+91 80 6659 8700
+91 80 6696 3333
info@subex.com
www.subex.com

November 13, 2019

To
BSE Limited
The National Stock Exchange of India Limited

Dear Sir/Madam,

Sub: Press Release-Subex releases the State of IoT Security Report India for Q3 2019

As per Regulation 30 of the SEBI (LODR) Regulations, 2015, please find enclosed the Press Release which the Company intends to make.

Kindly broadcast the same on your website on November 13, 2019.

Thanking you.

Yours truly,
For Subex Limited

G V Krishnakanth
Company Secretary & Compliance Officer

Subex releases the State of IoT Security Report India for Q3 2019

26 percent rise in attacks reported; quality and volume of attacks show a significant increase

13th NOVEMBER 2019, BENGALURU, INDIA - Subex today released the findings of its State of Internet of Things (IoT) Security Report for the third quarter (July-September 2019) of this calendar year in Bangalore today. The report, based on threat intelligence data gathered from across 16 cities all over India, outlines key sectors being attacked, the methods of attack, malware, and variants deployed and key cities that are being attacked and studied by hackers, malware developers and hacktivist groups.

Key findings:

- Mumbai, New Delhi, and Bengaluru are attracting the maximum number of cyberattacks
- Smart cities, financial services, and transportation sectors lead the sectoral rankings in terms of cyberattacks
- The unit cost of malware rises leading to hackers procuring malware from new sources to target the country
- The number of cyberattacks registered a 26 percent jump in the quarter
- A strong correlation between cyberattacks and regional geopolitical episodes
- Corrosion attacks on firmware register a significant rise
- Connected infrastructure components linked to smart cities, industries, transportation infrastructure and data centers clear targets for hackers

The study identified over 3500 modular malware samples in the country registering a whopping 37 percent increase. Malware of varying degrees of sophistication are being reported from a variety of deployments including new projects surrounding renewable energy. Most malware detected (36 percent) could be traced to sources on the Darkweb while as much as 14 percent of malware couldn't be traced to a known source pointing to the arrival of new actors and malware shops on the scene.

The detection of malware connected with critical infrastructure projects has also registered an increase. This implies that hackers are targeting large scale disruption and are working to increase the cost associated with managing such projects as also negatively impact future investments in them. High reconnaissance activity detected points to hackers monitoring systems and response mechanisms to thwart and limit attempts to intervene to detect malware, contain the infection and also trace the sources of cyberattacks.

Activities linked to cyberattacks are concentrated in Bangalore, New Delhi, and Mumbai. These three cities together accounted for roughly 38 percent of all attacks registered by us.

Independent hackers are increasingly feeling the need to monetize cyberattacks as the unit cost of malware has risen in the last quarter. Further, it is becoming increasingly difficult to source high-grade malware from multiple sources due to various factors.

"The volume and complexity of malware detected in the country are a clear source of concern. As the digital footprint of India increases through capital intensive projects, hackers are targeting data and large scale disruption like never before. The increase in cyberattacks against the country and the strong geopolitical correlation indicate high levels of interest in targeting our critical infrastructure. At both ends of the spectrum i.e., high-quality malware deployed for strategic objectives and operational malware meant for a specific purpose, hackers are working to improve their ability to monetize cyberattacks. We hope this report helps frame a coordinated response to the challenge posed by hackers and adversarial groups," said Vinod Kumar, Managing Director and CEO, Subex.

Subex will also be releasing similar state of IoT Security reports for ASEAN and the Middle East over the next few weeks while a global version of the report is expected to come out in early December.

About Subex

Subex is a pioneer in enabling Digital Trust and Optimization for Communication Service Providers. Founded in 1992, Subex has spent over 25 years in enabling 3/4th of the largest 50 CSPs globally achieve competitive advantage. By leveraging data which is gathered across networks, customers, and systems coupled with its domain knowledge and the capabilities of its core solutions, Subex helps CSPs to drive new business models, enhance customer experience and optimize enterprises.

Subex leverages its award-winning product portfolio in areas such as Revenue Assurance, Fraud Management, Asset Assurance and Partner Management, and complements them through its digital solutions such as IoT Security and Insights. Subex also offers scalable Managed Services and Business Consulting services.

Subex has more than 300 installations across 90+ countries.

In case of any queries, please reach out to-

Sandeep Banga
Marketing and Communications
+91 99168 24122
sandeep.banga@subex.com

Prachi Zalani
Genesis Burson Marsteller
+91 96069 00307
Prachi.zalani@genesis-bcw.com

-END-