**Sophos ontleedt Dharma Ransomware-as-a-Service-aanvallen die tijdens COVID19 de KMO’s onder vuur nemen**

* *Dharma is een van de meest winstgevende ransomware-families*
* *Dharma is te vergelijken met franchise ransomware of ‘fastfood’: overal en gemakkelijk voor iedereen te verkrijgen*
* *Identificeert zichzelf als "Toolbox" en lanceert aanval met ‘Have fun, bro!’*

Oosterhout, 1 september 2020 – **Sophos heeft** [**‘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/)**’ gepubliceerd. Het rapport geeft inzicht in een geautomatiseerd aanvalsscript, naast een toolset die is gemaakt door ransomware-operators. Samen met back-end infrastructuur en kwaadaardige tools worden die aan cybercriminele kopers verkocht. Het rapport laat ook zien hoe Dharma zich in 2020 op kleine en middelgrote bedrijven (KMO) richt.**

Dharma is sinds 2016 bekend als een van de meest winstgevende ransomware-families, door het servicegebaseerde business model gericht op massamarkten. Onder meer de broncodes waarvan er vele varianten zijn, worden online beschikbaar gesteld of te koop aangeboden.

Het belangrijkste doel voor de Dharma RaaS-aanvallen die zijn geanalyseerd, zijn de KMO’s, waarbij 85% van de aanvallen in 2020 gericht was op blootgestelde toegangstools zoals Remote Desktop Protocol (RDP). Dat zegt het ransomware-herstelbedrijf Coveware, het bedrijf dat ook ontdekte dat de Dharma-losgeldeisen over het algemeen vrij laag waren (gemiddeld €7.270).

"Dharma is een franchise-ransomware, te vergelijken met fastfood: overal en gemakkelijk beschikbaar voor vrijwel iedereen", aldus Sean Gallagher, senior threat researcher bij Sophos. "Ransomware-as-a-service, zoals Dharma, vergroot het aantal mensen dat verwoestende ransomware-aanvallen kan uitvoeren. Dat is op zich al zorgwekkend in normale tijden. Maar op dit moment, nu veel bedrijven zich aanpassen aan de pandemie en tegemoetkomen aan de behoefte van snelle ondersteuning voor thuiswerkend personeel en een uitgedunde IT-afdeling, worden de risico's van deze aanvallen groter. Kleine bedrijven worden hierdoor kwetsbaar, en door deze situatie wordt IT-ondersteunend personeel belemmerd om systemen adequaat te bewaken en te beheren zoals ze dat normaliter zouden doen."

Afnemers van Dharma-ransomware leunen bijna volledig op een menugestuurd PowerShell-script dat de componenten installeert en opstart die nodig zijn om ransomware over het netwerk van het doelwit te verspreiden. Wanneer het masterscript wordt uitgevoerd, identificeert het zichzelf als ‘Toolbox’ en lanceert het de aanval met het bericht ‘Have fun, bro!’

Het aanvalsproces is onder meer sterk afhankelijk van het misbruik van open source-tools. Decodering is een verrassend ingewikkeld proces dat in twee fasen plaatsvindt. Slachtoffers die contact zoeken voor herstelsleutels krijgen een eerste-fase-tool die details van al hun gecodeerde bestanden onttrekt. Geassocieerden delen deze gewonnen gegevens vervolgens met hun operators, die een decoderingssleutel in de tweede fase voor de bestanden verstrekken. Hoe effectief dit proces is bij het daadwerkelijk herstellen van gegevens voor het doelwit, hangt volgens het Sophos-onderzoek sterk af van de vaardigheden en gemoedstoestand van die geassocieerden. Sophos zag bijvoorbeeld af en toe dat gelieerde ondernemingen een deel van de sleutels achterhielden als hefboom om extra losgeld te eisen.

"Met zoveel losgeldeisen van miljoenen dollars, spraakmakende doelwitten en geavanceerde tegenstanders zoals WastedLocker die het nieuws halen, kan het gemakkelijk zijn om te vergeten dat bedreigingen zoals Dharma springlevend zijn, waardoor een hele reeks cybercriminelen meerdere kleinere doelwitten in het vizier nemen om een ​​fortuin binnen te halen, achtduizend dollar per keer”, sluit Gallagher af.

**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, GSM 0497251816.