Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

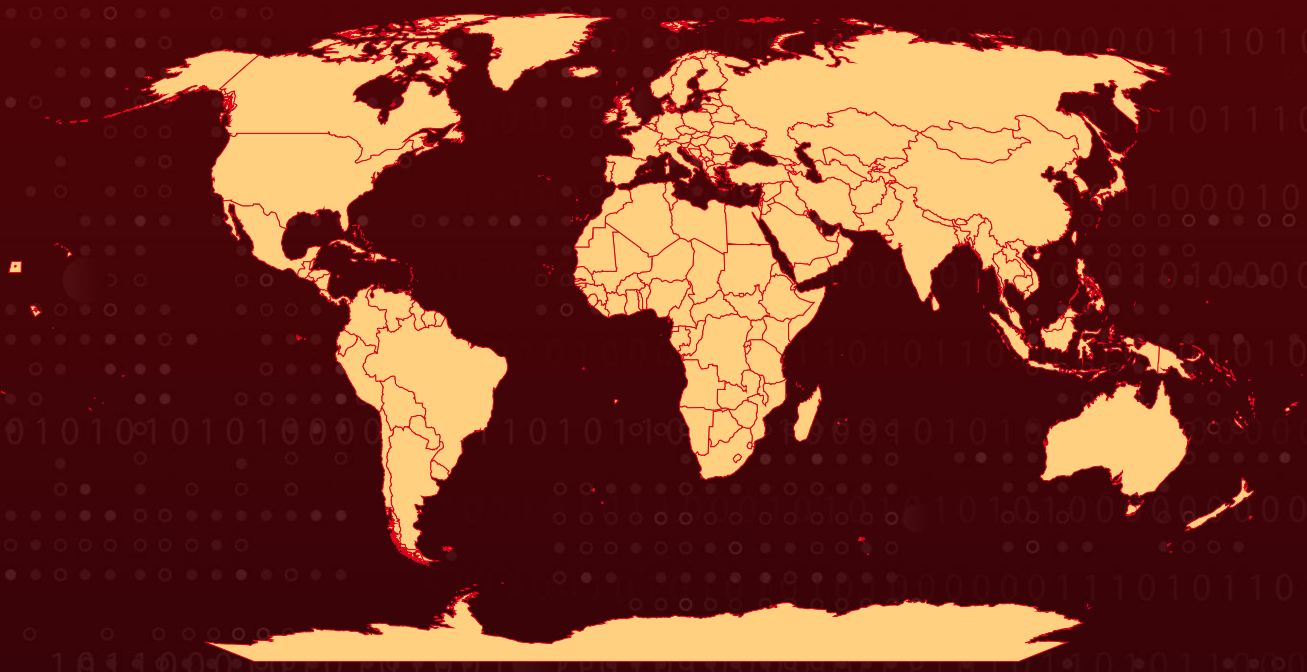
Supply Chain Attack on Chrome Browser Extensions

Date of Publication	Admiralty Code	TA Number
January 24, 2025	A1	TA2025019

Summary

Attack Began: November 2024
Targeted Region: Worldwide
Targeted Industries: Technology, Advertising
Affected Platform: Google Chrome
Attack: A recent supply chain attack compromised over a dozen Chrome browser extensions, impacting hundreds of thousands of users. The attackers used phishing campaigns to target developers, gaining access via a malicious OAuth application to publish malware-laden updates. The malicious code harvested sensitive data, including API keys, session cookies, and credentials from services like ChatGPT and Facebook for Business. This campaign highlights the growing risk of supply chain attacks and the need for stronger security measures for developers and users alike.

Attack Regions



Attack Details

#1 A recent sophisticated supply chain attack targeted Chrome browser extensions, impacting hundreds of thousands of users. The campaign exploited a phishing attack against extension developers, convincing them to authorize access to a malicious OAuth application disguised as "Privacy Policy Extension." Once access was granted, attackers deployed malicious versions of legitimate extensions through the Chrome Web Store. Among the compromised extensions were popular tools such as Cyberhaven, VPNCity, GraphQL Network Inspector, VidHelper and others.

