

RH-ISAC INTELLIGENCE TRENDS SUMMARY JULY-SEPTEMBER 2026 AND 2026 HOLIDAY THREAT TRENDS REPORT

INTELLIGENCE TRENDS SUMMARY JULY-SEPTEMBER 2026

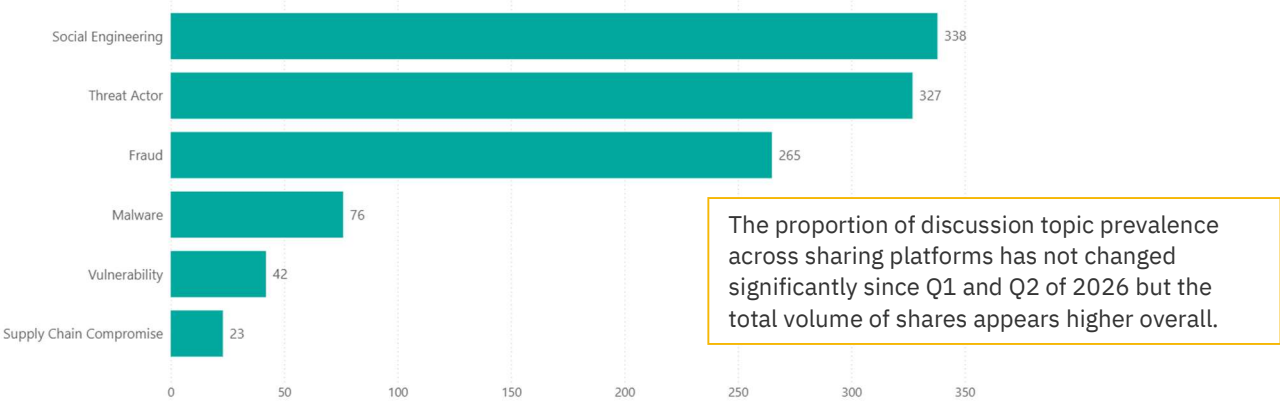
Executive Summary

Analysis of intelligence sharing during the third quarter of 2026 showed that the top reported threats by volume continued to reflect the steady reliance by threat actors on tried and tested threat vectors like fraud, social engineering, and malware. RH-ISAC intelligence team reporting focused on threats related to emerging agentic commerce ecosystems, major changes in the npm and ClickFix threat landscapes, and Famous Chollima activity.

Threat Landscape

Top Sharing Trends

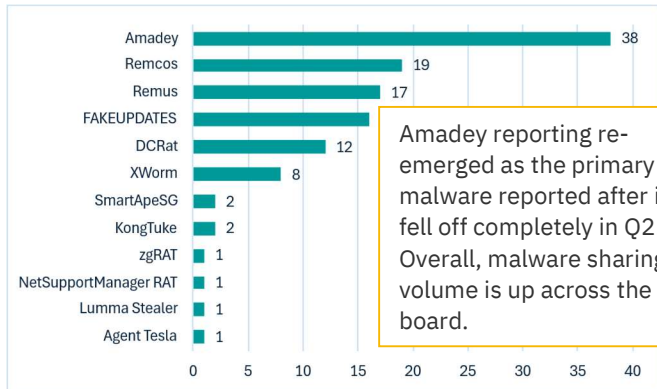
Sourced from RH-ISAC Core Member sharing.



Top MISP Trends

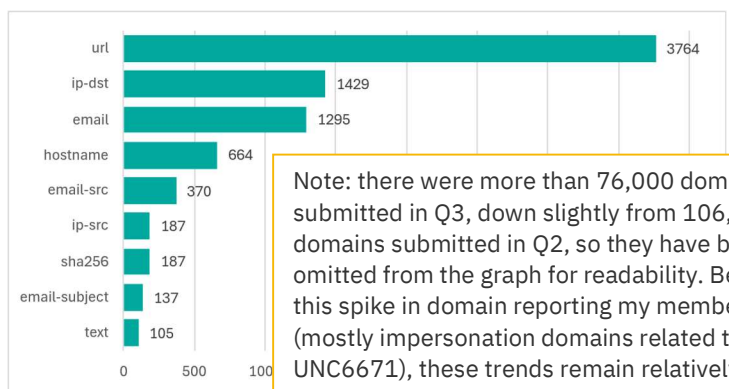
Sourced from RH-ISAC Core Member sharing

