MOBILE BANKING FRAUD VIA SMS IN NORTH AMERICA: WHO'S DOING IT AND HOW

Cathal Mc Daid
AdaptiveMobile Security, Ireland

Email cathal.mcdaid@adaptivemobile.com

ABSTRACT

Nearly every day, cybercriminals are using scams over mobile messaging to execute several types of money-stealing mobile attacks on North American banks. This paper will use real-world data obtained from various mobile operators showing cybercriminal activity to provide a unique, valuable look into the methods used by these bank phishers.

We will use data from actual SMS attacks that have been blocked to provide a detailed and in-depth view of the various techniques used by cybercriminals, as well as the linguistic evolution of SMS bank scam attacks. We will analyse the changes in SMS messages in relation to the bank scams as well as showing the techniques that the attackers are using to bypass and defeat defences in place.

The paper will present statistical detail on various aspects of the attacks, we will also look at one of the most important subjects, and the reason why these attacks are so successful: how scammers use the recipient/victim cell numbers. We will look at the relationship between the recipient numbers and the attacked financial institutions and what correlations can be made. Finally, this paper will look at the similarities and differences between today's attacks and those from the past.

ALIVE AND TEXTING

Many people have already 'buried' SMS multiple times during the last few years [1–3]. The common reasons cited are that this form of communication is old-fashioned, outdated, and has been replaced by messaging apps etc. However, in reality many people and businesses continue to use this simple way of delivering information – every mobile device can send and receive SMS messages, and while volumes may be declining [4], every mobile device will continue to support it for the foreseeable future. But as it goes with almost any popular technology: where there's popularity there will be crime.

There are many types of SMS scam campaigns in different countries [5–7]. What determines the most prevalent depends on the services popular in a certain country or region and the nature of criminal organizations that have taken root during the period in which mobile messaging has been available.

DETAILS OF THE ATTACK

Within North America, one of the most popular types of SMS scam attacks are bank phishing messages. These attacks have been used by several groups of mobile-based cybercriminals for several years now. Keeping in mind the theory of economic incentives for attackers – i.e. an attacker will only carry out a particular attack if they benefit from it – then this means that a consistent number of people who receive these messages trust them and give away sensitive information to the criminals responsible for sending them. The following is a typical example of such a message:

```
(Auburn University FCU) 24HRS ALERT: Your VISA Check
Card #413809 is deactivated. Please call our 24 hours
line (334) 209-[REDACTED]
```

The structure is pretty simple: the bank name goes first, then there's a partial credit card number. After that there's a call-to-action, which consists of a request for the victim to call certain phone number. While it may seem simple, every part of the message is designed to do two things: avoid various defences and increase the conversion rate. The conversion rate is the number of messages that lead to a successful phishing result.

First, a potential victim receives the message, which looks somewhat legitimate. If a person is not aware that banks and financial institution don't normally send such messages and don't ask customers to call some sort of '24-hour hotline', then there's a reasonable probability that they will call this number and give away their credit card details to the attackers. Like many cyber scams, the attackers in this case are hunting a credit card number with additional information such as expiry date, CVV code and PIN code.

If a victim makes a call to the number in the message, they will hear an automatic voice responder claiming 'your card has been blocked, please provide us with the following information in order to unblock it'. The actual number that is dialled usually forwards to another phone number which has an interactive voice response (IVR), which is capable of handling multiple different calls at once. Variants of the voice message played to the victim are available on the Internet [8], but in general it is a combination of samples of a commercial institution's 'real' recorded messages – normally the name of the brand – and sampled words from other sources. After the initial recording a victim will be asked to enter (using the keypad on their phone) the number of their credit card, PIN code, CVV code and expiry date. In other words, all sensitive information. Again, any real financial institution or bank will never ask its customers for such details via this method. But if an attacker obtains these details he's able to use this data to buy various items online. After the victim has entered the details, another recording typically tells them to wait at least 24 hours before contacting their bank. The aim of this is to give the attackers a window of opportunity in which to use the stolen data.

The use of an IVR is one of the 'signature' moves of this particular cybercriminal group, along with specific efforts to avoid detection. One of these is quite interesting in how it's done and what it says about defences in the past. To illustrate, see if you can spot the difference between these two words:

DEACTIVATED DEACTlVATED

You may have noticed that the capital 'i' in the second word has been replaced with 'l'. It may be easy to spot on paper or in any text document, but it wouldn't be easy to spot the replacement in an SMS message, especially if we are talking about simple cell phones. This replacement was a very common techniques used by cybercriminals sending fake banking alert messages a couple of years ago. At that time it was the most popular way of bypassing the various simple filters used by mobile operators. Since then, the group running these attacks has moved onto more sophisticated methods in order to bypass filters and deliver the message to potential victims.

