Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

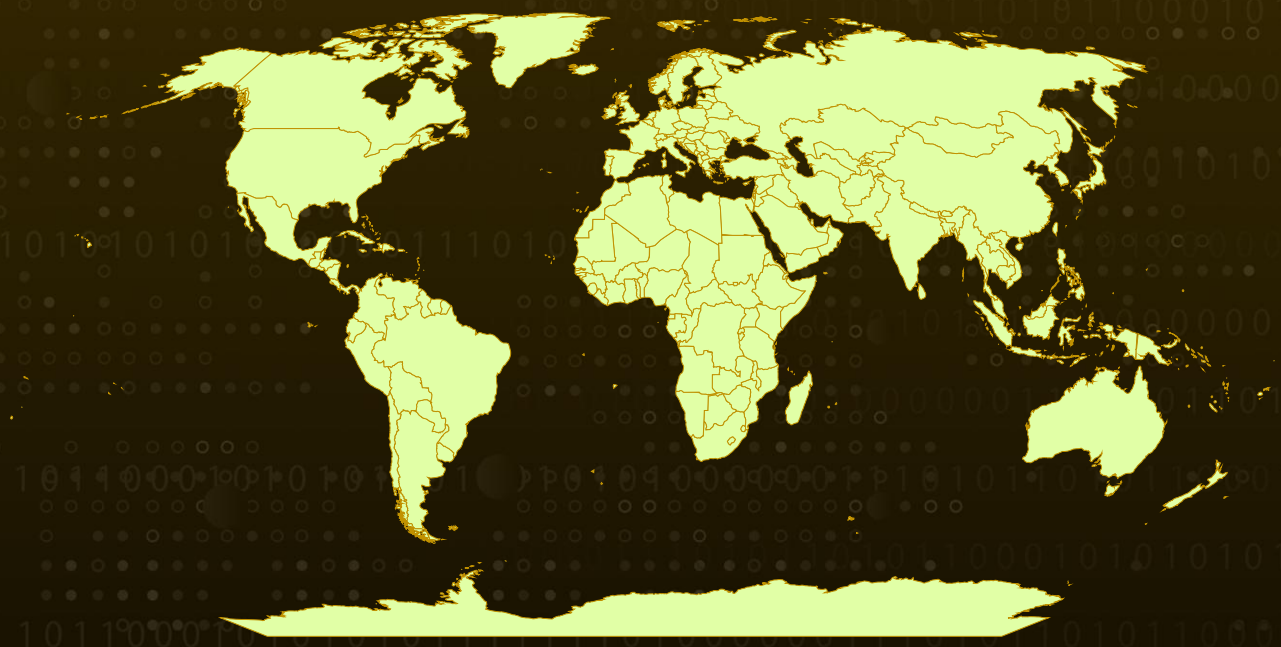
Malicious Chrome Extensions Hijacking Enterprise HR Platforms

Date of Publication	Admiralty Code	TA Number
January 20, 2026	A1	TA2026019

Summary

First Seen: August 18, 2021
Targeted Region: Worldwide
Targeted Industries: Human Resources, Enterprise Resource Planning (ERP)
Affected Platform: Google Chrome (browser extensions)
Attack: A coordinated malicious browser extension campaign has been uncovered in which five Chrome extensions pose as legitimate tools for enterprise HR and ERP platforms such as Workday, NetSuite, and SAP SuccessFactors. Operating in unison, these extensions covertly steal authentication tokens, disrupt incident response by manipulating administrative interfaces, and ultimately enable full account takeover through session hijacking. By combining continuous cookie exfiltration, deliberate blocking of security controls, and direct session injection, the campaign creates a dangerous imbalance where unauthorized access can be detected but cannot be effectively contained or remediated through normal defensive measures.

Attack Regions



Attack Details

#1 A coordinated cluster of five malicious Chrome extensions has been uncovered, specifically crafted to infiltrate enterprise HR and ERP platforms, including Workday, NetSuite, and SAP SuccessFactors. While presented as productivity and access-management tools, these extensions work in concert to steal authentication tokens, suppress incident response actions, and ultimately enable full account takeover through session hijacking. Four of the extensions are linked to the publisher databycloud1104, with a fifth operating under software access but relying on the same backend infrastructure. Collectively, they have already reached over 2,300 users, underscoring the campaign's scale and intent.

#2 At a technical level, the campaign relies on a blend of cookie exfiltration, browser-level manipulation, and session injection. The extensions continuously extract critical session cookies, particularly those used for authentication, and transmit them to attacker-controlled servers. Some go further by actively injecting stolen cookies back into browsers, allowing threat actors to assume valid user sessions without ever needing credentials or multi-factor authentication. In parallel, other extensions manipulate the DOM to block access to security and administrative pages, effectively preventing defenders from managing sessions, rotating credentials, or reviewing audit logs once compromise is suspected.

#3 The extensions are marketed with polished branding, professional mockups, and reassuring language around security and productivity. Their permission requests resemble those of common enterprise tooling, and their privacy policies explicitly claim that no user data is collected or misused. None discloses any cookie harvesting or monitoring behavior. This disconnect between presentation and behavior allows the extensions to blend seamlessly into corporate workflows, especially for administrators and consultants managing multiple enterprise tenants.

#4 All five extensions use common API paths, identical lists of monitored security extensions, and similar obfuscation and anti-debugging techniques designed to frustrate inspection. Some actively detect and disable developer tools, while others interfere with password field inspection to hide credential handling. Two extensions are dedicated almost entirely to blocking security-critical pages, ensuring that even when suspicious activity is detected, responders are unable to take corrective action.