MALWARE



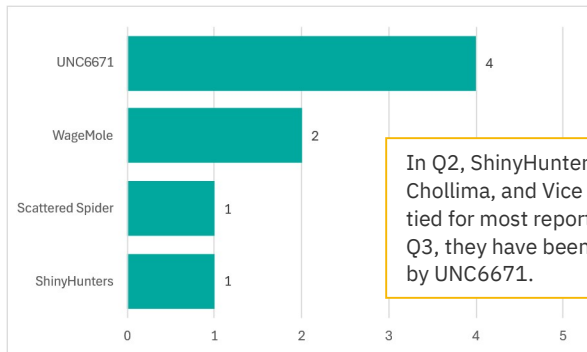
Amadey reporting re-emerged as the primary malware reported after it fell off completely in Q2. Overall, malware sharing volume is up across the board.

ATTRIBUTE TYPES



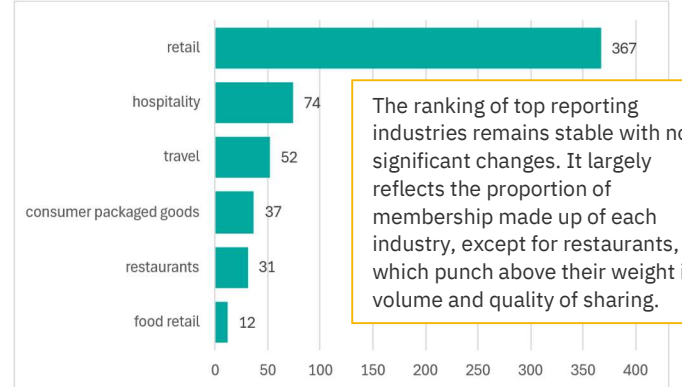
Note: there were more than 76,000 domains submitted in Q3, down slightly from 106,000 domains submitted in Q2, so they have been omitted from the graph for readability. Beyond this spike in domain reporting my members (mostly impersonation domains related to UNC6671), these trends remain relatively static, while volume remains up.

THREAT ACTORS



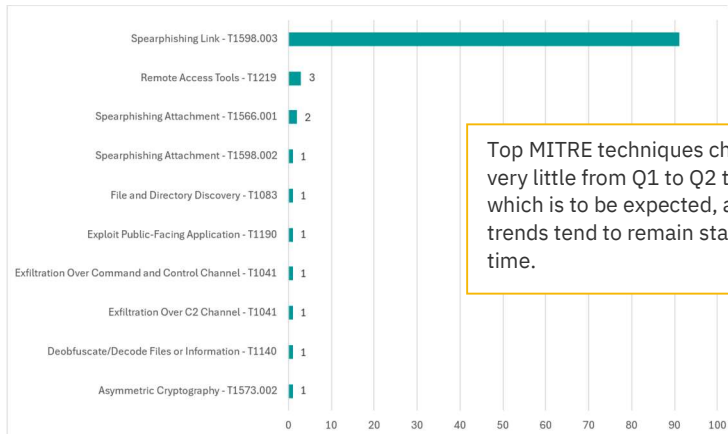
In Q2, ShinyHunters, Famous Chollima, and Vice Spider were tied for most reported TA. In Q3, they have been overtaken by UNC6671.

MEMBER INDUSTRIES



The ranking of top reporting industries remains stable with no significant changes. It largely reflects the proportion of membership made up of each industry, except for restaurants, which punch above their weight in volume and quality of sharing.

