**‘Gootloader’ infecteert internetgebruikers in het geheim met malware en ransomware**

* *Gootloader houdt zelfs technisch geschoolde IT-gebruikers voor de gek*
* *Tot nu toe ontdekt in Duitsland, Frankrijk, de Verenigde Staten en Zuid-Korea*
* *België is gewaarschuwd, aldus beveiligingsexperts van Sophos*

Oosterhout, 1 maart 2021 – **Onderzoek van Sophos toont aan hoe criminelen de infectiemethode voor financiële malware "Gootkit" hebben omgezet in een complex platform voor een breed scala aan malware, waaronder ransomware. Gootloader-aanvallers, zoals de criminelen door Sophos worden benoemd, bereiken hun doel door legitieme websites te hacken om vervolgens de inhoud subtiel te wijzigen. Hierdoor kunnen de websites verschillende inhoud aan verschillende bezoekers laten zien.**

De criminelen manipuleren de Search Engine Optimization (SEO): wanneer iemand een vraag in een zoekmachine (zoals Google) invoert, de gehackte websites in de topresultaten verschijnen. Wat er gebeurt nadat gebruikers op een link naar een gehackte website hebben geklikt, is afhankelijk van de locatie van hun land.

Wanneer een gebruiker uit een land dat geen ‘doelwit’ is op een gehackte website klikt, krijgt hij bijvoorbeeld onschuldige inhoud te zien en gebeurt er niets. Maar wanneer gebruikers uit een van Gootloader's doellanden op een gehackte website klikken, krijgen ze een pagina te zien met een nep-discussieforum over het onderwerp dat ze hebben opgevraagd, met dezelfde termen die ze in de zoekmachine hebben getypt. De nepwebsites zien er hetzelfde uit, of ze nu in het Engels, Duits of Koreaans zijn.

“Het nepdiscussieforum bevat een bericht van een ‘sitebeheerder’ met een link naar een download”, stelt John Veldhuis, beveiligingsspecialist bij Sophos. “De download is een schadelijk bestand. Wanneer doelwitten erop klikken, begint de volgende fase van infectie. Vanaf dit punt gaan de aanvallen undercover en leveren ze de kwaadaardige lading met behulp van een breed scala aan ontwijkingstechnieken om detectie door beveiligingstools te voorkomen.”

Gootloader levert momenteel financiële malware in Duitsland, maar ook in de VS en Zuid-Korea. De aanvallers Eerdere operaties waren gericht op Frankrijk. “Andere landen, zoals België, kunnen volgen”, vult Veldhuis aan.

Gabor Szappanos, directeur bedreigingsonderzoek bij Sophos, voegt toe: "De makers van Gootloader gebruiken een aantal trucs en technieken die zelfs technisch geschoolde IT-gebruikers voor de gek kunnen houden. Gelukkig zijn er enkele waarschuwingssignalen waar internetgebruikers op kunnen letten. Deze omvatten Google-zoekresultaten die verwijzen naar websites voor bedrijven die geen logische verbinding hebben met het advies dat ze lijken te bieden; advies dat precies aansluit bij de zoektermen die in de beginvraag zijn gebruikt; en een 'prikbord'-achtige pagina die er identiek uitziet als de voorbeelden uit het Sophos-onderzoek, met tekst en een downloadlink die ook precies overeenkomt met de zoektermen die in de eerste Google-zoekopdracht werden gebruikt.”

**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:**

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