VB2021
localhost

7 - 8 October, 2021 / vblocalhost.com

# FROM MATCH FIXING TO DATA EXFILTRATION – A STORY OF MESSAGING AS A SERVICE

**Robert Neumann**
Acronis, Hungary

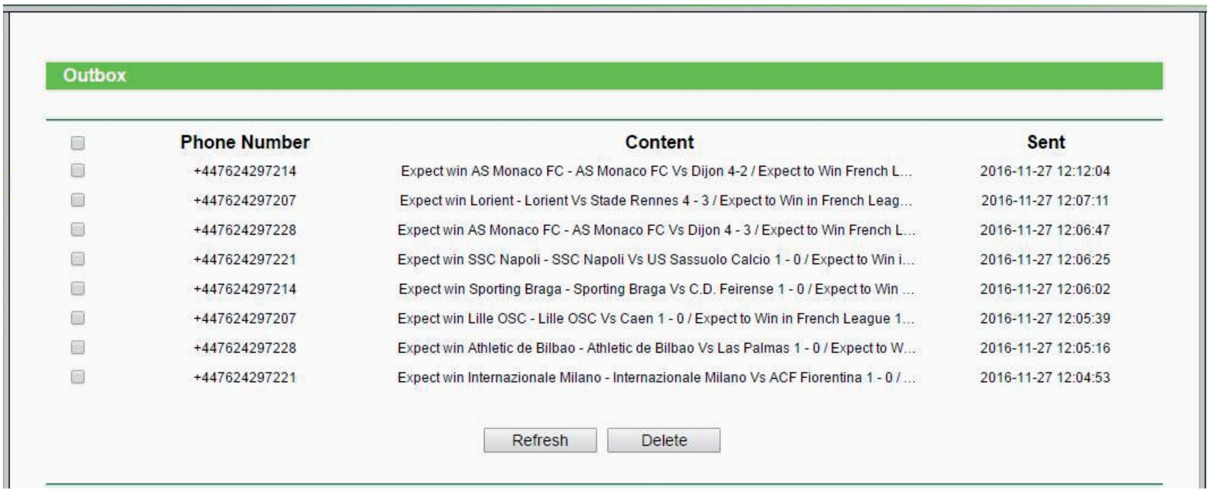
**Gergely Eberhardt**
Search-Lab, Hungary

robert.neumann@acronis.com
gergely.eberhardt@search-lab.hu

## INTRODUCTION

In late 2016 when we were first approached by a small business about unsolicited SMS messages, we were pretty much expecting a case involving a mobile threat. Instead, it was reported that strange outgoing messages were being sent from the company's SOHO router capable of 3G/LTE functionality. The issue was noticed only due to the unexpectedly high monthly invoice. The initial investigation by the company's IT department revealed dozens of short text messages (SMS [1]) being sent to a foreign country. The content didn't show much variation, focusing always on the same theme: betting on sport events.

The device was identified as a *TP-Link MR6400* router, but it was unclear as to what was contributing to the outgoing messages. The only thing ruled out early on was intentional or accidental action carried out by the company itself. It was only the IT staff that had access to the device's administration interface, and the default admin password had been modified right after the setup of the equipment.



Outbox

| □ | Phone Number | Content | Sent |
|---|---|---|---|
| □ | +447624297214 | Expect win AS Monaco FC - AS Monaco FC Vs Dijon 4-2 / Expect to Win French L... | 2016-11-27 12:12:04 |
| □ | +447624297207 | Expect win Lorient - Lorient Vs Stade Rennes 4 - 3 / Expect to Win in French Leag... | 2016-11-27 12:07:11 |
| □ | +447624297228 | Expect win AS Monaco FC - AS Monaco FC Vs Dijon 4 - 3 / Expect to Win French L... | 2016-11-27 12:06:47 |
| □ | +447624297221 | Expect win SSC Napoli - SSC Napoli Vs US Sassuolo Calcio 1 - 0 / Expect to Win i... | 2016-11-27 12:06:25 |
| □ | +447624297214 | Expect win Sporting Braga - Sporting Braga Vs C.D. Feirense 1 - 0 / Expect to Win ... | 2016-11-27 12:06:02 |
| □ | +447624297207 | Expect win Lille OSC - Lille OSC Vs Caen 1 - 0 / Expect to Win in French League 1... | 2016-11-27 12:05:39 |
| □ | +447624297228 | Expect win Athletic de Bilbao - Athletic de Bilbao Vs Las Palmas 1 - 0 / Expect to W... | 2016-11-27 12:05:16 |
| □ | +447624297221 | Expect win Internazionale Milano - Internazionale Milano Vs ACF Fiorentina 1 - 0 / ... | 2016-11-27 12:04:53 |

*Figure 1: Example of the initial football-themed outgoing messages.*

## ROUTERS WITH 3G/LTE FUNCTIONALITY

For decades, consumer and SOHO routers had only one primary WAN connection option dedicated to broadband connectivity. Mobile connections could not be considered as stable or fast enough until around the birth of 3G. With 3G finally providing reliable connectivity and transfer speeds, their adoption slowly began on multiple fronts.

Mobile connectivity also become popular in places where traditional options were absent for some reason. Initially, they were available in the form of USB modems, which were sufficient for providing Internet access, but lacked most of the firewall functionality that traditional routers had already had for years. Embedding a mobile interface into classic routers had two clear benefits: the 3G or LTE connection could be used as a fallback option in case the primary broadband one went down, and the hardware-based firewall functionality was finally there.

## DEEPER INSPECTION OF THE DEVICE

Once we got hold of a similar *MR6400* device, we could start looking for possible security issues or misconfigurations. The main goal was to get familiar with how the SMS functionality worked and verify whether it could be exploited in any way. It did not take long to discover that the SMS interface could be accessed not only via the web interface, but also through an API. The API option made it possible to send messages remotely, however proper access control seemed to be lacking while using this method.

This is unfortunately a rather common mistake some IoT developers make when implementing such API functionality. They often assume that no functions will be used without logging into the device via the web interface first, hence there won't be proper access control implemented for the externally accessible APIs. In our case this meant that someone with malicious intent could be abusing the device remotely over the Internet for sending SMS messages to any number and any country that was supported by the SIM card. To make matters worse, such an attacker could stay completely hidden as there is no way of differentiating whether an SMS was sent via the vulnerability or through the web interface as both are done using the exact same API – and there is no IP address logging either.

## THE VULNERABILITY

First, we did a quick search to see what vulnerabilities had been reported for *TP-Link* devices in the recent past. There was a local file disclosure [2] found by Stefan Viehböck on a different device which also affected the *MR6400* model. Using this vulnerability an attacker could read any file on the device including ‘passwd’ (which contains the root password). However, in order to access the SMS functionality the admin password was required, rather than the root password. With some additional effort we were able to access the admin password as well, as it was used in creating the ‘dropbearpwd’ file, which is located at:

http://<device_ip>/fs/../../tmp/dropbear/dropbearpwd

In fact, it was not the password itself, but the MD5 hash of the password, which is just enough for using in the Authorization cookie.

We also found notes about previous firmware updates, indicating the fixing of some SMS-related vulnerabilities, and since our test device already had that fix incorporated, it was time to dig deeper into the inner workings of the administration interface. For the modification of the modem-related settings the web interface would mostly issue GET requests, but in the case of the ‘lteWebCfg’ CGI, a POST method was used. By default, every request required authentication except for accessing some specific directories and the deviceInfo.htm file. The exception of the latter was checked by the ‘strstr’ function in the query file path, and the GET handler would finally decide the necessary action based on the start of the path. This resulted in an authentication bypass for GET requests in the following way:

http://<device_ip>/userRpm/StatusRpm.htm/deviceInfo.htm

POST requests were only used for accessing the LTE chipset of the device via the ‘/userRpm/lteWebCfg’ CGI handler. After checking the content of the Authorization and Referer headers the JSON data was passed from the application side to the LTE chipset – to the QCMAP_Web_CLIENT application – in its original form. The authorization check verified whether the Authorization cookie existed and contained data. Unfortunately, it did not care whether the Base64-encoded Authorization cookie was correct, so the following request was also authorized:

```
"POST /userRpm/lteWebCfg HTTP/1.1
Host: <device_ip>
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http:// <device_ip>/
Connection: close
Content-Length: 30
Cookie: Authorization=a

{"module":"status","action":0}"
```

Using the ‘lteWebCfg’ CGI request every LTE-related function could be accessed, including the sending of SMS messages, reading both incoming and outgoing SMS queues, gathering SIM lock information and modifying LAN and time settings. Interestingly, the client-side JavaScript code also clearly lacked proper error handling.

