbaar aan consumenten. Het bedrijf heeft zijn hoofdkantoor in Oxford (VK) en wordt op de London Stock Exchange onder het symbool *‘SOPH’* verhandeld. Voor meer informatie: [www.sophos.com](http://www.sophos.com).

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

Square Egg Communications, Sandra Van Hauwaert, sandra@square-egg.be, GSM 0497 251816.