IRON SPEAR
BUSINESS & INDUSTRIAL CYBER SECURITY
VANCOUVER•CALGARY•REGINA•WINNIPEG

Browser Extension Security

Small Add-ons, Big Risk - What to Do About It

Introduction to Iron Spear

IRON SPEAR

FOUNDED IN 2012

For over 12 years, we have been committed to providing solutions to meet the needs of our clients, whether they are looking for security compliance, control testing, or program development and operation.

WE ARE PARTNERS, NOT VENDORS

We believe in a partnership approach with our clients. Iron Spear is committed to the long-term relationship with our clients to support their ongoing cyber needs and does not nickel and dime on every project.

WE ARE PRACTICAL

One of our beliefs is, that if we are not able to implement it, we will not recommend it. We do not believe in textbook recommendations. Rather, we want to see our clients achieve their objectives.

CANADIAN OWNED AND OPERATED

We have offices in Vancouver, Calgary, Regina and Winnipeg, offering services across North America.

WE ARE EXPERIENCED

Our team has backgrounds in a wide range of industries and provides the trusted methods, approaches, and standards of quality that are expected by our clients.

WE ARE INDEPENDENT

Iron Spear is not contracted to security technology vendors. Rather, we believe in working with our clients to determine the requirements that meet their needs and then identifying best-of-breed products that match the requirements.

Research Team

Franz Erasmus

- Offensive Security Operator & Practice Lead

Danie van Heerden

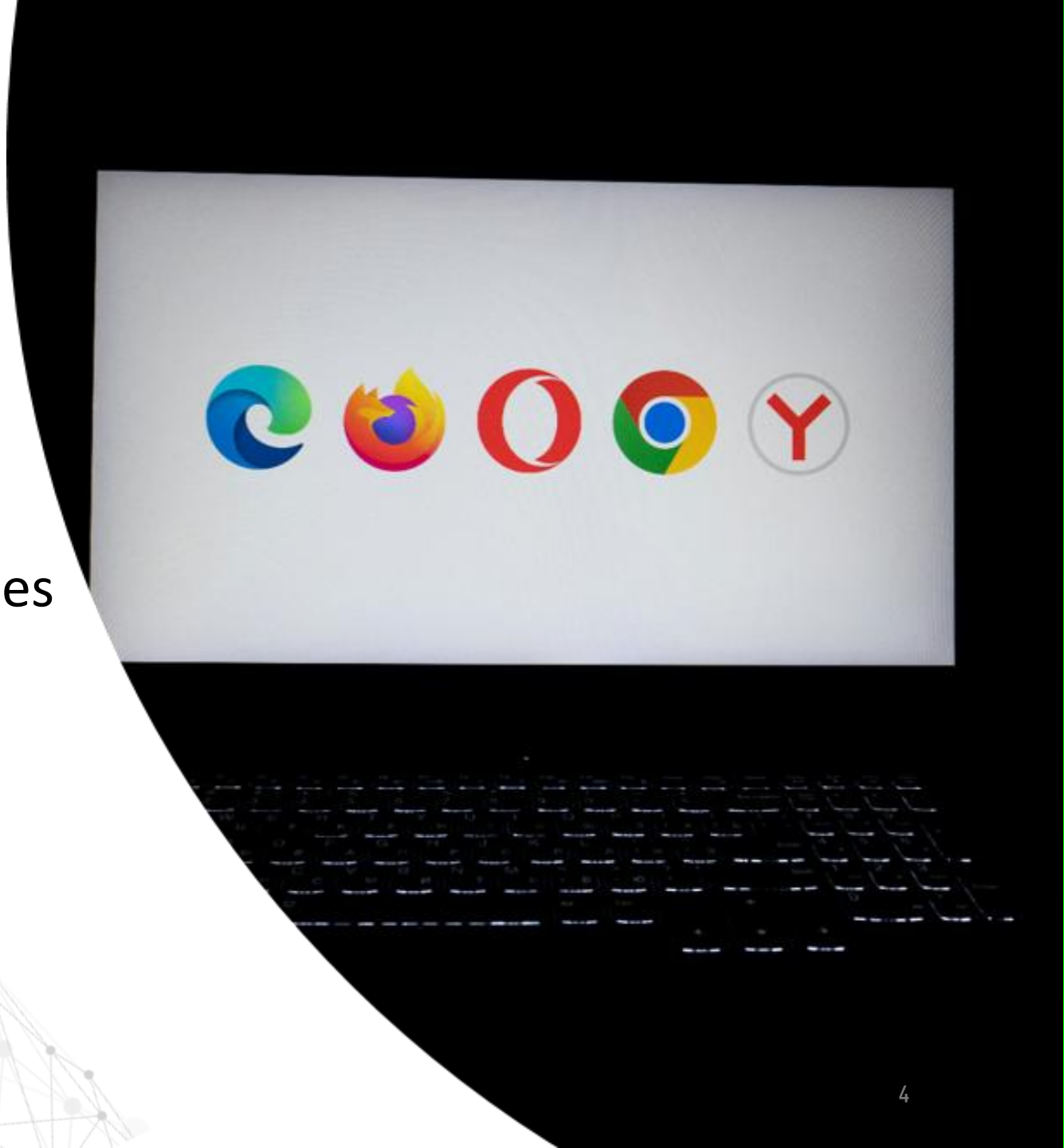
- Senior Cybersecurity Operator & Researcher

