SophosLabs enthüllt: Wie Cyberbetrüger Google-Formulare nutzen

Phishing und Schadsoftware ebnen oft den Weg für Ransomware oder Datendiebstahl. Die aktuellste Analyse der SophosLabs zeigt, wie die Betrüger Google Forms für ihre Zwecke nutzen.

Sophos hat unter dem Titel: „Phishing and Malware Actors Abuse Google Forms for Credentials, Data Exfiltration“ einen neuen Analysereport veröffentlicht, der sich mit der missbräuchlichen Nutzung von Google Forms durch Cyberkriminelle beschäftigt.

„Das Ausmaß, mit dem Angreifer Google Forms für sich verwenden, kam ans Licht, als wir untersuchten, wie Schadsoftware die Verschlüsselung missbraucht, um Aktivitäten und Kommunikation zu verschleiern“, erklärt Sean Gallagher, Senior Threat Researcher bei Sophos. „Google Forms macht es Cyberkriminellen dabei besonders leicht: die Formulare sind einfach umzusetzen und vertrauenswürdig, sowohl für die Organisation als auch für den Konsumenten. Der Datenstrom zu und vom Service ist durch Transport Layer Security (TLS)-Verschlüsselung geschützt, so dass er sich nicht so einfach von den Verteidigern inspizieren lässt. Das ganze Set-up beinhaltet also im Wesentlichen eine kostenlose Angriffsinfrastruktur.“

Die Analyse zeigt, dass der häufigste Missbrauch von Google Forms in den Bereichen Phishing und Betrug stattfindet, was eher wenig Qualifikation erfordert. Zunehmend lassen sich aber Anzeichen beobachten, dass Angreifer die Plattform für komplexere Attacken nutzen. In den Beispielen setzten die Kriminellen Google Forms für Datenexfiltration und Schadsoftware Command-and-Control ein.

Sieben Arten der kriminellen Nutzung von Google Forms fielen den Sophos-Analysten besonders ins Auge:

1. Phishing: Google warnt Nutzer auf jeder Seite von Forms, keine Passwort-Details preiszugeben. Dennoch fanden die Sophos-Experten verschiedene Beispiele, bei denen Angreifer potenzielle Opfer dazu bringen wollten, ihre persönlichen Zugangsdaten in ein gefälschtes Google Formular einzutragen. Diese sind oft verbunden mit schadhaften Spam-Kampagnen.

2. Schadhafte Spam-Kampagnen: Eine der größten Quellen für diese Phishing-Links im Spam waren „Abmeldelinks“ in betrügerischen Marketing-E-Mails. Sophos fing eine Reihe dieser Phishing-Kampagnen ab, die es auf Microsoft-Online-Konten, inklusive Office365, abgesehen hatten. In den Spams hieß es, dass die E-Mail-Konten des Empfängers geschlossen werden, wenn er diese nicht sofort verifiziert. Dabei wurde ein gefälschter Link mitgeschickt, der zwar mit Microsoft-Grafiken versehen war, aber bei dem es sich ganz eindeutig nicht um ein echtes Google-Formular handelte.

3. Diebstahl von Zahlungskarten: Betrüger auf Anfängerniveau verwenden vorgefertigte Google-Forms-Entwurfsvorlagen gerne, um Daten aus Kartenbezahlungen mithilfe von gefälschten und scheinbar sicheren E-Commerce-Seiten zu stehlen.

4. PUAs (Potentially Unwanted Applications), wie zum Beispiel Werbesoftware: Besonders Windows-Nutzer sind oft davon betroffen. Diese Anwendungen gebrauchen Google-Forms-Seiten heimlich, während die Web-Anfragen gesammelt und automatisch an die Formulare weitergeleitet werden – eine Nutzer-Interaktion ist nicht nötig.

5. Gefälschte Nutzeroberfläche für schädliche Android-Apps: Sophos entdeckte einige schadhafte Android-Anwendungen, die Google Forms dazu verwenden, Daten zu erfassen ohne eine Backend-Webseiten programmieren zu müssen. Die meisten dieser Apps waren Werbesoftware oder PUAs, so auch SnapTube, eine Video-App, die Entwicklern Einnahmen via Werbebetrug generieren und die eine Google-Formular-Seite für Bewertungen beinhaltet.

6. Datenlöschung: Die Analysten spürten eine Anzahl von noch raffinierteren Bedrohungen auf, die Google Forms für sich nutzen. Dazu gehören beispielsweise schadhafte Windows-Anwendungen, die Web-Anfragen an Google Forms einsetzen, um gestohlene Computerdaten in eine Google-Tabelle zu „schieben".

7. Teil einer größeren, bösartigen Cyberangriff-Infrastruktur: Sophos hat eine Nummer von PowerShell-Skripten entdeckt, die mit Google Forms interagieren. Die Experten waren dann in der Lage nachzustellen, wie ein PowerShell-Skript dazu verwendet werden kann, Windows Profildaten von einem PC einzusammeln und automatisch in ein Google-Formular einzufügen.

Sean Gallagher empfiehlt außerdem: „Google schließt häufig Konten, die mit einem massenhaften Missbrauch von Anwendungen in Verbindung stehen, inklusive Google Forms. Eine seltenere aber gezielte Nutzung von Google Forms durch Schadsoftware könnte allerdings unentdeckt bleiben. Anwender sollten deshalb hellhörig werden, wenn sie Links auf Google-Formulare oder andere scheinbar legitime Links zur Berechtigungsfreigabe entdecken und dabei nicht blind TLS-Traffic zu scheinbar bekannten Domains, wie doc.google.com, vertrauen."

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 www.sophos.de.

Neu: 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
Ariane Wendt +49-172-4536839
sophos@tc-communications.de