MITRE ATT&CK TECHNIQUES

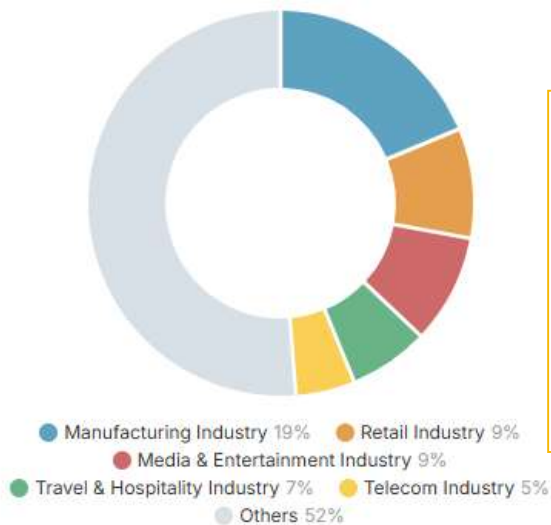


Top MITRE techniques changed very little from Q1 to Q2 to Q3, which is to be expected, as these trends tend to remain stable over time.

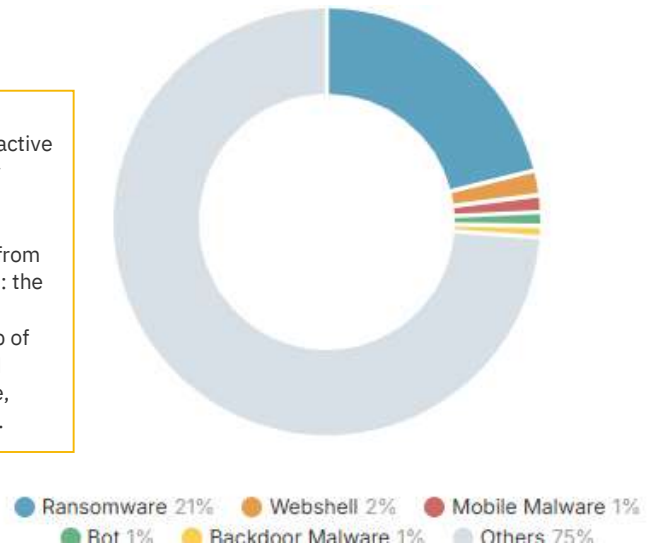
Top Industry Trends

Sourced from Feedly Industry Tracking for industries within RH-ISAC purview.

