Malicious Browser Plugins

The attackers install plugins in the browser. This can be used as part of C2 and persistence. The browser is the new endpoint.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Firewall Log Review
Network Threat Hunting - Zeek/RITA Analysis

TOOLS

Grammarly is a Keylogger
graniet/chromebackdoor

https://www.kaspersky.com/blog/browser-extensions-security/20886

https://github.com/graniet/chromebackdoor

Backdoors & Breaches™

PERSISTENCE

Created by: **BLACK HILLS** | Information Security