23.09.2015

XURA

Digital Communications

The Arsenal of SMS Scammers Spammers and Fraudsters

The Arsenal of SMS Scammers Spammers and Fraudsters

SMS scammers use every exploitation opportunity to:

- Increase their reach
- Minimise costs
- Reduce detection

Understanding the tools of the trade is important because attempts to subvert standard routes are constantly evolving

Exploitation of mobile networks

Illicit commercial activity was once limited to the Internet world but, has now expanded to mobile networks including the messaging channel. As with online cybercrime, this initially manifested as isolated individual acts to become increasingly more sophisticated and professional over time. While there are exploitation similarities between the Internet world and the mobile world, techniques and tools used are very different. This whitepaper talks about a few of the numerous tools in the arsenal of SMS scammers, spammers and fraudsters. Advanced exploits often utilise multiple tools and approach vectors combined in new ways. In fact, new exploitation methods are probably being formulated at this very moment. Staying ahead of this ever growing wave requires understanding the motivations and tools used.

The allure

For the dubious entrepreneur, the mobile ecosystem is a new universe of apps and monetisation models that offers a vast landscape of opportunity. One should never underestimate the ingenuity of those seeking creative ways to make money, even if only a few dollars here and there. At scale, a few dollars here and there repeated thousands of times soon becomes a substantial flow of funds.

The mobile marketing ecosystem is awash in billions of dollars. Estimates from industry groups say that the U.S. economic impact of mobile marketing activity is expected to be $400 Billion in 2015 alone. In this world, monetisable triggers come from pay for performance activity such as clicks, downloads, registrations, video ads, referrals, games and surveys. For the criminal mind, the temptation to exploit this ecosystem is significant by creatively pushing the boundaries of acceptable behaviour.

Marketing via SMS is an incomparably efficient way to generate monetisable activity with the mobile handset. 98% of all text messages are opened and read within seconds. That is because consumers live on their mobile handsets and are offer a highly engaged audience. For the scammer, they are prime targets. The result is that network operators face a flood of spam traffic and must work diligently to stay ahead of the game. Every effort to manage illegitimate traffic is countered with increasingly clever tricks to subvert the operator's control. The consequence is that a significant percentage of all SMS traffic is spam or fraud related in some way. Xura has seen volumes as high as nearly 20% of total traffic in some regions. This has significant impact on the operator with revenue loss from unbillable traffic or fraudulent tariffing and increased customer care costs and subscriber churn.

Promotional Messaging or SPAM

The fundamental way a bulk SMS sender makes money is by broadcasting promotional messages for a fee. Marketing or advertising firms pay to have volumes of messages sent to subscribers that meet particular geographic or demographic criteria. This model works but creates tremendous pressure on aggregators of low-cost bulk SMS to lower distribution costs and increase reach. Their primary goal is to provide message traffic at a lower price than the network operators themselves. They will seek every opportunity to 'optimise' costs wherever they can. This motivation is the driving force behind many of the tools and techniques used in the arsenal of SMS scammers, spammers and fraudsters.

The Arsenal of SMS Scammers Spammers and Fraudsters

The Arsenal of SMS Scammers, Spammers, and Fraudsters

SMS based exploitation providers actively explore every opportunity to increase their impact while minimising costs and opportunity for detection. This often blurs the line between legitimate business behaviours and others that are shady or simply unacceptable. Mobile network operators have to continuously address an increasingly complex and dynamically evolving volume of spam and fraudulent attempts to subvert standard routes. The following sections cover some of the tools and techniques in the arsenal available to scammers, spammers and fraudsters.

Grey Routing

Mobile operators in different regions use a variety of international routes to send traffic back and forth. These can be grouped into three types known as white routes, black routes and grey routes. Grey routing traffic is a very appealing method for bulk SMS providers to minimise traffic costs but does push legal limits and presents a number of challenges to the mobile network operator. They are difficult to evaluate, monitor and control and come with hidden costs such as interconnection fees.

