From Russia with love: Ausgefeilte Social-Engineering-Kampagne hat es auf Zugangsdaten von 800 Organisationen abgesehen

Innerhalb von 51 Tagen verschickte eine Gruppe von Angreifern, die vermutlich aus Russland stammt, mehr als 2.000 Phishing-E-Mails an fast 800 Unternehmen und Organisationen aus den Bereichen Regierung, Gesundheitswesen, Energie und kritische Infrastrukturen. Die Ziele befanden sich in Großbritannien, Australien, Frankreich, Deutschland, Österreich, Italien sowie in den USA und Niederlanden.

Die E-Mails zeichneten sich durch eine ungewöhnliche, hochgradig personalisierte Technik aus: die Einbettung eines Webseiten-Logos, das von einer eigenen Seite der Zielperson stammt, in die Phishing-Seite selbst. Nach dem Öffnen wurden die Zielpersonen aufgefordert, ihre Passwörter in die Anmeldeseite der scheinbar eigenen Webseite einzugeben. Anschließend schleusten die Angreifer die gestohlenen Passwörter in ihre Telegram-Kanäle ein.

Offenbar haben die Angreifer das Wissen über online nachvollziehbare Communities ausgenutzt, wodurch das Sophos-Team auf die Kampagne aufmerksam wurde. Andrew Brandt von Sophos X-Ops erhielt zunächst eine E-Mail von einem der Angreifer, als er für die örtliche Schulratswahl in Boulder, Colorado, USA, kandidierte, wobei der Angreifer vorgab, einer seiner Mitkandidaten zu sein. Als die ersten BEC-E-Mails (Business Email Compromise) fehlschlugen, wechselten die Angreifer zu Phishing-E-Mails und schickten Andrew eine E-Mail mit einem Anhang, der die Anmeldeseite für seine scheinbar persönliche Kampagnen-Website enthielt.

„Die BEC-Kampagne war zwar recht einfach gestrickt, zeigt jedoch, dass die Angreifer geschickt eine Analyse der online verfügbaren, sozialen Kontakte im Umfeld der Zielperson ausnutzen, um möglichst realistisch zu wirken“, so Andrew Brandt. „Bedeutend ausgefeilter war hingegen der nachfolgende Social-Engineering-Versuch. Die Verwendung von grafischen Elementen, die die Zielperson selbst nutzt, zeigt die Raffinesse, mit der Betrüger ihre Attacken mittlerweile vorbereiten.“

Detaillierte Einblicke in die Social-Engineering-Kampagne finden Sie im englischsprachigen Report „From Russia with Love: Credential Theft Attack Uses Sophisticated Social Engineering Techniques to Target 800 Organizations Worldwide”.

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