#2 The malicious code injected into these extensions was designed to harvest sensitive user data, including API keys, session cookies, and authentication tokens. Notably, the attack targeted data from services such as ChatGPT and Facebook for Business, enabling the threat actors to collect credentials, session details, and user-specific metadata. This stolen data could potentially be sold, used for further cyberattacks, or abused to propagate fraudulent activities, such as running malicious Facebook Ads.

#3 Investigations revealed that the attacker's infrastructure had been active since at least 2023, leveraging phishing emails and malicious websites to distribute compromised extensions. The phishing emails used fake notifications about Chrome Web Store policy violations, redirecting victims to legitimate-looking Google login pages that allowed the attackers to hijack extension permissions. The malicious extensions used command-and-control (C2) servers to fetch configuration files that determined which data to target, enabling the attackers to customize their payload for each victim.

#4 Security researchers identified over a dozen compromised extensions and uncovered the attacker's broader infrastructure, which included a network of domains hosted on Vultr servers. These domains facilitated phishing, redirection, and data exfiltration activities, allowing the attackers to sustain their operations. The scale and methodology of this campaign highlight a shift in the attacker's tactics from distributing standalone malicious extensions to compromising legitimate ones via supply chain attacks.

Recommendations

- **Uninstall Compromised Extensions:** Immediately remove identified compromised extensions. Only reinstall them after verifying a clean version has been published by the developer.
- **Revoke and Reset Credentials:** Revoke session cookies, API keys, and authentication tokens linked to affected accounts. Change passwords for compromised services and enable two-factor authentication (2FA).
- **Secure Development Environment:** Use robust security measures such as multi-factor authentication (MFA) for accessing developer accounts, code repositories, and distribution platforms.
- **Monitor for Suspicious Activity:** Regularly review account activity logs for unauthorized access or unusual behavior, especially for financial or business accounts like Facebook for Business.
- **Stay Vigilant Against Phishing:** Avoid clicking on suspicious links or granting permissions to unfamiliar apps. Always verify the authenticity of emails and requests from service providers before acting.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0006 Credential Access	TA0008 Lateral Movement	TA0005 Defense Evasion	TA0010 Exfiltration
TA0011 Command and Control	T1589 Gather Victim Identity Information	T1204.002 Malicious File	T1204 User Execution
T1583 Acquire Infrastructure	T1583.001 Domains	T1583.004 Server	T1059 Command and Scripting Interpreter
T1586 Compromise Accounts	T1587 Develop Capabilities	T1195 Supply Chain Compromise	T1566.002 Spearphishing Link

T1586.003 Cloud Accounts	T1566 Phishing	T1059.007 JavaScript	T1550.001 Application Access Token
T1550 Use Alternate Authentication Material	T1528 Steal Application Access Token	T1539 Steal Web Session Cookie	T1036 Masquerading
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel
T1567.002 Exfiltration to Cloud Storage	T1589.002 Email Addresses		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	4e42ac21ed5898fd75221a2f1164a107, b4690045862e6c21fb180dd6dcb6b6b3
SHA256	b0827dc54349b10098a7370ada4ea44ba668b264ccca2db5676be1c32e6cc154, d303047205dabec8e2d34431e920ebe3478ca80a18f57bf454da094aca0e10aa
IPv4	149[.]28[.]117[.]236, 45[.]77[.]5[.]196, 65[.]20[.]99[.]178, 108[.]61[.]23[.]192, 136[.]244[.]113[.]231, 136[.]244[.]115[.]219, 137[.]220[.]48[.]214, 140[.]82[.]45[.]42, 144[.]202[.]101[.]155, 149[.]248[.]2[.]160, 149[.]248[.]44[.]88, 149[.]248[.]56[.]63, 149[.]28[.]124[.]84, 155[.]138[.]253[.]165, 185[.]92[.]222[.]127, 45[.]76[.]225[.]148

