Allot Telco Security Trends Report Reveals CSP Security Services Prove Highly Effective in Protecting Consumers from Mobile and IoT Threats

Findings show almost two billion security threats blocked during four-month period across seven million subscribers

HOD HASHARON, Israel, June 12, 2018 /PRNewswire/ -- Allot Communications Ltd. (NASDAQ: ALLT) (TASE: ALLT), a global provider of leading innovative network intelligence and security solutions for service providers worldwide, released findings from its Telco Security Trends Report, revealing a dynamic and automated threat landscape in which consumers lack the security expertise to effectively protect themselves. Mobile and Internet of Things (IoT) continue to be primary attack vectors, contributing to a spike in cryptojacking, adware, and distributed denial of service (DDoS) attacks.

The Telco Security Trends Report is based on anonymous data gathered from four communications service providers (CSPs) across Europe and Israel, who between them, protect seven million customers. It found that during the period from November 2017 to February 2018, nearly two billion mobile security threats were blocked – an average of two each day per mobile device. Of those security protections:

- Almost one billion were triggered by cryptomining malware, the leading security threat, corresponding to the rise in cryptocurrency valuation in late 2017/early 2018
- Over one hundred million threats were triggered by adware only
- Forty thousand threats were triggered by direct attacks in the form of ransomware and banking trojans

The escalating IoT Threat Landscape?

As part of this study, Allot set up honeypots simulating consumer IoT devices and exposed them to the Internet. Results showed immediate successful attacks, peaking at a rate of over one thousand per hour, with findings revealing that a device can get infected within 42.5 seconds of being connected to the Internet. There was also an increase of unique IP

addresses attacking the honeypots over time, from 44 per day to a peak of 155 per day in less than a month of exposure.

Connected devices are forecast to grow to almost 31 billion worldwide by 2020. To help combat rising threats across this expanding mobile and IoT attack surface, the Telco Security Trends Report found that CSPs are best positioned to deliver a unified, multilayer security service delivered at the network level to the mass market. By merging value-add network-based security with built-in customer engagement capabilities, CSPs can simultaneously achieve rapid customer acquisition and high adoption rates of 40 percent, while generating incremental revenue.

"Cybercrime has become rampant across the growing mobile and IoT attack surface due to the financial motivation it provides" said Ronen Priel, VP Product Management at Allot. "CSPs can differentiate themselves from the competition by offering value-added security services to subscribers who are constantly under attack, while generating incremental revenue. It's a win-win for both the CSP and subscriber."

Read the full Telco Security Trends Report on how CSPs can help deliver value-added security to the mass market while generating significant revenue: [LINK]

About Allot

Allot Communications Ltd. (NASDAQ, TASE: ALLT) is a provider of leading innovative network intelligence and security solutions for service providers worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-based security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our industry leading network-based security as a service solution has achieved over 50% penetration with some service providers and is already used by over 18 million subscribers in Europe. Allot. See. Control. Secure. For more information, visit www.allot.com.

Safe Harbor Statement

This release contains forward-looking statements, which express the current beliefs and expectations of Company management. Such statements involve a number of known and unknown risks and uncertainties that could cause our future results, performance or achievements to differ significantly from the results, performance or achievements set forth in such forward-looking statements. Important factors that could cause or contribute to such differences include risks relating to: our ability to compete successfully with other companies offering competing technologies; the loss of one or more significant customers; consolidation of, and strategic alliances by, our competitors, government regulation; the timing of completion of key project milestones which impact the timing of our revenue recognition; lower demand for key value-added services; our ability to keep pace with advances in technology and to add new features and value-added services; managing lengthy sales cycles; operational risks associated with large projects; our dependence on third party channel partners for a material portion of our revenues; and other factors discussed under the heading "Risk Factors" in the Company's annual report on Form 20-F filed with the Securities and Exchange Commission. Forward-looking statements in this release are made pursuant to the safe harbor provisions contained in the Private Securities Litigation Reform Act of 1995. These forward-looking statements are made only as of the date hereof, and the company undertakes no obligation to update or revise the forward-looking statements, whether as a result of new information, future events or otherwise.

Contacts
Allot
Vered Zur
VP Marketing

+972-9-761-9241
vzur@allot.com

Red Lorry Yellow Lorry for Allot
US – Justin Ordman
+1-857- 217- 2886

UK – Emma Davies
+44 (0)20 7403 8878
allot@rlyl.com