**Sophos déconstruit les attaques de Dharma, le Ransomware-as-a-Service qui menace les PME pendant la pandémie de Covid-19**

*Des attaques ciblent les entreprises qui pratiquent le télétravail et utilisent des protocoles de bureau à distance vulnérables*

Oosterhout, le 1 Septembre 2020 – [**Sophos**](https://www.sophos.com/fr-fr.aspx)**, leader mondial en solution de cybersécurité Next-Gen, annonce la publication de « [Color by Numbers: Inside a Dharma Ransomware-as-a-Service (RaaS) Attack](https://news.sophos.com/en-us/2020/08/12/color-by-numbers-inside-a-dharma-ransomware-as-a-service-attack/) », un rapport qui offre pour la première fois une analyse en profondeur d’un script et d’un ensemble d’outils automatisés créés par des opérateurs de ransomwares et fournis à des cybercriminels accompagnés d’une infrastructure back-end et de programmes malveillants. Le rapport montre la manière dont Dharma cible les PME en 2020.**

En dépit du fait que [l’existence de Dharma a été révélée en 2016](https://www.sophos.com/fr-fr/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf), il s’agit de l’une des familles de ransomwares qui engendre le plus de profits à l’heure actuelle et ce, en raison de son modèle commercial qui s’appuie sur une offre de services destinés à un marché de masse. De nombreuses itérations de son code source ont été publiées en ligne ou proposées à la vente, donnant naissance à d’innombrables variations.

Les principales cibles de Dharma et de son offre de Ransomware-as-a-Service (RaaS) sur lesquelles a porté l’analyse de Sophos sont des PME, avec 85 % des attaques détectées en 2020 portant sur des outils d’accès exposés aux menaces, comme les protocoles de bureau à distance (RDP). Ces conclusions émanent de la société Coveware, spécialiste de la récupération de données ciblées par ransomwares, qui a également découvert que les demandes de rançon liées à Dharma étaient généralement assez peu élevées, avec un montant moyen de 8 620 USD.

« Dharma est le fast-food franchisé des ransomwares : facilement et largement accessible à tous, ou presque, » déclare Sean Gallagher, l’un des principaux chercheurs en charge des menaces chez Sophos. « En temps normal, c’est en soi assez inquiétant. Mais à l’heure actuelle, alors que de nombreuses entreprises s’adaptent à la pandémie et tentent de répondre au besoin pressant de support pour les employés qui travaillent à distance et avec des équipes IT surmenées, les risques que de telles attaques aient lieu sont décuplés. Les petites entreprises, qui ont dû s’équiper et mettre en place une force de travail à distance à l’improviste, se retrouvent avec des infrastructures et des appareils vulnérables et des équipes de support IT qui ne sont pas en mesure d’assurer un suivi adéquat et une gestion adaptée des systèmes, comme ils le feraient d’ordinaire. »

Comme le montre le rapport de Sophos, une fois que les clients Dharma, désignés sous le nom d’affiliés, ont acheté les outils et trouvé un point d’entrée dans l’entreprise cible, ils se reposent entièrement sur un script PowerShell, doté d’un menu, qui installe et lance les composantes nécessaires à la diffusion du ransomware sur l’ensemble du réseau ciblé. Lorsque le script principal s’exécute, il se manifeste sous la forme d’une « Toolbox » et lance son attaque accompagnée du message « *Have fun, bro!* » (en français : « Amuse-toi bien, mec !  »).

Ce type de cyberattaque repose largement sur le détournement d’outils open-source, ainsi que de versions gratuites d’outils commerciaux. Le déchiffrement des données, étonnamment complexe, se déroule en deux étapes. Les entreprises ciblées qui contactent les affiliés pour obtenir des clés de récupération reçoivent un premier outil qui extrait les détails de tous les fichiers chiffrés. Les affiliés envoient ensuite les données extraites à leurs opérateurs, qui fournissent une seconde clé pour déchiffrer les fichiers. Les études montrent que le degré d’efficacité en matière de restauration réelle des données ciblées dépend largement des compétences et du bon-vouloir des affiliés. Par exemple, Sophos a constaté que, dans certains cas, les affiliés gardaient des clés pour eux, afin de formuler de nouvelles demandes de rançon.

 « Étant donné le nombre de demandes de rançons s’élevant à plusieurs millions de dollars, la renommée des entreprises ciblées et les techniques de pointe utilisées par les cyberattaquants comme [WastedLocker](https://news.sophos.com/en-us/2020/08/04/wastedlocker-techniques-point-to-a-familiar-heritage/) qui font actuellement la une, il est facile d’oublier que les menaces émanant de Dharma et d’autres outils similaires sont bel et bien présentes et fournissent les moyens à une toute autre classe de cybercriminels de frapper des cibles multiples et d’amasser des fortunes, huit mille dollars à la fois. » conclut Sean Gallagher.

**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, GSM 0497251816.