LEADING, EGYPT-BASED OFFENSIVE SECURITY AND DARK WEB MONITORING BUSINESS - BUGUARD - ANNOUNCES SEED FUND RAISE

Fund raise led by A15, the leading MENA Venture Capital firm

Buguard leads protection against the growing dark web cyber threat: GCC expansion planned in 2023

Cairo, Egypt – 7 August 2023 – Buguard, the Cairo-based offensive security and dark web monitoring company, announces the successful completion of a US$500,000 seed fund raise.

The fund raise was led by A15, the leading MENA venture capital firm, and renowned as one of the most prominent backers of early-stage start-ups in the region, with participation from angel investors.

The capital is Buguard's first external funding, with the company having been bootstrapped since its 2021 launch. Proceeds will be used to grow Buguard's team, focusing on product, sales, and channel partnerships.

Buguard offers offensive security services including penetration testing and vulnerability assessment, phishing simulation, compromise assessment, threat intelligence and red teaming. Since it commenced operations, Buguard has served many of Egypt's leading businesses in their respective fields including Paymob, Fawry, EFG-Hermes, Halan, Lucky, Thndr, MaxAB, Eksab, Rabbit Mart, amongst others. Buguard has developed a global client base spanning Saudi Arabia, the United States, France, Australia, Japan, the United Kingdom, Singapore, and the United Arab Emirates.

Alongside its existing offensive security services, Buguard is proud to announce the official launch of *Dark Atlas*, its new SaaS product for dark web monitoring and account takeover prevention.

The dark web is a hidden part of the internet often used by cybercriminals to distribute malware which can lead to capturing of personal credentials such as usernames, passwords, and payment card details. The impact of such attacks can be significant, causing financial loss, reputation damage, and loss of stakeholder trust. In its Cost of a Data Breach Report, IBM Security reported the average cost of a data breach in 2022 was $4.35 million, an all-time high. The same report highlighted that use of stolen or compromised credentials remains the most common cause of a data breach. Stolen or compromised credentials were the primary attack vector in 19% of breaches in the 2022 study and the top attack vector in the 2021 study, having caused 20% of breaches.

Youssef Mohamed, Founder and Chief Technology Officer of Buguard, said:

"We are delighted to announce our fund raise, and I thank A15 for its great support. The world of dark web cyber threats is very real, dynamic and growing. Any company can be a victim and one must be prepared. Our team at Buguard is hand-picked and includes some of the world's leading security researchers and engineers, coupled with a subscription-based, SaaS product - Dark Atlas - that goes broader and deeper than existing alternative solutions.

"We are already globally facing with clients across the world, but our immediate strategy is to grow even stronger in the GCC. We look forward to expanding into Saudi Arabia during 2023 and using our proceeds to help fulfil our significant growth potential."

Buguard has several competitive differentiators. For data leak monitoring, most products focus on public data breaches, which means publicly exposed databases. *Dark Atlas* is much broader and

deeper than alternative solutions. It monitors compromised devices for information stealer malware such as Redline, Raccoon, and Vidar, which are the root causes of most material data breach incidents and pose a serious threat as the stealer malware exfiltrates saved credentials from the victims' browsers and has the relevant URL within which the credentials can be used.

It also monitors dark web marketplaces, hacking forums, underground channels, and private clouds to identify and help neutralize breaches across different venues. Buguard recently managed to identify and utilise a coding flaw that allowed it to lock out operators of the Mars Stealer malware, a data-stealing malware as a service which allows cybercriminals to rent access to the infrastructure to launch their own attacks, from their own servers and release their victims.

Also, *Dark Atlas* add-on features offer clients extra protection by monitoring third-party/vendors threats landscape and C-level personal emails. It also proactively puts clients a step ahead of attack impersonators and phishing attacks, by discovering all the similar/impersonation domains for clients' brands.

Karim Beshara, A15 General Partner, commented:

"We have been very impressed by the domain expertise exhibited in Buguard's security researchers and engineers and are very excited to partner with Youssef and Buguard's best-in-class team. Threats posed by ever evolving cybercriminal tactics are a serious threat to businesses, both large and small. It is becoming increasingly important to take proactive measures to protect against these threats. Buguard does just that through its security services and Dark Atlas."

Buguard was founded by Youssef Mohamed in 2021. Its consultancy team comprises highly skilled security researchers and senior offensive security engineers. The team is renowned for finding critical security vulnerabilities in almost every big tech giant such as Yahoo, PayPal, Twitter, Snapchat, Mail.Ru, Epic Games, Amazon, eBay, Microsoft, Dell, Adobe, AT&T, Vodafone, and the U.S. Department of Defence.

<ends>

Further information

Thoburns

Johanna Lawson-Dick

j.lawsondick@thoburns.com

+44 7539031841

Buguard

Public Relations & Corporate Communications

Press@buguard.io