SIP Based Malware & Ransomware Attacks against 4G VoLTE & 5G Networks

A White Paper From Velona Systems
Tony Friar, Chief Technical Officer

IN DEFENSE OF YOUR BUSINESS VELONA

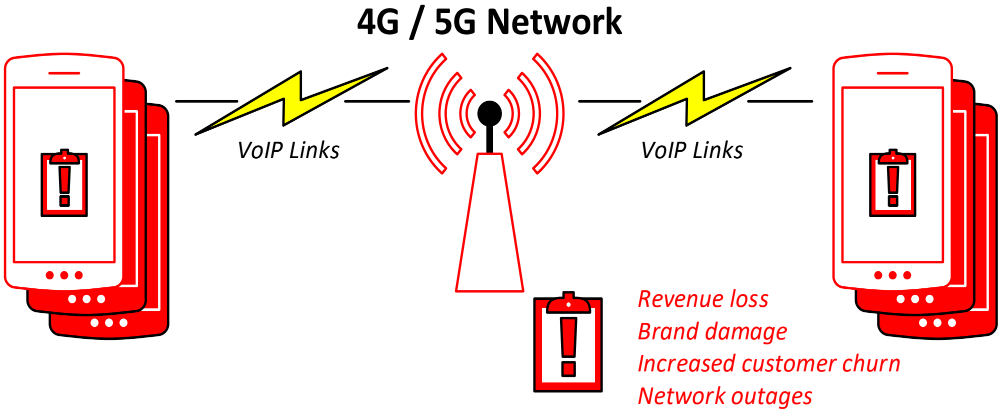
SIP Based Malware & Ransomware Attacks against 4G VoLTE & 5G Networks

As traditional mobile phone networks move to 4G and then 5G, nearly five billion more devices will enter the Voice over IP (VoIP) population. This immediately transforms VoIP from the 100 billion-dollar-market it is today into a three to four trillion-dollar-market.

Given the far higher prize on offer, it will attract far larger numbers and more sophisticated breeds of hackers, resulting in massive acceleration in the frequency and variety of VoIP attacks against 4G and 5G networks. Mobile Network Operators are already seeing SIP based Denial of Service attacks against their core networks that originate from VoLTE devices and SIP interconnects.

VoIP, for all its flexibility and many advantages over legacy systems, comes with a wide range of vulnerabilities. Given the wide-ranging estate 5G will bring, it will only take a small number of Mobile Network Operators (MNOs) who fail to protect their equipment to jeopardize everyone.

Through the use of hacked and malware infected user mobile devices the core network will become much more vulnerable to Denial of Service (DoS) attacks and to Toll Fraud attacks.



A sophisticated DoS attack using malware and/or ransomware infected mobile devices could result in severe network outages whose cause is very difficult to detect and remedy. This could result in network outage lasting for an extended period of time (possibly days or more), which can be repeated by the attackers on-demand (for example, if a ransom from the mobile network provider is not paid).

Without an adequate defence, the resulting network outage(s) could be extremely damaging to the MNO's business, leading both to brand damage and significant revenue loss.

Toll Fraud becomes a greater revenue opportunity

As well as Denial of Service attacks that cause network outages, the size of the 5G market means Toll Fraud becomes a far greater revenue opportunity for hackers who may choose to use more sophisticated attack strategies, beyond those currently seen - which are largely based on SIP attack kits. For example, they may choose to use Malware infected 4G/5G mobile devices.

Today's Toll Fraud attackers typically send as many calls as possible to Premium Rate numbers in order to maximise the revenue that they are stealing before detection. MNOs have begun to react to this threat by various measures, such as, enforcing spend limits. However, when large numbers (tens or hundreds of thousands) of mobile devices can be infected with Malware a more sophisticated approach could be put in train whereby the infected devices each make a very low number of calls over an extended period of time. This fraud approach, called Trickle Toll Fraud, is very difficult to detect and can lead to significant long-term revenues for the hackers.

Over time the MNO's customers will start to realise that there are calls on the monthly bills that they did not make. This leads to customer complaints, which take time and money to investigate and resolve, and which will eventually lead to brand damage before the malware-based Toll Fraud is finally uncovered. It is possible that without the correct forensics available to the MNO, customers saying that they did not make a specific call to a specific number may well not be believed at first. This will lead to frustration on behalf of the customers and result in customers moving operator (churn).

Denial of Service (DoS) Attacks

The DoS attacks described above can take the form of one or more of the following:

Type of Attack	**Description**
Malformed SIP Messages	A SIP Malformed Message Attack (also known as SIP Fuzzing) involves sending a SIP message that is either not compliant to the relevant SIP specification(s) or which is compliant but which the SIP stack / SIP parser of the target is not able to process correctly (e.g. due to an implementation issue / bug).
Call Flooding / Mass Calling	Call Flooding / Mass Calling) is a DoS attack that involves sending large numbers of calls towards a specific target or targets with the intention of preventing the normal operation of the target.
SIP Message Flooding	A SIP Message Flooding attack involves sending more SIP messages to the target(s) under attack than the target(s) can deal with.
Incomplete SIP Transactions	A SIP Incomplete Transaction attack involves not responding to a SIP message that the target of the attack has sent.