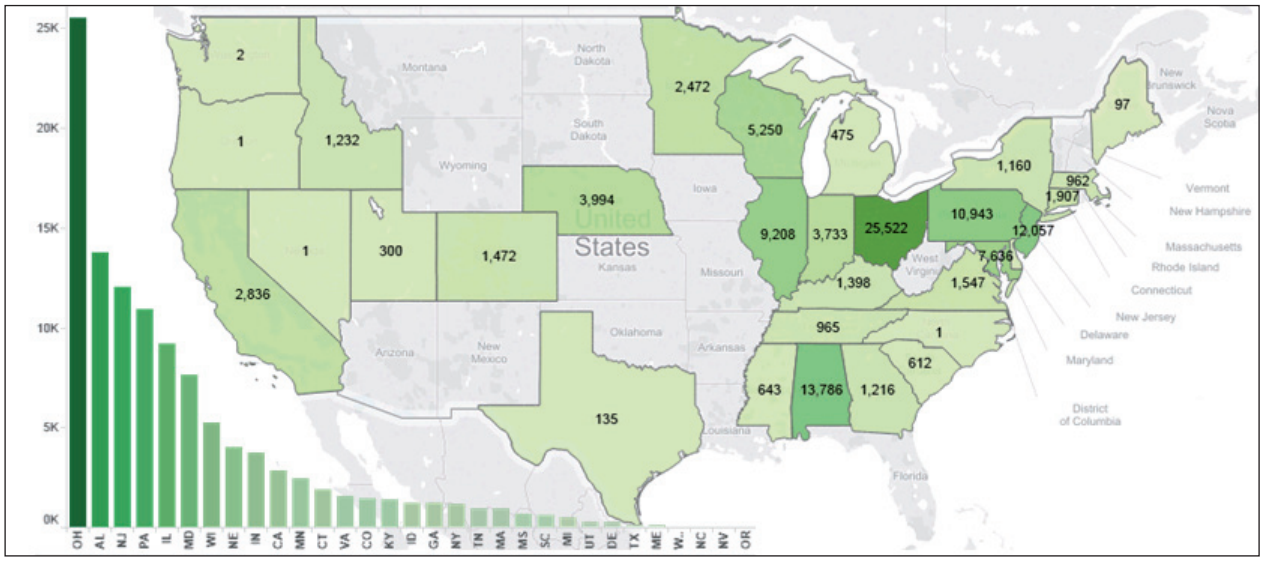

Figure 1: Distribution of bank phishing messages among various states in the US.

TARGETING BY PHONE NUMBER

Now we have some knowledge of the attack, we can look at the influence of phone numbers. First let us look to see what areas are being targeted. Figure 1 shows the distribution of bank phishing messages among various states in the US. From October 2014 to January 2015, messaging security systems deployed by *AdaptiveMobile* within North American mobile operators blocked 112,220 separate phishing messages. This accounted for just under 4% of all spam messages blocked at the time. While relatively small, each message can have a much greater impact on the victim than other types of messaging attacks, due the impact on their personal banking details.

We are able to plot the geographic areas that receive these attacks due to the unique nature of the North American Numbering Plan (NANPA). The North American numbering plan is shared by the USA, Canada and the Caribbean Islands and defines how phone numbers are allocated within these countries. All numbers (both mobile and landline) are geographically allocated. This allows us to plot out the states in Figure 1. Unfortunately, the same technique also helps mobile spammers to target local areas using an ingenious method of social engineering.

