E-Mail-Bombing und Voice Phishing: Cyberkriminelle missbrauchen Microsoft Teams als Einfallstor

Sophos X-Ops hat eine aktive Bedrohungskampagne näher untersucht, bei der zwei verschiedene Gruppen von Bedrohungsakteuren Unternehmen infiltrieren, indem sie die Funktionalität der Office-365-Plattform missbrauchen und anschließend versuchen, Daten abziehen oder Ransomware platzieren. Besonders perfide: die Angreifer verwenden eine Kombination aus E-Mail-Bombing mit bis zu 3.000 Nachrichten in weniger als einer Stunde und anschließenden Sprach- bzw. Videoanrufen via Teams, auch als Voice Pishing oder Vishing bekannt.

Nach dem Versenden der ersten Spam-Nachrichten geben sich die Angreifer als technischer Support des betroffenen Unternehmens aus, rufen über Teams an und bieten ihre „Hilfe“ bei der Lösung des Problems an. Wenn der Mitarbeiter den Anruf entgegennimmt und den Kriminellen mittels Quick Assist oder der Bildschirmfreigabe von Microsoft Teams die Kontrolle über den Computer erteilt, starten die Anrufer das Ausrollen der Schadsoftware. Im Rahmen seiner Untersuchungen hat Sophos X-Ops Verbindungen der in dieser Kampagne aktiven Cyberkriminellen zu den russischen Bedrohungsgruppen Fin7 und Storm-1811 aufgedeckt.

Die Einschätzung von Sean Gallagher, Principal Threat Researcher bei Sophos: „Obwohl die Ausnutzung von Fernverwaltungstools und der Missbrauch legitimer Dienste an sich nicht völlig neu sind, beobachten wir, dass immer mehr Bedrohungsgruppen diese Taktiken anwenden, um Unternehmen jeder Größe ins Visier zu nehmen. Dies ist eine aktive Bedrohungskampagne, die wir weiterhin intensiv verfolgen. Da die Standardkonfiguration von Microsoft Teams es jedem Besitzer eines Teams-Kontos ermöglicht, zu chatten oder Mitarbeiter eines Unternehmens anzurufen, sind viele Unternehmen potenziell anfällig für diese Bedrohung. Zudem nutzen viele Unternehmen externe Anbieter für ihren IT-Support, sodass ein Anruf von einer fremden Nummer mit der Bezeichnung „Helpdesk-Manager“ nicht unbedingt Alarmglocken schrillen lässt. Da Sophos weiterhin neue MDR- und IR-Fälle im Zusammenhang mit diesen Taktiken sieht, raten wir Unternehmen, die Microsoft 365 verwenden, in höchster Alarmbereitschaft zu sein. Sie sollten Konfigurationen überprüfen sowie externe Kontonachrichten sowie Fernzugriffstools, die nicht regelmäßig verwendet werden, nach Möglichkeit blockieren.“

Eine detaillierte Analyse der Angriffe finden sich im englischsprachigen Blogartikel „Sophos MDR tracks two ransomware campaigns using email bombing and Microsoft Teams vishing“.

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/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
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