Neue Untersuchung von Sophos zeigt: Qakbot-Botnet wandelt auf Emotets Spuren und wird immer gefährlicher

Qakbot führt detaillierte Profil-Scans der infizierten Computer durch, lädt zusätzliche Module herunter und bietet eine ausgeklügelte Verschlüsselung. Ausgangspunkt für die Angriffe: Die Cyberkriminellen klinken sich geschickt in reale E-Mail-Kommunikationsstränge ein

Wiesbaden, 10. März 2022 – Sophos hat eine technische Analyse von Qakbot veröffentlicht,aus der hervorgeht, dass das Botnet immer fortschrittlicher und gefährlicher für Unternehmen wird. In dem Artikel Qakbot Injects Itself into the Middle of Your Conversations beschreiben die SophosLabs eine aktuelle Qakbot-Kampagne, die zeigt, wie sich das Botnet durch E-Mail-Thread-Hijacking verbreitet und eine Vielzahl von Profilinformationen von neu infizierten Computern sammelt. Dazu gehören unter anderem alle konfigurierten Benutzer:innen-Konten und -Berechtigungen, installierte Software und laufende Dienste. Das Botnet lädt darüber hinaus eine Reihe von zusätzlichen, bösartigen Modulen herunter, welche die Funktionalität des Kern-Botnets erweitern.

Der Malware-Code von Qakbot zeichnet sich durch eine unkonventionelle Verschlüsselung aus. Diese dient auch dazu, den Inhalt der Kommunikation zu verschleiern. Sophos hat die schädlichen Module sowie das Befehls- und Kontrollsystem des Botnets entschlüsselt und so herausgefunden, wie Qakbot seine Anweisungen erhält.

Die Qakbot-Infektionskette
Bei der von Sophos analysierten Kampagne fügte das Botnet schädliche Nachrichten in bestehenden E-Mail-Verkehr ein. Die E-Mails enthalten einen kurzen Satz und einen Link zum Download einer Zip-Datei, die eine schädliche Excel-Datei enthält. Die Benutzer:innen wurden aufgefordert, Inhalte zu aktivieren, um die Infektionskette zu aktivieren. Sobald das Botnet ein neues Ziel infiziert hatte, führte es einen detaillierten Profil-Scan durch, teilte die Daten mit seinem Command-and-Control-Server und lud dann mindestens drei verschiedene bösartige Module in Form von Dynamic Link Libraries (DLL) herunter, die dem Botnet eine breitere Palette an Möglichkeiten bieten.

Die eingeschleusten Module bestanden aus:
- Einem Modul, das Code zum Stehlen von Passwörtern in Webseiten einfügt
- Einem Modul, das Netzwerk-Scans durchführt und Daten über andere Rechner in der Nähe des infizierten Computers sammelt
- Einem Modul, das die Adressen von einem Dutzend SMTP-E-Mail-Servern (Simple Mail Transfer Protocol) ermittelt und dann versucht, eine Verbindung zu jedem einzelnen Server herzustellen und Spam zu versenden

Bekannte Vorläufer für einen Ransomware-Angriff
„Qakbot ist ein modulares Botnet, das für mehrere Zwecke einsetzbar ist und per E-Mail verbreitet wird. Cyber-Kriminelle nutzen es als Zustellungs-Tool für Malware immer häufiger, ähnlich wie Trickbot und Emotet“, sagt Andrew Brandt, Principal Threat Researcher bei

Sophos. „Unsere Analyse zeigt die Erfassung detaillierter Opferprofildaten, die Fähigkeit des Botnets, komplexe Befehlssequenzen zu verarbeiten sowie eine Reihe von Modulen, die die Funktionalität der zentralen Botnet-Engine erweitern."

Botnet-Infektionen sind ein bekannter Vorläufer für einen Ransomware-Angriff. Dies liegt nicht nur daran, dass Botnets potenziell Ransomware liefern. Botnet-Entwickler:innen können auch ihren Zugang zu den infizierten Netzwerken verkaufen oder vermieten. So sind die Sophos-Teams beispielsweise auf Qakbot-Samples gestoßen, die Cobalt Strike Beacons, also den ersten Fuß in der Tür zum Unternehmensnetzwerk, direkt an einen infizierten Host liefern. Sobald Qakbot-Betreiber den infizierten Computer benutzt haben, können sie den Zugang zu diesen Beacons an ihre Kundschaft weitergeben, vermieten oder verkaufen.

Was tun gegen Qakbot?
Sophos empfiehlt, ungewöhnlichen oder unerwarteten E-Mails mit Vorsicht zu begegnen, selbst wenn es sich bei den Nachrichten um Antworten auf bestehendem E-Mail-Verkehr zu handeln scheint. In der von Sophos untersuchten Qakbot-Kampagne war die Verwendung lateinischer Ausdrücke in URLs ein potenzielles Warnsignal.

Zudem sollten Sicherheitsteams überprüfen, ob die von ihren Sicherheitstechnologien bereitgestellten Verhaltensschutzmechanismen eine Qakbot-Infektion verhindern. Netzwerkgeräte warnen Administratoren auch, wenn ein infizierter Benutzer versucht, sich mit einer bekannten Command-and-Control-Adresse oder -Domäne zu verbinden. Sophos Endpoint-Produkte, wie z.B. Intercept X, schützen Anwender:innen, indem sie die Aktionen und Verhaltensweisen von Angreifern erkennen.

Weitere Informationen sind unter Qakbot Injects Itself into the Middle of Your Conversations bei SophosLabs Uncut erhältlich.

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

Über Sophos
Sophos ist ein weltweit führender Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Verbrauchern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen

Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist in Oxford, U.K. Weitere Informationen unter http://www.sophos.de.

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