If we look at the structure of a typical number from North America, we can see that the first three digits are the NPA (area code), the next three are the NXX (switch), and the last four are the subscriber number.

```
+1 – XXX – XXX – XXXX
```

Bank spammers have found an additional usage of the phone numbers for social engineering purposes: the sender of the phishing message and the call-to-action (CTA) number within the message often have the same area code as the recipient. This actually makes it look more legitimate than if they were different. E.g. for the following message the sender was 1-309-361-XXXX and the recipient 1-309-363-XXXX. The area code 309 is for Peoria, Illinois.

```
This is an automated alert from South Side Bank.
*VISA Debit/Card #43315201 reactivation required.
Please call 24hrs (309) 282-[REDACTED]
```

Figure 2 shows the overlap between the state of the area code of the spammer (sender), target (recipient) and message (CTA number in message). Basically half of all bank scam messages have a match between all three (a 'triple match') while ~65% have match between at least two. We can clearly see that this overlap is deliberate, and considering that it takes effort for an attacker to obtain and use sender numbers and call-to-action numbers with the same code as the recipient, there must be a good reason for that. The reason becomes more apparent later as we consider the type of financial institute being attacked.

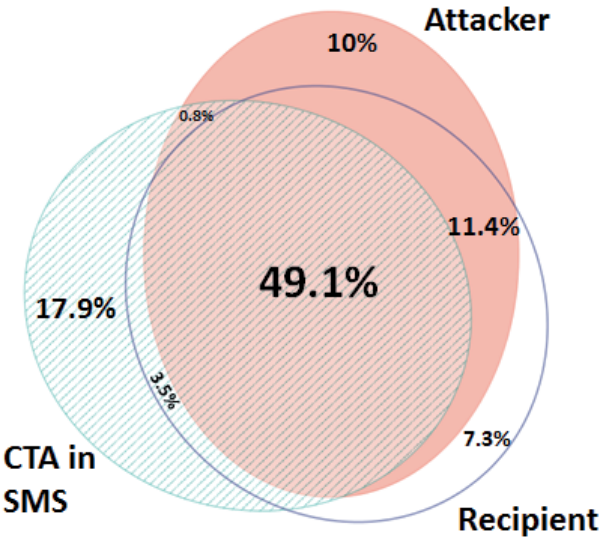

Figure 2: Overlap between the state of the area code of the spammer (sender), target (recipient) and message (CTA number in message).

WHO ARE THE TARGETS?

By plotting the attacks in more detail, based on the NPA and NXX locations, we can see that the vast majority of attacks are happening in the East Coast of the US (see Figure 3). The

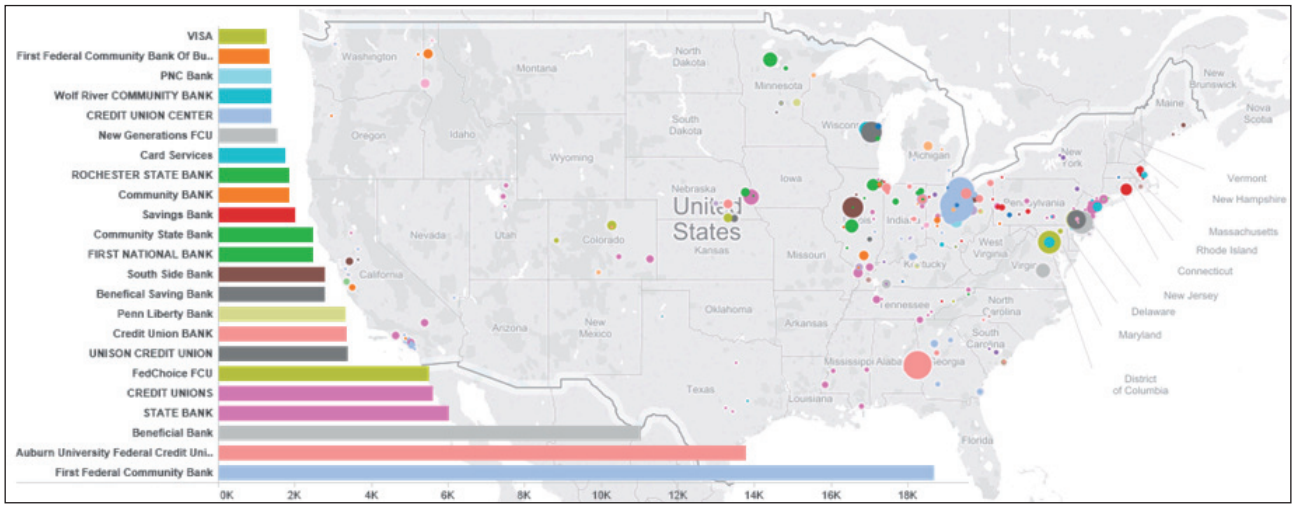

Figure 3: We can see that the vast majority of all attacks are happening in the East Coast of the US.

three most targeted financial institutions during this period are:

- First Federal Community Bank
- Auburn University Federal Credit Union
- Beneficial Bank.