TARGETED INDUSTRIES

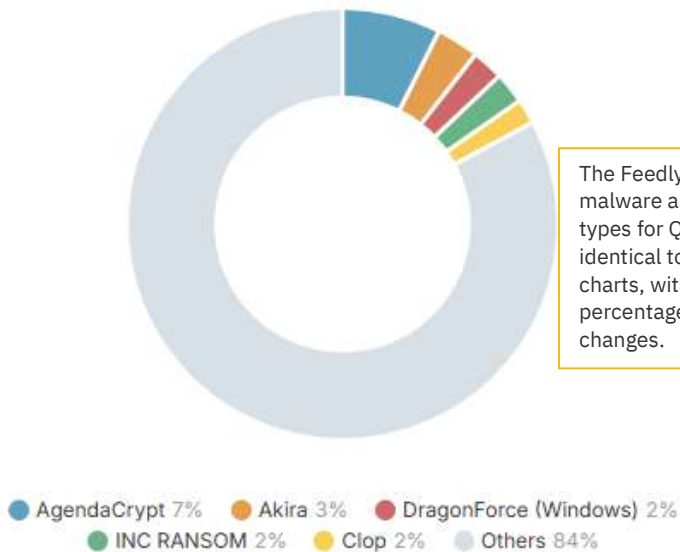


MALWARE TYPES

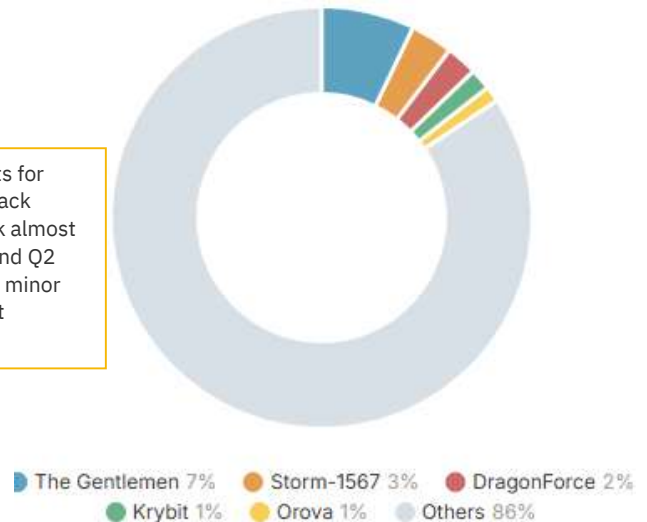


The top targeted industries and most active malware reported by Feedly cyberattack intelligence did not significantly change from Q1 to Q2 to Q3. Note: the Others category of industries is made up of electronics, food and beverage, agriculture, gaming, and aviation.

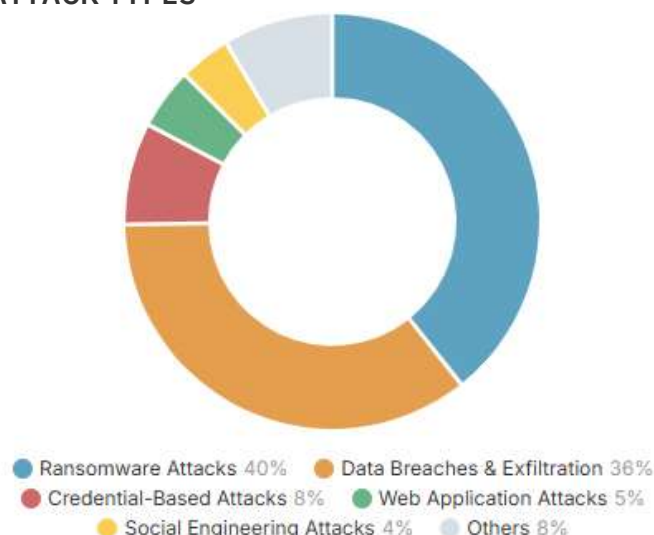
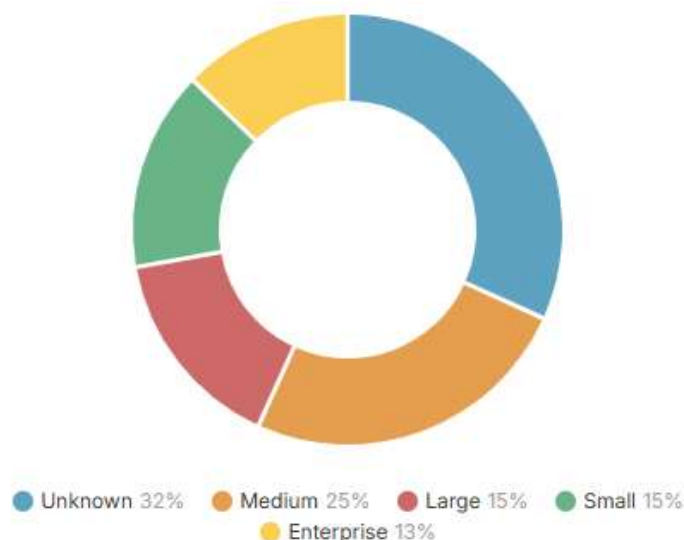
MOST ACTIVE MALWARE



MOST ACTIVE THREAT ACTORS



The Feedly charts for malware and attack types for Q3 look almost identical to Q1 and Q2 charts, with only minor percentage point changes.



