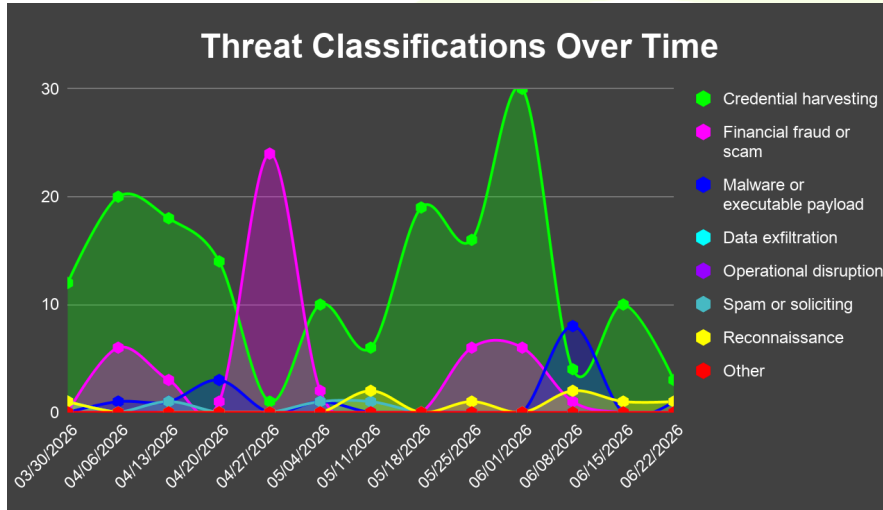


2026 Q2 CSOC Threat Report

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.



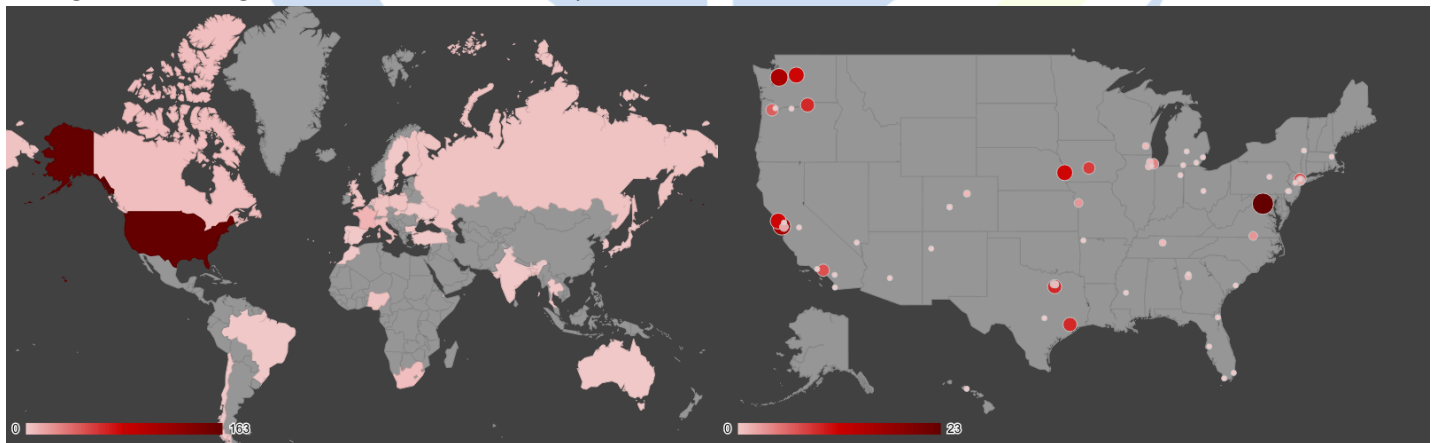
Evasion & Delivery Techniques	04/01/2026	05/01/2026	06/01/2026
Business Email Compromise (BEC)	45	43	43
VIP or Employee Impersonation	7	10	17
Thread Hijacking / Fake Reply	0	6	1
QR Code	0	0	0
Calendar Invite (ICS)	1	0	0
Attachment-Based Delivery	11	2	3
Obfuscated Link	49	33	33
Suspected AI-Generated Content	0	7	9
Brand Impersonation	53	30	28
Living Off Trusted Sites (LOTS)	18	21	13
Supply Chain Poisoning	0	0	0
Session Hijacking	18	15	4
Callback or Out-of-Band	3	3	3
Insider Threat	1	0	1
Typosquatting	8	1	4

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

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:

- Amazon.com, Inc. - 13
- Fastly, Inc. - 10
- Cloudflare, Inc. - 7
- Google LLC - 7
- OVH SAS - 5
- Microsoft Corporation - 5