#5 Taken together, these extensions represent a containment nightmare for affected organizations. Continuous token theft ensures attackers always possess fresh sessions, while administrative lockouts make traditional remediation ineffective. Security teams may detect anomalies through logs or alerts, yet find themselves unable to disable accounts, rotate credentials, or enforce new policies. In extreme cases, organizations are left with only disruptive options, such as migrating users to entirely new accounts. The campaign highlights how malicious browser extensions can quietly undermine enterprise security controls and why heightened scrutiny of “productivity” add-ons is now a critical defensive requirement.

Recommendations

- **Remove Malicious Extensions Immediately:** Users who have installed any of the five identified extensions (DataByCloud Access, Tool Access 11, DataByCloud 1, DataByCloud 2, or Software Access) should remove them from their browsers immediately and verify removal through chrome://extensions.
- **Perform Enterprise-Wide Extension Audit:** Security teams should conduct a comprehensive audit of all browser extensions installed across the organization, specifically searching for the identified extension IDs and any extensions from the databycloud1104 or Software Access publishers.
- **Reset Credentials for Affected Platforms:** All users who may have been exposed should perform password resets for Workday, NetSuite, SuccessFactors, and any other enterprise platforms accessed through compromised browsers.
- **Implement Browser Extension Allowlisting:** Deploy enterprise browser management policies that restrict extension installation to pre-approved extensions only, preventing users from installing unvetted extensions from the Chrome Web Store.
- **Deploy Network Detection Rules:** Implement network monitoring rules to detect HTTP/HTTPS traffic to the identified C2 domains and alert on any outbound connections to newly registered or low-reputation domains.
- **Enforce Multi-Factor Authentication:** Ensure robust MFA is enabled on all enterprise platforms, particularly Workday, NetSuite, and SuccessFactors, to provide an additional layer of protection against session hijacking.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0009 Collection	TA0011 Command and Control	T1539 Steal Web Session Cookie	T1185 Browser Session Hijacking
T1176 Software Extensions	T1176.001 Browser Extensions	T1027 Obfuscated Files or Information	T1562 Impair Defenses

T1562.001 Disable or Modify Tools	T1518 Software Discovery	T1071 Application Layer Protocol	T1071.001 Web Protocols

Indicators of Compromise (IOCs)

TYPE	VALUE
Email	admin[@]databycloud[.]com, softwareaccess0908[@]gmail[.]com
Chrome Extension ID	oldhjammhkghhahhhdcifmmlefibciph, ijapakghdgckgblfgjobhcfglebbkebf, makdmacamkifdldldlelollkkjnoiedg, mbjjeombjeklkbndcjgmfcdhfbjngcam, bmodapcihjhklpogdpblefpepjolaoij
Domains	api[.]databycloud[.]com, api[.]databycloud[.]com/api/v1/mv3, api[.]software-access.com, api[.]software-access[.]com/api/v1/mv3, wss[:]//api[.]software-access[.]com, user[.]software-access[.]com, admin[.]software-access[.]com

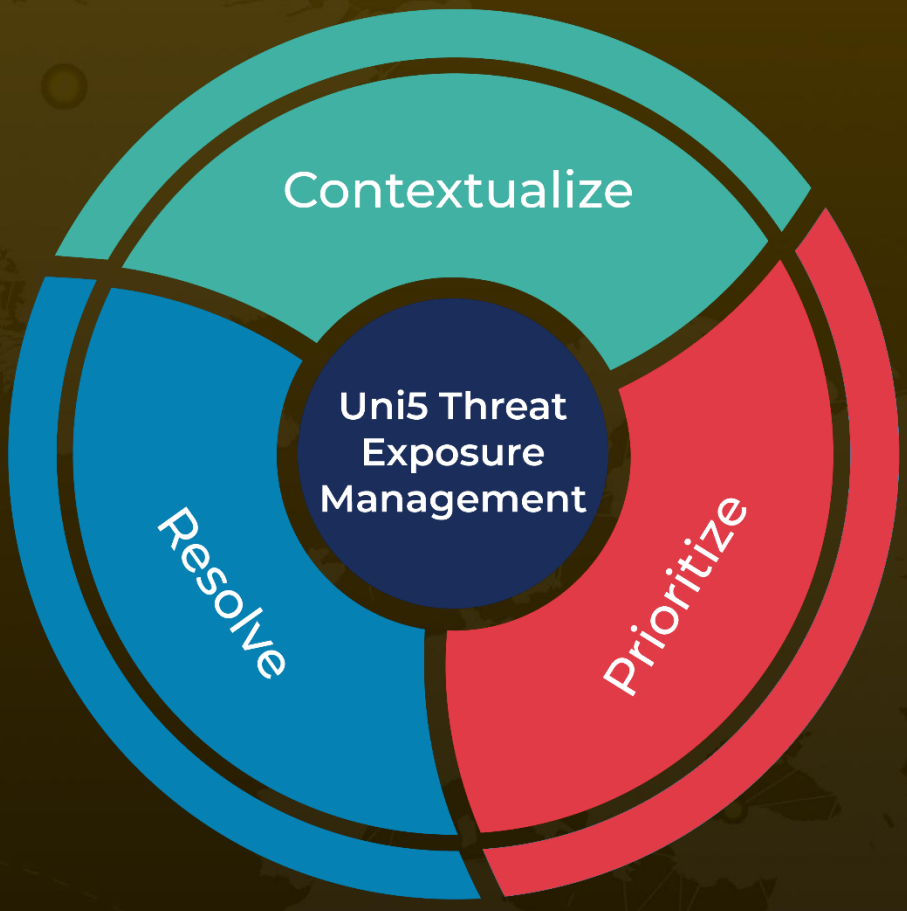
References

https://socket.dev/blog/5-malicious-chrome-extensions-enable-session-hijacking

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 20, 2026 • 8:30 AM

More at www.hivepro.com