White route – A white route is where both the source and destination are standardised, legally agreed upon terminations. This generally means the operators have an agreement which outlines the charges and the manner in which SMS traffic will be conveyed over their networks.

Black route – Opposed to a white route, a black route is illegal on both source and destination ends. This means that there has not been a contractual agreement between the parties involved to provide SMS traffic and traffic from either party is therefore unlawful over such a route.

Grey route – Sometimes referred to as “special carrier arrangements” or “settlement by-pass” , grey routes are generally defined as a legal connection between two parties that is being exploited by a third party to route traffic at the lowest rate possible by manipulating the origination or termination information. Some bulk SMS providers exploit the difference in settlement rates, and route traffic via intermediate networks while also re-originating the message to the network it terminates in, making the message appear either as on-net or domestic as opposed to international. This allows an unscrupulous bulk SMS provider to incur the lowest cost possible and achieve their delivery needs. With the complexity and interconnectivity of most mobile networks, it is difficult, if not impossible, for operators to detect traffic passing through or terminating in their networks using unidentified routes.

Not all traffic from bulk SMS providers should be considered as spam nor does all grey route traffic originate from bulk SMS providers. However, there is a correlation that warrants operator attention simply because bulk SMS traffic has been known to exploit the difference in settlement rates by routing traffic via intermediate networks and re-originating the message to the network it terminates in, thus changing the rating tariff.

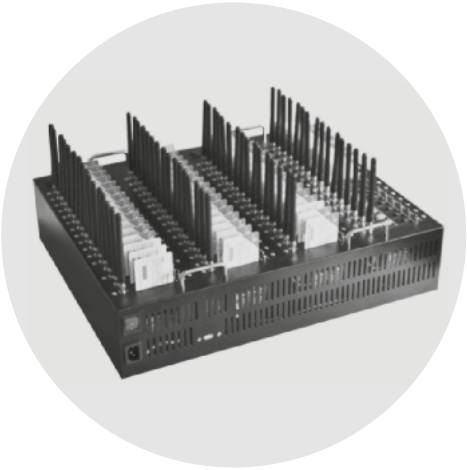
The Arsenal of SMS Scammers Spammers and Fraudsters

SIM Farming

SIM Farms are computers connected to a bank of mobile phone SIM cards each with an account on a network with a favourable tariff such as an “unlimited SMS” bundle. The SIM farm cycles through the bank of SIM cards sending bulk SMS traffic and improperly exploits what is essentially a consumer based tariff.

The use of SIM Farms is an example of how some unethical bulk SMS service providers push the limits of the law. This method of SMS delivery is not technically illegal but clearly a breach of the operator’s intent of providing a consumer based tariff. In many cases, the term and conditions forbid “unlimited SMS” bundles being used for advertising, marketing or bulk delivery campaigns. But, the low prices of these tariffs make it attractive for intermediate entities to provide bulk SMS delivery service to SMS aggregators.

SIM Farm hardware: There are many different types of bulk SMS delivery appliances available on the black market and even for sale on public auction sites such as Alibaba. Typically they function as “GSM modem pools” with multiple SIM card slots and connect to a computer orchestrating the overall campaign. This SIM Farm device acts as an Internet short message gateway much in the same way that mobile network carriers would enable legitimate service providers to handle bulk-text-sending. Message sending throughput and speeds vary by device but ranges of tens of thousands of messages per hour are not uncommon. This makes it a tempting tool for scammers and fraudsters.



App Farming

App Farming extends the concept of bulk SMS delivery to individual handsets. Handset owners download a special app that enables the user to allocate a volume of SMS messages from their handset to be used by the mobile marketing agency and share in the revenue generated by this activity. In effect, the app turns the user’s handset into a single node SIM farm. App providers claim that messaging traffic will not be SPAM but consist of verification codes, departure/arrival flight times, booking confirmations etc… from banks, airlines, hotels, other apps and websites. While the app itself and the activity that it enables is not technically illegal, it does cross over into an ethical and legal grey zone similar to the scenario where a user, consciously or not, may allow their terminal to be used for hacking or sharing illegal content. For mobile network operators, the result is a mix of traffic from that handset that is both legitimate and questionable.

