**Sophos Threat Report omvat ransomware en andere trends die IT-beveiliging in 2021 vormgeven**

*Rapport biedt 3D-weergave van cyberaanvaltrends van SophosLabs, evenals van Sophos' dreigingsjagers, snelle antwoorden en cloudbeveiligings- en AI-experts*

**Oosterhout,** 18 november 2020 – **Sophos publiceert vandaag het** [**Sophos 2021 Threat Report**](https://www.sophos.com/en-us/labs/security-threat-report.aspx)**. Hierin wordt aangegeven hoe ransomware en snel veranderend gedrag van aanvallers het dreigingslandschap en IT-beveiliging in 2021 zullen bepalen. Het rapport biedt een driedimensionaal perspectief op beveiligingsdreigingen en -trends, vanaf het begin tot de daadwerkelijke impact.**

De drie belangrijke trends in in het rapport:

**1. Kloof tussen ransomware-operators aan beide ‘uiteinden’ zal groter worden**
Aan de ‘hoge kant’ zullen de ransomwarefamilies die op groot wild jagen hun tactieken, technieken en procedures (TTP's) blijven verfijnen en veranderen om zich meer ontwijkend op grotere organisaties met losgeld van meerdere miljoenen dollars te richten. Aan de andere kant van het spectrum verwacht Sophos een toename van het aantal aanvallers op ‘instapniveau’ die op zoek zijn naar menugestuurde ransomware-for-rent waarmee ze zich op grote hoeveelheden kleinere prooien kunnen richten.

Een andere [ransomwaretrend](https://news.sophos.com/en-us/2020/08/04/the-realities-of-ransomware-extortion-goes-social-in-2020/) is "secundaire afpersing", waarbij de aanvallers (naast de gegevensversleuteling) dreigen vertrouwelijke informatie te publiceren wanneer er niet aan hun eisen wordt voldaan. “Het bedrijfsmodel van ransomware is dynamisch en complex. In 2020 zag Sophos een duidelijke trend dat tegenstanders zich differentiëren in termen van vaardigheden en doelen. We hebben echter ook gezien dat ransomwarefamilies de beste tools van hun soort deelden en zelfbenoemde samenwerkingskartels vormden”, zegt Chester Wisniewski, hoofdonderzoeker bij Sophos. “Sommigen leken hun koffers te pakken en verdwenen, behalve dat enkele van hun tools en technieken weer opdoken onder het mom van een nieuwkomer, Egregor. Als de ene dreiging verdwijnt, komt er snel een andere in de plaats. In veel opzichten is het bijna onmogelijk om te voorspellen waar ransomware naartoe zal gaan, maar de aanvalstrends die dit jaar in ons dreigingsrapport worden besproken, zullen waarschijnlijk doorzetten in 2021."

2. **Alledaagse dreigingen (waaronder commodity-malware) vereisen serieuze aandacht**
Dergelijke dreigingen kunnen lijken op malware op een laag niveau, maar ze zijn ontworpen om voet aan de grond te krijgen binnen een doelwit, daar essentiële gegevens te verzamelen en gegevens terug te delen met een command-and-control-netwerk voor verdere instructies. Als menselijke operators achter dit soort dreigingen zitten, zullen ze elke gecompromitteerde machine controleren op zijn geolocatie en andere waardevolle tekens, en vervolgens toegang tot de meest lucratieve doelen verkopen aan de hoogste bieder.

“Uit Sophos’s analyse is het duidelijk dat verdedigers commodity-malware serieus moeten nemen. Elke infectie kan tot een andere leiden. Veel beveiligingsteams zullen het gevoel hebben dat zodra malware is geblokkeerd of verwijderd en de besmette machine is schoongemaakt, het incident is voorkomen”, aldus Wisniewski. "Ze realiseren zich misschien niet dat de aanval waarschijnlijk op meer dan één machine was gericht en dat schijnbaar veel voorkomende malware zoals Emotet en [Buer Loader](https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/) kan leiden tot [Ryuk](https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/), Netwalker en andere geavanceerde aanvallen, die IT misschien pas opmerkt als de ransomware wordt [geïmplementeerd](https://news.sophos.com/en-us/2020/08/04/the-realities-of-ransomware-five-signs-youre-about-to-be-attacked/). Het onderschatten van ‘kleine’ infecties kan erg duur uitvallen."

