


MESSAGETAP: Who's Reading Your Text Messages?

 [fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html](https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html)

FireEye Mandiant recently discovered a new malware family used by APT41 (a Chinese APT group) that is designed to monitor and save SMS traffic from specific phone numbers, IMSI numbers and keywords for subsequent theft. Named MESSAGETAP, the tool was deployed by APT41 in a telecommunications network provider in support of Chinese espionage efforts. APT41's operations have included state-sponsored cyber espionage missions as well as financially-motivated intrusions. These operations have spanned from as early as 2012 to the present day. For an overview of APT41, see our August 2019 blog post or our full published report. MESSAGETAP was first reported to FireEye Threat Intelligence subscribers in August 2019 and initially discussed publicly in an APT41 presentation at FireEye Cyber Defense Summit 2019.

MESSAGETAP Overview

APT41's newest espionage tool, MESSAGETAP, was discovered during a 2019 investigation at a telecommunications network provider within a cluster of Linux servers. Specifically, these Linux servers operated as Short Message Service Center (SMSC) servers. In mobile networks, SMSCs are responsible for routing Short Message Service (SMS) messages to an intended recipient or storing them until the recipient has come online. With this background, let's dig more into the malware itself.

MESSAGETAP is a 64-bit ELF data miner initially loaded by an installation script. Once installed, the malware checks for the existence of two files: *keyword_parm.txt* and *parm.txt* and attempts to read the configuration files every 30 seconds. If either exist, the contents are read and XOR decoded with the string:

```
http://www.etsi.org/deliver/etsi_ts/123000_123099/123040/04.02.00_60/ts_123040v040200p.pdf
```

Interestingly, this XOR key leads to a URL owned by the European Telecommunications Standards Institute (ETSI). The document explains the Short Message Service (SMS) for GSM and UMTS Networks. It describes architecture as well as requirements and protocols for SMS.

These two files, *keyword_parm.txt* and *parm.txt* contain instructions for MESSAGETAP to target and save contents of SMS messages.

- The first file (*parm.txt*) is a file containing two lists:
 - *imsiMap*: This list contains International Mobile Subscriber Identity (IMSI) numbers. IMSI numbers identify subscribers on a cellular network.
 - *phoneMap*: The *phoneMap* list contains phone numbers.
- The second file (*keyword_parm.txt*) is a list of keywords that is read into *keywordVec*.

Both files are deleted from disk once the configuration files are read and loaded into memory. After loading the keyword and phone data files, MESSAGETAP begins monitoring all network connections to and from the server. It uses the libpcap library to listen to all traffic and parses network protocols starting with Ethernet and IP layers. It continues parsing protocol layers including SCTP, SCCP, and TCAP. Finally, the malware parses and extracts SMS message data from the network traffic:

1. SMS message contents
2. The IMSI number
3. The source and destination phone numbers

The malware searches the SMS message contents for keywords from the *keywordVec* list, compares the IMSI number with numbers from the *imsiMap* list, and checks the extracted phone numbers with the numbers in the *phoneMap* list.

