Red Piranha Shuts Down Ransomware Gang Targeting Australian Legal Sector

Red Piranha has delivered a decisive blow to one of the most advanced phishing campaigns ever detected in the Australian legal sector.

Red Piranha Shuts Down Ransomware Gang Targeting Australian Legal Sector

MELBOURNE, VICTORIA, AUSTRALIA, April 3, 2025 /EINPresswire.com/ -- Red Piranha, Australia's leading cybersecurity company and creator of the Crystal Eye Unified Threat Management platform, has delivered a decisive blow to one of the most advanced phishing campaigns ever detected in the Australian legal sector. The target? A shadowy cybercrime group called SAIGA, which had quietly been breaching Australian legal firms using phishing-as-a-service (PaaS) kits, adversary-in-the-middle (AiTM) proxy attacks, and MFA-bypass techniques to infiltrate Microsoft Office 365 environments.

> This takedown highlights the importance of having advanced threat detection and response capabilities embedded at every layer of defence."
>
> *Adam Bennett, CEO of Red Piranha*

"Threat actors are becoming increasingly sophisticated, deploying adversary-in-the-middle (AiTM) phishing kits capable of defeating MFA and EDR solutions," said Adam Bennett, CEO of Red Piranha. "This takedown highlights the importance of having advanced threat detection and response capabilities embedded at every layer of defence."

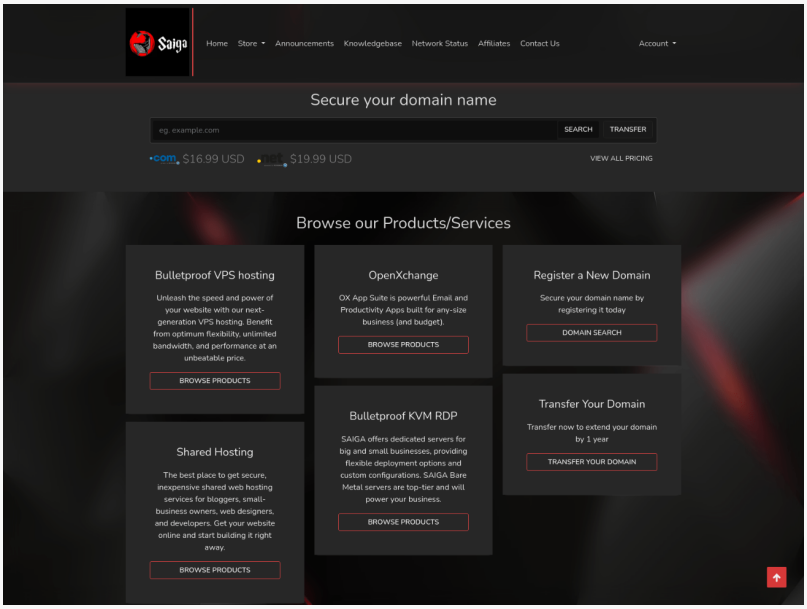
The takedown marks a significant milestone in the fight against phishing-as-a-service (PaaS) operations and ransomware attacks and highlights Red Piranha's leadership in threat detection, investigation, and response.

Inside the SAIGA Group's Phishing Campaign

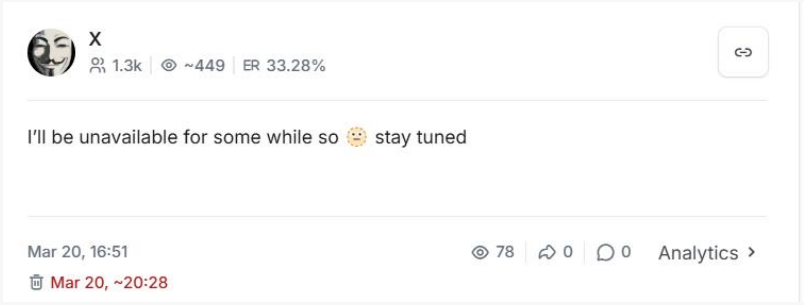
In February 2025, Red Piranha's security threat research team uncovered what would become

one of the most significant investigations of the year so far. It began with what appeared to be a routine email phishing attempt targeting a legal office associated with one of the Red Piranha clients.