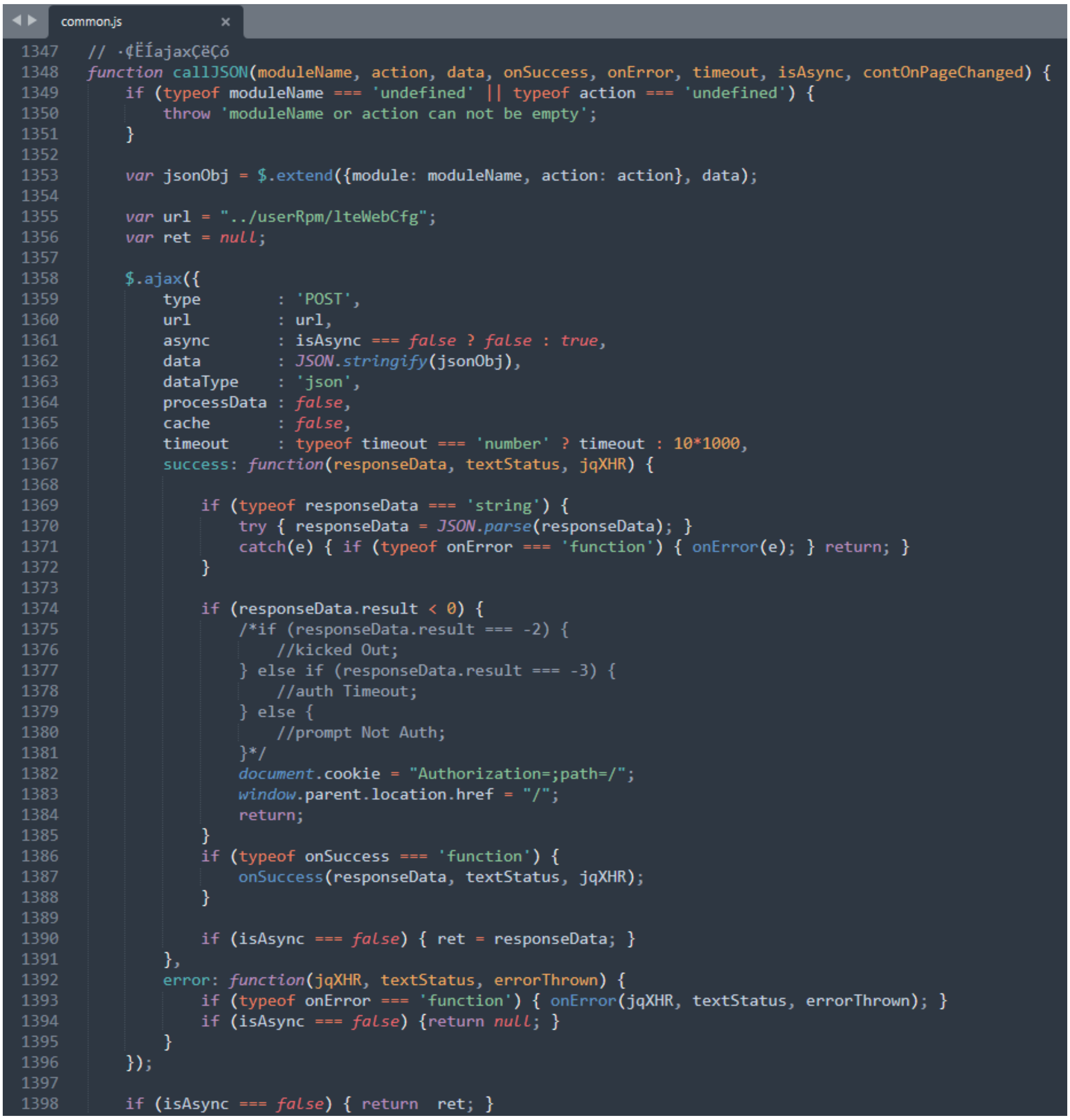
Figure 2 (on the following page) shows an example of the client-side JavaScript code for handling the lteWebCfg request.

After discovering the above, some basic verification was done in order to gain a better understanding of how many devices are available on the Internet with this vulnerability. The vendor was also contacted about all the issues and vulnerabilities found in this model. At this point we decided to put further investigation on hold and only continue monitoring our test device.

## DIFFERENT MODELS AND HARDWARE REVISIONS

Before reverting to such a monitoring phase, there was an extended search as we wanted to verify whether other models from the same vendor were also affected by the same issue. As stated earlier, the traditional routers had no 3G/LTE capabilities for a long while, and when the first devices advertised as such hit the market, that only meant that you could plug supported USB modems into them. Ideally, vendors would provide a compatibility list of devices that can work in conjunction with their routers. Modems being external devices here also meant that no SMS functionality was implemented in the router’s firmware, only basic connectivity options were provided. In the case of *TP-Link*, this changed when the *MR6400* came to market. Firmware analysis of the traditional devices compared to the *MR6400* revealed lots of similarities, however the ‘lteWebCfg’ API seemed only to be present in the firmware of this particular model.

*TP-Link* has a rather broad product portfolio focusing on the consumer and SOHO space. New product launches are rather frequent, but at the same time existing products might be updated internally or modified, resulting in new hardware



```
// ·¢ËÍajaxÇëÇó
function callJSON(moduleName, action, data, onSuccess, onError, timeout, isAsync, contOnPageChanged) {
    if (typeof moduleName === 'undefined' || typeof action === 'undefined') {
        throw 'moduleName or action can not be empty';
    }

    var jsonObj = $.extend({module: moduleName, action: action}, data);

    var url = "../userRpm/lteWebCfg";
    var ret = null;

    $.ajax({
        type        : 'POST',
        url         : url,
        async       : isAsync === false ? false : true,
        data        : JSON.stringify(jsonObj),
        dataType    : 'json',
        processData : false,
        cache       : false,
        timeout     : typeof timeout === 'number' ? timeout : 10*1000,
        success: function(responseData, textStatus, jqXHR) {

            if (typeof responseData === 'string') {
                try { responseData = JSON.parse(responseData); }
                catch(e) { if (typeof onError === 'function') { onError(e); } return; }
            }

            if (responseData.result < 0) {
                /*if (responseData.result === -2) {
                    //kicked Out;
                } else if (responseData.result === -3) {
                    //auth Timeout;
                } else {
                    //prompt Not Auth;
                }*/
                document.cookie = "Authorization=;path=/";
                window.parent.location.href = "/";
                return;
            }
            if (typeof onSuccess === 'function') {
                onSuccess(responseData, textStatus, jqXHR);
            }

            if (isAsync === false) { ret = responseData; }
        },
        error: function(jqXHR, textStatus, errorThrown) {
            if (typeof onError === 'function') { onError(jqXHR, textStatus, errorThrown); }
            if (isAsync === false) {return null; }
        }
    });

    if (isAsync === false) { return  ret; }
```

*Figure 2: Example of the client-side JavaScript code for handling lteWebCfg request.*

revision. Depending on the popularity of a given device, hardware revisions would usually range from one to five. That often means that different firmware must be provided for the different hardware revisions to maintain compatibility.

After looking at the firmware of a dozen different models in a close-to-10-year scale, including basic routers, mobile routers and 3G/LTE-capable successors of the *MR6400*, we made two main discoveries, which were related. First, there were no other routers prior to the existence of the *MR6400* model with embedded SMS functionality, and more importantly there was already a revamped firmware in the works by the time the *MR6400* hit the market. As a result, starting with hardware revision v3 the firmware no longer contained the 'lteWebCfg' API, and newer devices – such as the *MR200* or *MR400* – were utilizing the newly developed firmware code.

This puts the *MR6400* in a unique position and might partly explain the lack of extra effort for the missing access control implementation on that specific API. We have to state that *TP-Link* was at least backporting the newly developed firmware for the v1 and v2 hardware revisions as well. We highly advise updating to that version as it also contains several other fixes (LTE_GATEWAYv3_1.11.0_0.9.1_up_boot(200325)_2020-06-12_15.48.55.bin).