Kent Grimbeek

- Cybersecurity Operator & Researcher

Agenda

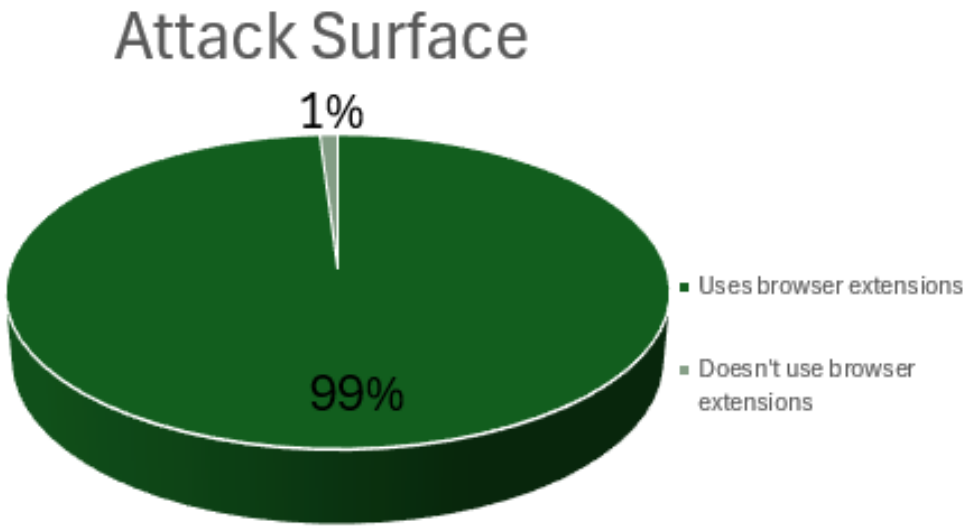
- Why Browser Extensions Matter
- Real-World Incidents
- Hidden Risks & Attack Vectors
- Key Security Risks
- Enterprise Management Strategies
- Key Takeaways
- Browser Extension Attack Demo
- Q&A



Why Browser Extensions Matter

IRON SPEAR

- Indispensable productivity tools
- 99% of enterprise users have at least one extension installed
- Over 50% of employees use more than 10 extensions
- Widespread adoption introduces a significant security concern
- Extensions are often overlooked in security programs



Real-World Exploits in 2025

IRON SPEAR

cybernews®

Massive browser hijack: extensions turn Trojan and infect 2.3M Chrome and Edge users

Published: 9 July 2025

Last updated: 14 July 2025

Ernestas Naprys, Senior Journalist

Image by Cybernews.

Source: Cybernews, July 2025

ars TECHNICA

SIGN IN

WEAK LINK IN THE CHAIN

Time to check if you ran any of these 33 malicious Chrome extensions

Two separate campaigns have been stealing credentials and browsing history for months.

