Sprunghafter Anstieg von Phishing-Attacken mit SVG-Grafikdateien

Malware und Phishing, die über die beliebten und viel genutzten SVG-Grafik- und Bilddateien eingeschleust werden, erleben nach den Beobachtungen von Sophos X-Ops seit Januar 2025 einen rasanten Anstieg.

In einem neuen Report von Sophos X-Ops berichten die Sicherheitsexperten von einem sprunghaften Anstieg von Malware- und Phishing-Angriffen, die mit Hilfe von SVG-Dateien durchgeführt werden. Die Cyberkriminellen nutzen das weit verbreitete SVG-Grafikformat verstärkt für ihre Zwecke und versuchen damit die automatische Erkennung von Phishing- und Spamschutzlösungen zu umgehen.

Unter Beobachtung stehen die maliziösen Machenschaften mit dem SVG-Bildformat seit 2024. Das skalierbare SVG-Vektorgrafik-Dateiformat (Scalable Vector Graphics) ist die vom World Wide Web Consortium (W3C) empfohlene Spezifikation zur Beschreibung zweidimensionaler Vektorgrafiken und seit 2001 in Gebrauch. Alle gängigen Browser unterstützen SVG und weltweit haben weit über die Hälfte aller Webseiten SVG-Grafiken im Einsatz.

Die generellen Vorteile von SVG sind der Grund, weshalb auch Cyberkriminelle zunehmend intensiv auf dieses Format für ihre illegalen Aktivitäten setzen. Einerseits lässt die weite Verbreitung von SVG-Grafiken diese für den Anwender auch in Phishing-E-Mails als ungefährlich erscheinen. Auf der anderen Seite nutzen die Cyberkriminellen die Tatsache, dass SVG-Formate im Vergleich zu anderen, rein binären Bild-Formaten wie JPG oder TIF, auch einen Teil XML-Code im Gepäck haben. Dies ermöglicht es den Angreifenden, ihren Code leicht einzubinden und unbemerkt zu transportieren. Beim Empfänger oder Anwender lösen die Grafik-Dateien nach dem Öffnen – das vielfach automatische erfolgt – ihre bösartigen Aktionen unbemerkt im Hintergrund aus.

„Dass Cyberkriminelle das SVG-Dateiformat für ihre Angriffe nutzen, wissen wir und wir haben unsere Spam- und Phishing-Schutzlösungen auf diese Angriffsvariante vorbereitet. Das perfide an dieser Angriffsmethode ist, dass der Anwendende keinerlei Anhaltspunkte mehr bekommt, um zu entscheiden, ob etwas Phishing ist oder nicht. Beim Einbetten von Malware in den XML-Code läuft alles im Hintergrund ab. Die wichtige Sicherheitskomponente, die ein verantwortungsvoller Mitarbeitender darstellt, ist damit weitgehend ausgeschaltet. Ergo müssen die technischen Erkennungsmethoden inklusive KI umso mehr darauf trainiert sein, ungewöhnliches Verhalten auf Arbeitsrechnern und im Netzwerk zu erkennen und abzuwehren“, erklärt Michael Veit, Cybersecurity-Experte bei Sophos.

Laut Sophos X-Ops nimmt die Raffinesse der Angriffe mit dem SVG-Dateiformat zu. Zudem haben die Cyberkriminellen ihre Methoden verfeinert, um noch überzeugender zu wirken. Jetzt fanden die Security-Spezialist:innen in diesem Zusammenhang auch lokalisierte Phishing-Seiten, die auf die Landessprachen ihrer Angriffsziele abgestimmt sind.

Die neuesten Erkenntnisse zur böswilligen Nutzung von SVG-Dateiformaten für Phishing-Angriffe werden vom Sophos X-Ops Team hier detailliert beschrieben: https://news.sophos.com/en-us/2025/02/05/svg-phishing/

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