As we didn't find any other affected models that would expand the scope of the research, we occasionally took a look at our honeypot device to see if there was any development regarding the messages. Meanwhile, the company originally reporting the issue to us went for the quick and easy fix: they put a barring on foreign numbers via the operator, which made the wave of unwanted messages stop.

It’s worth noting that telecommunication companies often act the same way as financial institutes do when it comes to fraud of these types: if the case is a one-off or the issue can’t be resolved by them, they simply credit the invoice for their customers and move on.

## WHAT’S THE DEAL ABOUT FOOTBALL?

Research was resumed as soon as the infrequent monitoring of the test device provided additional message types besides the football-themed ones. There were more of this type as well, so we once again went back to investigate those. All the football-themed messages had the same structure and they only focused on the biggest leagues, such as the Premier League, Serie A or La Liga, along with international events such as the Champions League or qualifiers for the European Championship. All the messages were aiming only for two outcomes: either a win or a draw (they actually misspelled ‘draw’ as ‘drew’ all the time).

Another suspicious trait was the sending date of the messages: they were all sent just a day prior to match day. This dissolved our initial take on the subject – they certainly did not give the impression that they were being sent by someone just bullying and trying to generate an extra high invoice by sending out dozens of international text messages. On the other hand, if the campaign was, as we theorized, about match fixing, then there were some conditions to be met. A simplistic bet on a win or draw wouldn’t be as beneficial as betting on the exact final result. Alternatively, if someone wanted to manipulate the odds, that would require tens of thousands of messages resulting in the same number of bets at the end. Destination phone numbers looked like ordinary cell phone numbers in the international format and nothing resembled a direct bet to a related portal.

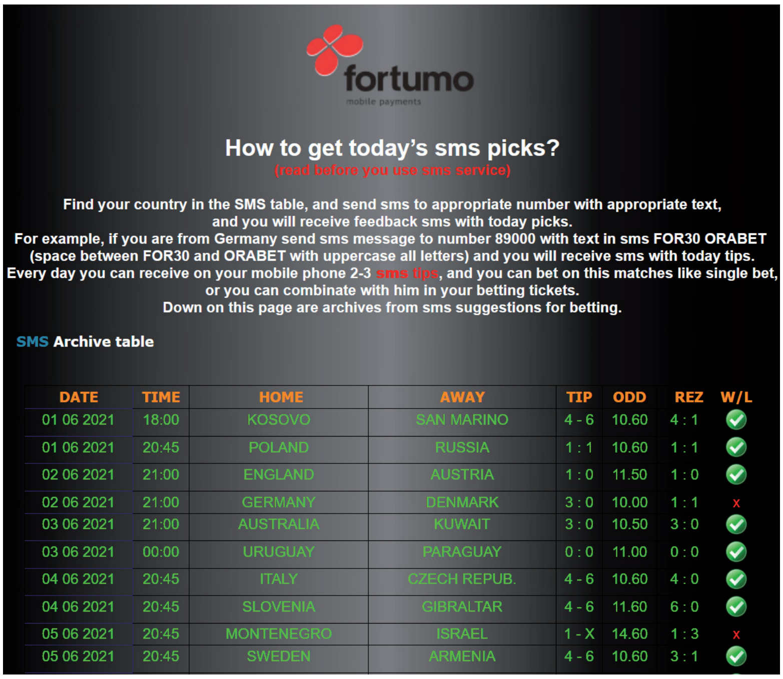
```
"index":1846,"to":"+447937404370","content":" Expect win Rome - Rome Vs Croton 3 - 1 / Expect to
Win in Serie A Class A Match 2016/2017","sendTime":"2016-09-20 17:22:43"

"index":1845,"to":"+447937404360","content":" Expect win Real Madrid - Real Madrid Vs Villarreal
4 - 2 / Expect to Win in Spanish Leagu Matche 2016/2017","sendTime":"2016-09-20 17:22:07"

"index":1844,"to":"+447937404353","content":" Expect win Barcelona - Barcelona Vs Atletico Madrid
4 - 2 / Expect to Win in Spanish Leagu Match 2016/2017","sendTime":"2016-09-20 17:21:28"
```

Our other theory was that only some bets were ‘real’, and the rest were just decoys, with a system (e.g. every fifth) on the receiving end to differentiate them. For this to work at least some of the bets would have to match real results, and that was something we could actually verify. Unfortunately, matching the bets against actual scores wasn’t providing the results we expected. The probability of a win or draw was around 50–60%, but for the exact matches it was only occasional.

By the time we had concluded this, another idea had started to form. Betting on sport events in the first half of the last decade was vastly different compared to how it is nowadays. There have been countless portals trying to monetize people’s ability to receive bets on their mobile phones while charging them a small amount. All that was needed was a service attached to a specific phone number, and it could even be advertised offline in TV, newspapers, etc. As with everything, there have been legitimate services, but also many operating in the grey zone. Setting up and running such a service involves different types of costs – the infrastructure, the advertisements, and a continuous cost for sending out the messages to all those people willing to pay. If this latter cost could somehow be removed from the equation that would render such a service even more profitable.



How to get today’s sms picks?

(read before you use sms service)

Find your country in the SMS table, and send sms to appropriate number with appropriate text,
and you will receive feedback sms with today picks.
For example, if you are from Germany send sms message to number 89000 with text in sms FOR30 ORABET
(space between FOR30 and ORABET with uppercase all letters) and you will receive sms with today tips.
Every day you can receive on your mobile phone 2-3 sms tips, and you can bet on this matches like single bet,
or you can combinate with him in your betting tickets.
Down on this page are archives from sms suggestions for betting.

SMS Archive table

| DATE | TIME | HOME | AWAY | TIP | ODD | REZ | W/L |
|---|---|---|---|---|---|---|---|
| 01 06 2021 | 18:00 | KOSOVO | SAN MARINO | 4 - 6 | 10.60 | 4 : 1 | ✓ |
| 01 06 2021 | 20:45 | POLAND | RUSSIA | 1 : 1 | 10.60 | 1 : 1 | ✓ |
| 02 06 2021 | 21:00 | ENGLAND | AUSTRIA | 1 : 0 | 11.50 | 1 : 0 | ✓ |
| 02 06 2021 | 21:00 | GERMANY | DENMARK | 3 : 0 | 10.00 | 1 : 1 | x |
| 03 06 2021 | 21:00 | AUSTRALIA | KUWAIT | 3 : 0 | 10.50 | 3 : 0 | ✓ |
| 03 06 2021 | 00:00 | URUGUAY | PARAGUAY | 0 : 0 | 11.00 | 0 : 0 | ✓ |
| 04 06 2021 | 20:45 | ITALY | CZECH REPUB. | 4 - 6 | 10.60 | 4 : 0 | ✓ |
| 04 06 2021 | 20:45 | SLOVENIA | GIBRALTAR | 4 - 6 | 11.60 | 6 : 0 | ✓ |
| 05 06 2021 | 20:45 | MONTENEGRO | ISRAEL | 1 - X | 14.60 | 1 : 3 | x |
| 05 06 2021 | 20:45 | SWEDEN | ARMENIA | 4 - 6 | 10.60 | 3 : 1 | ✓ |

*Figure 3: Example of a website offering football tips by SMS.*

Note that these classic sport-centric portals are already beyond their peak, as social media has gathered even more ground – for example, people started to form private groups and chat rooms for similar activities – and mobile in-app purchases have become available. In parallel with that, most countries have tightened regulations around premium rate services, resulting in the easy ways of monetization disappearing from the criminal's arsenal.

