Ottawa Area ISD Technology Services

Ottawa Area ISD CSOC

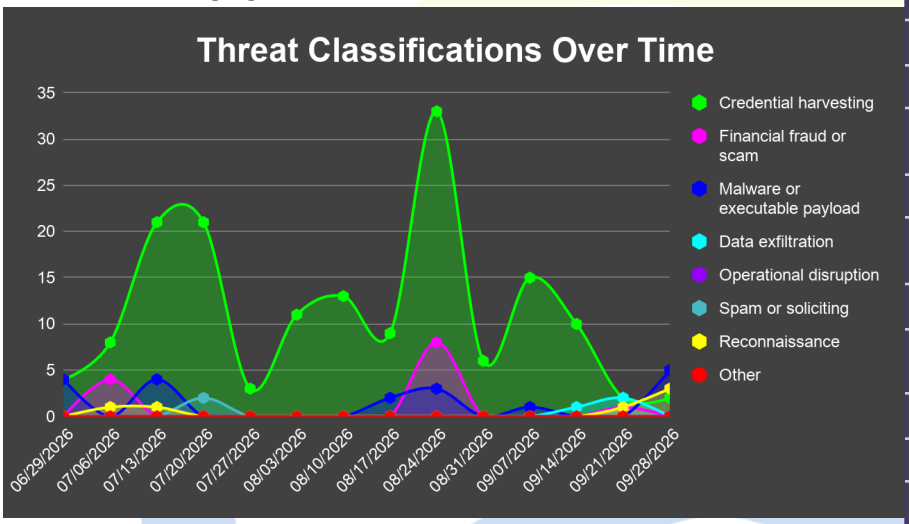
07/01/2026 - 09/30/2026

2026 Q3 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.



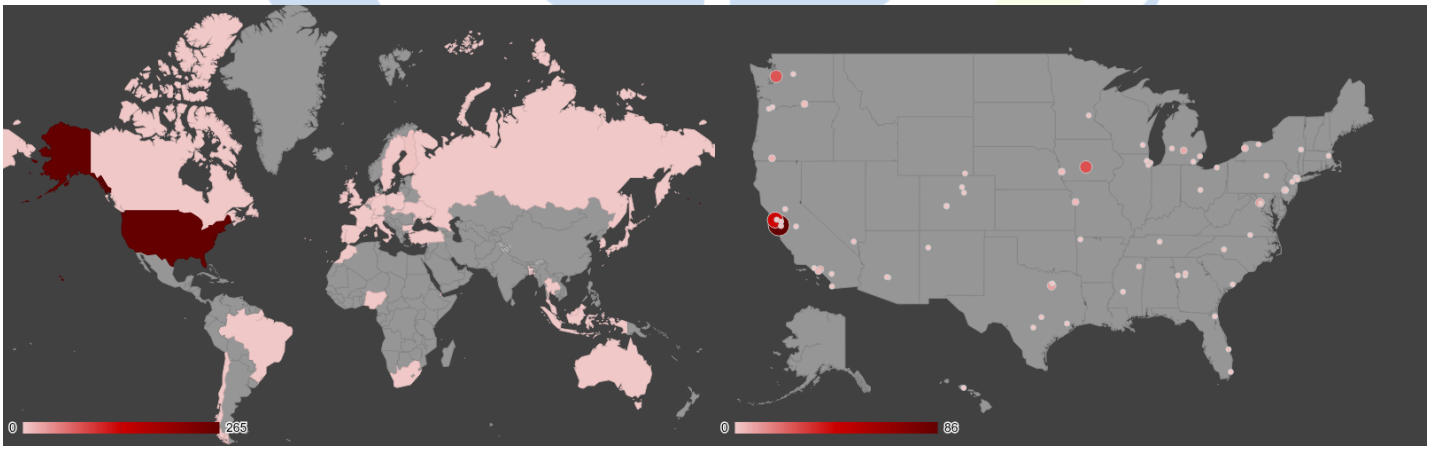
Evasion and Delivery Techniques (right)

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.

Evasion & Delivery Techniques	07/01/2026	08/01/2026	09/01/2026
Business Email Compromise (BEC)	63	70	40
VIP or Employee Impersonation	5	12	12
Thread Hijacking / Fake Reply	2	6	0
QR Code	0	0	0
Calendar Invite (ICS)	0	10	2
Attachment-Based Delivery	6	15	0
Obfuscated Link	42	59	31
Suspected AI-Generated Content	24	2	1
Brand Impersonation	39	62	20
Living Off Trusted Sites (LOTS)	18	41	13
Supply Chain Poisoning	0	0	0
Session Hijacking	30	55	25
Callback or Out-of-Band	0	0	4
Insider Threat	0	1	0
Typosquatting	0	0	0
Fake CAPTCHA	0	2	1
Remote Access Tool (RAT)	8	3	3
Google Drive Share	2	3	6

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. - 15
- Cloudflare, Inc. - 13
- GSL Networks Pty Ltd - 12
- Google LLC - 4
- Rocks Computer Services, LLC - 3
- Cogent Communications, LLC - 3