**Media alert**

***Van roofdier tot hoog risicovaccin:***

**Sophos volgt WannaCry’s evolutie**

* *WannaCry-opsporingen blijven in de miljoenen lopen: in augustus alleen al 4,3 miljoen detecties;*
* *Duizenden varianten met korte levensduur blijven maar komen: 12.480 varianten eind 2018 ontdekt, 6.963 in augustus 2019 (80 procent daarvan is nieuw);*
* *Een analyse van zo’n 2.000 WannaCry-monsters uit 2018 toont aan dat ze zijn aangepast om de beroemde 'kill-switch’ te omzeilen, maar ze kunnen geen data versleutelen.*

Oosterhout, 18 september 2019 - **Sophos lanceert een rapport over WannaCry en wat er op de dag van deze wereldwijde malwareuitbraak in mei 2017 en daarna is gebeurd. SophosLabs toont aan dat de WannaCry-dreiging onverminderd voortgaat - met miljoenen detecties elke maand. En hoewel de originele malware niet is bijgewerkt, worden er vele duizenden kortlevende varianten vrijgegeven.**

WannaCry blijft een gevaar en dat is grotendeels te wijten aan de nieuwe varianten die de 'kill-switch’ kunnen omzeilen. Toen Sophos-onderzoekers echter een aantal varianten van monsters analyseerden en uitvoerden, ontdekten ze dat deze geen gegevens konden versleutelen als gevolg van codecorruptie.

Door de manier waarop WannaCry zich verspreidt - controleert of een computer al besmet is en zo ja, op naar de volgende - is een besmetting met een inerte versie van de malware een effectieve bescherming tegen een besmetting met een actieve versie. Kort gezegd: nieuwe malwarevarianten treden op als een toevallig vaccin, en biedt ongepatchte en kwetsbare computers immuniteit tegen een volwaardige WannaCry-ransomware aanval. Het feit dat deze computers tijdens de WannaCry-aanvallen zijn misbruikt, betekent dat de patch, die meer dan twee jaar geleden is uitgebracht ter bescherming tegen WannaCry, nooit is geïnstalleerd.

De originele WannaCry-malware werd 407 keer door SophosLabs-onderzoekers opgespoord; sindsdien hebben zij 12.480 varianten van de oorspronkelijke code geïdentificeerd. Bij nadere inspectie van meer dan 2.700 samples (goed voor 98 procent van de opsporingen) bleek dat ze zich allemaal hadden aangepast om de 'kill-switch’ te omzeilen - een specifieke URL die, als de malware er verbinding mee maakt, automatisch het infectieproces beëindigt.

In augustus 2019 detecteerde Sophos 4,3 miljoen WannaCry-exemplaren. Het aantal waargenomen verschillende varianten was 6.963; hiervan waren er 5.555 (gelijk aan 80 procent) nieuwe bestanden. Sophos-onderzoekers hebben ook de eerste verschijning van de meest verspreide, corrupte versie die twee dagen na de WannaCry-aanval uitbrak, ontdekt. Die is alleen nog niet ‘in het wild’ waargenomen.

"De WannaCry-uitbraak van 2017 heeft het dreigingslandschap voorgoed veranderd. Ons onderzoek benadrukt hoeveel niet-gepatchte computers er nog zijn en hoeveel andere patches er ook zijn genegeerd”, zegt Peter Mackenzie, security specialist bij Sophos en hoofdauteur van het onderzoek. “Sommigen hebben geluk gehad, omdat zij varianten van de malware hebben opgelopen die hen immuun hebben gemaakt tegen nieuwe versies. Maar geen enkele organisatie zou hierop mogen vertrouwen. In plaats daarvan zou de standaardpraktijk moeten zijn dat er een beleid is dat zowel het installeren van patches wanneer deze beschikbaar zijn, als het toepassen van een robuuste beveiligingsoplossing ten behoeve van alle endpoints, netwerken en systemen, voorschrijft.”

**Persinformatie**Sandra Van Hauwaert, Square Egg Communications, sandra@square-egg.be, GSM 0497251816

**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 bij Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com).