## YOUR CODE IS...

As the real trigger point for resurrecting the research was the arrival of new message types, it was about time to have a closer look at them. The first surprise was that there were over two dozen new types, the second was that most of them were strange. There were multiple messages falling into a category we called 'code sending' – the messages were the indication of a new activation or verification code being sent, sometimes even borrowing names of popular instant messaging applications such as *Telegram*.

```
{"index":1349,"to":"+447537606021","sendTime":"2018-06-11 11:58:13","content":"your phone
verfication is 4584"}
{"index":2368,"to":"+48780203110","sendTime":"2018-10-09 02:54:41","content":"your phone code is
2545"}
{"index":2074,"to":"+48780203110","sendTime":"2018-10-08 17:53:12","content":"Telegram code
is:16278"}
{"index":1035,"to":"+447537600282","sendTime":"2018-03-11 12:50:36","content":"vip code:8rlK"}
{"index":12129,"to":"+447452222002","sendTime":"2018-05-02 07:50:44","content":"card code:gtC5"}
```

Our initial take was that someone might be trying to use these devices as SMS gateways, but there were some issues with that. Either the messages were of a constant type and repeating the very same content over and over or, if actual code values were changing, then the recipient phone numbers were falling into a small batch. Taking the number of similar messages into account, both phone numbers and code values should change frequently in the case of an SMS gateway. Still, looking at the timestamps of the outgoing messages – which usually varied between one and 90 seconds – made it clear that the process was at least semi-automated and definitely not manual.

```
{"index":1792,"to":"+37258992200","sendTime":"2018-10-08 16:34:39","content":"your phone code is
2545"}
{"index":1791,"to":"+37258992200","sendTime":"2018-10-08 16:34:27","content":"your phone code is
2545"}
{"index":1790,"to":"+37258992200","sendTime":"2018-10-08 16:34:15","content":"your phone code is
2545"}
{"index":1789,"to":"+37258992200","sendTime":"2018-10-08 16:34:02","content":"your phone code is
2545"}
{"index":1788,"to":"+37258992200","sendTime":"2018-10-08 16:33:50","content":"your phone code is
2545"}
```

## THERE MUST BE MONEY INVOLVED

Examining the rest of the message types drew us closer to a theory that money must be involved at some point. The sheer number of messages, the two dozen different types, and the geographical distribution of the affected devices all pointed in a direction which made bullying simply unreasonable. The obvious pick would be the exploitation of premium rate services, but, for that, hundreds of recipient phone numbers had to be verified and some additional context had to be gathered. A big chunk of our data was already outdated – sometimes by years – which made it even more difficult to retrieve information on the phone numbers used. SIM cards can easily be replaced, and if there was any criminal intent behind the scenes then the chance of using burners on the receiving end was rather high.

Up to this point during the investigation our focus was on the outgoing messages, but we noticed something strange with regard to how indexes worked in the message log. Normally, the index number of the messages would simply be incremented one by one, but sometimes there were gaps. Paying extra attention to those gaps revealed both small (1–5) and big (100+) jumps in the indexing. The latter could be explained by a complete reset of the device – at least we had our fair share of experience from the past of how those were usually implemented. While one would expect devices utilizing NVRAM to have a full wipe of its content in the case of a factory reset, often the implementation was simply overwriting a number of variables with a default value – but not all of them. Accepting that indexes could survive a reset operation of the router was far from undoubted. The smaller gaps seemed more interesting, and when the idea came to us to start paying attention to the incoming messages as opposed to only the outgoing ones, things started to fall into place.

## THE SINGAPORE CASE

Suddenly the small gaps disappeared, or more precisely, they were filled by the incoming content. More importantly, it could be identified if an outgoing message involved an incoming reply later on. This was bringing a smaller number of messages into our focus, ones which would otherwise fall into the needle in a haystack category. On one particular device located in Singapore there were half a dozen incoming messages from *Codapay*, providing notifications about completed purchases on *Boku*, a big e-commerce portal supporting mobile payments.

```
{"index":371,"from":"CodapayÂ¡","content":"Your purchase from Boku is complete. S$16.05
has been added to your monthly bill. Thank you for using Codapay. CS: http://bitly.
com/2JZnPYQ","receivedTime":"2018-08-10 13:51:09","unread":true}
```

```
{"index":369,"from":"CodapayÂ¡","content":"From Boku: Send 133 as a NEW SMS to 146053202
to charge S$16.05 to your M1 bill. Do not reply to this message. CS: http://bitly.
com/2JZnPYQ","receivedTime":"2018-08-10 13:50:36","unread":true}
```

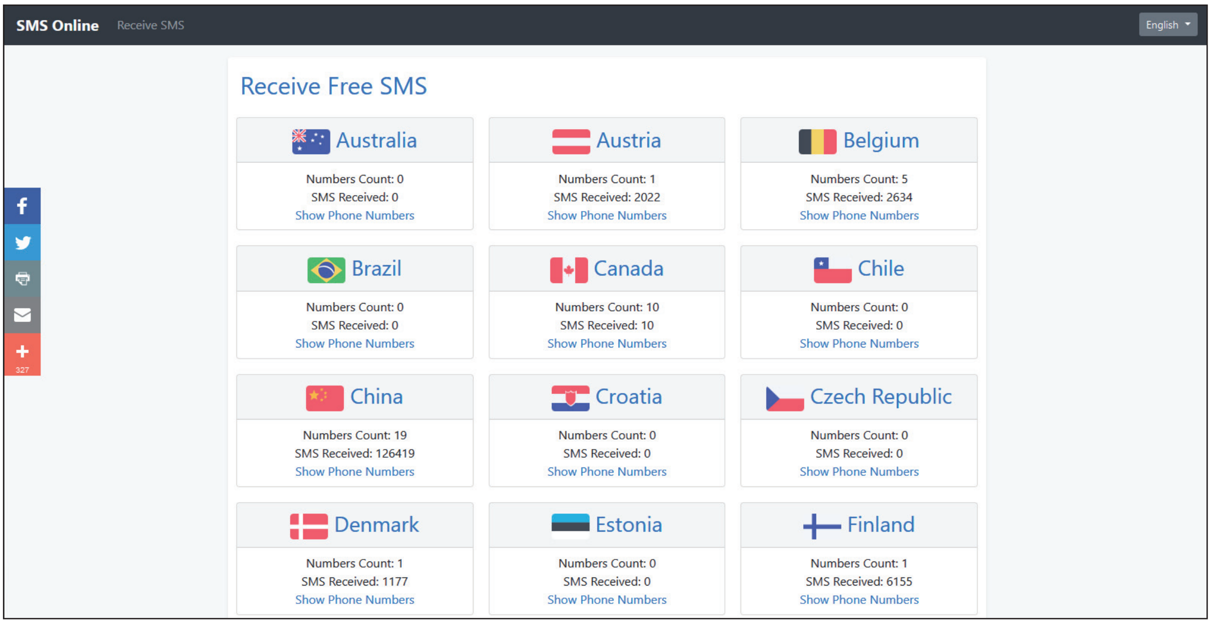
```
{"index":368,"from":"CodapayÂ¡","content":"Your purchase from Boku is complete. S$16.05
has been added to your monthly bill. Thank you for using Codapay. CS: http://bitly.
com/2JZnPYQ","receivedTime":"2018-08-10 13:50:19","unread":true}
```

```
{"index":365,"from":"CodapayÂ¡","content":"From Boku: Send 604 as a NEW SMS to 146053202
to charge S$16.05 to your M1 bill. Do not reply to this message. CS: http://bitly.
com/2JZnPYQ","receivedTime":"2018-08-10 13:49:13","unread":true}
```

Looking at the outbox in the same timeframe highlighted domestic messages with three-letter codes for their content. Even more interestingly, on the very same day just minutes prior to these was an unknown phone number with country code of +7. This specific country code belongs to Russia. Instead of drawing a quick conclusion we decided to start looking for some additional context.

```
{"index":366,"to":"146053202","content":"406","sendTime":"2018-08-09 22:49:36"}
{"index":363,"to":"146053202","content":"212","sendTime":"2018-08-09 22:48:18"}
{"index":360,"to":"146053202","content":"927","sendTime":"2018-08-09 22:47:28"}
{"index":357,"to":"146053202","content":"988","sendTime":"2018-08-09 22:46:29"}
{"index":354,"to":"+79653944057","content":"4444","sendTime":"2018-08-09 22:40:14"}
{"index":350,"to":"+79653944057","content":"555","sendTime":"2018-08-08 18:01:40"}
```

It turned out that the Russian number belonged to a web-based free SMS service that people can use if they are unwilling to provide their real phone number for receiving activation codes and the like. In fact, the same SMS service was also used a day prior to the *Boku* purchases. In short, once the perpetrator found an exploitable device, they tested the vulnerable state by using a fee SMS service, and once they got confirmation, they quickly carried out multiple small purchases within a few minutes. Timestamps of the events suggested that this could be done manually. The total value of the purchases was low – about 70 USD – either intentionally, so as not to raise suspicion, or as more of a test run.