DAN GOODIN – JAN 3, 2025 4:15 A.M. | 143

Credit: Getty Images

Source: Arstechnica, January 2025

GitLab Security Tech Notes

Tech Note - Malicious browser extensions impacting at least 3.2 million users

13 February 2025 - GitLab Threat Intelligence

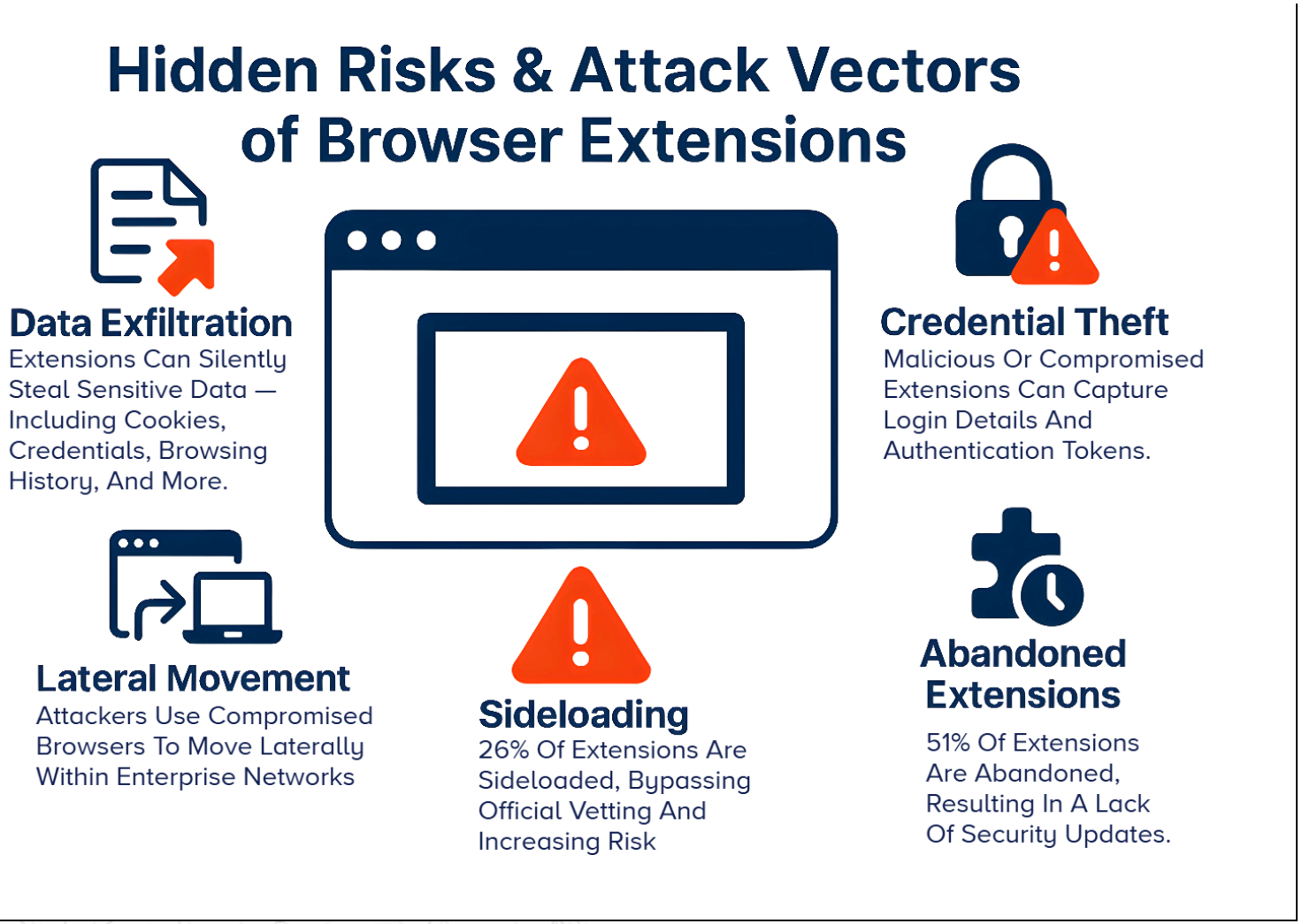
Key Points

- We identified a cluster of at least 16 malicious Chrome extensions used to inject code into browsers to facilitate advertising and search engine optimization fraud. The extensions span diverse functionality including screen capture, ad blocking and emoji keyboards and impact at least 3.2 million

Source: GitLab, February 2025

Hidden Risks & Attack Vectors

IRON SPEAR



Key Security Risks

IRON SPEAR

High-Risk Permissions:

53% of users have extensions with high/critical risk scopes

Sensitive Data Access

Cookies, passwords, browsing history, etc.

