****

**Onderzoek Sophos:**

**“Zeven jaar oude datadief ‘Agent Tesla’ blijft bedreiging vormen”**

*Agent Tesla na al die jaren nog actief via e-mailspam*

**Oosterhout, 3 februari 2021** – ‘Datadief’ Agent Tesla blijft zeven jaar na zijn ontdekking nog steeds een doorn in het oog, wijst een Sophos-rapport uit. In de laatste bevindingen van de onderzoekers worden de nieuwste functies en functionaliteit van Agent Tesla onthuld.

Agent Tesla ontvreemdt data van webbrowsers, e-mailclients, VPN-clients en andere software die gebruikersnamen en wachtwoorden opslaat. Agent Tesla kan toetsaanslagen vastleggen terwijl gebruikers aan het typen zijn (bijvoorbeeld bij het invoeren van wachtwoorden) maar ook screenshots vastleggen. Op deze manier kan de kwaadwillende Agent Tesla zien wat er op het scherm van nietsvermoedende gebruikers staat.

De meer recente versie van deze ‘info stealer’ kan de Telegram-berichtenservice gebruiken om met zijn operators te communiceren, evenals het Tor-softwareprogramma (erg populair op het dark web) om zo activiteiten als het verwijderen van gestolen data te verbergen. Het probeert ook softwarecodes te wijzigen om de beveiliging te blokkeren.

"Agent Tesla-malware is al meer dan zeven jaar actief, maar het blijft een van de meest voorkomende bedreigingen voor Windows-gebruikers", zegt Sean Gallagher, senior security researcher bij Sophos. “Agent Tesla’s voorkomende methode is het verzenden van kwaadaardige spambijlagen. De e-mailaccounts die worden gebruikt om Agent Tesla te verspreiden, zijn vaak legitieme, maar gehackt accounts. Organisaties en consumenten moeten, zoals altijd, e-mailbijlagen van onbekende afzenders voorzichtig behandelen en alle bijlagen verifiëren voordat ze worden geopend."

**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](mailto:sandra@square-egg.be), GSM 0497251816.