Receive Free SMS

Australia
Numbers Count: 0
SMS Received: 0
Show Phone Numbers

Austria
Numbers Count: 1
SMS Received: 2022
Show Phone Numbers

Belgium
Numbers Count: 5
SMS Received: 2634
Show Phone Numbers

Brazil
Numbers Count: 0
SMS Received: 0
Show Phone Numbers

Canada
Numbers Count: 10
SMS Received: 10
Show Phone Numbers

Chile
Numbers Count: 0
SMS Received: 0
Show Phone Numbers

China
Numbers Count: 19
SMS Received: 126419
Show Phone Numbers

Croatia
Numbers Count: 0
SMS Received: 0
Show Phone Numbers

Czech Republic
Numbers Count: 0
SMS Received: 0
Show Phone Numbers

Denmark
Numbers Count: 1
SMS Received: 1177
Show Phone Numbers

Estonia
Numbers Count: 0
SMS Received: 0
Show Phone Numbers

Finland
Numbers Count: 1
SMS Received: 6155
Show Phone Numbers

*Figure 4: Example of a website offering free SMS services.*

## THE IRISH CASE

Another device, located in Ireland, seemed to be receiving multiple confirmations of successful donations of 2-4 EUR on a weekly basis. Unfortunately, the root cause of those could not be tracked as message indexing was already starting at 541. This indicates a device reset, likely due to a failed attempt at stopping the donations.

```
{"index":829,"from":"Three","receivedTime":"2021-06-06 18:02:43","content":"From Three: Your
pay by mobile purchase of EUR 4 for World Vision Ireland has been applied.Three is authorised
by a third party to conclude the sale of goods/services to you. For the VAT treatment of this
transaction, see http://bit.ly/1xgwpSn","unread":true}
```

```
{"index":828,"from":"Three","receivedTime":"2021-06-06 18:02:43","content":"From Three: Your pay
by mobile purchase of EUR 2 for Pieta House has been applied.Three is authorised by a third party
to conclude the sale of goods/services to you. For the VAT treatment of this transaction, see
http://bit.ly/1xgwpSn","unread":true}
```

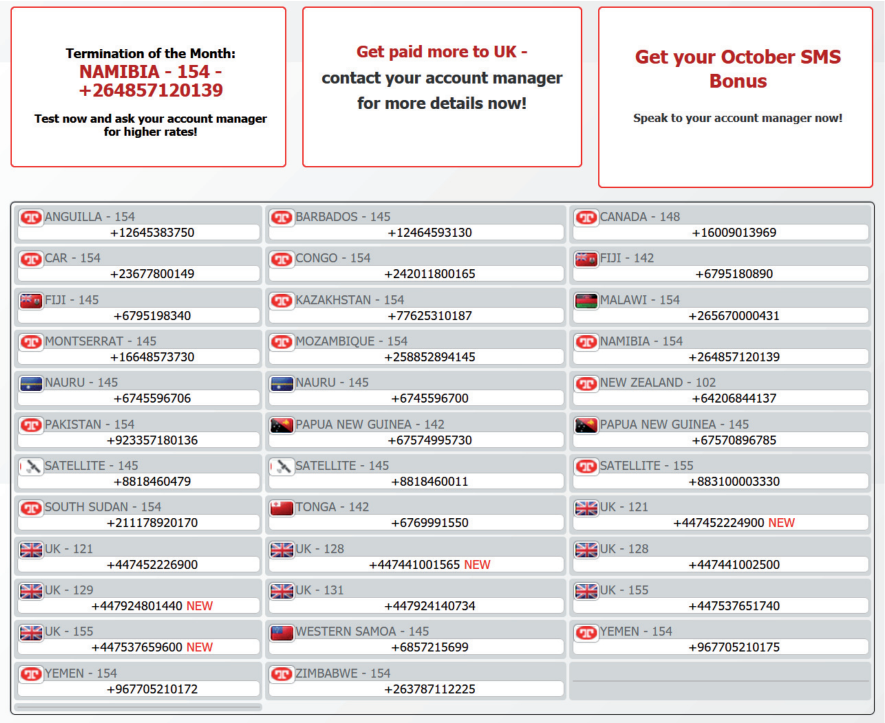
```
{"index":827,"from":"50300","receivedTime":"2021-06-06 18:00:52","content":"Thank you
for your 2 Euro donation to Pieta. SP www.likecharity.com Donation receipt 2288 Helpline
0766805278","unread":true}
```

```
{"index":826,"from":"50300","receivedTime":"2021-06-06 18:00:43","content":"Thank you for your
4 Euro donation to World Vision Ireland. SP www.likecharity.com Donation receipt 2289 Helpline
0766805278","unread":true}
```

Having said that – and thanks, again, to the incoming queue – another small batch of outgoing messages were brought into focus. In March 2021 there were about half a dozen messages sent to varying numbers with varying content. This time the timeline suggested more of an automated processing.

```
{"index":789,"to":"+265670000440","sendTime":"2021-03-21 18:59:26","content":"45555"}
{"index":788,"to":"+44792476990","sendTime":"2021-03-21 18:58:50","content":"46655"}
{"index":787,"to":"+447441056300","sendTime":"2021-03-21 18:58:26","content":"5655"}
{"index":786,"to":"+6768482290","sendTime":"2021-03-21 18:57:56","content":"4666"}
{"index":785,"to":"+67570896370","sendTime":"2021-03-21 18:57:25","content":"5888"}
{"index":784,"to":"+447537658500","sendTime":"2021-03-21 18:56:50","content":"55555"}
{"index":783,"to":"+447452222200","sendTime":"2021-03-21 18:56:19","content":"5524"}
```

The country codes belonged to three different countries and the numbers would lead to no easy conclusion as, with very few exceptions, they mainly appeared on fake and questionable dating sites. These exceptions revealed yet another web-based SMS service, this time appearing as a legitimate business that, amongst other things, offers premium rate services for its customers. The numbers were located on the company's test portal where one could test whether routes are paid or not to a specific destination. Upon further investigation, surprisingly similar services were found, sometimes it was the very same staff represented in the contact section of the site and only the main site design was changed, sometimes it was an exact copy. When we ran through all the test portal numbers on our logs, it brought up some interesting results. Besides half a dozen exact matches there were numbers where only the last two or three digits differed. This combined with the fact that our logs cover a timeframe of five years made us positive that the same services have been used in the past and the numbers they provide change rather frequently.



Termination of the Month:
NAMIBIA - 154 -
+264857120139
Test now and ask your account manager for higher rates!

Get paid more to UK -
contact your account manager
for more details now!

Get your October SMS Bonus
Speak to your account manager now!

| | | |
|---|---|---|
| ANGUILLA - 154<br>+12645383750 | BARBADOS - 145<br>+12464593130 | CANADA - 148<br>+16009013969 |
| CAR - 154<br>+23677800149 | CONGO - 154<br>+242011800165 | FIJI - 142<br>+6795180890 |
| FIJI - 145<br>+6795198340 | KAZAKHSTAN - 154<br>+77625310187 | MALAWI - 154<br>+265670000431 |
| MONTSERRAT - 145<br>+16648573730 | MOZAMBIQUE - 154<br>+258852894145 | NAMIBIA - 154<br>+264857120139 |
| NAURU - 145<br>+6745596706 | NAURU - 145<br>+6745596700 | NEW ZEALAND - 102<br>+64206844137 |
| PAKISTAN - 154<br>+923357180136 | PAPUA NEW GUINEA - 142<br>+67574995730 | PAPUA NEW GUINEA - 145<br>+67570896785 |
| SATELLITE - 145<br>+8818460479 | SATELLITE - 145<br>+8818460011 | SATELLITE - 155<br>+883100003330 |
| SOUTH SUDAN - 154<br>+211178920170 | TONGA - 142<br>+6769991550 | UK - 121<br>+447452224900 NEW |
| UK - 121<br>+447452226900 | UK - 128<br>+447441001565 NEW | UK - 128<br>+447441002500 |
| UK - 129<br>+447924801440 NEW | UK - 131<br>+447924140734 | UK - 155<br>+447537651740 |
| UK - 155<br>+447537659600 NEW | WESTERN SAMOA - 145<br>+6857215699 | YEMEN - 154<br>+967705210175 |
| YEMEN - 154<br>+967705210172 | ZIMBABWE - 154<br>+263787112225 | |