RH-ISAC 2026 HOLIDAY THREAT TRENDS REPORT

Executive Summary

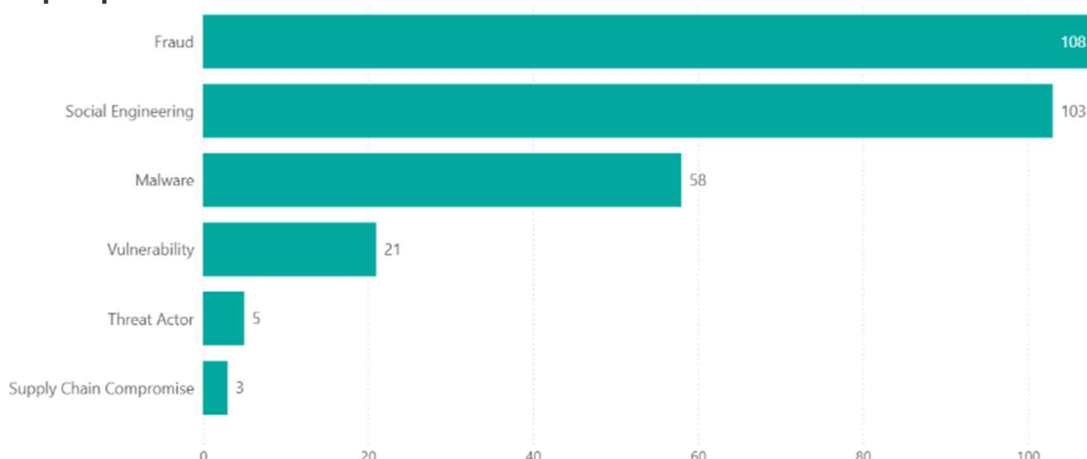
Every year during Q4, the RH-ISAC Intelligence Team conducts a study into threat activity reported by the RH-ISAC Core Member community for the holiday season (1 October to 31 December) for the past two years to examine changes in the threat landscape over time for the busy season. As our Core Members prepare for peak business volume, the prevailing thought for years has been that same threat actor activity. Currently available data from members does not corroborate this notion. For the past several years, sharing trends for Q4 have not significantly diverged from other times of the year. Core Members do not, by and large, report spikes in targeting or intrusion attempts during the holiday period.

The primary change the RH-ISAC Intelligence Team wishes to highlight for the 2026 holiday period is the emerging threat landscape related to the increasing leverage of AI agents by sellers and buyers to manage commerce.

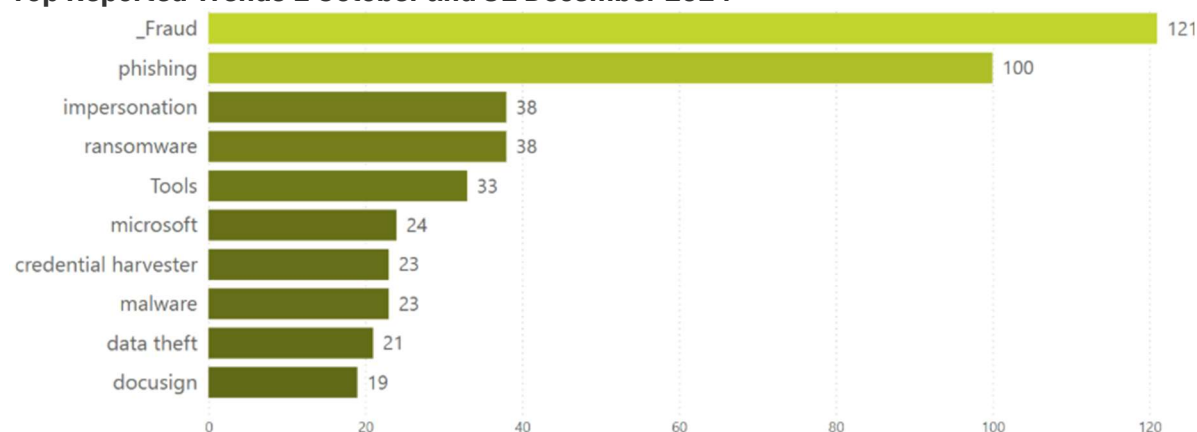
Prior Year Trends

As demonstrated in the following charts, the major trends for threat activity reported by Core Members for 2025 and 2024 are largely the same: fraud activity, social engineering in a variety of formats, malware activity, and threat actor behaviors. These Q4 numbers for 2025 and 2024 do not show significant divergence from the Q3 results for those years.

