


Top Private Equity Firm Prevents Possible Breach of Portfolio Company

The Customer

 Portfolio of across multiple industries including financial services, technology, healthcare, consumer goods, and more

 Over \$8 billion in assets



“We very likely narrowly avoided a catastrophic network intrusion for our portfolio company. The ROI on Flare’s monitoring is massive, as a strong cybersecurity posture is extremely important throughout the venture cycle.”

– Security Team Director, Private Equity Firm

Threat actors can cause major breaches with initial access obtained through the Genesis Market: a clear web market selling infected computers, offering buyers credentials and cookies belonging to the infected devices’ owners. Threat actors can then use social engineering techniques to elevate their level of access, sometimes all the way up to source code.

Cybercriminals continue to innovate their methods of attack, and a single stolen string of text or cookie can possibly lead to millions of dollars in costs and potential ransomware attacks. Security teams can become overwhelmed with the sheer amount of information needed to analyze to respond to threats.

A relatively small piece of stolen sensitive information can cause a massive data breach, which would be disastrous for the future valuation or M&A activities of the private equity firm’s portfolio companies.

Challenge: Private Equity Firm's External Attack Surface Includes Portfolio Companies

For a private equity firm, their external attack surface spans to include all of their portfolio companies. If the evaluation process for an M&A turns up an infected device, this could greatly impact the valuation of the company and ROI for the private equity firm.

With Flare, this private equity firm prevented a potentially catastrophic network intrusion for one of its portfolio companies. The Flare platform alerted the organization's security team about an infected device for sale on the Genesis Market that contained cookies for a webmail server located inside the company internal network among other banking and payment application credentials.



“We reduced risk greatly by finding and mitigating a serious threat that could have impacted.”

- Security Team Director, Private Equity Firm

Benefit: Red Teamer Finds Infected Device Before Threat Actors Do

Due to the very specific subdomain shown in the Genesis listing (webmail.companyname.com), the private equity firm's red team analyst had a high level of confidence that the infected computer belonged to an employee of the portfolio company.

Following approval from the portfolio company, the security team obtained access to the credential for sale. This provided access to the corporate mailbox of the employee, including:

- a huge amount of attachments
- personal information
- other documents that could easily be leveraged by a malicious actor

Both the investment firm and their portfolio company agreed that this infected computer access, sold on Genesis Market for about \$100, could have had disastrous consequences for the firm.

Gartner **4.9**
Peer Insights™ ★★★★★

[Sign Up for a Free Trial](#)



flare.io

hello@flare.io