The Arsenal of SMS Scammers Spammers and Fraudsters

SMS Spamming Software

Various SMS-spamming software packages are available online and from underground sources depending on the region and platform requirements required. Typically, the software is presented to state that it should not be used for SMS spamming, mobile spam, unsolicited SMS or bulk SMS broadcasting, however, the design of the software clearly enables this function which can be unethically exploited.

Sample – SMSCaster E-Marketer is a desktop texting software package that uses an Internet based SMS gateway and a tethered mobile phone, GSM modem or cellular terminal connected to the computer. The tethering connection can be done via a USB data cable, serial data cable or Bluetooth COM port depending upon user preference and technology setup. The intent is to allow the user to send bulk marketing & advertising SMS and receive response SMS from the computer. Screenshots of the SMSCaster user interface are shown below:

Sample – SMSMessage Platform is a cloud based SMS broadcast service from Brazil that provides bulk SMS delivery to the user supplied address list. Services listed include spoofing of the sender's ID.

The Arsenal of SMS Scammers Spammers and Fraudsters

Premium Rate Fraud

Premium-rate telephone numbers are typically used to provide services such as adult chat, directory enquiries, weather forecasts, contestant voting and technical support. Calls are routed in the same manner as toll-free telephone numbers but charges are billed at very different rates depending upon the service. These charges may range from a flat 'flagfall' fee to a cost per minute rates.

Scammers use broadcast SMS messages to entice subscribers to initiate a premium rated call with scams such as "You've won a free cruise" or "Hi, it's me, I'm still waiting for your call" or "Notice of undelivered package, please call us". In this way, these scams are an SMS variant of the Wangiri premium rate fraud in which calls are made to handsets and disconnected after a single ring. Curious subscribers who return the 'missed call' finds that the number is premium rated and may be offering anything from "free cruises" to sex services. Depending upon the scam, charges may run into hundreds of dollars and enable the scammers to make millions of dollars in a very short span of time.

Another form of premium rate fraud is to discretely subscribe victims to premium SMS services via trickery or malicious mobile apps. Typically subscribers wanting premium services would send a text message to initiate the subscription then receive a confirmation message from the provider with a response required to confirm and complete subscription. Malicious apps have been discovered that initiate the subscription and automatically generate the necessary replies and confirmations then delete the messages to erase all traces of what occurred. The subscriber is often not aware this has happened until charges appear on the next billing cycle.

Tariff Fraud

There are two primary types of SMS tariff fraud activity that mobile network operators see:

SMS spoofing: Uses a mobile switch emulator in a roaming scenario to replace the sender's identity with the identity of an unsuspecting subscriber. The emulator sends messaging traffic to the home SMSC as if the victim was roaming on a different network. This enables the attacker ability to broadcast messages with all charges incurred by the victim for the fraudulent traffic.

SMS faking: Uses false information on the Signalling Connection Control Part (SCCP) and/or Mobile Application Part (MAP) for the originating party to gain unauthorised access to the network. This enables the attacker to broadcast free messages by faking the network of origins. The victim in this case is the network operator who is transmitting unbillable traffic.

The Arsenal of SMS Scammers Spammers and Fraudsters

Dynamic Message Modification

SMS scammers use sophisticated techniques to modify message content as the campaign progresses over time and provide sufficient variance to avoid detection. The elements of modification may include:

Change Campaign Versions: Use multiple variations of campaign content within same attack.

