

PDI analyzed more than **4 trillion security events** to understand how cyberattacks are evolving.

Here are the key trends shaping today’s threat landscape—and what they mean for your environment. For deeper analysis, mitigation guidance, and prevention strategies, watch the full analyst briefing.

View the PDI Threat Intelligence Webinar

|                  |                                       |                                                                                                   |                                                                                                    |                                                                                                          |
|------------------|---------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| What’s Happening | <b>247%</b> surge in exploit activity | <b>35%</b> increase in Ransomware YoY                                                             | <b>Firewalls &amp; VPNs</b> heavily targeted                                                       | <b>Speed &amp; extortion</b> Accelerating attacks                                                        |
|                  | Why It Matters                        |  More Downtime |  Fraud Exposure |  Compliance Pressure |

## Exploits and Edge Device Security

|                  |                                            |                                                                                                                         |                                                                                                                                                                                                                                                                                                                         |
|------------------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What’s Happening | <b>210%</b> more firewall exploit attempts |                                                                                                                         | <b>How PDI Can Help</b> <ul style="list-style-type: none"><li>• Managed firewall services backed by a 24/7 SOC</li><li>• Continuous edge visibility across distributed environments</li></ul> <div>View PDI Analyst Overview</div> |
|                  | Why It Matters                             | Perimeter compromise disrupts operations before detectionRemote access failures cascade across distributed environments |                                                                                                                                                                                                                                                                                                                         |

## Ransomware and Extortion Trends

|                  |                                                                                                                                                                                                                                                                            |                                                                                         |                                                                                                                                                                                                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What’s Happening | Ransomware surged 61% in Q4 due to expanding access paths <ul style="list-style-type: none"><li>• Phishing</li><li>• Supply Chain Attacks</li><li>• Social Engineering</li><li>• Initial Access Brokers</li><li>• Exposed Software</li><li>• Credential Stuffing</li></ul> |                                                                                         | <b>How PDI Can Help</b> <ul style="list-style-type: none"><li>• 24/7 SOC detection and rapid containment</li><li>• Intelligence-driven monitoring across retail environments</li></ul> <div>View PDI Analyst Overview</div> |
|                  | Why It Matters                                                                                                                                                                                                                                                             | Faster attacks reduce the time to respondLayered extortion amplifies operational impact |                                                                                                                                                                                                                                                                                                                  |

## Dark Web and Infostealer Dynamics

|                  |                                                                                                          |                                                                                               |                                                                                                                                                                                                                                                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| What’s Happening | <b>DOWN 24%</b> Market activity down 24% after enforcement actionNew infostealers quickly filled the gap |                                                                                               | <b>How PDI Can Help</b> <ul style="list-style-type: none"><li>• Continuous monitoring for credential exposure</li><li>• Risk prioritization tied to real-world exploitation trends</li></ul> <div>View PDI Analyst Overview</div> |
|                  | Why It Matters                                                                                           | Stolen credentials enable “quiet” accessDelayed detection increases fraud and compliance risk |                                                                                                                                                                                                                                                                                                                        |

Analysis based on threat intelligence collected between January 1 and December 31, 2025, from PDI-monitored environments and additional global sources.

- PDI delivers:
- ✓ Retail-first security expertise
  - ✓ SOC-backed detection and response
  - ✓ Visibility across networks and edge systems
  - ✓ Support for compliance and operational resilience

Discover what this means for your environment

Learn How PDI Can Help