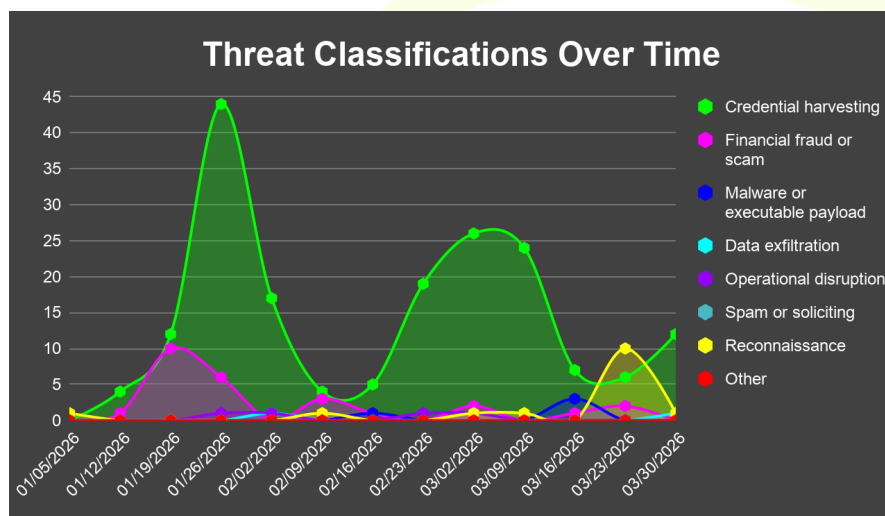


2026 Q1 CSOC Threat Report

Prepared by the Ottawa Area Cybersecurity Operations Center

Threat Classifications Over Time (below)

This chart shows the volume of incidents by threat classification across the reporting period. Tracking classifications over time highlights trends in the types of threats targeting districts and helps identify shifts in attacker behavior or emerging risks.



Evasion & Delivery Techniques	01/01/2026	02/01/2026	03/01/2026
Business Email Compromise (BEC)	61	45	67
VIP or Employee Impersonation	20	2	7
Thread Hijacking / Fake Reply	1	1	7
QR Code	0	1	0
Calendar Invite (ICS)	2	0	1
Attachment-Based Delivery	0	4	8
Obfuscated Link	21	32	47
Suspected AI-Generated Content	16	0	3
Brand Impersonation	56	24	66
Living Off Trusted Sites (LOTS)	41	27	28
Supply Chain Poisoning	0	0	0
Session Hijacking	8	11	22
Callback or Out-of-Band	12	1	3
Insider Threat	1	2	1

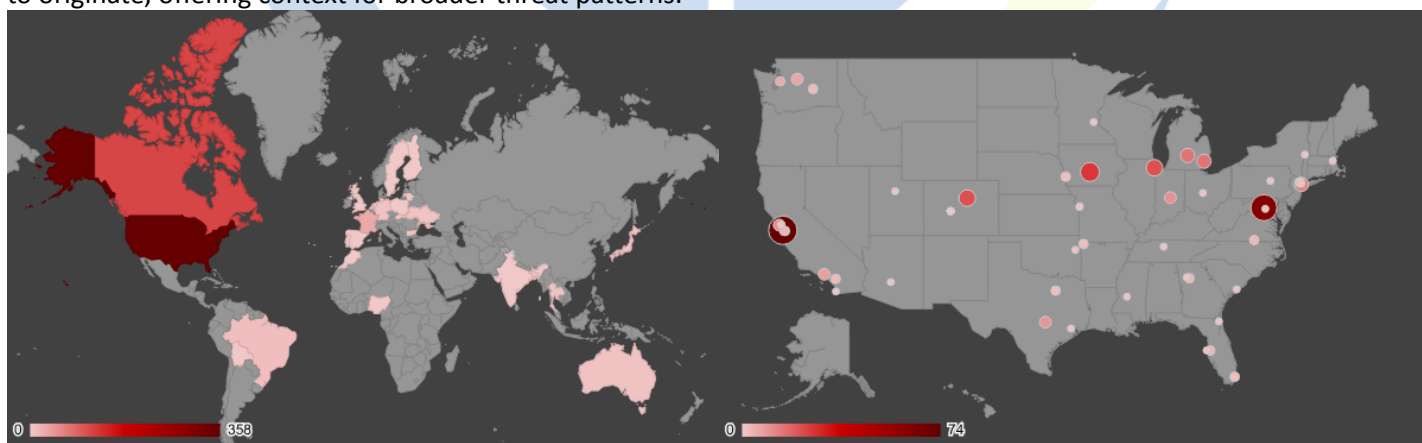
Evasion and Delivery Techniques (right)

The heat map visualizes the frequency of evasion and delivery techniques observed in incidents. It helps identify which methods attackers most often use to bypass defenses or reach users, allowing the CSOC to prioritize detection and mitigation efforts.

Threat Geolocation

Data displayed from CSOC inception (7/1/2025) through present

These maps display the geographic origin of known threats based on available network indicators such as IP addresses or domains. The global and U.S. views provide a high-level perspective on where activity associated with incidents appears to originate, offering context for broader threat patterns.



Top offenders:

- Cloudflare, Inc. - 31
- OVH SAS - 27
- Amazon.com, Inc. - 26
- Shenzhen Tencent Computer Systems Company Limited - 12
- Cloudflare London, LLC - 10