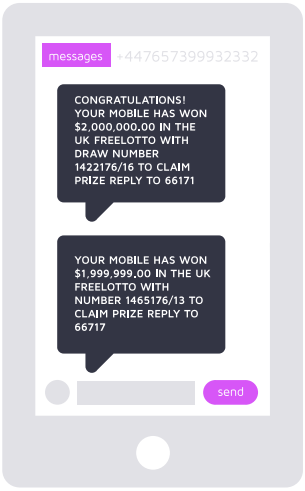
Message Personalisation: Use available recipient information (number, name, location, time, date etc.) to personalise message content.

Spread Campaign Duration: Attacks could last several weeks without interruption, targeting groups of subscribers at a time that could be geographically distributed.

Changing call-to-action URLs: Using URL shorteners to provide variation between messages in campaign.

Modify Campaign Batches: Use variation in quantities of messages sent or days and times of campaigns to avoid detection.

Sender number variation: Use large pools of target MSISDNs to provide high variation of numbers within the campaign which mimics peer to peer message traffic.



Phishing

Phishing attacks are partly psychological and partly technical. The goal of the attack is to get the victim to do something by creating a sense of urgency and requesting immediate action. Phishing is particular effective on mobile phones due to the nature of the handset 'always on' subscribers constantly checking messages. Combining a spoofed sender identification and carefully worded urgent communication, subscribers can be fooled into taking the desired actions. The goal of the phishing attack may be getting subscribers to call certain numbers to extract confidential information such as financial or account information like a user name and password, Social Security number, birth date, ATM PIN or credit card information that can be used to commit fraud or other crimes.

Location Sniffing "Silent SMS" (a.k.a. "Stealth SMS")

A "Type 0" message or silent SMS is part of the GSM technical specification with the original purpose of supporting Over-The-Air (OTA) provisioning of Wireless Application Protocol (WAP) settings. It is also widely used by many police force and intelligence services to locate suspects or missing persons. The message is sent to the handset with instruction to acknowledge receipt of the message and discard content. This enables the sender to know that the handset is active without the recipient having any indication. There will be no message notification or message in the SMS inbox. In this way Silent SMS are used to secretly check whether a user's handset is turned on or not.

The Arsenal of SMS Scammers Spammers and Fraudsters

With the addition of information from the cell tower and radiolocation technology, the mobile device can be located with accuracy somewhere between 50 –200 meters. While this technique has been used quietly by law enforcement agencies for years, there has been a recent surge in “Type 0” message volumes in some networks coinciding with the adoption of smart phones. The likely source of this surge are handset apps that exploit “Type 0” SMS to provide status or location data without the awareness of the person being tracked.

Malware/Spyware

Computer hacking and nefarious behaviour has invaded the mobile handset to become the latest cybercrime trend. With the penetration of smartphones and increased handset usage, subscriber data is exposed in ways that were previously unavailable and criminals are rapidly developing new ways to exploit this exposure. And, as with desktop cybercrimes, the schemes and exploits are wide and varied. In fact, McAfee Security has recorded thousands of variants of mobile malware. Many of these mimic online threats such as clicking dangerous links but, others are unique to the mobile device ecosystem.

Mobile Malware can consist of various behaviours including: Viruses meant to reproduce itself, Worms meant to send copies of themselves to other nodes and Trojans designed to provide unauthorised access to the infected node. The functional intent of malware covers a broad range including accessing personal information, causing you to incur specious charges to simply alter your handset functionality to enable future access. As with other complex forms of attack, the techniques and methods are often combined and evolve all the time.

SMS Forwarder Trojans

SMS forwarders are handset based malware Trojans designed to steal authentication or verification codes sent via text messages for malicious purposes. Many companies use SMS as the bearer for authentication or verification services such as site registration, password resetting, and online payments. SMS Forwarder Trojans monitor text messages sent by certain phone numbers associated with online service providers and banks to intercept authentication or verification codes that are then forwarded to cybercriminals. Some Trojans also delete the text messages they intercept to hide traces of infection.