Top Reported Trends 1 October and 31 December 2025



Top Reported Trends 1 October and 31 December 2024



RH-ISAC Fraud Insights for 2026 Holiday Season

Executive Summary

As noted in the prior year threat trends, fraud continues to plague membership throughout the holiday season. While fraud is a general topic and is comprised of many different types, it is not bound to a single area within our industry. Over the last few years, we have observed similar fraud activity move between retail, hospitality, food service, etc. with similar tactics being employed during each campaign. Based on historical member sharing, the most common fraud types affecting our membership base during the holiday season include, but not limited to, brand impersonation, employee/CEO impersonation, refund fraud, and payment fraud.

Fraud Types & Strategies

Brand impersonation is highly common throughout the holiday season as threat actors aim to steal both personally identifiable information (PII) and payment card details from your consumer base. With brands using various seasonal promotions

Agentic Commerce Heads into Peak Season: Familiar Fraud Through New Traffic

Executive Summary

If you have not read the RH-ISAC agentic commerce report, *Agentic Commerce: Strategic Frontiers, Operational Readiness, and the Expanding Threat Surface*, it provides the background this section builds on.

The RH-ISAC intel team assesses with moderate confidence that most agentic commerce risk this holiday season will come from existing fraud types, such as card testing, account takeover, and checkout-page card theft, delivered through a growing volume of AI-driven traffic. Attacks aimed at shopping agents are documented as researcher demonstrations, lab results, and attempted payloads. Public reporting does not document confirmed fraud losses from such attacks. Attackers are also running AI agents of their own against merchants. [Gambit Security documented](#) a campaign in which agent tools were used to compromise online retailers, with more than 600,000 payment card records taken from two companies. This assessment rests on vendor telemetry and a small number of primary research reports.

[Adobe expects AI-referred](#) traffic to U.S. retail sites to rise 130% year over year, with the largest increases on Thanksgiving (159%), Black Friday (95%), and Cyber Monday (88%). Companies should classify agent traffic and tighten login and checkout controls before Thanksgiving, including a review of checkout pages for injected scripts. Companies that operate agents should also review how those agents handle untrusted web content.

Community Impact

Commerce accounted for nearly half (48%) of AI bot traffic on Akamai's global network from July to December 2025. Of the [commerce web attacks](#) that targeted API endpoints from January 2024 to December 2025, hospitality accounted for 33% and travel for 9%. [In HUMAN's 2025 data](#), travel and hospitality received 19.2% of agentic traffic, behind retail and e-commerce at 46.6%.

[Adobe forecasts](#) \$275.1 billion in U.S. online holiday spending from November 1 to December 31, including \$47.5 billion during Cyber Week.

Akamai reports that commerce organizations, like most other industries, place more than 90% of their AI bot activity in a "monitor" category and allow about three-quarters of the remaining activity to pass unrestricted, [which Akamai describes](#) as looser than in other industries.

In a February [2026 U.S. survey by HUMAN](#), only 11.7% of respondents were comfortable with an AI booking travel deals without asking for approval, while 42.6% were comfortable if it asked for final approval before payment. Based on that survey, many agent purchases this season will likely keep a human approval step, which puts the approval screen itself in scope for manipulation.

Technical Details

Fraud Arriving Through Agent Traffic

HUMAN reports carding rates on heavily-targeted travel and hospitality businesses reached 17.6% of checkout requests in 2025, up from 3.1% in 2022. The median in 2025 was 0.35%. One airline's rate of attempted carding attacks rose from under 1% of transactions in early 2025 to over 8% at the summer peak, then fell back below 1% by year end. HUMAN's research team also observed a carding-like pattern mediated by an AI agent. They state the threat actor rapidly cycled through multiple credit-card additions and repeated payment-completion attempts to see which card would authorize. [The sequence included](#) 11 card-add attempts and 6 payment attempts across two sessions, followed by a pivot to loyalty-point redemption after the card paths failed, mirroring established carding workflows, but executed through an AI browser agent. These figures measure attempts across HUMAN's own customers and come from a vendor report.