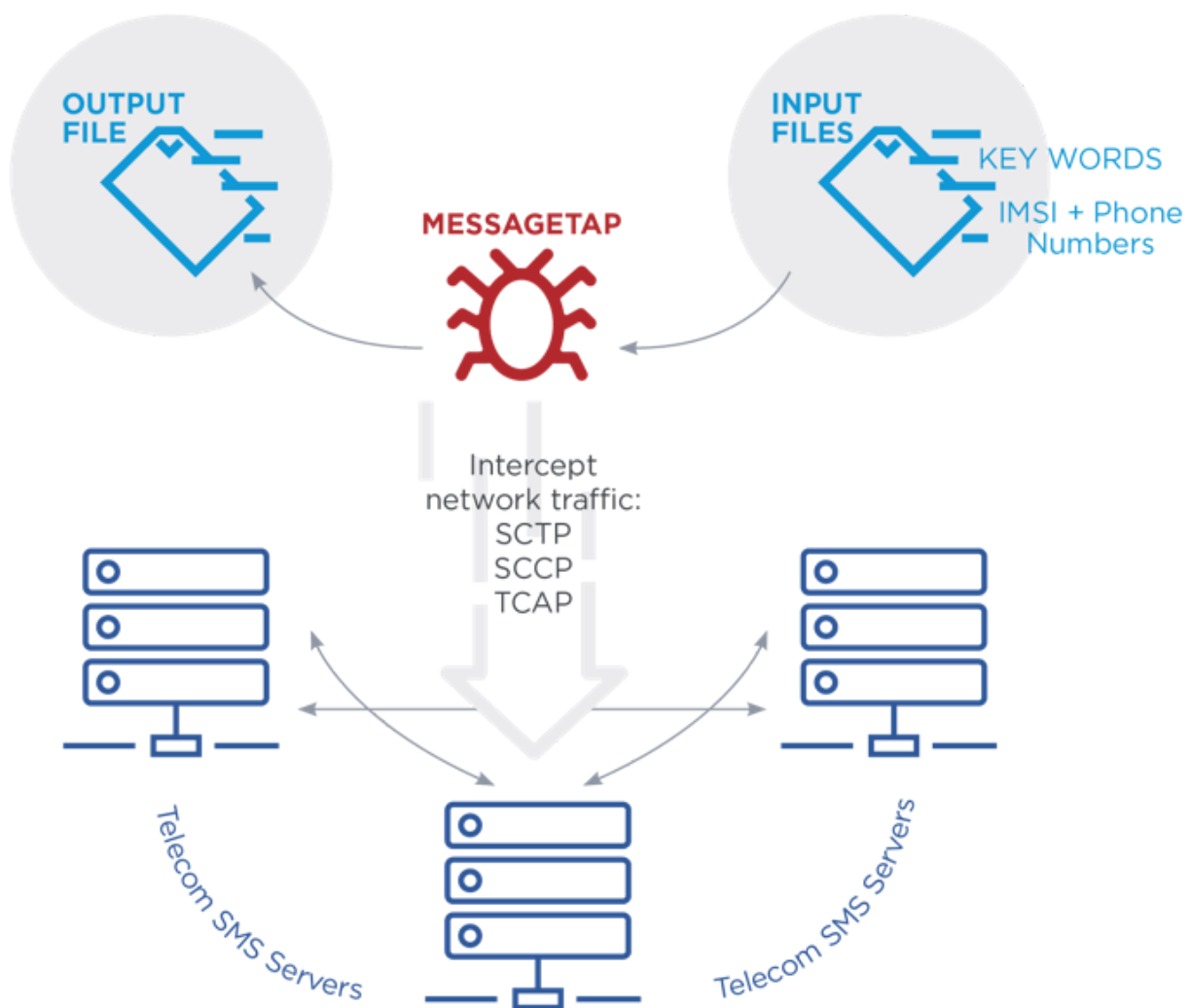


Figure 1: General Overview Diagram of MESSAGETAP

If the SMS message text contains one of the *keywordVec* values, the contents are XORed and saved to a path with the following format:

```
/etc/<redacted>/kw_<year><month><day>.csv
```

The malware compares the IMSI number and phone numbers with the values from the *imsiMap* and *phoneMap* lists. If found, the malware XORs the contents and stores the data in a path with the following format:

```
/etc/<redacted>/<year><month><day>.csv
```

If the malware fails to parse a message correctly, it dumps it to the following location:

```
/etc/<redacted>/<year><month><day>_<count>.dump
```

Significance of Input Files

The configuration files provide context into the targets of this information gathering and monitoring campaign. The data in *keyword_parm.txt* contained terms of geopolitical interest to Chinese intelligence collection. The two lists *phoneMap* and *imsiMap* from *parm.txt* contained a high volume of phone numbers and IMSI numbers.

For a quick review, IMSI numbers are used in both GSM (Global System for Mobiles) and UMTS (Universal Mobile Telecommunications System) mobile phone networks and consists of three parts:

1. Mobile Country Code (MCC)
2. Mobile Network Code (MNC)
3. Mobile Station Identification Number (MSIN)

The Mobile Country Code corresponds to the subscriber's country, the Mobile Network Code corresponds to the specific provider and the Mobile Station Identification Number is uniquely tied to a specific subscriber.