Elevated Enterprise Risk

Higher permissions in corporate environments

Data Leakage

Unintentional data leakage to external servers

Policies

Many extensions lack privacy policies

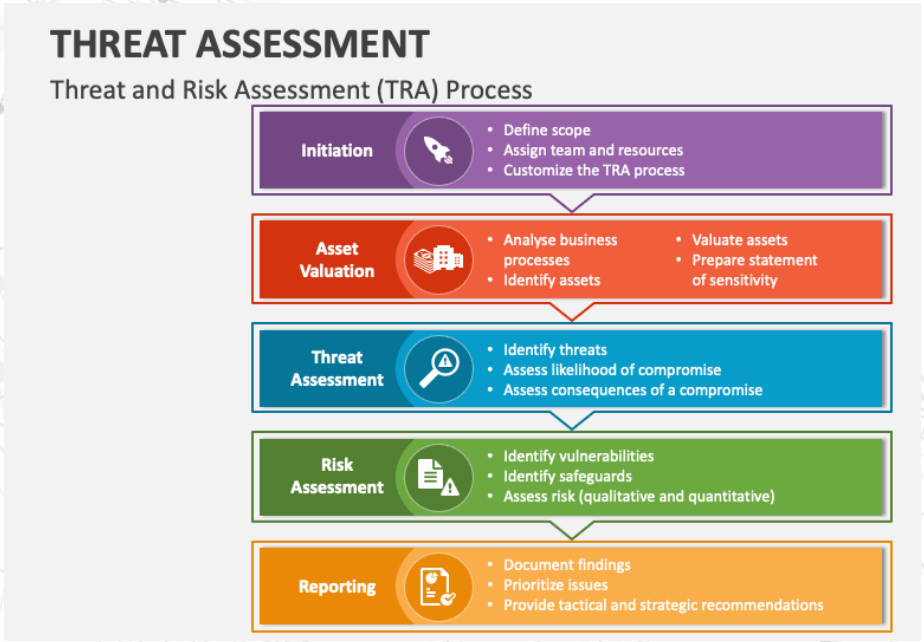
Risk Multiplyer: Generative AI & VPN Extension Risks

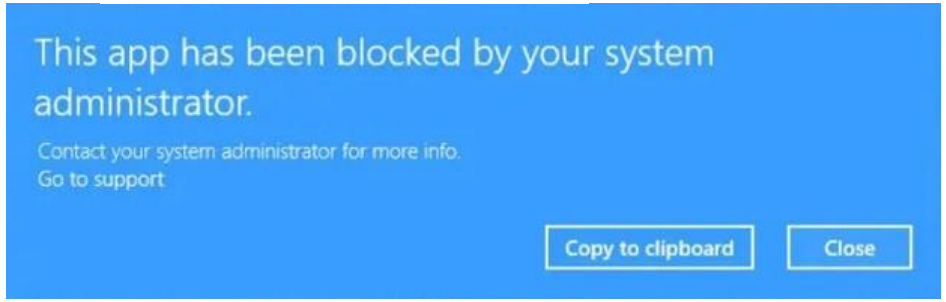
20%+ of enterprise users have GenAI-enabled extensions

VPN extensions: high-risk permissions (webRequest API, cookies)

