****

**Sophos montre comment une attaque de ransomware Conti de cinq jours se déroule au jour le jour**

Oosterhout, 16 februari 2021 – **Les chercheurs et les intervenants en cas d’incident de Sophos dévoilent ce qui se passe réellement lorsque des attaquants pénètrent dans le réseau d’une entreprise avec l’intention de voler des données et de lancer une attaque avec le ransomware Conti, un ransomware « double extorsion » exploité par l'homme. Les attaquants volent les données de leurs cibles avant de les chiffrer, puis menacent d’exposer les informations volées sur le site « Conti News » si l’entreprise ne paie pas la rançon.**

Sophos Rapid Response, l’équipe de réponse aux incidents de Sophos 24h / 24 et 7j / 7, a été appelée pour contenir, neutraliser et enquêter sur l'incident, qui s'est déroulé sur cinq jours, du compromis initial à la reprise des opérations. La série d'articles de Sophos reconstitue l'attaque telle qu'elle s'est produite au jour le jour et fournit des informations techniques sur le comportement d'attaque de Conti ainsi que des conseils aux défenseurs.

La note « les réalités de Conti Ransomware », comprend : un suivi de l’attaque Conti Ransomware au jour le jour ; une analyse de l’attaque y compris les indicateurs de compromis (IoC) et les tactiques, techniques et procédures (TTP) et enfin un aperçu technique par des chercheurs des SophosLabs qui décrivent à quoi s'attendre lorsqu’une entreprise a été touché par un ransomware Conti. C’est un guide essentiel pour les administrateurs informatiques confrontés à l'impact d'une attaque Conti, avec des conseils sur la marche à suivre immédiatement et une liste de contrôle en 12 points pour les aider à enquêter sur l'attaque. La liste de contrôle guide les administrateurs informatiques à travers tout ce que les attaquants Conti pourraient faire sur le réseau et les principaux TTP qu'ils sont susceptibles d'utiliser. L'article comprend également des recommandations d'action.

« Lors d'attaques où les humains sont aux commandes, les adversaires peuvent s'adapter et réagir à des situations changeantes en temps réel», a déclaré Peter Mackenzie, directeur de Sophos Rapid Response. « Dans ce cas, les attaquants avaient simultanément eu accès à deux serveurs, donc lorsque la cible a détecté et désactivé l'un d'entre eux - et a cru qu'elle avait arrêté l'attaque à temps - les attaquants ont simplement basculé et continué leur attaque en utilisant le deuxième serveur. Avoir un « plan B » est une approche courante pour les attaques humaines et un rappel que ce n'est pas parce qu'une activité suspecte sur le réseau s'est arrêtée que l'attaque est terminée. »

Le site « Conti News » a publié à ce jour des données volées à au moins 180 victimes. Sophos a créé un profil de victimologie basé sur les données publiées sur Conti News (couvrant environ 150 entreprises dont les données avaient été publiées au moment de l'analyse).

Dans les entreprises qui n’ont pas accès à une équipe de sécurité informatique dédiée, ce sont souvent les administrateurs informatiques qui sont directement en ligne de mire pour une attaque de ransomware », a déclaré Mackenzie. « Ce sont eux qui viennent au travail un matin pour découvrir que tout est verrouillé et qu’une note de rançon menaçante est à l'écran, parfois suivie d'e-mails tout aussi menaçants et même d'appels téléphoniques. Sur la base de nos expériences de chasse aux menaces de première main, nous avons développé une liste d'actions qui aidera les administrateurs informatiques à traverser les premières heures et les premiers jours très difficiles et stressants après une attaque du ransomware Conti, à comprendre où ils peuvent obtenir de l'aide et à jeter les bases pour un avenir plus sûr. »

**Conseils immédiats pour les défenseurs**

• Arrêtez le protocole RDP (Remote Desktop Protocol) connecté à Internet pour empêcher les cybercriminels d'accéder aux réseaux

• Si vous avez besoin d'accéder à RDP, placez-le derrière une connexion VPN

• Utilisez une sécurité en couches pour prévenir, protéger et détecter les cyberattaques, y compris les capacités de détection et de réponse des points finaux (EDR) et des équipes d'intervention gérées qui surveillent les réseaux 24h / 24 et 7j / 7

• Soyez conscient des cinq premiers indicateurs qu'un attaquant est présent pour arrêter les attaques de ransomware

• Avoir un plan d'intervention efficace en cas d'incident en place et le mettre à jour au besoin. Si vous n’avez pas la certitude de disposer des compétences ou des ressources nécessaires pour le faire, pour surveiller les menaces ou pour répondre aux incidents d’urgence, envisagez de vous tourner vers des experts externes pour obtenir de l’aide.

Les produits de sécurité Sophos bloquent le ransomware Conti et ses fichiers associés.

Plus d’informations : [**A Conti Ransomware Day-By-Day**](https://news.sophos.com/en-us/2021/02/09/conti-ransomware-attack-day-by-day/)**.**

**À propos de Sophos**En tant que leader mondial en solution de cybersécurité Next-Gen, Sophos protège plus de 400 000 entreprises, de toutes tailles et dans plus de 150 pays, contre les cybermenaces actuelles les plus avancées. Développées par les SophosLabs, une équipe présente dans le monde entier et spécialisée dans le renseignement sur les menaces et la science des données, les solutions Cloud-Native et basées sur l'IA de Sophos protègent les systèmes endpoint (les ordinateurs portables, les serveurs et les périphériques mobiles) ainsi que les réseaux contre les techniques de cyberattaque évolutives, notamment les ransomwares, les malwares, les exploits, l'exfiltration de données, le phishing, et bien plus encore. Sophos Central, la plateforme de management Cloud-Native, intègre l'ensemble des produits Next-Gen de Sophos, y compris la solution Intercept X endpoint et le pare-feu XG Next-Gen, via un système unique de « sécurité synchronisée » accessible via un ensemble d'API. Sophos commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 53 000 partenaires et fournisseurs de services gérés (MSP : Managed Service Provider). Sophos met également ses technologies commerciales innovantes à la disposition des particuliers via Sophos Home. Le siège de l’entreprise est basé à Oxford, au Royaume-Uni. Plus d'informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contacts presse :**Sandra Van Hauwaert, Square Egg Communications, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816