In some cases, a Malformed SIP Message sent from a single device will be sufficient to cause a network outage. In such a case the use of SIP based Malware is not needed and the attackers can use a single hacked VoLTE mobile device.

The other forms of attack require a large number of infected devices to act together to generate a large number of SIP messages. Different IMS cores (and even the SBCs used to protect the IMS core) are vulnerable in different ways and an attack could use one or more of the above-mentioned attack types, depending on the infrastructure manufacturer and software versions of the system being attacked.

The current protections are simply not enough

At present, existing mechanisms designed to protect the IMS core within 4G and future 5G networks can only provide limited protection against such threats. A belief that Core Network Session Border Controllers (SBCs) and IPsec encryption provide the required protection gives a false sense of security. The infected devices will be able to use the 4G LTE IPsec tunnels so are already 'inside'.

SBCs will usually only detect obviously Malformed SIP Messages and need specific configuration to detect and block SIP messages that may comply with standards, but which are unusual, and which can cause DoS attacks to devices and nodes behind the SBC or even in some cases to the SBC itself. Large numbers of such configurations can result in performance issues. SBCs often also have problems correlating combinations of the attacks mentioned above. In even small and medium sized 4G networks there can literally be millions of SIP messages over a very short period of time and finding the specific message without the appropriate tools to detect Malformed SIP Messages can be extremely difficult if not impossible within the time needed to prevent the next attack.

What is required to eradicate Voice Malware and DoS attacks?

A real-time system continually analysing SIP messages, which knows and learns what is normal and what is not, and alerts when a problem is identified is needed. Such a system can detect Malformed SIP Messages, SIP Messages that meet the SIP specifications, but which are abnormal, as well as other forms of DoS attack.

Such a system would also need to have the ability to use SIP Fingerprinting to identify SIP endpoints that are in reality SIP attack kits, and to raise alerts warning of their presence. Fingerprinting uses DNA level analysis of the SIP message to accurately recognise the device manufacturer, model and even software version, by looking at the many different parameters and their structure found in SIP messages.

As well as monitoring the normal IMS 4G VoLTE ingress points (the Access SBC), egress point (the Interconnect SBC) and possibly other IMS interfaces, 5G systems will need to monitor any SIP signalling that passes between 5G network slices.

Dealing with Toll Fraud

Detection of any Toll Fraud caused by and controlled by Malware requires the real-time analysis of the SIP signalling. Not only does such real-time analysis allow for faster detection times it also allows access to fields and parameters in the SIP messages that may be indicative that the call has been originated from a mobile device that has been infected with Malware. SIP Fingerprinting and SIP Malformed Message Detection can play a major part in detecting Toll Fraud Malware.

Detecting Trickle Toll Fraud caused by Malware infected mobile devices is difficult as many of the traditional mechanisms used to detect toll fraud are not sufficient given the different calling patterns of the toll fraud. Such calling patterns can be very dynamic and may appear random if a large number of infected devices are used in the Toll Fraud. It is also possible that the Malware could receive updates from an external source that allows it to be 'reconfigured' if the original target numbers have been blocked.

Trickle Toll Fraud detection requires an in-depth understanding of the dynamic calling patterns that Malware infected devices (4G VoLTE, IR.51 VoWiFi and future 5G devices) can use.

Velona's approach to protecting 4G/5G networks

Velona provides a range of products and services for VoIP security to identify and detect SIP based Malware and Ransomware attacks in 4G VoLTE and 5G networks.

Threat Management for VoIP

1. SIP Fingerprinting library (available as an OEM product for C and Java) allows the manufacturer, model and often software version of SIP packets to be identified, so that legitimate and non-legitimate signalling can be easily separated.

2. SIP Malformed Message Detection library (also available as an OEM product for C and Java) allows the identification of not only SIP signalling that is not compliant with the relevant standards, but also the identification of SIP messages that are unusual and could indicate a DoS attack.

3. WATCHER is an off-the-shelf solution that includes SIP Fingerprinting, SIP Malformed Message Detection, Mass Calling Detection, Message Flooding Detection and Toll Fraud Detection.

4. CRACKER is a Cloud SaaS Verification and Testing platform to enable MNOs look for weaknesses in SIP security and affordably run Load Testing, and SIP parser / Torture testing so that they can fully verify they are deploying solutions which have the required Advanced Security robustness built in to their deployments.

VELONA IN DEFENSE OF YOUR BUSINESS

www.velonasystems.com
(+353) 21 242 8400 | email info@velonasystems.com
Velona Systems Limited, 2nd Floor, 11 Anglesea Street, Cork, Ireland T12 CYR8