**Media alert**

**Matrix geanalyseerd:**

**“De trend voor gerichte ransomware zet zich voort”**

* *Sophos is in de ransomwarefamilie Matrix gedoken*
* *Primaire toegang via firewalls waarvoor Remote Desktop Protocol is ingeschakeld*
* *Zoals reeds aangegeven in Sophos Threat Report 2019: gerichte ransomware-aanvallen winnen aan populariteit*

Oxford, 30 januari 2019 - **Sophos heeft vandaag een rapport gepubliceerd over de ransomwarefamilie ‘Matrix’. Deze malware is actief sinds 2016 en Sophos heeft hiervan 96 samples gevolgd. Net als eerdere gerichte ransomware zoals BitPaymer, Dharma en SamSam hebben de aanvallers endpoints met Matrix geïnfecteerd, op netwerken ingebroken en deze endpoints via Remote Desktop Protocol besmet. In tegenstelling tot andere ransomwarefamilies richt Matrix zich slechts op één apparaat op het netwerk in plaats van zich door een organisatie te verspreiden.**

In het rapport heeft SophosLabs ’reverse engineering’ toegepast op technieken die door de aanvallers worden gebruikt, evenals methoden die zijn ingezet om slachtoffers financieel te duperen. De Matrix-criminelen hebben hun aanvalsparameters in de loop der tijd geraffineerd ontwikkeld waarbij nieuwe bestanden en scripts zijn toegevoegd om deze zo op het netwerk in te zetten.

Matrix-ransomwareregels zijn ingebed in de aanvalscode, maar slachtoffers weten niet hoeveel ze moeten betalen voordat ze contact met de aanvallers hebben opgenomen. Bij Matrix gebruiken cybercriminelen een cryptografisch beschermde, anonieme instant messaging-dienst (bitmsg.me) die inmiddels is stopgezet waarbij de ‘criminele auteurs’ zijn teruggekeerd naar het gebruik van normale e-mailaccounts. De kwaadaardigen achter Matrix vragen naar cryptocurrency als losgeld in de vorm van een equivalent van de dollar.

Het is onduidelijk of de vraag naar losgeld een opzettelijke poging tot misleiding is of slechts een poging om zich tussen fluctuerende wisselkoersen van cryptocurrency te begeven. Op basis van de communicatie die SophosLabs met de aanvallers had, bedroeg het losgeld 2.500 dollar. De aanvallers verlaagden uiteindelijk de losgeldsom toen de onderzoekers geen antwoord meer gaven over de vragen rondom de gestelde eisen.

Matrix is ​​te vergelijken met het *Swiss Army Knife* van de ransomwarewereld, met nieuwere varianten die in staat zijn om te scannen en potentiële computerslachtoffers te vinden nadat ze in het netwerk zijn ingebracht. Hoewel volumes klein zijn, maakt dat het niet minder gevaarlijk; Matrix evolueert continu en nieuwere versies verschijnen terwijl aanvallers lessen trekken uit iedere aanval.

Het [Sophos Threat Report 2019](https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-2019-threat-report.pdf) belicht het feit dat gerichte ransomware het gedrag van hackers stimuleert, en dat organisaties te allen tijde waakzaam moeten blijven.

**Sophos adviseert de volgende vier maatregelen:**

• Beperk de toegang tot afstandsbedieningsapplicaties zoals Remote Desktop en Virtual Network Computing;

• Voltooi kwetsbaarheidsscans en penetratietests over het netwerk; neem het recente testrapport door en houd cybercriminelen buiten;

• Gebruik multi-factor authenticatie voor gevoelige interne systemen, zelfs voor werknemers op het LAN of VPN;

• Creëer back-ups, zowel offline als offsite. Ontwikkel een noodherstelplan dat het herstel van data en systemen voor de hele organisaties beslaat.

Meer informatie vind je hier: [www.sophos.com/matrix](http://www.sophos.com/matrix)

**Voor meer persinformatie:**

Sandra Van Hauwaert, Square Egg Communications, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816.

**Over Sophos**

Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com).