The Arsenal of SMS Scammers Spammers and Fraudsters

Message Flooding

SMS flooding is simply sending large volumes of messages to either a particular target group of numbers or to the entire network. When used for target groups, the attacker's goal is normally to harass or provide annoyance. Although, in some cases, the flooding might be an attempt to inundate the subscriber to bury legitimate messages in the flood to minimise readability chances. Flooding is also used with limited success to overwhelm network resources in DoS attacks. Both types of flooding are primarily malicious intent with the goal not being monetary gain.

The New World of SS7 Network Exploitation

Signalling is the central nervous system of the mobile operator's network with mission-critical real-time data on subscriber identity, status, location, technology and servicing network elements. This enables the authentication of subscribers and their devices, performs call setups, authorises charging, enforces data policies, manages quality of service, and enacts roaming or interconnection agreements. Gaining access to this information and using it for commercial purposes in acceptable ways can be very valuable in the right hands. Or, it can be very risky if used by the wrong people in unacceptable ways.

Someone with the right technical skill and malicious intent can now exploit the mobile network and its subscribers. Attackers with the right expertise might build a node to emulate a mobile operator or perhaps penetrate a provider's network through a device such as a GGSN. While location data, for example, is used by the operator to perform certain functions which are legitimate and acceptable, the IP transport layer was not designed to detect acceptable versus unacceptable traffic. As example, there are number of entry points in a SS7 network exposed at various levels:

- Peer relationship between operators;
- STP connectivity;
- SIGTRAN protocols;
- VAS systems, e.g. SMSC, IN;
- Signalling Gateways, MGW;
- SS7 Service providers (GRX, IPX);
- GT translation;
- ISDN terminals;
- GSM phones;
- LIG (Legal Interception Gateways);
- 3G Femtocell;
- SIP encapsulation.

The Arsenal of SMS Scammers Spammers and Fraudsters

Therefore, SS7 exploits that take various forms including:

- To obtain the mobile subscriber's confidential identity (IMSI)
- To determine the subscriber's location
- To block a subscriber from receiving incoming calls and text messages
- To intercept a subscriber's incoming SMS messages. This includes the ability to send a confirmation message and alter the subscriber's message
- To send a request to transfer funds between a subscriber's accounts
- To manipulate the subscriber's profile to bypass billing
- To redirect incoming calls
- To deny incoming calls

Summary

The mobile marketing ecosystem is awash in billions of dollars with an entirely new universe of apps and monetisation models available with which the dubious entrepreneur might realise financial gain without actually working. SMS marketing is a reliable method used to generate some of this monetisable activity. And, with every significant flow of monetary activity, there is a powerful temptation to exploit.

Providers and enablers of bulk SMS traffic seek every opportunity to increase their impact while minimising costs and opportunity for detection. The result is often creative attempts to subvert standard transport routes with new tools and techniques that may blur the lines of legitimacy. The consequence to the mobile network operator is an increasingly complex and dynamically evolving volume of scams, spam and fraud attempts.

Operators can minimise the commercial allure that drives spam & fraud traffic with comprehensive network control and access. Xura's solution provides the operator with

360 degree control to effectively address conditions within their network where fraud, fakes, spoof and spam exist with a speed and flexibility unrivalled by other market solutions.

Why Xura

We offer our customers a pathway to next generation digital technology. Our thinking unlocks the possibilities of no boundaries communications.

For over 20 years, we have been working with Communications Service Providers (CSPs), operators and enterprises all over the world, helping them to meet the needs of tomorrow's multi-device, multi-services consumers.

We offer clever ways to financially realise opportunities from existing technology, while guiding customers to richer communications solutions by creating innovative products and services to disrupt digital.

We help 8 out of the top 10 global operators reach over 3 billion endpoints.

We are the enabler making the future of digital communications services happen.

Xura. We think beyond.

The Arsenal of SMS Scammers Spammers and Fraudsters

Definitions

"White Route" A route where both the source and destination are standardised legally agreed upon terminations. This generally means the operators have an agreement which outlines the charges and the manner in which SMS traffic will be conveyed over their networks.