But this wasn't just another scam. It was the gateway to an expensive, previously undetected cybercrime operation run by a group known as SAIGA. As Red Piranha security team dug deeper, they quickly realized that they had stumbled onto a sprawling Phishing-as-a-Service (PaaS) ecosystem one far more advanced, organized, and dangerous. The email that triggered the investigation was alarmingly convincing. It replicated the company's branding, featuring real employee signatures and a fake "View Documents" link that redirected victims to a fraudulent Google Sites page. From there, users were lured into a cloned Microsoft 365 login screen, built using a sophisticated Adversary-in-the-Middle (AiTM) phishing kit.



SAIGA Store, billing.saiga-store-hub.com (web.archive.org)



Dismantling the Threat Actor SAIGA

The moment a user entered their email address, the phishing kit sprang into action verifying credentials in real time against Microsoft servers, pulling in company logos, and harvesting cookies and session tokens.

The stolen data, including email addresses, passwords, session cookies, and even network information, was immediately pushed to Telegram bots controlled by SAIGA operators. This was no smash-and-grab it was a fully operational credential interception machine, designed for persistence and scale.

The phishing infrastructure was found to be part of a broader campaign orchestrated by SAIGA Group, a ransomware-as-a-service (RaaS) and financial crime syndicate operating largely via Telegram. The group offered high-priced phishing kits and services to criminal clients worldwide.

Their phishing kits included real-time credential validation, proxy login mechanisms, and tools

for long-term access and lateral movement within compromised environments.

Red Piranha's security investigation revealed a vast and active criminal infrastructure:

123 phishing domains used in active campaigns
70 Telegram bots delivering stolen data to threat operators
Over 8,000 compromised credentials harvested from legal and professional email systems
Extensive use of AiTM tactics to bypass MFA
Real-time credential validation via proxied logins to Microsoft servers

SAIGA's phishing pages were supported by a backend built on Evilginx, customized with Telegram-based alerting and integrated cookie theft for persistent access. The operation's infrastructure included C2 servers, phishing dashboards, and obfuscated code to avoid detection.

Through advanced threat hunting and OSINT, Red Piranha was able to uncover connections between Telegram usernames, bot tokens, and server-side configurations, mapping out the full extent of the SAIGA campaign.

Dismantling the Threat Actor SAIGA

Armed with this intelligence, Red Piranha launched a coordinated counteroffensive. Within days of public disclosure, the SAIGA network began to crumble. Their phishing domains stopped resolving or returned API errors. Telegram channels vanished, renamed, or went private. Gitea and GitLab repositories were scrubbed.

Even the TikTok account was deleted. The infrastructure that had once delivered stolen data in real time went dark. This wasn't just an investigation it was a dismantling. Red Piranha didn't just discover SAIGA's tools; they exposed its users, disrupted its operations, and shattered its footprint.

Beyond the technical win, the investigation sent a clear message to the legal sector: sophisticated phishing campaigns have evolved beyond simple deception. With attackers now bypassing MFA through AiTM tactics and credential hijacking, traditional defences are no longer sufficient.

Law firms and high-value industries must adopt real-time Threat Detection, Investigation, and Response (TDIR) capabilities if they hope to stay ahead of modern threat actors. Red Piranha's proactive measures didn't just protect one client, they pre-emptively secured countless others.

In line with its role as the sole APAC member of the Cyber Threat Alliance, Red Piranha distributed all Indicators of Compromise (IOCs) including domains, hashes, bot tokens, and IP addresses across its Crystal Eye threat platform and the wider threat intelligence community.

By feeding this intelligence directly into its intrusion prevention, DNS sinkholing, and anti-phishing mechanisms, Red Piranha ensured SAIGA's infrastructure could no longer operate undetected. As of March 2025, over 88 criminal users were believed to be operating under SAIGA, with 123 domains and 64 unique usernames linked to the group. Thanks to this investigation, those numbers are no longer growing they're collapsing.

What started with a single phishing email evolved into a campaign takedown that reverberated across the cybercrime underworld. Red Piranha exposed not just a phishing kit, but an entire PaaS economy. SAIGA operated in the shadows. Red Piranha turned on the lights.

About Red Piranha
Red Piranha is an Australian cybersecurity firm specializing in unified threat management and advanced threat intelligence. Its flagship product, Crystal Eye, provides enterprise-grade security to organizations globally, integrating firewall, endpoint protection, threat intelligence, and security orchestration into a single platform.

As the only APAC-based member of the Cyber Threat Alliance, Red Piranha collaborates internationally to ensure timely, intelligence-driven cybersecurity outcomes for its clients.

Swati Gupta
Red Piranha
0402337485
email us here
Visit us on social media:
Facebook
X
LinkedIn
Instagram
YouTube