Attackers Using AI Agents

Gambit Security recovered the staging server of an operator that used three open-source AI tools, Hermes, Strix, and Cairn, to find and exploit online retailers. Skimmers were ordered against at least 27 named victims and confirmed in place on 19, and a fraud partner counted more than 600,000 card records taken from two companies. Gambit lists a hospitality company, an airline, and a Japanese travel booking site among the targets, but describes access to some victims only as "some level of access." [The report](#) is interim, and part of its evidence comes from AI-generated logs that Gambit says may be inaccurate.

NorForge separately found exposed Cairn operator panels through internet scanning, including one cluster configured with the Chinese language with more than 1,100 attack projects spread across 14 dashboards likely associated with this group. Targets were e-commerce sites mostly in the US, Japan, and Australia, and [NorForge could not confirm](#) most victim outcomes.

Attacks on Shopping Agents

Unit 42 documented indirect prompt injection on public websites in March 2026 and cataloged 22 payload techniques. Payment-related examples included hidden instructions that tried to force a purchase through a Stripe link and trigger a \$5,000 transfer through PayPal. A third targeted an AI ad-review agent and tried to get a scam ad approved. [Unit 42 states](#) it is not aware of confirmed successes against deployed ad-review agents.

Researchers have demonstrated hijacking of agentic browsers. At Black Hat USA 2026, Zenity Labs showed that hidden instructions in the content an agent reads, such as an email, a calendar invite, or a web page, could redirect agents in five browsers. In one demonstration, an agent had Amazon's shopping assistant order an item on the victim's credit card for shipment to the attacker. [Zenity's release](#) does not claim exploitation in the wild.

Guardio Labs found earlier that Perplexity's Comet browser, asked to buy an Apple Watch, completed a purchase on a fake store Guardio built. [In some runs](#) it auto filled the saved card and address without asking for confirmation.

F-Secure tested a deliberately permissive shopping agent in a lab. A poisoned product review sent the agent to a phishing page in 12% of runs, and the agent submitted personal data there. [The test does not](#) measure how often this happens in the real world.

Protocols and Verification

[Visa's Trusted Agent Protocol](#) has merchants verify a signature (RFC 9421) on each agent request, using the agent's public key. [Mastercard states](#) that only registered agents can transact through Agent Pay. [Google announced](#) its Universal Commerce Protocol (UCP) in January 2026, compatible with its Agent Payments Protocol (AP2).

Visa's page describes how verification works. Neither Visa's nor Mastercard's public page states how many merchants or agents use its protocol, or which attacks it covers. [A July 2026 preprint](#) tested three platforms, including Google's AP2 reference implementation, and reported 33 structural weaknesses in lab conditions with no real funds moved.

Preparation and Mitigations

Security researchers and service providers have recommended a cautious posture and provided guidance on preliminary steps that can help reduce risks before peak shopping season:

1. Classify agent traffic and move it from monitor-only to enforced policy. Log it separately and apply rate limits. Where a protocol such as Visa's Trusted Agent Protocol is supported, verify agent signatures.
2. Tighten card-testing and account takeover controls ahead of Cyber Week. Set velocity limits on card additions and payment attempts and review use of stored payment credentials.
3. Show full line items on any screen where a user approves an agent purchase. [Unit 42 identifies](#) a total-only approval screen as a way to approve a hidden item unknowingly.
4. For any agent your organization operates or sponsors, treat retrieved web content as untrusted input and require human approval for purchases. Limit the agent's payment and data permissions. [Unit 42 recommends](#) design-level defenses because models cannot reliably separate instructions from data.
5. Review checkout pages for injected third-party scripts. [Gambit published](#) the skimmer domains and loader pattern it observed in the campaign, which members can use to hunt.
6. Share any observations of agent-driven fraud with the RH-ISAC.