Neue Spam-Welle spült Ransomware in E-Mail-Postfächer - Bösartige E-Mails mit JavaScript-Anhängen besser sofort löschen

Vor einem dramatischen Anstieg gefährlicher Spam-Mails mit JavaScript-Anhängen warnt der europäische IT-Security-Hersteller ESET. Diese sind nicht nur lästig, sondern haben zudem die Ransomware namens "Shade" (oder auch "Troldesh") im Gepäck. Wer den JavaScript-Anhang unvorsichtigerweise anklickt, aktiviert ihn und lädt sich ungewollt die Erpressersoftware auf den eigenen Rechner. Aktuell schwappt die Spam-Welle von Russland aus in Richtung Deutschland.
"Bereits von Oktober bis Mitte Dezember 2018 beobachteten wir eine Spam-Kampagne, die Shade einsetzte. Seit Januar 2019 erleben wir wohl den Nachfolger", sagt Thomas Uhlemann, Security Specialist von ESET. Neben Russland sind die Ukraine, Frankreich und nun auch Deutschland betroffen. Offensichtlich stehen Unternehmen ganz gezielt im Fokus der Angreifer: "ESET-Telemetriedaten zeigen, dass die Angriffe exakt zu den Zeitpunkten pausieren, an denen Unternehmen ihre Arbeit reduzieren. Das war zum einen die Weihnachtszeit und zum anderen sind es die Wochenenden in der aktuellen Kampagne", erläutert Uhlemann.

Shade-Ransomware

Erstmals entdeckten Experten die Verschlüsselungs-Malware im Jahr 2014, die seitdem immer wieder mal ab- und auftauchte. Die Ransomware ist imstande, eine Vielzahl an Dateitypen auf der Festplatte zu verschlüsseln. Die Opfer der Angriffe können dann nicht mehr auf ihre im Rechner gespeicherten Informationen zugreifen. Sie erhalten lediglich die von anderen Angriffen dieser Art bekannten Zahlungsanweisungen. Diese Aufforderungen sind in einer TXT-Datei in Russisch und Englisch auf allen Laufwerken des infizierten Computers abgelegt.

Verbreitung per E-Mail und über manipulierte WordPress-Seiten
In Spam-Mails wird das JavaScript als getarnter Anhang "Information" versendet. Einmal extrahiert, lädt das Script einen bösartigen Loader herunter, der von ESET-Produkten als Win32/Injector erkannt wird. Das Perfide an der Methode ist die vermeintliche Quelle des sogenannten Loaders: Die Malware-Entwickler missbrauchen legitime WordPress-Webseiten als unfreiwillige Hosts. Diese werden über massive Brute-Force-Angriffe von Bots gekapert und dienen dann als Speicher für Bilddateien, die mit Schadcode verseuchten sind. ESET entdeckte bereits Hunderte dieser Dateien im Internet, die alle auf "ssj.jpg" enden. Um sich gegenüber dem Betriebssystem zu legitimieren, ist der Loader darüber hinaus mit einer vermeintlichen Signatur von Comodo versehen. Dadurch wird seine Identifizierung im System erschwert.

Schadcode tarnt sich als Systemprozess

Um sich noch besser zu tarnen, gibt sich der Loader als legitimer Systemprozess Client Server Runtime Process (csrss.exe) aus. Die Schadsoftware kopiert sich selbst in C:ProgramDataWindowsWindowscsrss.exe, wobei "Windows" ein versteckter Ordner ist, der von der Malware erstellt wurde. Er befindet sich normalerweise nicht im ProgramData-Verzeichnis. Die Malware, die sich nun als Systemprozess ausgibt, verwendet Versionsdetails, die von einer legitimen Windows Server 2012 R2-Binärdatei kopiert wurden.

So kann man sich effektiv schützen

Um nicht Opfer der neuen Ransomware-Welle zu werden, sollten Anwender immer die Authentizität von E-Mails prüfen, bevor sie Anhänge öffnen oder auf Links klicken. Für Gmail-Benutzer ist es nützlich zu wissen, dass Gmail JavaScript-Anhänge in empfangenen und gesendeten E-Mails bereits seit fast zwei Jahren blockiert.

Anwender können derartige Bedrohungen am besten durch einen zuverlässigen Malware-Schutz aussperren. Verschiedene Module in ESET-Sicherheitsprodukten erkennen und blockieren unabhängig voneinander bösartige JavaScript-Dateien. Auch Betreiber von WordPress-Websites können einiges tun, um nicht von Cyberkriminellen für ihre Zwecke missbraucht zu werden. Neben dem Einsatz einer hochwertigen Sicherheitslösung gehören die Nutzung eines sicheren Passworts sowie einer Zwei-Faktor-Authentifizierung. Ausserdem sollten Webseitenbesitzer unbedingt sicherstellen, dass WordPress selbst sowie WordPress-Plugins und -Designs regelmässig aktualisiert werden.