"Black Route" A route illegal on both source and destination ends. This means that there has not been a contractual agreement between the parties involved to provide SMS traffic, and traffic from either party is therefore unlawful over such a route.

"Grey Route" A route where a legal connection may exist on one end but prohibited at the other end i.e. the origination or termination. Grey routes are also referred to as "settlement by-pass", "special carrier arrangements", or various other unclear terms in use by different groups.

"SIM" Subscriber Identity Module is an integrated circuit (embedded into a removable plastic card) that securely stores the IMSI and the related key used to identify and authenticate subscribers on mobile telephony devices (e.g. mobile phones, computers).

"Sandbox" A concept used by Java Card, in which pre-installed programs like Visa or PayPal apps are shielded from one another and the rest of the SIM card.

"DES encryption" A previously predominant algorithm for the encryption of electronic data. Now considered to be insecure for many applications due to its 56-bit key size being too small. The algorithm is considered to be practically secure in the form of Triple DES (3DES). In recent years, the cipher has been superseded by the AES (Advanced Encryption Standard).

"OTA" Over-the-Air is a technology used to communicate with, download applications to, and manage a SIM card without being connected physically to the card.

"A2P" Application to Peer. Message initiated by an application and destined to mobile handsets.

"P2P" Peer to Peer. Messages exchanged between mobile handsets.

"PLMN" Public Land Mobile Network is a regulatory term in telecommunications. A PLMN is a network that is established and operated by an administration or a recognised operating agency (i.e. here meant as the mobile operator) for the specific purpose of providing land mobile telecommunication services to the public.

"IMSI" International Mobile Subscriber Identity is used to identify the user of a cellular network and is a unique identification associated with all cellular networks. It is stored as a 64-bit field and is sent by the phone to the network. It is also used for acquiring other details of the mobile in the HLR.

"HLR" Home Location Register is a central database that contains details of each mobile phone subscriber that is authorised to use the GSM core network. There can be several logical, and physical HLRs per PLMN, though one IMSI / MSISDN pair can be associated with only one HLR (which can span several physical nodes) at a time.

"SS7" Signalling System No. 7 is a set of telephony signalling protocols which are used to set up most of the world's public switched telephone network telephone calls. The main purpose is to set up and tear down telephone calls. Other uses include number translation, local number portability, prepaid billing mechanisms, short message service (SMS), and a variety of other mass market service.

The Arsenal of SMS Scammers Spammers and Fraudsters

CGI (Cell Global Identity) is a standard identifier for a GSM network used to identify a certain cell of the Location Area.

CID (Cell ID) is an identifier of a base station.

GMSC (Gateway MSC) is an edge switch.

GSMA (GSM Association) Association of mobile operators formed in 1995 to support standards of the GSM mobile telephone system.

HLR (Home Location Register) is a register that contains data about mobile phone subscribers.

IMEI (International Mobile Equipment Identity) is an international unique mobile equipment ID.

IMSI (International Mobile Subscriber Identity) is used to identify the user of a cellular network and is a unique identification associated with all cellular networks.

LAC Local Area Code.

MAP (Mobile Application Part) is an SS7 application subsystem for mobile communication.

MCC Mobile Country Code.

MNC Mobile Network Code.

MSC is a Mobile Switching Centre, a specialised automatic telephone system.

MSISDN (Mobile Subscriber Integrated Services Digital Number) is a number uniquely identifying a subscription in a mobile network.

MSRN Mobile Station Roaming Number.

SMS (Short Message Service) is a text messaging service component of mobile communication systems.

SS7 (Signalling System 7) is a common channel signalling system used for international and local phone networks all over the world.

USSD (Unstructured Supplementary Service Data) is a protocol used by GSM cellular telephones to communicate with the service provider's computers.

VLR (Visitor Location Register) is a database that contains information about subscribers roaming within the territory.

For more information
Please visit our website xura.com
or email contactxura@xura.com