Makros sind out, Malvertising ist in: Kriminelle nutzen manipulierte KI-Anzeigen für sich

Cyberkriminelle sind heutzutage Betrüger mit Trendbewusstsein! Den Hype um Künstliche Intelligenz nutzen sie geschickt für ihre Zwecke: in manipulierten Anzeigen rund um KI platzieren sie Banking-Trojaner und Infostealer. Die Sophos-Forensiker haben sich diesen Malvertising-Fall genauer angesehen.

Sophos X-Ops verzeichnet seit Anfang dieses Jahres eine Wiederbelebung des Einsatzes von Malvertising in verschiedenen Malware-Kampagnen, sowohl in seiner Telemetrie als auch im vermehrten Auftauchen dieses Themas in Untergrundforen. Malvertising, die Bezeichnung für eine Methode, schädlichen Code in digitale Werbung zu injizieren, ist kein neues Thema und auch kein neues TTP für Angreifer.

Allerdings kommt die Technik in den letzten Monaten wieder vermehrt zum Einsatz, möglicherweise aufgrund der neuen Schutzmaßnahmen von Microsoft gegen bösartige Makros aus dem Internet – ebenfalls eine beliebte Übermittlungsmethode für Schadcodes.

Bei der aktuellen Untersuchung eines kriminellen Marktplatzes fand X-Ops eine Reihe von Anzeigen für manipulierte Google Ads-Konten und sogenannte „Black SEO"-Services. Dabei handelt es sich um Dienste, die Angreifern dabei helfen sollen, ihre bösartigen Websites ganz oben in den Suchergebnissen zu platzieren.

BatLoader und IcedID – die Malvertising-Stars
Zwei der bemerkenswertesten Malware-Familien, die sich in den letzten Monaten Malvertising zunutze gemacht haben, sind BatLoader und IcedID. IcedID tauchte erstmals im Jahr 2017 als Banking-Trojaner auf, der darauf ausgelegt war, Bankzugangsdaten zu stehlen. In jüngerer Zeit haben Angreifer IcedID eingesetzt, um als erste Stufe eines Ransomware-Angriffs Zugriff auf gezielte Netzwerke zu erhalten. Frühere IcedID-Malvertising-Angriffe beinhalteten bösartige Anzeigen, die über Google-Anzeigen für bürobezogene Kommunikationstools wie Slack, Microsoft Teams und WebEx verbreitet wurden.
BatLoader ist traditionell ein Tool für Cyberkriminelle, um Nutzersysteme mit ausgefeilter Malware zu infizieren, insbesondere mit Infostealern wie RaccoonStealer. Während frühere Malvertising-Kampagnen mit BatLoader die Suche der Anwender nach IT-Tools ausgenutzt haben, machen sich neuere Kampagnen den Hype um Künstliche Intelligenz zunutze.

Christopher Budd, Director Threat Research bei Sophos X-Ops: „Malvertising hat für Kriminelle viele Vorteile. Genauso wie seriöse Werbetreibende ihre Anzeigen sorgfältig ausrichten, können Kriminelle Malvertising nutzen, um Nutzer gezielt anzusprechen, insbesondere in geografischer Hinsicht. Zudem ist es für Verteidiger oft schwierig, diese Art von Malware-Kampagnen aufzuspüren und zu bekämpfen. Grundsätzlich haben wir festgestellt, dass die Angreifer technischen Trends folgen. So versuchen die neuesten, schädlichen Anzeigen nicht nur mit beliebten IT- und Kommunikations-Apps, sondern auch mit KI-Tools wie ChatGPT oder MidJourney Klicks zu generieren. Hier ist erhöhte Wachsamkeit geboten, zudem es sehr wahrscheinlich ist, dass Kriminelle ihre Malvertising-Kampagnen weiter ausbauen und professionalisieren werden."

Detaillierte Infos zu den X-Ops-Untersuchungen gibt es in dem englischen Blogbeitrag „Malvertising campaigns using paid ads result in infostealer and backdoor attacks".

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