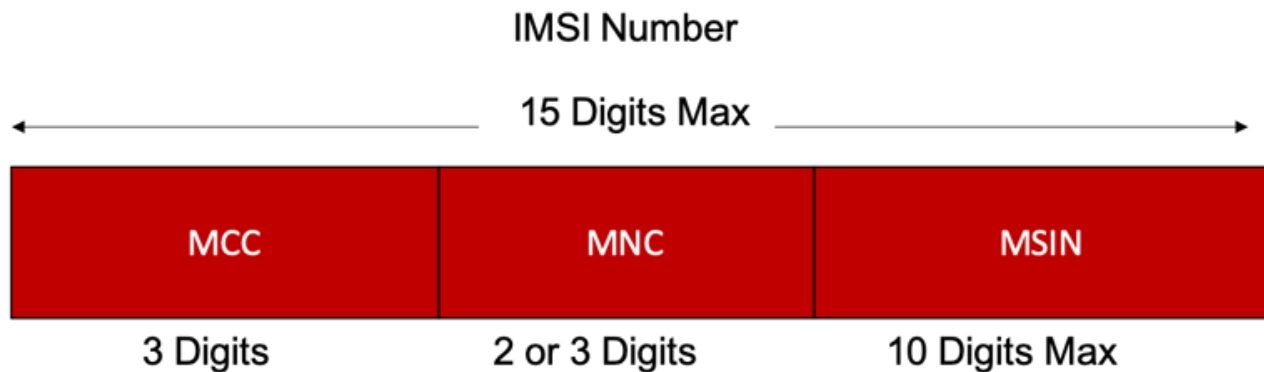


Figure 2: IMSI number description

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.

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, FireEye Mandiant also identified the threat actor interacting with call detail record (CDR) databases to query, save and steal records during this same intrusion. The CDR records corresponded to foreign high-ranking individuals of interest to the Chinese intelligence services. 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.

Looking Ahead

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. 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. Strategic access into these organizations, such as telecommunication providers, enables the Chinese intelligence services an ability to obtain sensitive data at scale for a wide range of priority intelligence requirements.

In 2019, FireEye observed four telecommunication organizations targeted by APT41 actors. Further, four additional telecommunications entities were targeted in 2019 by separate threat groups with suspected Chinese state-sponsored associations. Beyond telecommunication organizations, other client verticals that possess sensitive records related to specific individuals of interest, such as major travel services and healthcare providers, were also targeted by APT41. This is reflective of an evolving Chinese targeting trend focused on both upstream data and targeted surveillance. For deeper analysis regarding recent Chinese cyber espionage targeting trends, customers may refer to the FireEye Threat Intelligence Portal. This topic was also briefed at FireEye Cyber Defense Summit 2019.

FireEye assesses this trend will continue in the future. Accordingly, both users and organizations must consider the risk of unencrypted data being intercepted several layers upstream in their cellular communication chain. This is especially critical for highly targeted individuals such as dissidents, journalists and officials that handle highly sensitive information. Appropriate safeguards such as utilizing a communication program that enforces end-to-end encryption can mitigate a degree of this risk. Additionally, user education must impart the risks of transmitting sensitive data over SMS. More broadly, the threat to organizations that operate at critical information junctures will only increase as the incentives for determined nation-state actors to obtain data that directly support key geopolitical interests remains.

FireEye Detections

- FE_APT_Controller_SH_MESSAGETAP_1
- FE_APT_Trojan_Linux64_MESSAGETAP_1
- FE_APT_Trojan_Linux_MESSAGETAP_1
- FE_APT_Trojan_Linux_MESSAGETAP_2
- FE_APT_Trojan_Linux_MESSAGETAP_3

Example File

- **File name:** mtlserver
- **MD5 hash:** 8D3B3D5B68A1D08485773D70C186D877

This sample was identified by FireEye on VirusTotal and provides an example for readers to reference. The file is a less robust version than instances of MESSAGETAP identified in intrusions and may represent an earlier test of the malware. The file and any of its embedded data were not observed in any Mandiant Consulting engagement

References

Acknowledgements

Thank you to Adrian Pisarczyk, Matias Bevilacqua and Marcin Siedlarz for identification and analysis of MESSAGETAP at a FireEye Mandiant Consulting engagement.