3. **Alle rangen zullen in toenemende mate misbruik maken van legitieme tools**
Door misbruik van legitieme tools kunnen tegenstanders onder de radar blijven terwijl ze zich door het netwerk verplaatsen totdat ze klaar zijn om het grootste deel van de aanval te starten. Voor aanvallers die door een natiestaat worden gesponsord, is er het extra voordeel dat het gebruik van gemeenschappelijke tools toeschrijving moeilijker maakt.

Nogmaals Wisniewski: "Het misbruik van [alledaagse tools](https://news.sophos.com/en-us/2020/02/25/how-i-learned-to-stop-worrying-and-love-grey-hat-tools/) en technieken om een ​​actieve aanval te verhullen, kwam prominent naar voren in Sophos' [evaluatie](https://news.sophos.com/en-us/2020/08/04/the-realities-of-ransomware-the-evasion-arms-race/) in 2020. Deze techniek stelt traditionele beveiligingsbenaderingen op de proef, omdat het verschijnen van bekende tools niet automatisch een waarschuwing geeft. Dit is waar het snelgroeiende gebied van door mensen geleide dreigingsjacht en beheerde dreigingsrespons echt tot zijn recht komt. Menselijke experts kennen de subtiele sporen waarnaar ze moeten zoeken, zoals een legitiem hulpmiddel dat op het verkeerde moment of op de verkeerde plaats wordt gebruikt. Voor getrainde dreigingsjagers of IT-managers die gebruik maken van Endpoint Detection and Response (EDR)-functies, zijn deze signalen handvatten die beveiligingsteams kunnen waarschuwen voor een potentiële indringer en een aanval die gaande is."

**Andere trends uit het Sophos 2021 Threat Report:**

* Aanvallen op servers: aanvallers hebben zich gericht op serverplatforms met zowel Windows als Linux, en hebben deze platforms gebruikt om organisaties van binnenuit aan te vallen
* De impact van de COVID 19-pandemie op de IT-beveiliging, zoals de beveiligingsuitdagingen van thuiswerken met behulp van persoonlijke netwerken die worden beschermd door zeer uiteenlopende beveiligingsniveau
* De beveiligingsuitdagingen waarmee cloudomgevingen worden geconfronteerd: cloud computing heeft met succes het grootste deel van de zakelijke behoeften aan veilige computeromgevingen op zich genomen, maar staat voor andere uitdagingen dan die van een traditioneel bedrijfsnetwerk
* Gemeenschappelijke services zoals RDP- en VPN-concentrators, die een aandachtspunt blijven voor aanvallen op de netwerkperimeter. Aanvallers gebruiken RDP ook om lateraal binnen doorbroken netwerken te bewegen
* Softwaretoepassingen die traditioneel werden gemarkeerd als 'mogelijk ongewenst' omdat ze een overvloed aan advertenties leverden, maar zich bezighielden met tactieken die in toenemende mate niet te onderscheiden zijn van openlijke malware
* De verrassende terugkeer van een oude bug, VelvetSweatshop - een standaard wachtwoordfunctie voor eerdere versies van Microsoft Excel - gebruikt om macro's of andere kwaadaardige inhoud in documenten te verbergen en geavanceerde detectie van dreigingen te omzeilen
* De noodzaak om benaderingen uit de epidemiologie toe te passen om ongeziene, niet-gedetecteerde en onbekende cyberdreigingen te kwantificeren om hiaten in detectie beter te overbruggen, risico's te beoordelen en prioriteiten te stellen

Het volledige Sophos 2021 Threat Report is beschikbaar op [www.sophos.com/threatreport](http://www.sophos.com/threatreport).

**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 bedreiginginformatie 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.