*Figure 5: Example of a test portal of a premium rate provider.*

## KEYWORDS OF DIFFERENT KINDS

Out of a dozen strange message types there was one we kept returning to. These messages followed the format of two keywords and two codes, where the latter consisted of one letter and one or two digits. The keywords were simplistic, focusing around the same theme, for example IT terms such as laptop, floppy, mouse, screen, hard drive, or clothing oriented such as shirt, watch, coat, gloves, pants and so on.

```
{"index":301,"to":"+447509649690","content":"CLOTHING,SHIRT,A12:B1","sendTime":"2018-07-06
13:18:17"}

{"index":300,"to":"+447509649690","content":"CLOTHING,GLOVES,A13:B","sendTime":"2018-07-06
13:18:01"}

{"index":299,"to":"+447509649690","content":"CLOTHING,VEST,A1:B","sendTime":"2018-07-06
13:17:11"}

{"index":298,"to":"+447509649690","content":"CLOTHING,SOCKS,A9:B","sendTime":"2018-07-06
13:15:59"}

{"index":297,"to":"+447509649690","content":"CLOTHING,SANDALS,A1:B","sendTime":"2018-07-06
13:15:41"}
```

For a brief period, our idea was that these could be successors of the slowly disappearing football-themed messages in an obfuscated fashion – keywords could represent teams, while codes could represent scores. The main problem with that theory was the extremely repetitive nature of some of the keywords. We were about to write this type off our list as 'unresolved' when we noticed a strange similarity. Completely unrelated devices appeared to be sending out the exact same batch of messages within a few seconds, which strengthened our idea of parallelization and distributed processing.

**Device A (IP: 5.204.***.*)**

```
{"index":29,"to":"+447452221108","sendTime":"2018-06-29 13:27:18","content":"LAPTOP,MOUSE,A1:B"}

{"index":28,"to":"+447452221107","sendTime":"2018-06-29
13:26:49","content":"LAPTOP,HARDDRIVE,A13:B"}

{"index":27,"to":"+447452221106","sendTime":"2018-06-29
13:26:19","content":"LAPTOP,SCANNER,A12:B1"}

{"index":26,"to":"+447452221103","sendTime":"2018-06-29
13:25:36","content":"LAPTOP,MONITOR,A11:B1"}

{"index":25,"to":"+447452221102","sendTime":"2018-06-29
13:24:43","content":"LAPTOP,FLOPPYDISK,A1:B12"}

{"index":24,"to":"+447452221101","sendTime":"2018-06-29
13:21:32","content":"LAPTOP,FLOPPYDISK,A1:B12"}
```

**Device B (IP: 84.224.***.***)**

```
{"index":153,"to":"+447452221108","sendTime":"2018-06-29 13:27:16","content":"LAPTOP,MOUSE,A1:B"}

{"index":152,"to":"+447452221107","sendTime":"2018-06-29
13:26:47","content":"LAPTOP,HARDDRIVE,A13:B"}

{"index":151,"to":"+447452221106","sendTime":"2018-06-29
13:26:18","content":"LAPTOP,SCANNER,A12:B1"}

{"index":150,"to":"+447452221103","sendTime":"2018-06-29
13:25:33","content":"LAPTOP,MONITOR,A11:B1"}

{"index":149,"to":"+447452221102","sendTime":"2018-06-29
13:24:41","content":"LAPTOP,FLOPPYDISK,A1:B12"}

{"index":148,"to":"+447452221101","sendTime":"2018-06-29
13:21:30","content":"LAPTOP,FLOPPYDISK,A1:B12"}
```

## CHANGING GEARS

All the previous use cases were falling into the low volume category with regard to the number of outgoing messages. Things got even more obscure when our focus shifted towards some of the high-volume ones. One device in Poland seemed to be freshly set up in May 2018 and the very first incoming message was about a monthly invoice of 202,53zl. Fast forward one month and a similar message arrived from the carrier, however this time the amount was 985,70zl and all of a sudden the message index was already at 1358. Going even further, the same invoice arrived on a monthly basis and the amount stabilized at a constant 202,05zl.

```
{"index":1361,"from":"T-Mobile","receivedTime":"2018-07-27 14:07:15","content":"2018-07-25
wystawilismy fakture nr 524411890718. Kwota do zaplaty 202,05zl, do 2018-08-08. Fakture mozesz
sprawdzic i oplacic w latwy sposob korzystajac z aplikacji Moj T-Mobile w swoim telefonie
(kliknij http://t-mobile.pl/aplikacja). Dziekujemy za wplate.\r","unread":true}
```

```
{"index":1358,"from":"T-Mobile","receivedTime":"2018-06-27 16:13:58","content":"2018-06-25
wystawilismy nr fakture 524320810618. Kwota do zaplaty 985,70zl, do 2018-07-09. Fakture mozesz
sprawdzic i oplacic w latwy sposob korzystajac z aplikacji Moj T-Mobile w swoim telefonie
(kliknij http://t-mobile.pl/aplikacja). Dziekujemy za wplate.\r","unread":true}

{"index":1,"from":"T-Mobile","receivedTime":"2018-05-27 08:07:53","content":"2018-05-25
wystawilismy nr fakture 524263940518. Kwota do zaplaty 202,53zl, do 2018-06-08. Fakture mozesz
sprawdzic i oplacic w latwy sposob korzystajac z aplikacji Moj T-Mobile w swoim telefonie
(kliknij http://t-mobile.pl/aplikacja). Dziekujemy za wplate.\r","unread":true}
```

It didn’t take long to figure out what had happened. After the initial invoice message there were a couple of ‘tests’ carried out, and then came a mass messaging of over 1,200 SMS with the very same content. There were only six different recipient numbers, all of UK numbers, and everything was done in less than 10 hours.

```
{"index":18,"to":"+447452318075","sendTime":"2018-06-11 02:25:53","content":"your phone
verfication is 4584"}

{"index":17,"to":"+447452318075","sendTime":"2018-06-11 02:25:49","content":"your phone
verfication is 4584"}

{"index":16,"to":"+447452318075","sendTime":"2018-06-11 02:25:44","content":"your phone
verfication is 4584"}

{"index":15,"to":"+447452318075","sendTime":"2018-06-11 02:25:38","content":"your phone
verfication is 4584"}

{"index":8,"to":"+447537606028","sendTime":"2018-06-11 02:17:35","content":"test"}

{"index":7,"to":"+447537606028","sendTime":"2018-06-11 02:10:04","content":"test"}

{"index":6,"to":"+447537606100","sendTime":"2018-06-10 18:29:24","content":"447537606100"}

{"index":3,"to":"+447537606100","sendTime":"2018-06-10 18:22:54","content":"447537606100"}

{"index":2,"to":"+972567674700","sendTime":"2018-06-10 18:22:44","content":"+972567674700"}
```

Doing the basic maths resulted in about 0.18 USD per message, which could be considered a standard SMS rate from Poland to the UK. Still, it was serious damage (close to 215 USD total) to whoever the owner of that device and SIM card was.

Note that similar test phases were discovered on multiple devices prior to an outgoing campaign throughout the whole research. The messages were either sent to free SMS services or unverified/unknown phone numbers with content resembling a simplistic test message (‘test’, ‘tst’, ‘asd’, ‘0’, ‘1’, etc.).