When you look at the other financial institutions attacked it quickly becomes obvious that there is a dearth of large banking organizations like *Wells Fargo*, and an emphasis on smaller credit unions and banks. There are also a number of 'generic' names such as 'Credit Unions' and 'State Bank'. To make sense of this, if we plot the attacks by the number of states to which the message was sent (y-axis) and the number of targets to which the attack message was sent (x-axis), we see a particular pattern[1], as shown in Figure 4.

Here, we see that the tactics vary between either sending a lot of attack messages involving a named, specific bank or credit union which is in a few or one state (bottom right sector), and sending blander/more generic messages to multiple states (top left sector).

Of the two tactics the named method seems more common. Putting this together with the lack of major/nationwide financial institutions, we can say that the vast majority of attacks by this group are against the customers of various

[1] Note bubble size is number of messages sent. For these attacks the number of messages sent ≈ number of recipients.

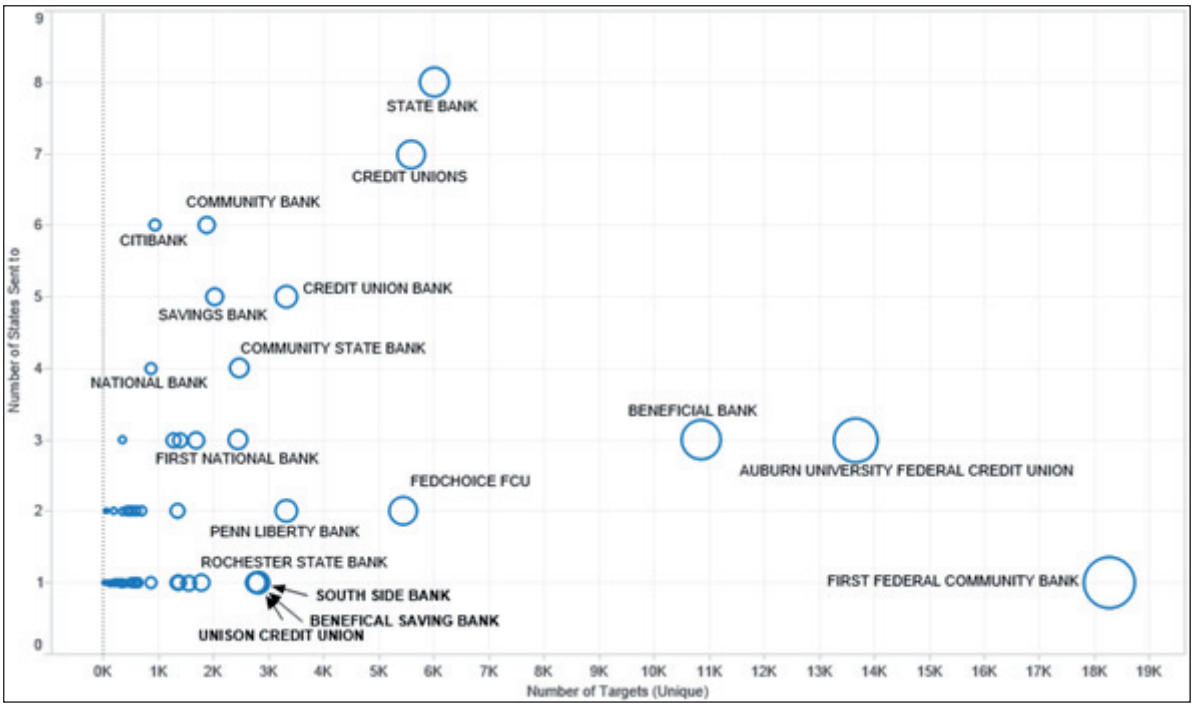

Figure 4: Plotting the attacks by number of states to which the message was sent against the number of targets to which the message was sent, reveals a particular pattern.

local financial institutions. The main/most popular national banks are not targeted at the moment (although they may have been in the past). It is theorized that this group of cybercriminals have decided to adopt this strategy for several reasons:

- It is more likely that local banks/credit unions have local customers, and therefore the combination of the local sending number, bank name and CTA might look more plausible for a potential victim.
- It is possible that the fraud prevention or security departments of small credit unions/banks may not be as quick to spot or react to attacks as those of large banks.

