Cyberattacken auf Hotels: gefälschte Beschwerden, vermeintliche Anfragen, schadhafte Dokumentationen

Kriminelle nutzen zunehmend den wohlmeinenden Servicegedanken von Hotelmitarbeitenden aus: Sophos X-Ops hat mehrere Fälle einer ungewöhnlichen „Malspam"-Kampagne aufgedeckt, die sich an Hotels auf der ganzen Welt richtet und mit Hilfe einer Social-Engineering-Komponente konkret die Emotionen des Servicepersonals ausnutzt. Die Attacken mit der Schadsoftware RedLine Stealer, die auf das Abschöpfen von Zugangsdaten spezialisiert ist, konnte aktuell in Spanien, Frankreich, Deutschland, der Schweiz, den Vereinigten Arabischen Emiraten sowie in den USA nachgewiesen werden.

Es startet mit Phishing und gefälschten Beschwerden oder harmlos wirkenden Anfragen
Die Angreifer melden sich zunächst mit Beschwerden über schwerwiegende Probleme, die der Absender angeblich bei einem kürzlichen Aufenthalt im angeschriebenen Hotel hatte, oder mit der Bitte um Informationen, die bei einer möglichen zukünftigen Buchung helfen könnten. Zu diesen gefälschten Beschwerden gehören Geschichten über gestohlene Gegenstände, Krankheiten im Hotel, Allergien gegen Reinigungsmittel und sogar versuchte Vergiftungen.

...dann folgt die Schadsoftware passwortgeschützt
Sobald das Hotelpersonal auf den ersten Phishing-Versuch reagiert, antworten die Angreifer mit einer umfangreicheren „Dokumentation" entweder für die Informationsanfrage oder die Beschwerde. Dabei handelt es sich um eine passwortgeschützte Archivdatei, die die Schadsoftware enthält. Sobald die Datei aktiviert wird, kommt RedLine Stealer zum Einsatz. Auch wenn diese Malware nicht besonders ausgefeilt ist, kann der Schaden doch enorm sein. Mit den gestohlenen Zugangsdaten können sich die Cyberkriminellen Zugang zu weiteren Hotelanlagen zu verschaffen oder entwendete Informationen an andere Kriminelle verkaufen. Während sich dieser Angriff direkt gegen Hotelmanager oder Mitarbeiter richtet, stellt die Gefährdung der Privatsphäre von Hotelgästen einen potenziell riesigen Kollateralschaden dar.

Appell ans Hotelpersonal: Obacht, wenn Anfragende Informationen verweigern
Andrew Brandt, Principal Threat Researcher bei Sophos, zu der neuen Masche: „Ein solcher Angriff, bei dem wohlmeinende Hotelmanager und Mitarbeiter ausgenutzt werden, kann nicht nur dem Hotel, sondern auch den dort übernachtenden Gästen Probleme bereiten, die sich aus verschiedenen Gründen auf die Diskretion des Hotelpersonals verlassen. Denn solche Attacken nehmen dem Hotelpersonal die Möglichkeit, die Privatsphäre der Kunden zu schützen, wenn die gestohlenen Zugangsdaten missbraucht werden. Hotelmitarbeiter und Frontline-Manager sollten besonders vorsichtig sein, wenn die Person, die das Hotel kontaktiert, sich weigert, in der Nachricht selbst grundlegende Informationen anzugeben, wie z. B. den Namen des registrierten Gastes, dessen Aufenthaltsdaten oder die Reservierungsnummer. Aus technologischer Sicht schieben ein moderner Endpoint-Schutz sowie Zweifaktorauthentifizierung vielen dieser Angriffe einen Riegel vor."

Weitere Infos und Beispiele zu der "Hospitality-Spamkampagne" finden sich im englischsprachigen Sophos-Blog.

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, 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