## TOP GUNS

After a fair number of small-scale campaigns, it was about time to consider the opposite end as well. Two of the largest ones observed consisted of several thousands of messages and went on for months. Another device located in Singapore had over 9,000 of the very same messages sent to a lone number which, by country code, belonged to Russia. The case reminded us of the Poland one above, but with at least eight times more outgoing messages and the damage done must have been scaled accordingly.

```
{"index":9624,"to":"+79697531497","sendTime":"2019-11-08 07:37:17","content":"send code
is;213200"}

{"index":9623,"to":"+79697531497","sendTime":"2019-11-08 07:37:04","content":"send code
is;21555"}

{"index":9622,"to":"+79697531497","sendTime":"2019-11-08 07:36:55","content":"send code is;9999"}

{"index":9621,"to":"+79697531497","sendTime":"2019-11-08 07:36:46","content":"send code
is;65563"}

{"index":9620,"to":"+79697531497","sendTime":"2019-11-08 07:36:37","content":"send code
is;77485"}
```

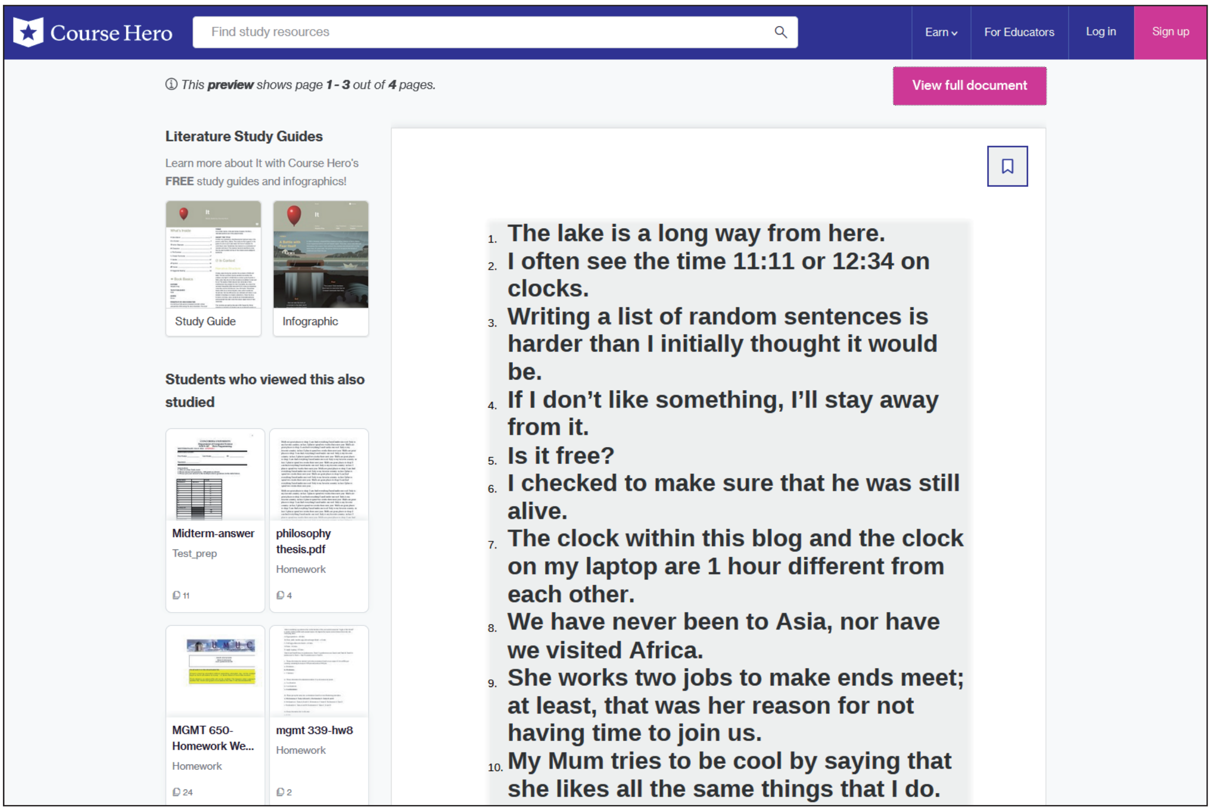
Probably one of the most interesting cases was related to a router located in Israel. Instead of all the previously known message types, we were presented with over 10,000 of what looked like grammatically correct English sentences, except their content made no sense at all. We could match some of the one-liners to song titles from *YouTube* and to well-known quotes from movies, books and other literature, but we were still struggling with a logical explanation besides that the heavy variation of the content was only necessary to bypass the fraud detection utilized by the carriers. We noted the initial test phase and also a pattern in the recipient numbers as they were consecutive and must have been obtained in a small batch.

```
{"index":11191,"to":"+447669350552","sendTime":"2020-07-12 20:05:03","content":"Toddlers feeding
raccoons surprised even the seasoned park ranger."}

{"index":11190,"to":"+447669350551","sendTime":"2020-07-12 20:05:03","content":"Had he known what
was going to happen, he would have never stepped into the shower."}
```

```
{"index":11189,"to":"+447669350550","sendTime":"2020-07-12 20:05:03","content":"Nudist colonies
shun fig-leaf couture."}
{"index":11188,"to":"+447640157049","sendTime":"2020-07-12 20:05:03","content":"I often see the
time 11:11 or 12:34 on clocks."}
{"index":11187,"to":"+447640157048","sendTime":"2020-07-12 20:05:03","content":"She borrowed the
book from him many years ago and hasn't yet returned it."}
{"index":11186,"to":"+447640157047","sendTime":"2020-07-12 20:05:03","content":"There should have
been a time and a place, but this wasn't it."}
{"index":11185,"to":"+447640157046","sendTime":"2020-07-12 20:05:03","content":"He had a vague
sense that trees gave birth to dinosaurs."}
```

Out of some wild ideas, we tried to treat them as a specific acrostic cipher implementation, but the outcome wasn't fruitful and the lack of any additional context made further investigation pointless. Interestingly, a portion of the quotes later also turned up on sites such as *Course Hero* or *Scribd* in documents which contained nothing else.



1. The lake is a long way from here.
2. I often see the time 11:11 or 12:34 on clocks.
3. Writing a list of random sentences is harder than I initially thought it would be.
4. If I don't like something, I'll stay away from it.
5. Is it free?
6. I checked to make sure that he was still alive.
7. The clock within this blog and the clock on my laptop are 1 hour different from each other.
8. We have never been to Asia, nor have we visited Africa.
9. She works two jobs to make ends meet; at least, that was her reason for not having time to join us.
10. My Mum tries to be cool by saying that she likes all the same things that I do.

*Figure 6: Example of a document containing matching quotes.*

## DATE MANIPULATION AND HYPERLINKS

Fuelling the obscurity of the case, this was a unique campaign as it also exploited a vulnerability in the firmware which made manipulation of system time possible. Due to that we couldn't precisely measure for how long the whole campaign lasted. The starting date was May 2020, and even though the last outgoing message had a timestamp of July 2020, the month portion of the date was changed multiple times in between – even to values out of bound (52,17,28). As the internal message index was still intact, the original order of the messages could be still determined and one could have built some language-driven AI to look for further correlations, but that was out of the scope of our research.

