Ein Paket in der Schweiz:
Bei Anruf Scam

Zuerst traf es ein Schweizer Unternehmen: Sophos entdeckt ausgeklügelte neue Kompromittierungsmethoden und Social Engineering-Techniken.
Die Kombination von Telefon- und E-Mail-Ködern in dieser komplexen Angriffskette weist auf neue Taktiken hin, die von Cyberkriminellen eingesetzt werden, um ihre Malware zu verbreiten.

Sophos hat im Rahmen der Untersuchung eines infizierten Computers eine perfide, kombinierte Angriffstaktik offengelegt: Alles begann mit einem harmlos klingenden Anruf.

Die analysierten Informationen zeigen eine komplexe neue Angriffstaktik, die glaubwürdige Telefon- und E-Mail-Kommunikation miteinander kombiniert, um die Kontrolle über Unternehmensnetzwerke zu übernehmen und Daten abzuführen. Die Malware selbst wurde dabei auf äußerst ungewöhnliche Weise geliefert: ein Anrufer überzeugte das Angriffsziel, eine E-Mail-Nachricht zu öffnen, die keinen Text enthielt, sondern als Grafik gestaltet war, um einer Outlook-E-Mail-Nachricht zu ähneln. Damit wurde der Download einer verlinkten bösartigen Electron-App ausgelöst.

„Ich möchte eine Lieferung an Ihren Standort bringen."
Der Anrufer erklärte dem Mitarbeiter, er sei ein Lieferfahrer mit einem dringenden Paket für einen der Unternehmensstandorte, aber niemand sei dort, um das Paket in Empfang zu nehmen. Er bat um eine neue Lieferadresse am Standort des Mitarbeiters. Um das Paket erneut zustellen zu können, müsse der Mitarbeiter ihm einen Code vorlesen, den die Versandfirma per E-Mail senden würde. Noch während der Anrufer am Telefon mit dem Mitarbeiter sprach, erhielt dieser die angekündigte E-Mail-Nachricht. Die E-Mail-Nachricht besagte, dass eine an die Nachricht angehängte PDF-Datei den erforderlichen Code enthielt.

Diese E-Mail, in perfektem Französisch verfasst, löste die anschließende Angriffskette aus. Tatsächlich war die gesamte Nachricht ein Fake, der nur aussah wie eine E-Mail mit einem PDF-Anhang. Sowohl der "Anhang" als auch die Textnachricht waren in Wirklichkeit nur statische Bilder, die in den Nachrichtentext eingebettet waren. Unter Anleitung des Betrügers am Telefon klickte der Mitarbeiter auf das Bild, was zum Download der Malware führte.

Sie wussten: Man(n) spricht deutsch
Obwohl die E-Mail-Nachricht wie erwähnt in französischer Sprache verfasst war, deuten technische Hinweise darauf hin, dass die Angreifer bereits wussten, dass die Schweizer Zielperson möglicherweise deutschsprachig ist. Die Sophos-Analysten konnten zudem nachvollziehen, dass die Angreifer möglicherweise den Anrufempfänger persönlich ins Visier genommen hatten und eine aufwändige Social Engineering-Angriffskette erstellten. Diese führte dazu, dass die Cyberkriminellen kurzzeitig die Kontrolle über den Computer des Mitarbeiters übernahmen, bevor dieser buchstäblich den (Ethernet-)Stecker aus dem kompromittierten Computer zog. Der aufmerksame Mann spürte, dass etwas nicht stimmte und trennte den infizierten Computer vom Netzwerk. Leider jedoch nicht mehr rechtzeitig, bevor die schädliche Nutzlast aktiv war.

"Dieser Angriff war äußerst gezielt. An diesem Freitag war nur eine Person im Büro, und die Angreifer kannten wahrscheinlich die Identität dieser Person. Die Verwendung eines Bildes, das sich als E-Mail tarnt, ist ebenfalls etwas, das wir bisher nicht gesehen haben. Allerdings ist es clever. Das Anhängen eines tatsächlichen PDF löst oft Alarm auf Systemen aus, da sie

häufig zur Verbreitung von Malware verwendet werden, und E-Mails mit PDFs landen oft in Spam-Filtern", sagte Andrew Brandt, Principal Researcher bei Sophos.

Nach dem Eindringen in das Netzwerk nutzten die Kriminellen Malware, um nach einer Vielzahl von Informationen zu suchen, einschließlich Buchhaltungssoftware-Daten, Cookies, Browsing-Verlauf sowie Passwörtern und Kryptowährungs-Wallets. Um ihre Datenausschleusung zu verbergen, verbanden die Angreifer das System mit Tor (dem Dark Web). Der Mitarbeiter, der den Braten schließlich roch und den Stecker zog, verhinderte schlimmere Folgen für sein Unternehmen.

Gekonnt „gescamt“ und es geht bereits weiter
"Diese Art von hoch raffiniertem Angriff zeigt, wie weit Cyberkriminelle gehen, um Abwehrwerkzeuge zu umgehen und das Vertrauen von Menschen zu gewinnen. Phishing-Angriffe sind äußerst effektiv, und wir haben gesehen, wie Angreifer ihre Social Engineering-Taktiken mit neuer Technologie weiterentwickeln. Obwohl Angreifer heutzutage eher E-Mails verwenden, bedeutet das nicht, dass Telefonanrufe veraltet sind. Wir schulen Mitarbeitende viel im Bereich E-Mail-Sicherheit, aber wir lehren sie nicht unbedingt, wie sie mit ungewöhnlichen Telefonanrufen umgehen sollen. In diesem Fall hat der Mitarbeiter schnell reagiert und geistesgegenwärtig gehandelt," sagte Brandt.

Nach dem Angriff auf das Schweizer Unternehmen entdeckte Sophos X-Ops einen weiteren Angriff mit demselben Vorgehen gegen ein Unternehmen in Australien. Welche Gruppe auch immer hinter diesen Angriffen steckt – sie ist wahrscheinlich immer noch aktiv, und Sophos wird die Situation überwachen.

Die gesamte, auch technisch detailliertere Beschreibung des Angriffs lesen Sie unter
https://news.sophos.com/en-us/2023/08/10/image-spam-attack/

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