The most popular CTA in all of these messages is a phone number. There are several reasons as to why this is so, but by using it there is no need for the user to have mobile access to the Internet.

Phone number CTA pros:

- works for all phones
- more accepted by all age groups
- pseudo-authentication
- more 'official' sounding.

Phone number CTA cons:

- IVRs are expensive to hack/set up.

This doesn't mean that there are no 'classic' phishing messages containing a URL, as is shown in the *Citibank* example below, however, this technique is not as common:

```
You have a new alert regarding your Citibank
account. Please click the link bellow to read it:
http://online.citibank.com.us-wl***.com
```

In fact, this message also seems to differ from the other types we have covered, in that it *does* cover a large national bank: *Citibank*. The fact that differences like this exist allows us to consider how many groups of criminals are active.

EMAIL-TO-SMS GROUP

To recap, the attacks have generally followed this pattern:

- Named local banks/credit unions are the main targets, as well as generic financial names
- Spamming is 'regional' (using the same area code for sender and recipient)
- Phone number CTAs are used, so users of all kinds of devices are vulnerable (simple phones and smartphones).

This type of scam was the main focus of our research and this paper. However, we should mention other types of banking scam, whose method and pattern is different enough for us to attribute it to at least one other bank phishing criminal organization currently active in North America.

Screenshots [9, 10] of these attacks are shown in Figures 5 and 6.

While it seems similar, there are differences. For one, these spam messages are sent primarily via email-to-SMS gateways, which explains the email address indicated to be the sender. These entry points typically have protection that is not optimized for mobile. Security here is built around

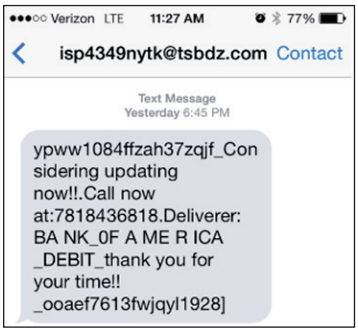

Figure 5: Screenshot of a different type of attack with extensive obfuscation.

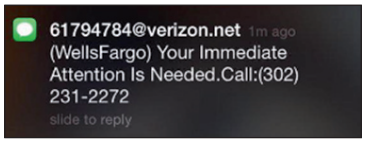

Figure 6: Screenshot of a different type of attack.

systems originally designed for email, not SMS. And you can see that the first message (Figure 5) doesn't look really 'official' and legitimate – there is extensive obfuscation.

Figure 7 is a plot of attacks of this type recorded based on complaints from mobile subscribers, as well as the bank name that is used. You can clearly see that there are differences in the targets and the distribution. The targets of these attacks include much larger banks, and there is much more cross-state activity. In fact, you can see that there is considerable West Coast activity – a considerable difference from the first 'gang' which seems primarily to target the East Coast. They also use URLs more frequently and the sender email address is mostly random. It is also important to mention that recently hacked IVRs have been used as the CTA number [11], again a difference.

The radically different methods and targets used to achieve the same end (bank phishing) allows us to divide the attacks into different groups, which combined with other internal intelligence, means we can say with some certainty that there are at least two different bank phishing organizations currently active in North America, and possibly more.

However, a different attack method does not always mean that a new 'group' is active. Criminal groups, and the mobile attacks they operate, generally evolve when put under pressure. In North America in the last two to three years, increasing defences against SMS phishing have led to a re-emergence of mainstream voice phishing attacks. Normally (but not always) such attacks target main banks. These attacks have a larger cost associated than SMS – they are slower, longer and more technical. But at the same time they can generate larger profits for attackers, and as an additional benefit, bank/credit unions' caller IDs can easily be spoofed. Bizarrely, it is easier to spoof a phone call in the US than it is a text message. Unfortunately, as protection from various types of SMS attacks gets better, these voice attacks may increase. Both groups we have profiled here are likely to use these voice attacks to deal with the increasing protection on the mobile messaging side.