The only other campaign to utilize date manipulation was also the only one where we observed the use of hyperlinks. The content was Arabic and resembled a standard spam or phishing scheme with a tinyurl link redirecting to another landing page. By the time of discovery, the redirection seemed to be off, but the recipient phone numbers were all different, as one would expect.

```
"index":556,"to":"+972545556369","content":"Ã™Â^Ã™ÂŠÃ™Â† Ã™Â…Ã˜Â§ Ã™ÂƒÃ™Â†Ã˜Âª Ã˜Â¬Ã™Â^Ã˜Â§Ã™Â"
Ã™Â…Ã˜Â¹Ã™Âƒ Ã˜Â¹Ã™Â"Ã™Â‰ Ã˜Â·Ã™Â^Ã™Â"Ã˜ÂÃ™Â…Ã™Â" Ã˜ÂªÃ˜Â·Ã˜Â¨Ã™ÂŠÃ™Â‚ Ã˜Â¬Ã™Â^Ã˜Â§Ã™Â"
Ã˜Â§Ã™Â"Ã˜Â¢Ã™Â† Ã™Â"Ã˜ÂªÃ˜ÂÃ˜ÂµÃ™Â" Ã˜Â¹Ã™Â"Ã™Â‰ Ã™Â□Ã˜Â±Ã˜ÂµÃ˜Â© Ã™Â"Ã˜Â±Ã˜Â¨Ã˜Â Ã™Â…
Ã˜Â¨Ã™Â"Ã˜Â° Ã™Â…Ã™Â"Ã™ÂŠÃ™Â^Ã™Â† Ã˜Â´Ã™ÂŠÃ™ÂƒÃ™Â" Ã™Â‚Ã™Â… Ã˜Â¨Ã˜ÂªÃ˜ÂÃ™Â…Ã™ÂŠÃ™Â"Ã™Â‡
Ã˜Â¹Ã˜Â¨Ã˜Â± Ã˜Â²Ã™ÂŠÃ˜Â§Ã˜Â±Ã˜Â© Ã™Â…Ã™Â^Ã™Â‚Ã˜Â¹Ã™Â†Ã˜Â§ https://tinyurl.com/
y7nvzcvp","sendTime":"2018-52-07 12:07:51"
```

```
"index":555,"to":"+972508431295","content":"Ã™Â^Ã™ÂŠÃ™Â† Ã™Â…Ã˜Â§ Ã™ÂƒÃ™Â†Ã˜Âª Ã˜Â¬Ã™Â^Ã˜Â§Ã™Â"
Ã™Â…Ã˜Â¹Ã™Âƒ Ã˜Â¹Ã™Â"Ã™Â‰ Ã˜Â·Ã™Â^Ã™Â"Ã˜ÂÃ™Â…Ã™Â" Ã˜ÂªÃ˜Â·Ã˜Â¨Ã™ÂŠÃ™Â‚ Ã˜Â¬Ã™Â^Ã˜Â§Ã™Â"
Ã˜Â§Ã™Â"Ã˜Â¢Ã™Â† Ã™Â"Ã˜ÂªÃ˜ÂÃ˜ÂµÃ™Â" Ã˜Â¹Ã™Â"Ã™Â‰ Ã™Â□Ã˜Â±Ã˜ÂµÃ˜Â© Ã™Â"Ã˜Â±Ã˜Â¨Ã˜Â Ã™Â…
Ã˜Â¨Ã™Â"Ã˜Âº Ã™Â…Ã™Â"Ã™ÂŠÃ™Â^Ã™Â† Ã˜Â´Ã™ÂŠÃ™ÂƒÃ™Â" Ã™Â‚Ã™Â… Ã˜Â¨Ã˜ÂªÃ˜ÂÃ™Â…Ã™ÂŠÃ™Â"Ã™Â‡
Ã˜Â¹Ã˜Â¨Ã˜Â± Ã˜Â²Ã™ÂŠÃ˜Â§Ã˜Â±Ã˜Â© Ã™Â…Ã™Â^Ã™Â‚Ã˜Â¹Ã™Â†Ã˜Â§ https://tinyurl.com/
y7nvzcvp","sendTime":"2018-52-07 12:07:50"
```

```
"index":554,"to":"+972505670031","content":"Ã™Â^Ã™ÂŠÃ™Â† Ã™Â…Ã˜Â§ Ã™ÂƒÃ™Â†Ã˜Âª Ã˜Â¬Ã™Â^Ã˜Â§Ã™Â"
Ã™Â…Ã˜Â¹Ã™Âƒ Ã˜Â¹Ã™Â"Ã™Â‰ Ã˜Â·Ã™Â^Ã™Â"Ã˜ÂÃ™Â…Ã™Â" Ã˜ÂªÃ˜Â·Ã˜Â¨Ã™ÂŠÃ™Â‚ Ã˜Â¬Ã™Â^Ã˜Â§Ã™Â"
Ã˜Â§Ã™Â"Ã˜Â¢Ã™Â† Ã™Â"Ã˜ÂªÃ˜ÂÃ˜ÂµÃ™Â" Ã˜Â¹Ã™Â"Ã™Â‰ Ã™Â□Ã˜Â±Ã˜ÂµÃ˜Â© Ã™Â"Ã˜Â±Ã˜Â¨Ã˜Â Ã™Â…
Ã˜Â¨Ã™Â"Ã˜Âº Ã™Â…Ã™Â"Ã™ÂŠÃ™Â^Ã™Â† Ã˜Â´Ã™ÂŠÃ™ÂƒÃ™Â" Ã™Â‚Ã™Â… Ã˜Â¨Ã˜ÂªÃ˜ÂÃ™Â…Ã™ÂŠÃ™Â"Ã™Â‡
Ã˜Â¹Ã˜Â¨Ã˜Â± Ã˜Â²Ã™ÂŠÃ˜Â§Ã˜Â±Ã˜Â© Ã™Â…Ã™Â^Ã™Â‚Ã˜Â¹Ã™Â†Ã˜Â§ https://tinyurl.com/
y7nvzcvp","sendTime":"2018-52-07 12:07:49"
```

Note that even though the value of the month was set to 52, the seconds are normally passing by as they should, however in the case of the previous campaign the date was properly frozen. That means whoever was responsible for that campaign went the extra mile and felt it was important enough to always re-adjust date to a fixed value prior to sending out a new message.

## DATA EXFILTRATION

The general idea of the *MR6400* devices being used for data exfiltration has been brought up multiple times over the years, but there was no evidence to back up that claim. In theory, once an attacker established a foothold in a target environment and was done with internal reconnaissance, a smaller amount of data such as login credentials, passwords, access codes or documents of high value could easily be encrypted by a symmetric algorithm (e.g. AES) then split into chunks to adhere to the 160-character limit of the SMS format and sent out using one of the compromised routers. There are certainly better alternatives present for such a purpose, yet IT security departments and SOCs might not be prepared to face a situation where one of their endpoints or servers directly connects to an external router just to proxy a few hundred characters worth of data towards a burner phone in a completely different destination. Right before concluding our research, we come across this:

```
{"index":76,"to":"+447452221550","sendTime":"2018-12-01 03:09:07","content":"http://
admin:admin@193.14.191.114/ "}
```

```
{"index":75,"to":"+265212341261","sendTime":"2018-12-01 00:54:39","content":"+265212341261"}
```

Whether this was just a test or the server in the message contained anything related to our research couldn't be verified due to about two years difference between the time of sending and time of discovery.

## MESSAGING AS A SERVICE

After a long consideration of all our findings, we came to one conclusion. Whoever discovered the vulnerability first in 2016 started to exploit it by running football-themed campaigns for over a year. Meanwhile, with an increasing number of exploitable devices an opportunity arose to capitalize on that by organizing routers into a manageable framework. Creating an SMS-focused service where complete anonymity is provided, with multiple thousands of devices there for 'renting out' and with basic load balancing implemented to be able to operate for an extended period of time.

The vulnerability could be discovered by multiple parties or it could be sold, and we are certain that this happened at some point. Judging by the nature of the observed campaigns, not everyone seemed to be interested in the long game of MaaS, instead some went for a quick win by which an alarm could easily be triggered depending on the fraud protection techniques used by the operator or by the owner of the device due to an unexpectedly high monthly invoice.

There are still thousands of *MR6400* devices in operational state hooked up to the Internet. In what condition they are, is hard to determine. They could have a vulnerable firmware installed, but also a SIM card with barring enabled by the operator – these are done even more often by default, especially for data-only SIM cards which are the ideal pick for routers – hence limiting or completely disabling outgoing SMS. The exploitation of these devices has not stopped; however, it seems to have reduced greatly over the years compared to its peak in 2018. The lack of interest from cybercriminals, the updating of the device's firmware to a non-vulnerable version, moving on to a newer vulnerable model with greater market share or the enabling of specific barring on the SIM cards could be all contributing to the decline.

## CONCLUSION

When it comes to IoT devices there are some long-standing issues to be resolved. The general state of security of these devices has slowly improved over the years, however it is still in a state that is far from ideal. Combining that with the currently deployed update mechanisms of such devices makes the problem even more serious. We can only expect improvements if vendors start to pay real attention to security issues (starting with critical ones) and some kind of auto-update functionality is listed as a top priority on every roadmap.

Exploiting a functionality of an IoT device with no noticeable effect on the device's main operation makes the exploitation even more challenging to be discovered. Our research has showcased that it is possible to exploit a device without unfortunate side effects, yet some of the consequences could be serious. The main CPU won’t be overloaded as it would if a coin miner was running, there are no mass outgoing queries as a sign of a DDoS attempt and no further breach of the local network will happen. Instead, the SMS capability might be heavily abused. This can result not only in an unexpectedly high monthly invoice but, similar to having a home Wi-Fi hacked, some unpleasant questions by law enforcement if the device has been part of criminal activities. The exploitation of the *MR6400* devices also demonstrates an unfortunate trend: the boundaries of traditional and cybercrime are increasingly overlapping.

## REFERENCES

[1] Wikipedia. SMS. https://en.wikipedia.org/wiki/SMS.

[2] Viehböck, S. TP-LINK Local File Disclosure. Packet Storm. April 2015. https://packetstormsecurity.com/files/131378/TP-LINK-Local-File-Disclosure.html.