Anatomie eines Atomic Stealer-Angriffs

Erfahren Sie, wie Atomic Stealer den Sprung von Social Engineering zum Diebstahl von Zugangsdaten schafft und so den Weg für tiefgreifende Kompromittierungen ebnet.

1

Aufklärungsarbeit

Bedrohungsakteure sammeln zuerst einmal Informationen über ihr Ziel, um sich auf den Angriff vorzubereiten.

BEISPIEL: Social-Engineering-Kampagnen identifizieren und erstellen Profile von Opfern.

2

Beschaffung von Tools

Cyber-Angriffstools basieren auf gewonnenen Erkenntnissen und werden gezielt für ihren Einsatz angepasst.

BEISPIEL: Bösartiger Code wird in eine legitim aussehende Anwendung eingebettet.

3

Verbreitung und Angriff

Die bösartige Anwendung wird über betrügerische Kanäle verbreitet.

BEISPIEL: Gesponserte Werbung verleitet Benutzer zum Herunterladen einer gefälschten App.

4

Ausnutzung von Schwachstellen

Eine gefälschte Eingabeaufforderung bringt den Benutzer dazu, Anmeldedaten preiszugeben.

BEISPIEL: Über eine manipulierte Update-Aufforderung werden Logins und vertrauliche Daten gestohlen.

5

Installation

Persistenzmechanismen erhalten den dauerhaften Zugriff nach der ersten Kompromittierung aufrecht.

BEISPIEL: Eine versteckte Hintertür ermöglicht den kontinuierlichen Zugriff auf das Gerät.

6

Übernahme & Kontrolle (C2)

Gestohlene Anmeldedaten werden für den Zugriff auf weitere Systeme und Daten verwendet.

BEISPIEL: Die Angreifer nutzen C2, um ihre Zugriffsrechte zu erweitern und sich im Netzwerk zu bewegen.

7

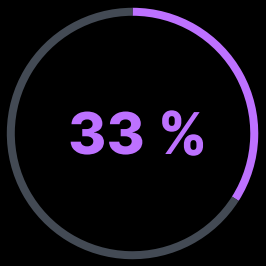
Aktionen zur Erreichung der Ziele

Angreifer nutzen den Zugang, um großflächig Schaden anzurichten.

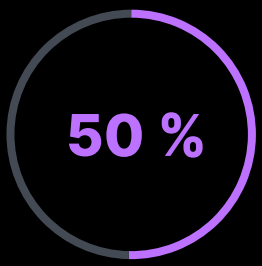
BEISPIEL: Account-Übernahme, Seitwärtsbewegung, Datendiebstahl und Erpressung.

jamf

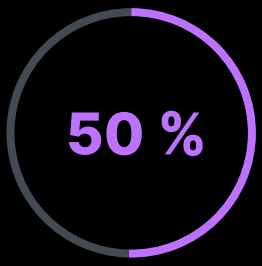
Warum AMOS wichtig ist



Infostealer-basierte Malware



Trojaner-basierte Angriffe



der Bedrohungen entziehen sich der Erkennung

QUELLE: **Jamf Security 360: Jährlicher Trendbericht für Macs 2026**

Holen Sie sich das White Paper