****

**Ransomware-variant Conti, de ‘dubbele afperser’ die vijf dagen lang werd gevolgd en geëlimineerd**

* *Retail, productie- en bouwbranche als top-3 van cybercriminelen*
* *Nog geen Belgische slachtoffers bekend van deze variant*
* *180 bedrijven slachtoffer tot nu toe; meeste slachtoffers in de VS (128)*

Oosterhout, 16 februari 2021 – **Met Conti is er een nieuwe ransomware-variant ontdekt. Conti is er een van het kaliber ‘dubbele afpersing’ waarbij de aanvallers data van hun slachtoffers ontvreemden voordat ze deze versleutelen. Vervolgens dreigen de cybercriminelen ermee dat zij de gestolen informatie op de 'Conti News'-site openbaar maken wanneer slachtoffers geen gehoor aan de losgeldvoorwaarden geven. Deze aanvalsstrategie en hoe ertegen op te treden, is terug te vinden in** [**A Conti Ransomware Day-By-Day**](https://news.sophos.com/en-us/2021/02/09/conti-ransomware-attack-day-by-day/)**.**

Het Sophos Rapid Response-team werd ingeschakeld om het incident, dat zich gedurende vijf dagen afspeelde vanaf het eerste compromis tot het herstel van de productie, in te dammen, te neutraliseren en te onderzoeken. "Bij aanvallen waarbij mensen de controle hebben, kunnen tegenstanders zich in real-time aanpassen en reageren op veranderende situaties", zegt Peter Mackenzie, manager van Sophos Rapid Response. “In dit geval hadden de aanvallers tegelijkertijd toegang gekregen tot twee servers. Toen het doelwit een van de servers detecteerde en (op tijd) uitschakelde, schakelden de aanvallers gewoon over en zetten zij hun aanval voort op de tweede server. Een ‘Plan B’ komt veel voor bij door ‘mensen’ geleide aanvallen. Het wil ook zeggen dat wanneer verdachte activiteiten op een netwerk een halt zijn toegeroepen het niet betekent dat de aanval écht voorbij is.”

De site ‘Conti News’ heeft gegevens gepubliceerd die tot op heden zijn gestolen van ten minste 180 slachtoffers. Sophos heeft een slachtofferschapsprofiel gemaakt op basis van de gegevens die op Conti News zijn gepubliceerd.

"Binnen bedrijven zonder een toegewijd IT-beveiligingsteam is het vaak de IT-beheerder zelf die oog in oog staat met een ransomware-aanval", aldus Mackenzie. "Zij zijn degenen die op een ochtend naar hun werk komen om te zien dat alles vergrendeld is met een losgeldbriefje op het scherm. Soms wordt dit opgevolgd met dreigende e-mails en telefoontjes. Op basis van onze ervaringen met het opsporen van bedreigingen uit eerste hand, hebben we een actielijst ontwikkeld die IT-beheerders door de zeer uitdagende en stressvolle eerste uren en dagen na een Conti ransomware-aanval heen helpt, te begrijpen waar ze hulp kunnen krijgen om de basis te leggen voor een veiligere toekomst.”

**Hoe je tegen Conti te weren?**

* Sluit toegang vanaf internet tot het Remote Desktop Protocol (RDP) af om cybercriminelen de toegang tot netwerken te ontzeggen
* Indien toegang tot RDP nodig is, plaats deze dan achter een VPN-verbinding
* Gebruik gelaagde beveiliging om cyberaanvallen te voorkomen, ertegen te beschermen en ze te detecteren (inclusief Endpoint Detection and Respons-mogelijkheden en beheerde responsteams die 24/7 netwerken bekijken)
* Let op de [vijf indicatoren](https://news.sophos.com/en-us/2020/08/04/the-realities-of-ransomware-five-signs-youre-about-to-be-attacked/) dat een aanvaller aanwezig is zodat een ransomware-aanval kan worden gestopt
* Zorg voor een effectief responsplan en werk dit indien nodig bij. Eventueel kan ook de hulp van een externe expert van toegevoegde waarde zijn

**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