TYPE	VALUE
URLs	https[://]app[.]checkpolicy[.]site/accept-terms-policy?e=victim[@]example[.]com, https[://]app[.]checkpolicy[.]site/extension-privacy-policy?e=victime[@]example[.]com, https[://]graphqlnetwork[.]pro/ai-graphqlnetwork
Email	chromewebstore-noreply[@]chromeforextension[.]com, chromewebstore-noreply[@]supportchromestore[.]com
Domains	adsblockforyoutube[.]site, adskiper[.]net, aiforgemini[.]com, bardaiforchrome[.]live, blockforads[.]com, castorus[.]info, chataiassistant[.]pro, chatgptextension[.]site, chatgptextent[.]pro, chatgptforsearch[.]com, checkpolicy[.]site, chromeforextension[.]com, chromewebstore-noreply[.]com, cyberhavenext[.]pro, dearflip[.]pro, extensionbuysell[.]com, extensionpolicy[.]net, extensionpolicyprivacy[.]com, geminiaigg[.]pro, geminiforads[.]com, goodenhancerblocker[.]site, gpt4chrome[.]live, gptdetector[.]live, gptforads[.]info, gptforbusiness[.]site, graphqlnetwork[.]pro, internetdownloadmanager[.]pro, internxtvpn[.]pro, iobit[.]pro, linewizeconnect[.]com, locallyext[.]ink, moonsift[.]store, openaigptforgg[.]site, parrottalks[.]info,

TYPE	VALUE
Domains	pieadblock[.]pro, policyextension[.]info, primusext[.]pro, promptheusgpt[.]info, savechatgpt[.]site, savegpt[.]pro, savegptforchrome[.]com, savegptforyou[.]live, savgptforchrome[.]pro, searchaiassitant[.]info, searchcopilot[.]co, searchgptchat[.]info, supportchromestore[.]com, tinamind[.]info, ultrablock[.]pro, uvoice[.]live, videodownloadhelper[.]pro, vidnozflex[.]live, wakelet[.]ink, wayinai[.]live, youtubeadsblocker[.]live, ytbadblocker[.]com, yujaverity[.]info

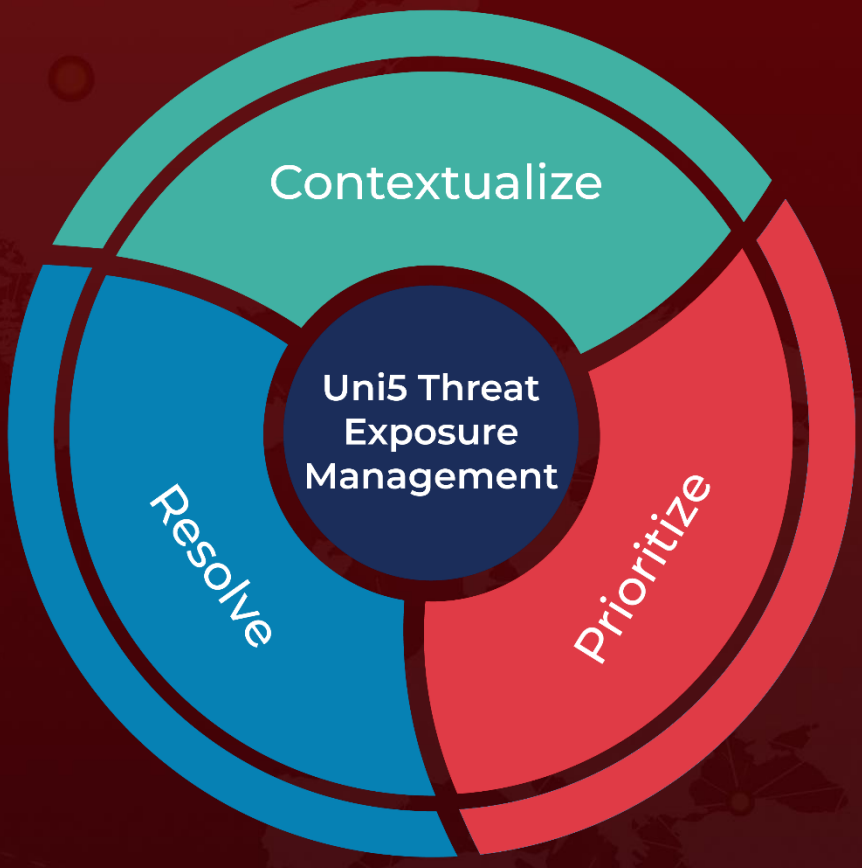
References

https://blog.sekoia.io/targeted-supply-chain-attack-against-chrome-browser-extensions/

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 24, 2025 . 6:30 AM

More at www.hivepro.com