Source : www.thehindu.com Date : 2021-08-29

‘RANSOMWARE WILL DOMINATE THE CYBERCRIME LANDSCAPE’

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Cyberthreats are evolving rapidly and becoming more sophisticated and complex. Operators leverage real-world events to deceive individual victims, enterprises and governments all over the globe, including in India, says ***Anil Valluri,*** *regional VP – India and SAARC, Palo Alto Networks. Excerpts:*

What is the latest from the world of ‘bad actors’?

Ransomware Evil, REvil or Sodinokibi, a ransomware-as-a-service (RaaS) operation has emerged as one of the world’s most notorious and latest ransomware operators. This criminal group provides adaptable encryptors and decryptors, infrastructure and services for negotiation communications, and a leak site for publishing stolen data when victims don’t pay the ransom demand.

As per our observation of cases, REvil and its affiliates pulled in an average payment of $2.25 million during the first six months of 2021.

Last month, it extracted $11 million payment from the U.S. subsidiary of the world’s largest meat packing company based in Brazil, demanded $5 million from a Brazilian medical diagnostics firm and launched a large-scale attack on dozens, perhaps hundreds, of companies that use IT management software from Kaseya VSA. Unit 42, a response-ready global team comprising threat researchers and cybersecurity consultants, has been monitoring threat actors involved in ransomware attacks and has worked over a dozen REvil cases so far this year.

What kind of cyberthreats are likely to increase?

Ransomware is going to dominate the cybercrime landscape. A report prepared by Unit 42 and The Crypsis Group incident response and digital forensics firm, notified several disturbing threat trends.

In 2020, the average ransom payment by organisations increased nearly threefold ($1,15,123 in 2019 to $3,12,493 in 2020); the highest ransom payment doubled ($5 million in 2019 to $10 million in 2020), and the highest ransomware demand also doubled ($15 million in 2019 to $30 million in 2020).

At least 16 different ransomware variants are now exploiting victims by encrypting and stealing/threatening to expose data. The NetWalker ransomware gang leveraged this tactic the most, having leaked data from 113 victim organisations globally.

Industry data indicated healthcare was the most targeted and vulnerable sector in 2020 and the sector continues to be under further attacks by RaaS models.

India too has witnessed similar attempts of attacks happening around COVID and vaccination.

Data witnessed a humongous growth in the last 18 months. Do we have any statistics available?

As per an annual study by IDC, DataSphere and StorageSphere forecasts, the quantum of data created and replicated experienced unusually high growth in 2020 due to a dramatic increase in the number of people working, learning, and entertaining themselves from home. Surprisingly, less than 2% of this new data was saved and retained into 2021. The rest was either ephemeral (created or replicated primarily for consumption) or temporarily cached and subsequently overwritten with newer data.

The cyber mafia has always been trying to keep pace with protection technology. How can we widen the gap?

The need of the hour is an integrated platform using ML (machine learning) and AI (artificial intelligence) to lift the burden off cybersecurity teams.

Using AI, the frequently observed threat data and multiple threat feeds can be automated and left to ML algorithms that can decipher attack patterns, leaving cybersecurity teams to spend time on advanced threat hunting.

We, at Palo Alto Networks, believe the future of cybersecurity depends on a platform approach, which will allow cybersecurity teams to focus on security rather than integrating solutions from different vendors.

The reputational, operational, legal, and compliance implications could be considerable if cybersecurity risks are neglected.

Our code of editorial values

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com