Credential Breach Hits U.S. Military & Defense Partners—Cyber Dagger CEO John Rodriguez on What Must Change

FBI, GAO, Treasury, Lockheed Martin and Honeywell Also Among Those Breached; Rodriguez Says It's a Wake-Up Call and EDR Alone Won't Protect You

DALLAS, TX, UNITED STATES, February 24, 2025 /EINPresswire.com/ -- When it comes to cybersecurity, most people assume that the U.S. military and top defense contractors—organizations responsible for safeguarding the nation's most sensitive information—have ironclad protections in place. But a recent cyber breach tells a different story.

> If an attacker can breach what are supposed to be some of the world's most secure environments, that should be a wake-up call. The cybersecurity industry needs to...start thinking like the adversary"
>
> *John Rodriguez, Cyber Dagger Founder and CEO*

A new report released in February 2025 revealed that hackers using infostealing malware successfully compromised credentials from high-profile organizations, including the U.S. Army, U.S. Navy, Boeing, Lockheed Martin, and Honeywell. According to a separate report by cybersecurity firm Hudson Rock, the infiltration also impacted the FBI, the Government Accountability Office (GAO) and the Treasury Department, which was breached through a BeyondTrust compromise.

"If an attacker can breach what are supposed to be some of the world's most secure environments, that should be a wake-up call," said John Rodriguez, CEO and founder of Cyber Dagger. "The cybersecurity industry needs to move beyond passive defense and start thinking like the adversary."

A VETERAN'S PERSPECTIVE ON CYBER THREATS

Rodriguez has spent years on the front lines of cybersecurity, dissecting attack patterns and helping organizations defend against real-world threats. His deep military background makes him uniquely qualified to assess and combat the dangers posed by cyber adversaries.

With more than a decade of service in the U.S. Air Force, Rodriguez has been at the forefront of

cybersecurity, specializing in offensive security and red team operations. He led red teams tasked with identifying vulnerabilities in military systems, consulted on offensive artificial intelligence advancements and served as a certified U.S. Air Force instructor, training red teams nationwide.

After transitioning from military service, Rodriguez launched Cyber Dagger, a service-disabled veteran-owned small business dedicated to providing advanced cybersecurity solutions. With more than 13 years of experience, his company helps organizations safeguard their systems against evolving and sophisticated cyber threats.

John's credentials as a certified USAF instructor and leadership in training Red Teams nationwide speak to his deep expertise.

WHY EDR SOLUTIONS ARE NOT ENOUGH

Rodriguez warns that these recent breaches expose a dangerous misconception—the belief that endpoint detection and response, or EDR, tools alone can provide full protection.

“Despite some EDR vendors marketing their solutions as highly effective or even fully protective in MITRE evaluations, the reality is that EDR tools alone do not provide a complete security solution,” Rodriguez said. “While companies like CrowdStrike, Microsoft, Trellix, Palo Alto Networks and SentinelOne participate in these evaluations, real-world threats often behave very differently from what is tested in controlled environments.”

Rodriguez, who has extensive experience with MITRE testing, cautions against placing too much trust in results from controlled assessments.

“When vendors know what to expect in an evaluation, they can tailor their detections to showcase their products in the best possible light,” he said. “The problem is that these tests don’t always reflect the diverse and adaptive tactics used by real threat actors with specific objectives. Relying solely on controlled performance metrics can be dangerously misleading.”

He urges organizations to think beyond traditional solutions and adopt a more proactive cybersecurity approach.

“If you value your data, don’t just take marketing claims at face value—do your own research, conduct trials and test products in real-world conditions,” Rodriguez said. “If infostealing malware can compromise what are supposed to be some of the world’s most secure environments, just imagine what advanced threat actors are capable of.”

FIVE CRITICAL CYBERSECURITY LESSONS FROM THE LATEST BREACHES

Rodriguez outlines five key takeaways from the recent malware breaches and what companies—large and small—must do to protect themselves in an increasingly hostile cyber landscape.

1). EDR solutions are not a silver bullet

Many organizations rely on EDR tools as their primary defense, but these solutions are far from foolproof. MITRE evaluations showcase a product’s effectiveness under controlled conditions, but real-world attacks are unpredictable and often bypass these tools. Organizations must layer multiple security measures to close the gaps.

2). Human error is still the biggest weakness

Infostealing malware typically infiltrates networks through phishing emails, compromised credentials and unsafe downloads—all stemming from human error. No technology can replace proper cybersecurity training and strong zero-trust policies that limit access to sensitive data.

3). Threat actors are constantly evolving

Hackers don’t follow a script. They adjust, experiment and evolve their techniques to stay ahead of cybersecurity defenses. This breach proves that even the most secure environments can be compromised when attackers find new ways to bypass detection. Organizations need to simulate real-world threats through red teaming and proactive threat hunting.

4). Supply chain security matters more than ever

The military and defense contractors work with a vast network of vendors, suppliers and partners—each of whom may have weaker security measures. A single compromised credential can serve as a backdoor into critical systems, making supply chain security a top priority.

5). Test your defenses like an attacker would

Instead of relying on security vendors’ claims, companies must actively test their own systems using real-world threat emulation. Organizations should trial security products in live environments, conduct red team exercises and regularly audit their defenses to ensure they can withstand advanced, adaptive threats.

“Don’t just take vendor claims at face value. Conduct real-world tests, trials and audits to understand the true resilience of your cybersecurity measures,” Rodriguez said.

ABOUT CYBER DAGGER:
Cyber threats aren’t slowing down, and neither should your security strategy. Cyber Dagger specializes in proactive threat emulation, red team operations and customized security solutions to help businesses stay ahead of evolving attacks. Whether you're a small business, enterprise or government contractor, Cyber Dagger's veteran-led team is equipped to identify vulnerabilities, simulate real-world threats and fortify your defenses before attackers can exploit them. Don’t wait for a breach to expose your weaknesses—take action now. Contact Cyber Dagger today to secure your organization and stay ahead of the next cyber threat.

Media Contact: John Rodriguez, Founder & CEO
Cyberdagger LLC
+1 210-773-6075
email us here
Visit us on social media:
LinkedIn
