OVER 5 LAKH MALWARE INFECTIONS DETECTED IN 4 LOCAL TELCO OPERATORS

TANZID SAMAD CHOUDHURY

INFOGRAPHICS: **ZARIF FAIAZ**

A staggering 5,25,820 counts of malware infections have been identified in the four telecom operators in the country, according to the Horizon Scanning Report for Bangladesh Telecom Operators prepared by the cyber threat intelligence researchers of Bangladesh e-Government CIRT (Computer Incident Response Team). These counts of malware infections have been accounted for during the first quarter of this year, i.e. from January 2022 to April 2022.

All four telecom operators in Bangladesh have a significant infection rate of numerous malware for network communications.

Grameenphone, having the highest subscriber base with 83.02 million users, leads the way with 294,657 total malware counts and 47 unique counts of malware infections. The virus called 'android.hummer' has the highest infection rate of 24.4%.

Coming in second place is Robi Axiata, with 104,578 total malware counts, having 40 unique counts of malware infections. The 'avalanche-andromeda' virus has a 12.85% infection rate and leads the malware chart for the second-largest telecom operator in the country.

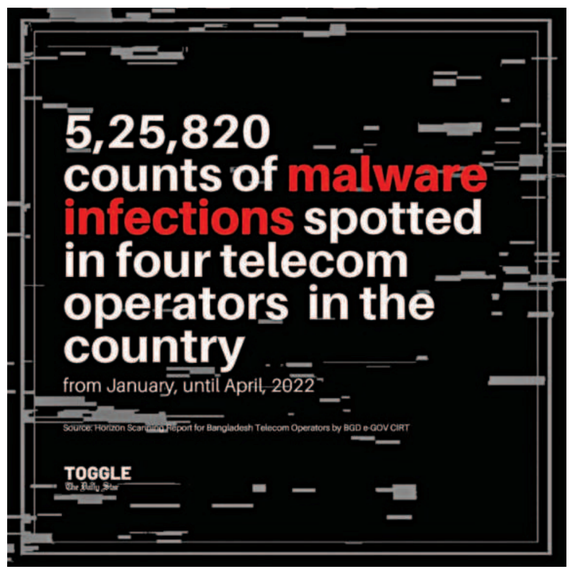
Meanwhile, Banglalink, having the third-highest subscriber base with 37.41 million users, has a total malware count of 98,423 with 31 unique cases of software infections. The infection rate is highest for the 'android.hummer' virus, as it has an infection rate of 21.64%.

Teletalk, the government-based telecom operator, has a total malware count of 28,162 with 31 unique malware infections. The 'avalanche-andromeda' virus has the highest count having an infection rate of 11.39%.

Unsurprisingly, all the operators have the highest number of infections in Dhaka, the capital city of Bangladesh.

According to a globally accessible knowledge base of hacking techniques based on real-world observations, developing and refining the necessary analytics is vital as it can aid in detecting evidence which can confirm the presence of malware.

It was observed that significant malware viruses, including 'android.



hummer' and 'avalanche-andromeda', were delivered by malicious applications through authorised App Stores on Android and iOS platforms or other means.

It may come as a surprise as authorised app stores need developer registration and use vetting techniques to detect malicious applications. However, hackers can bypass these settings by downloading changing codes while a program is running or by making information difficult to comprehend. They may also try to avoid getting caught by placing codes in a malicious application to deduce whether it is running in an app analysis environment or not.

The hackers may also employ fake IDs, credit cards, etc. to create developer accounts to publish malicious applications in the App Stores.

Contrarily, the hackers may use other delivery methods to place malicious applications into the users' smartphones. These include sending phishing links with emails, text messages, websites, QR codes, etc. Installing apps from third-party vendors can also lead you to give away your data to cybercriminals, as they can easily access the files on your smartphone upon installation. The users should always remain cautious when any email directs them to provide personal credentials to avoid potential infiltration into their accounts.

Users must practise caution when installing apps on their smartphones. Apple users need to provide explicit permission before installing third-party apps and should avoid these apps altogether unless they know the sources. On the other hand, Android users need to enable the "Unknown Sources" setting to install third-party apps. Hence, they should refrain from allowing this setting to prevent potential data theft from their devices.

App developers can take precautions to protect their account credentials and enable multi-factor verification upon availability. They should also safeguard their signing keys from falling into the wrong hands.

Bangladesh e-GOV CIRT suggested that telecom operators take the necessary measures to protect their IT infrastructure. They mentioned that the operators should check their detection tools to detect the IOCs (Indicator of Compromises) mentioned in the report. The operators can also monitor their networks to uncover any suspicious communications to the malicious IP addresses that have been included in the findings and enhance their capability to combat growing cyber threats.

Bangladesh e-GOV CIRT conducted this research to alert telecom operators about any malicious communications passing through their network so that the organisations can take necessary measures to reduce risks and avoid any potential cyber-attacks.

Md. Hasan, Head of External Communications, Grameenphone, said, "Malware infection is a growing phenomenon in today's cyber world. We at Grameenphone maintain the highest standard in protecting its operation from malware and always take measures to protect our customers."

"However, individual awareness is the first line of defence to protect individuals and enterprises from any such attack, and we need a more significant effort from the public and private sectors." he also mentioned.

Ankit Sureka, Head of Corporate Communications and Sustainability, Banglalink, said, "Banglalink always maintains the highest level of cyber security to fend off all sorts of cyberattacks. As individual customers used the IPs mentioned in the report, it was technically beyond our control to prevent them. Due to lack of online awareness, some customers often fall victim to such attacks and unknowingly download apps from malicious websites."

"In order to protect their security, we have already started running internet safety and awareness campaigns through various channels. We have also deployed IT & Network infrastructure security systems as per industry best practices and continuously monitor our infrastructures," he added.

Tarique M. Barkatullah, Project Director, Bangladesh e-GOV CIRT was unreachable for comments despite several attempts to reach him over the phone.

Bangladesh e-GOV CIRT conducted this research to alert telecom operators about any malicious communications passing through their network so that the organisations can take necessary measures to reduce risks and avoid any potential cyber-attacks.