Researchers unearth malware that siphoned SMS texts out of telco’s network

reader comments

30 with 26 posters participating

Share this story

Nation-sponsored hackers have a new tool to drain telecom providers of huge amounts of SMS messages at scale, researchers said.

Dubbed “Messagetap” by researchers from the Mandiant division of security firm FireEye, the recently discovered malware infects Linux servers that route SMS messages through a telecom’s network. Once in place, Messagetap monitors the network for messages containing either a preset list of phone or IMSI numbers or a preset list of keywords.

Messages that meet the criteria are then XOR encoded and saved for harvesting later. FireEye said it found the malware infecting an undisclosed telecom provider. The company researchers said the malware is loaded by an installation script but didn’t otherwise explain how infections take place.

Targeting upstream data sources

The security firm said Messagetap belongs to APT41, one of several advanced persistent threat hacking groups that researchers say is sponsored by the Chinese government. The

group is apparently using the malware to spy on high-ranking military and government officials. In a report, the researchers said the malware allows China's intelligence services to obtain a wide range of sensitive data at scale.

"The use of MESSAGETAP and targeting of sensitive text messages and call detail records at scale is representative of the evolving nature of Chinese cyber espionage campaigns observed by FireEye," the researchers wrote. "APT41 and multiple other threat groups attributed to Chinese state-sponsored actors have increased their targeting of upstream data entities since 2017. These organizations, located multiple layers above end-users, occupy critical information junctures in which data from multitudes of sources converge into single or concentrated nodes."

Messagetap's 64-bit Linux executable contains two configuration files. The first, parm.txt, contains lists of IMSI numbers and phone numbers of interest while keyword_parm.txt lists keywords. Both files are deleted from disk once loaded into memory. After that, Messagetap monitors all traffic passing over the network and looks for messages that match the criteria from the configuration text files. Messages sent to or from the phone or IMSI numbers are collected. Messages containing the keywords are also gathered. The malware parses all traffic at the Ethernet and IP layers and continues parsing protocol layers including SCTP, SCCP, and TCAP.

Enlarge / An overview of Messagetap.

Researchers recovered the contents of the configuration files and found a "high volume of phone numbers and IMSI numbers." Thursday's report continued:

> *The inclusion of both phone and IMSI numbers show the highly targeted nature of this cyber intrusion. If an SMS message contained either a phone number or an IMSI number that matched the predefined list, it was saved to a CSV file for later theft by the threat actor. The targeted phone numbers and IMSI numbers belonged to foreign high-ranking individuals of interest to the Chinese government.*
>
> *Similarly, the keyword list contained items of geopolitical interest for Chinese intelligence collection. Sanitized examples include the names of political leaders, military and intelligence organizations and political movements at odds with the Chinese government. If any SMS messages contained these keywords, MESSAGETAP would save the SMS message to a CSV file for later theft by the threat actor.*
>
> *In addition to MESSAGETAP SMS theft, Mandiant also identified the threat actor interacting with call detail record (CDR)*

> *databases to query, save and steal records for specific individuals during this same intrusion. Targeting CDR information provides a high-level overview of phone calls between individuals, including time, duration, and phone numbers. In contrast, MESSAGETAP captures the contents of specific text messages.*

While Messagetap isn’t likely to have monitored the vast majority of the infected telecom’s users, its existence shows that network providers aren’t the only entities that can tap phone networks. Its use demonstrates the prudence of not using phone networks to relay sensitive information unencrypted. The Signal messenger remains the best way to send encrypted texts between two phones.

https://arstechnica.com/?p=1594265