مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

DarkSpectre Browser Extension Threat Campaign

Tracking #:432318201

Date:02-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a large-scale, highly sophisticated browser extension–based threat campaign attributed to a threat actor dubbed DarkSpectre has been identified. The operation has been active for over 7 years and has compromised over 8.8 million users worldwide through at least three major malware campaigns.

TECHNICAL DETAILS:

A large-scale, highly sophisticated browser extension–based threat campaign attributed to a threat actor dubbed DarkSpectre has been identified. The operation has been active for over 7 years and has compromised over 8.8 million users worldwide through at least three major malware campaigns. 300+ browser extensions are impacted during more than seven years of activity. Unlike traditional extension malware, DarkSpectre leverages delayed activation logic, remote payload delivery, and configuration-driven behavior, allowing malicious functionality to be introduced long after marketplace approval.

Most notably, the Zoom Stealer campaign represents a shift from monetization-driven crime to systematic corporate intelligence collection, harvesting sensitive meeting links, credentials, participant lists, and speaker profiles in real time—constituting a serious corporate espionage risk.

Affected Platforms

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Opera Browser

Technical Details & Vulnerability Analysis

1. Core Vulnerability: Browser Extension Trust Model Abuse

Vulnerability Type:

Improper Trust Boundary Enforcement / Supply Chain Abuse

Browser marketplaces perform **static and short-term behavioral analysis** only at the time of submission. DarkSpectre exploits this gap by:

- Publishing fully legitimate extensions
- Maintaining benign behavior for **years**
- Accumulating users, ratings, and "verified" status
- Activating malicious logic later via:
    - Time-delayed triggers
    - Remote configuration updates
    - External payload downloads

This results in **persistent post-approval compromise** with no user visibility.

2. Time-Delayed Logic Bomb Activation

Affected Extensions:

Notably *"New Tab – Customized Dashboard"* and others

Vulnerability Mechanism:

- Hardcoded timers delay malicious execution for **48–72 hours**
- Activation probability reduced (e.g., ~10%) to evade sandbox testing

- Malicious behavior triggered only after marketplace review completion

Impact:

- Extensions appear legitimate during review
- Security scanners fail to observe malicious activity
- Threat persists undetected for extended periods

3. Remote Code Execution via External Payloads

Vulnerability Type:

Unrestricted Remote Script Execution

Technique:

- Extensions download encoded JavaScript payloads from attacker-controlled servers
- Payloads disguised as image files (PNG steganography)
- Decoded and executed in-browser using obfuscated eval() logic
- No extension update required for payload changes

Impact:

- Full execution control within browser context
- Ability to inject scripts into any visited website
- Credential harvesting, session hijacking, form injection possible

4. Excessive Permission Exploitation (The Zoom Stealer)

Vulnerability Type:

Over-Privileged Extension Permissions

Observed Behavior:

- Extensions request access to **28+ video conferencing platforms**
- Permissions unrelated to advertised functionality
- Cross-site scraping of:
  - Meeting URLs (with embedded passwords)
  - Meeting IDs and schedules
  - Registration status
  - Speaker names, titles, bios, photos
  - Company affiliations and branding assets

Data Exfiltration:

- Persistent WebSocket connections
- Real-time streaming of meeting activity
- Backend aggregation using Firebase and cloud functions

Impact:

- Unauthorized access to confidential meetings
- Intelligence gathering on corporate strategy, sales, M&A
- Enables impersonation, spear-phishing, and espionage

5. Dormant "Sleeper" Extensions

Risk Profile:

- 85+ extensions currently benign
- Years of positive reputation
- Designed solely to build user base
- Weaponized later via malicious updates or remote configuration

Indicators of Compromise (IOCS)

Attached File

RECOMMENDATIONS:

- Conduct a full audit of installed browser extensions.
- Remove extensions with:
  - Excessive or unrelated permissions
  - Unknown or unverified publishers
- Rotate compromised meeting links and credentials
- Block known malicious infrastructure and domains

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.koi.ai/blog/darkspectre-unmasking-the-threat-actor-behind-7-8-million-infected-browsers