Managing Extension Risk – Three Step Process

IRON SPEAR





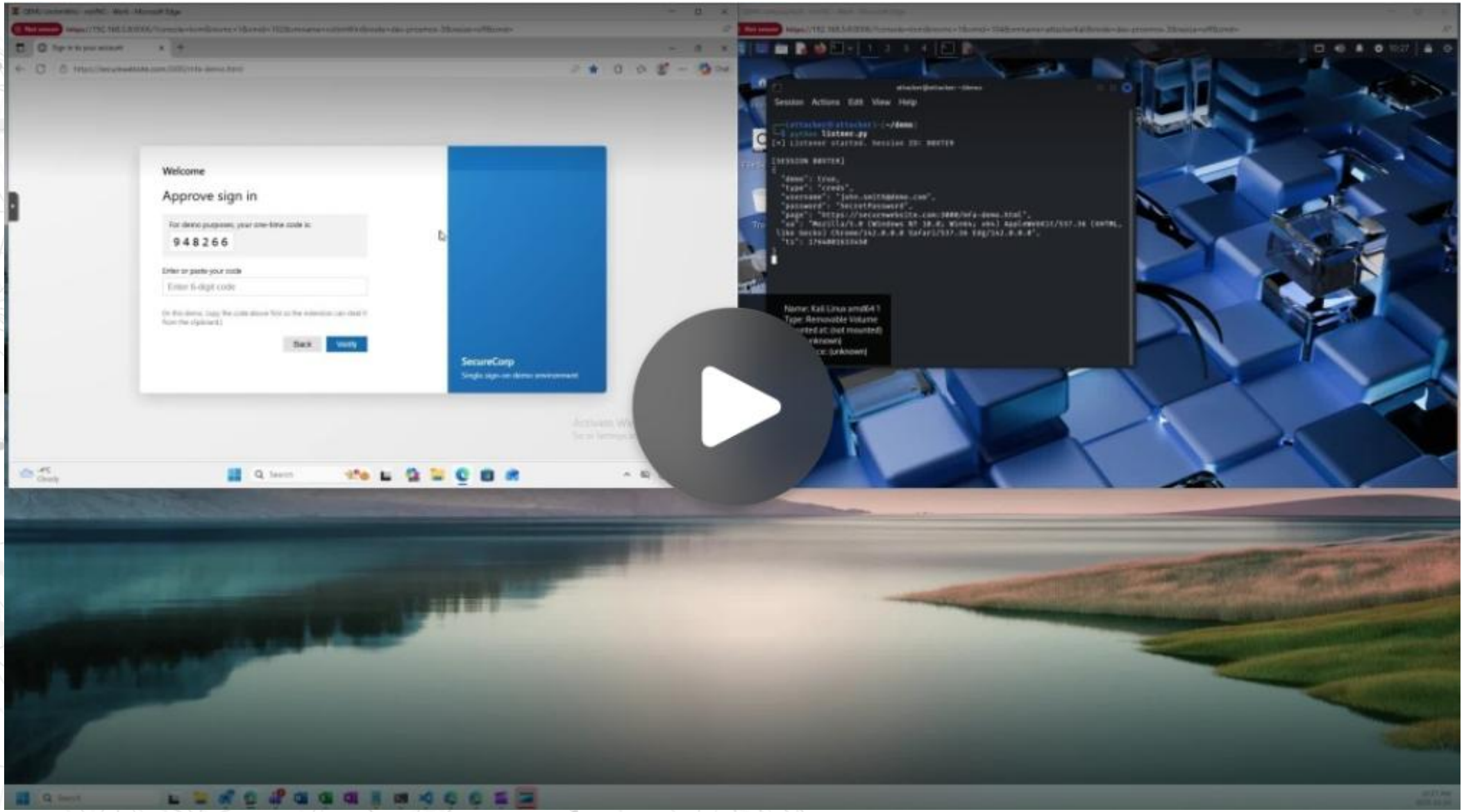
Key Takeaways

IRON SPEAR

- Extensions are a major, often overlooked, attack vector
- Both malicious and legitimate extensions can introduce privacy, compliance, and security risks
- Real-world incidents show potential for data exfiltration, credential theft, and lateral movement
- Effective management requires visibility, auditing, risk scoring, and strong policies—without crippling productivity

Demo

IRON SPEAR



IRON SPEAR

BUSINESS & INDUSTRIAL CYBER SECURITY

VANCOUVER•CALGARY•REGINA•WINNIPEG

Q&A

Website: https://ironspear.ca/

Call Us: 1.800.561.4007 (*Toll Free*)