

Arete's H1 2026 Crimeware Report Highlights Ransomware and Extortion Trends

The report explores key threat groups, initial access vectors, threat actor tactics, and the evolving role of AI in cyberattacks in the first half of 2026.

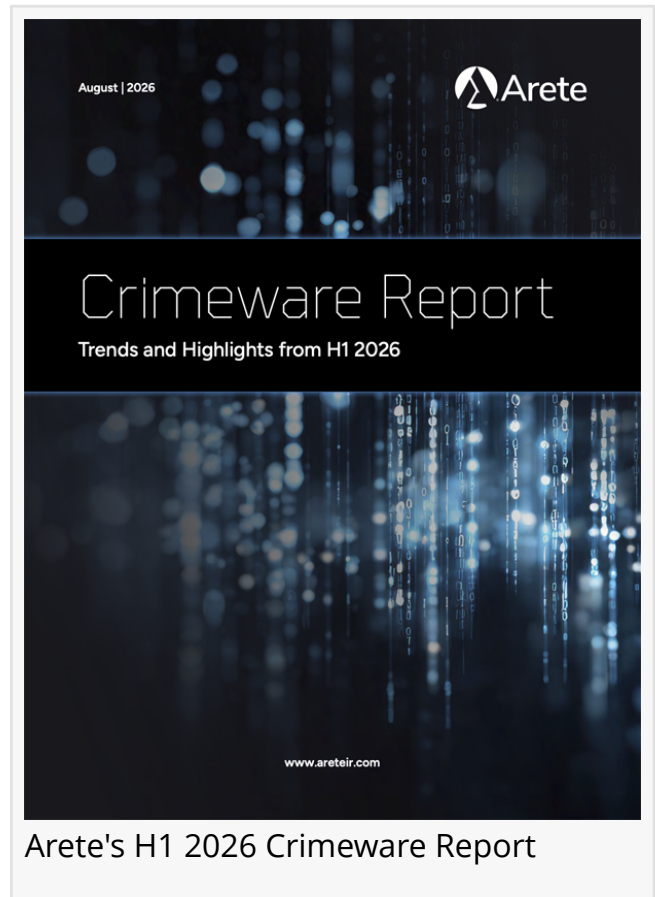
BOCA RATON, FL, UNITED STATES, August 28, 2026 /EINPresswire.com/ -- Arete, a leader in intelligence-led cyber risk solutions, released its H1 2026 Crimeware Report, highlighting key threat groups, initial access vectors, threat actor tactics, and the evolving role of AI in cyberattacks in the first half (H1) of 2026. Arete's global teams collect and analyze data from thousands of engagements to provide actionable intelligence to enterprises, insurance carriers, brokers, law firms, and financial institutions.

Key findings within the report:

- Akira, Qilin, and INC Ransom were the top three threat groups observed in H1 2026, collectively accounting for more than a third of all ransomware and extortion engagements that Arete responded to.
- Vulnerability exploitation, social engineering, and software supply chain compromises remained among the top initial access vectors.
- Threat actors demonstrated a growing focus on trusted third-party platforms, open-source ecosystems, and internet-facing technologies to gain initial access and expand their operational reach.

Threat groups also appeared to be increasingly using AI to analyze stolen victim data and identify high-value information to leverage for ransom extortion.

"In the first half of this year, we saw threat actors increasingly target trusted third-party platforms, open-source ecosystems, and internet-facing technologies," said Chris Martenson, Arete's Chief Data Officer. "Once again, threat actors have evolved their tactics, and the resulting





In the first half of this year, we saw threat actors increasingly target trusted third-party platforms, open-source ecosystems, and internet-facing technologies."

*Chris Martenson, Arete's Chief
Data Officer*

increased risk of high-impact supply chain attacks underscores the need for a dynamic, data-driven approach to cyber resilience," Martenson added.

Arete is committed to helping our partners and clients stay ahead of evolving cyber threats with standardized, intelligence-led detection, response, resolution, and resilience capabilities.

[Download Arete's H1 2026 Crimeware Report.](#)

About Arete

Arete helps organizations stay ahead of cyber threats with standardized, intelligence-led detection, response, resolution, and resilience capabilities. As cyber incidents increasingly intersect with financial crime, we operationalize cyber intelligence from thousands of engagements to drive defensible decisions across response, remediation, recovery, and payment. Our global team of experts provides unparalleled capabilities to address the entire cyber threat lifecycle, from incident response and restoration to advisory and managed security services. Learn more at areteir.com.

Annemarie Cyboron
Arete
marketing@areteir.com

This press release can be viewed online at: <https://www.einpresswire.com/article/936914322>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.