Red Piranha Releases 2026 Threat Intelligence Report Highlighting Shift in Global Cyber Threat Landscape

Red Piranha's 2026 Threat Intelligence Report analyses 80M+ security events, revealing rising cyber espionage, APT activity, and evolving attacker tactics.

Red Piranha's Annual Threat Intelligence Report highlights the rise of APTs and Cyber espionage

MELBOURNE, VICTORIA, AUSTRALIA, March 13, 2026 /EINPresswire.com/ -- Red Piranha, Australia's leading developer and manufacturer of advanced cybersecurity technology, has released its 2026 Annual Threat Intelligence Report, revealing a significant shift in the global cyber threat landscape as attackers increasingly prioritise cyber espionage, persistent access, and long-term intelligence gathering over immediate disruptive attacks.

The report analyses more than 80 million security events, tracking 110 advanced persistent threat (APT) campaigns and thousands of intrusion attempts across enterprise and critical infrastructure environments.

> "The findings reflect a clear evolution in attacker strategy and highlight the need for organisations to rethink how they approach threat detection."
>
> *Adam Bennett, CEO of Red Piranha*

The findings show that modern attackers are adopting espionage-led intrusion strategies, focusing on gaining access to identity systems, establishing persistence within networks, and maintaining covert access to sensitive environments.

Download our Threat Intelligence Report 2026

Key Findings from the Report:
1. Cyber espionage campaigns are increasingly driving modern intrusions, with attackers

prioritising stealth and intelligence gathering
2. Advanced Persistent Threat (APT) groups are adopting identity-based attack methods to gain long-term access to enterprise networks
3. Endpoint Detection and Response (EDR) bypass techniques are becoming deliberate attacker tradecraft
4. Living-off-the-Land techniques allow attackers to operate using legitimate system tools, reducing the likelihood of detection

The report highlights how attackers increasingly exploit identity systems, credentials, and legitimate administrative tools to move laterally across networks and maintain persistent access.

In many cases, disruptive payloads such as ransomware are only deployed after attackers have already established extensive access within a victim environment.

Implications for Security Leaders

The findings suggest that many organisations may still rely too heavily on endpoint-centric visibility, even as attackers adopt techniques specifically designed to evade traditional endpoint monitoring.

To defend against these evolving tactics, the report recommends expanding detection capabilities across identity systems, network traffic, cloud infrastructure, and endpoint telemetry, ensuring that a single blind spot does not allow attackers to maintain persistent access.

To support this approach, Red Piranha delivers Threat Detection, Investigation and Response (TDIR) capabilities through its Crystal Eye platform, combining behavioural analytics, threat intelligence, and cross-domain telemetry to help security teams identify advanced threats earlier in the attack lifecycle.

By correlating activity across multiple security layers, TDIR enables organisations to detect identity abuse, lateral movement, and Living-off-the-Land activity commonly used in advanced cyber espionage campaigns.

Akriti Joshi
Red Piranha
+61 8 6365 0450
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube

X