****

**Sophos lanceert Rapid Response Service om actieve cyberaanvallen te identificeren en te neutraliseren**

*Bliksemsnelle reactie op incidenten minimaliseert schade door aanvallen en verkort de hersteltijd*

Oosterhout, 28 oktober 2020 –  **Sophos lanceert Sophos Rapid Response, de eerste, tegen een vaste vergoeding, betaalde dienst voor incidenten op afstand die actieve cyberaanvallen identificeert en neutraliseert gedurende de volledige duur van 45 dagen. Sophos Rapid Response biedt organisaties een professioneel team van incidentrespondenten dat 24/7 klaar staat, dreigingsjagers én dreigingsanalisten om snel geavanceerde aanvallen te stoppen en tegenstanders uit hun netwerken te verwijderen. Hierdoor kunnen schade en kosten tot een minimum worden beperkt. Tevens leidt het tot een verkorte hersteltijd.**

Sophos Rapid Response heeft het eerste gebruik van de Buer-malware dropper voor ransomware ontdekt. In het nieuwe onderzoek "[Hacks for Sale: Inside Buer Loader's Malware-as-a-Service](https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service)" van Sophos Rapid Response en SophosLabs wordt beschreven hoe Buer Windows PC’s compromitteert, waardoor aanvallers een payload kunnen leveren. Sophos Rapid Response heeft een [golf van Ryuk-aanvallen](https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/) gedetecteerd die van nieuwe tools, technieken en procedures gebruik maakten. Sophos deed de ontdekking terwijl ze een van deze recente aanvallen migiteerde. Bij dit incident gebruikten volhardende aanvallers Buer in een poging de Ryuk-ransomware te lanceren, waarna ze hun inspanningen uitbreidden door het gebruik van Buer te combineren met andere soorten loader-malware.

"Als je wordt geraakt door een aanval, is tijd van essentieel belang. Elke minuut tussen aanvankelijk compromitteren en neutraliseren telt wanneer tegenstanders door de levenscyclus van een aanval racen”, aldus Joe Levy, Chief Technology Officer bij Sophos. "Geavanceerde aanvallen kunnen bedrijfsactiviteiten snel stoppen, en IT-managers die ransomware uit de eerste hand hebben meegemaakt, weten dit maar al te goed, en melden dat ze verhoudingsgewijs meer tijd moeten besteden aan de respons op incidenten en minder tijd aan het voorkomen van dreigingen dan degenen die niet zijn getroffen. Sophos Rapid Response verstoort actieve aanvallen, waardoor het complexe en tijdrovende proces van het stoppen van vastberaden aanvallers wordt geëlimineerd, zodat organisaties sneller weer normaal kunnen functioneren."

Sophos Rapid Response neutraliseert een breed scala aan beveiligingsincidenten, waaronder ransomware, netwerkinbreuken, hands-on aanvallen door cybercriminelen en meer. Het Sophos Rapid Response-team kan binnen enkele uren worden ingeschakeld en geactiveerd waarbij het merendeel van de aanvallen binnen 48 uur wordt behandeld.

"Dit jaar zijn verwoestende ransomware-aanvallen helaas een goudkoorts geweest voor cybercriminelen. Het is totaal anders dan wat de cyberbeveiligingsindustrie ooit heeft meegemaakt. Bijna 85% van de aanvallen waarbij Sophos Rapid Response was betrokken, had ransomware aan boord - met name Ryuk, REvil en Maze. Ik kan met vertrouwen zeggen dat de meeste andere aanvallen waarvoor we werden opgeroepen, ook zouden hebben geresulteerd in ransomware als we niet zo snel hadden gehandeld." Dat zegt Peter Mackenzie, incidentresponsmanager bij Sophos. “Gemakkelijk toegankelijke tools maken het voor aanvallers mogelijk om in een week tijd meer geld te verdienen dan de meeste mensen in hun leven zullen doen. Criminelen infiltreren netwerken en plannen hun aanvallen heimelijk op de achtergrond, voordat ze ransomware strategisch lanceren als de laatste lading - vaak tijdens de nachtelijke uren, wanneer niemand toekijkt, om het op zoveel mogelijk machines uit te voeren. Sophos Rapid Response onderneemt onmiddellijk actie om de brand te blussen. In het geval van een ziekenhuis dat we deze maand hielpen nadat het werd getroffen door Ryuk-ransomware en gedwongen werd te sluiten, betekende dit het verschil van leven of dood."

Sophos Rapid Response maakt deel uit van Sophos Managed Threat Response (MTR), een wereldwijd team dat proactieve, volledig beheerde services voor het opsporen van bedreigingen, detectie en respons biedt. Als een van de meest gebruikte Managed Detection and Response-diensten in de branche met meer dan 1.400 klanten onderscheidt Sophos ‘MTR’ zich door het vermogen om proactief actie te ondernemen namens een organisatie om bedreigingen in realtime te verminderen.

Zodra onmiddellijke bedreigingen zijn geneutraliseerd tijdens een Rapid Response-opdracht, schakelt het Sophos Rapid Response-programma over op continue monitoring 24/24 voor het proactief opsporen van bedreigingen, onderzoek, detectie en reactie van het Sophos MTR-team. Een dreigingsonderzoeksrapport geeft details over de ontdekkingen die zijn gedaan, de genomen acties en andere aanbevelingen voor herstel, waardoor organisaties het ontstaan ​​van aanvallen kunnen begrijpen, evenals welke activa zijn gecompromitteerd en gegevens zijn geopend en geëxfiltreerd.

Sophos Rapid Response is nu beschikbaar voor zowel bestaande als niet-Sophos-klanten. In tegenstelling tot traditionele incidentrespons en forensische services die complexe en langdurige implementaties vereisen met prijsstructuren per uur, is Sophos Rapid Response een aanbod op afstand met een vast prijsmodel op basis van het aantal gebruikers en servers van een organisatie. Sophos Rapid Response is er voor bedrijven van elke omvang, inclusief de kleinere organisaties, die tot nu toe niet gemakkelijk toegang hadden tot dergelijke diensten met een vaste fee per maand.

**Over Sophos**Als een wereldwijde leider in *next-gen* cybersecurity beschermt Sophos meer dan 400.000 organisaties, ongeacht bedrijfsgrootte, in meer dan 150 landen tegen de meest geavanceerde cyberdreigingen van vandaag. Aangedreven door SophosLabs, een wereldwijd team gespecialiseerd in dreiginginformatie en wetenschappelijke data, beveiligen Sophos’ cloud-native en AI-verbeterde oplossingen endpoints (laptops, servers en mobiele apparaten) en netwerken tegen immer evoluerende cybercriminele tactieken en technieken. Hieronder vallen onder meer geautomatiseerde en actieve, vijandige inbreuken, ransomware, malware, exploits, data-exfiltration, phishing en meer. Het cloudgebaseerde Sophos Central-platform integreert Sophos’ gehele portfolio - van Intercept X-endpointoplossing tot XG Firewall - in een enkel systeem: Synchronized Security.

Sophos-producten zijn exclusief verkrijgbaar via een wereldwijd kanaal van meer dan 53.000 partners en Managed Service Providers. Sophos stelt zijn innovatieve commerciële technologieën ook beschikbaar aan consumenten via Sophos Home. Het bedrijf is gevestigd in Oxford, Verenigd Koninkrijk. Meer informatie: [www.sophos.com](http://www.sophos.com).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**Sandra Van Hauwaert, Square Egg Communications, sandra@square-egg.be, GSM 0497251816.