Hafnium-Nutznießer: Ist DearCry als Prototyp ins Rennen geschickt worden?

Seit dem Bekanntwerden der Microsoft-Exchange-Lücken letzte Woche stehen Cyberattacken im Fokus, die diese Schwachstelle ausnutzen. Allen voran macht sich hier die Ransomware „DearCry“ einen unrühmlichen Namen, die auf den ersten Blick an einen prominenten Vorgänger namens „WannaCry“ erinnert. Die Sophos Labs haben sich die neue Malware einmal genauer angesehen und viele Hinweise darauf gefunden, dass es sich hier um einen noch nicht bekannten Ransomware-Prototyp handeln könnte.

Zunächst fällt bei der Analyse verschiedener DearCry-Beispiele auf, dass die Ransomware einen hybriden Ansatz zu verfolgen scheint. Die einzige andere den SophosLabs bekannte Ransomware mit diesem Ansatz ist WannaCry, wobei diese sich automatisch verbreitet und nicht wie DearCry von Menschen gehandhabt wird. Die Gemeinsamkeiten sind jedoch verblüffend: Beide erstellen zuerst eine verschlüsselte Kopie der angegriffenen Datei (Copy Encryption) und überschreiben dann die Originaldatei, um eine Wiederherstellung zu verhindern (In Place Encryption). Während die Opfer bei Copy Encryption möglicherweise einige Daten wiederherstellen können, stellt die In Place Encryption sicher, dass eine Wiederherstellung der Daten über Recovery-Tools nicht möglich ist. Berüchtigte, von Menschen betriebene Ransomware-Vertreten wie Ryuk, REvil, BitPaymer, Maze oder Clop verwenden z.B. nur die direkte Verschlüsselung.

Es gibt eine Reihe weiterer Ähnlichkeiten zwischen DearCry und WannaCry einschließlich der Namen und des Headers, der den verschlüsselten Dateien hinzugefügt wird. Diese Hinweise bedeuten aber nicht automatisch eine Verbindung zu den WannaCry-Entwicklern, zudem sich die Fähigkeiten von DearCry erheblich von WannaCry unterscheiden. Die neue Ransomware verwendet keinen Befehls- und Kontrollserver, verfügt über einen eingebetteten RSA-Verschlüsselungscode, zeigt keine Benutzeroberfläche mit einem Timer an und verbreitet sich - was am wichtigsten ist - nicht auf andere Computer im Netzwerk.

„Wir haben eine Reihe anderer ungewöhnlicher DearCry-Merkmale gefunden, darunter die Tatsache, dass die Ransomware scheinbar neue Binärdateien für neue Opfer erstellt hat“, so Mark Loman, Director, Engineering Technology Office bei Sophos. „Die Liste der angegriffenen Dateitypen hat sich ebenfalls von Opfer zu Opfer weiterentwickelt. Unsere Analyse zeigt außerdem, dass der Code nicht die Art von Anti-Erkennungsfunktionen enthält, die wir normalerweise von Ransomware erwarten würden, wie z.B. komprimierte Dateien oder Verschleierungstechniken. Diese und andere Anzeichen deuten darauf hin, dass DearCry möglicherweise ein Prototyp ist, der schneller als geplant eingesetzt wurde, um die aktuellen Sicherheitslücken bei Microsoft Exchange Servern auszunutzen.“

Auch hier sei noch einmal darauf hingewiesen, dass Unternehmen die aktuellen Microsoft-Patches schnellstmöglich installieren sollten, um die kriminelle Ausnutzung ihres Exchange Servers zu verhindern. Wenn dies nicht möglich ist, sollte der Server vom Internet getrennt oder von einem Rapid Response Team genau überwacht werden. Zudem ist durch das Aufspielen des Patches nicht alle in Butter, sondern eine forensische Untersuchung muss sicherstellen, dass nicht bereits Schadsoftware über die Lücke ins System gekommen ist und auf ihren Einsatz wartet.

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