"Diese neue Ransomware-as-a-Service-Familie steckt noch in den Kinderschuhen, aber unsere Ergebnisse deuten darauf hin, dass diese Ransomware in den Händen eines erfahrenen Angreifers großen Schaden anrichten kann."
Mark Loman, Director of Engineering bei Sophos

Ransomware-as-a-Service:
BlackMatter tritt aus dem DarkSide-Schatten

In einer neuen Analyse geben die Experten der SophosLabs einen Einblick in die Ransomware BlackMatter: demnach bestehen Ähnlichkeiten zur DarkSide Ransomware-as-a-Service (RaaS) und zu anderen Malwaregruppen wie REvil und LockBit 2.0. Viele Funktionen sind hierbei ähnlich, Details bleiben trotzdem individuell.

Wie hängen BlackMatter und die DarkSide RaaS zusammen? Sophos veröffentlicht Details, die auf den Analysen der Sophos Labs zur BlackMatter Schadsoftware beruhen, sowie auf den Erkenntnissen, die das Rapid Response Team aus einem Vorfall zog, in den BlackMatter involviert war.

Die Analyse beschreibt unter anderem neue, bislang unentdeckte Funktionen der BlackMatter Ransomware, wie sie die Dateiberechtigungen für jedes verschlüsselte Dokument zurücksetzt, um der Gruppe „Jeder" vollen Zugriff zu gewähren. Darüber hinaus geht es um Details, wie die Schadware über das gesamte Netzwerk verteilt wird sowie Informationen zu den Prozessen, die vor Bereitstellung der Ransomware beendet werden.

In der Untersuchung beschreiben die Sophos-Forscher außerdem, wie die von der BlackMatter-Ransomware verwendeten Taktiken, Techniken und Verfahren (TTPs) denen von DarkSide, REvil und LockBit 2.0 ähneln.
So präsentiert sich etwa ein "Zurücksetzen" des Hintergrundbildes in der Lösegeldforderung, das dem von DarkSide technisch sehr ähnlich ist. Ein Ansatz zur Multithreading-Dateiverschlüsselung erinnert ebenfalls DarkSide. Der Missbrauch des "abgesicherten Modus", wiederum gleicht sehr dem von REvil verwendeten Ansatz. Zudem zeigt sich eine Ausweitung der Rechte der Benutzerkontensteuerung (UAC), wie sie schon bei den Angriffen von DarkSide und LockBit 2.0 beobachtet wurde.
Auch die Verschlüsselung von Code-Strings, um eine statische Erkennung zu erschweren, gab es bereits bei DarkSide und REvil.

Mark Loman, Director of Engineering bei Sophos, bewertet die Ergebnisse so: „Unsere Analyse der Malware zeigt, dass es zwar Ähnlichkeiten mit DarkSide Ransomware gibt, der Code aber nicht identisch ist. Wie die mutmaßlichen Betreiber hinter der Ransomware behauptet haben, gibt es auch Ähnlichkeiten mit REvil und LockBit 2.0. Wir haben aber auch einige Merkmale gefunden, mit denen sich BlackMatter unterscheidet. Eines davon ist die Fähigkeit, Dateiberechtigungen zurückzusetzen, so dass jeder ein Dokument sehen kann. Eine Einstellung, an die IT-Administratoren denken müssen, um sie nach der Wiederherstellung von Dateien zurückzusetzen."

Die vollständige Analyse zur BlackMatter Ransomware finden Sie hier:
BlackMatter ransomware emerges from the shadow of DarkSide

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de