Atumcell Research Reveals Widespread Domain Spoofing Vulnerabilities Among Private Equity Firms and Portfolio Companies

55 percent of domains not fully protected. No firm has fully protected its entire portfolio despite growing threat from phishing

Atumcell

BOSTON, MA, UNITED STATES, November 25, 2024 / EINPresswire.com/ -- Atumcell, a leading provider of cybersecurity solutions for private equity firms, has released a new research brief uncovering a critical vulnerability in email domain protection across the private equity sector. The analysis, covering 159 middle-market PE firms and their 2,700+ portfolio companies, shows that a majority of domains remain susceptible to spoofing—a tactic commonly exploited by cybercriminals to launch phishing attacks.

> Private equity firms and their portfolio companies are high-value targets for phishing attacks due to their deep pockets and frequent high-stakes communication”
>
> *Matthew T. Carr, Head of Research & Technology*

Key Findings:
- 21% of domains are fully vulnerable to spoofing attacks.
- 34% of domains are only partially protected, indicating improper or incomplete configuration of email security protocols (SPF, DKIM, DMARC).
- Only 45% of domains are fully protected
- No PE firm analyzed has implemented full protection across its entire portfolio, highlighting a pervasive blind spot in cybersecurity.

“Private equity firms and their portfolio companies are high-value targets for phishing attacks due to their deep pockets and frequent high-stakes communication,” said Matthew T. Carr, Head of Research & Technology at Atumcell.

Domain spoofing is a gateway for sophisticated phishing attacks that can lead to data breaches,

financial loss, and reputational damage. Many companies underestimate this risk, often focusing on employee training without addressing the root cause: poorly configured email security settings. The new research from Atumcell ranks the top 20 PE firms based on their vulnerability, providing a roadmap for improving defenses.

“Atumcell’s goal with this research is to highlight a major threat that is remarkably widespread” said David E. Williams, Atumcell CEO. “PE firms should strive for a perfect score; there’s no reason not to achieve it. We’ve seen individual firms make remarkable progress across their portfolios once they focus their teams on it.”


Matthew T. Carr, Atumcell Head of Research & Technology


David E. Williams, Atumcell CEO

Additional Highlights:
- The research points out that security audits, penetration tests, and vulnerability scans often fail to address domain spoofing risks adequately.
- The analysis covered primary domains, but many firms have additional URLs (e.g., Atumcell’s own Atumscan.com) that remain unprotected despite not being used for email communication. These domains can still be exploited by attackers to trick users.
- Companies tend to blame employees for falling for phishing attacks. Before doing so they should secure their own domains against spoofing and restrict how their email clients handle messages from spoofable domains
- Atumcell offers a free spoof checking tool where users can determine whether any domain is spoofable and receive recommendations

on how to improve the configuration
- Atumcell’s cybersecurity operating system for private equity firms delivers a holistic view of portfolio-level security, enabling firms to monitor, manage, and improve their cybersecurity posture effectively.

About Atumcell

Atumcell provides a comprehensive cybersecurity operating system designed to meet the unique needs of private equity firms and their portfolio companies. With innovative tools and a strategic approach, Atumcell helps clients perform due diligence, protect their assets, enhance security maturity, and mitigate the risks of cyber threats. Atumcell’s advanced penetration testing offers comprehensive validation of security measure for PE firms and portfolio companies.

David E Williams
Atumcell Inc.
+1 617-671-8810
email us here