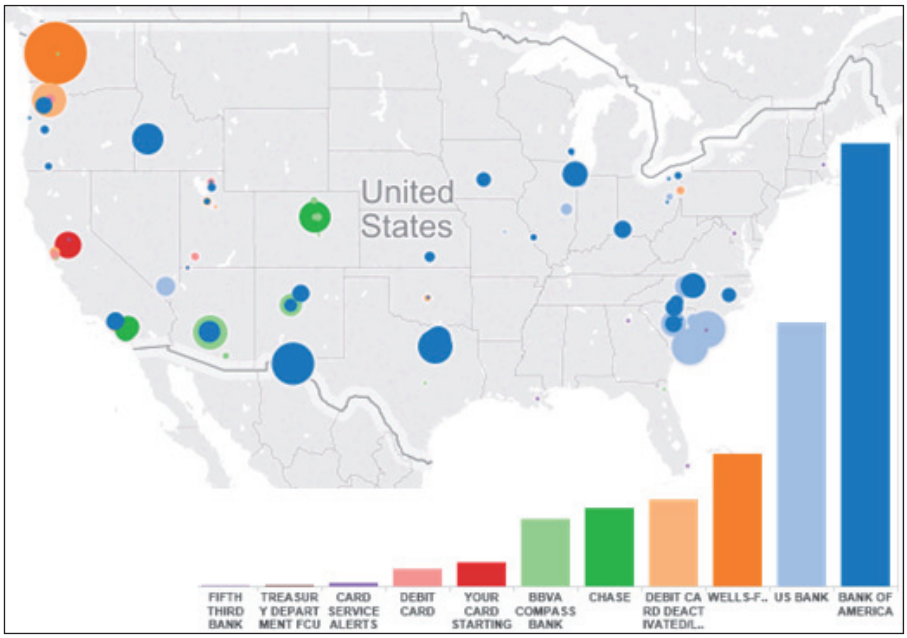

Figure 7: Plot of attacks recorded based on customer complaints from mobile subscribers.

CHANGING TEXT IN AN ONGOING ATTACK

In order to understand how scammers try to bypass various mobile messaging protection systems while at the same time making the message look like a legitimate one, let's look at the evolution of an attack message within one particular campaign. We will look at a message targeting *Auburn University FCU*, a credit union based in Auburn, Alabama, that was observed during the period of review.

The campaign started with the following message:

```
(Auburn University FCU) 24HRS ALERT: Your VISA Check
Card #413809 is deactivated. Please call our 24
hours line (334) 209-[****]
```

After some time the attackers deleted the first set of parentheses and '24HRS':

```
Auburn University FCU ALERT: Your VISA Check Card
#413809 is deactivated. Please call our 24 hours
line (334) 209-[****]
```

Next, they added the '-' symbol instead of a space before the word 'Please':

```
Auburn University FCU ALERT: Your VISA Check Card
#413809 is deactivated.-Please call our 24 hours
line (334) 209-[****]
```

In the fourth variant the '-' was replaced with '**':

```
Auburn University FCU ALERT: Your VISA Check Card
#413809 is deactivated.**Please call our 24 hours
line (334) 209-[****]
```

The fifth variant has one '*' instead of two:

```
Auburn University FCU ALERT: Your VISA Check Card
#413809 is deactivated.*Please call our 24 hours
line (334) 209-[****]
```

In the sixth variant of the message the '*' was placed before the word 'deactivated':

```
Auburn University FCU ALERT: Your VISA Check Card
#413809 is *deactivated. Please call our 24 hours
line (334) 209-[****]
```

The seventh variant is important because for the first time within the whole campaign the attackers made a significant change to the message:

```
Auburn University FCU ALERT: Your VISA Check Card
#413809 is locked.*Please call our 24 hours line
(334) 209-[****]
```

In the eighth variant attackers replaced the word 'locked' with 'frozen' and deleted 'VISA Check':

```
Auburn University FCU ALERT: Your card #413809 is
frozen.-Please call our 24 hours line (334) 209-
[****]
```

More changes occurred in the ninth message of the campaign:

```
Auburn University -FCU NOTICE-: Your card #413809 is
-limited-. Please call our 24 hours line (334) 209-
[****]
```

The word 'VISA' is back in the tenth message:

```
Auburn University -FCU NOTICE-: Your VISA #413809 is
limited.*Please call our 24 hours line (334) 209-
[****]
```

The attackers continue to use various synonyms:

```
Auburn University FCU NOTICE: Your VISA #413809 is
detained. Please call our 24 hours line 334-209-
[****]
```

Finally, the whole campaign is finished with more changes, the most extensive of the whole attack:

```
Auburn University FCU NOTICE: Your card starting
with 4138 is deact ivated. Please call our 24 hours
line 334-209-[****]
```

The attackers are making constant minor changes during periods of the campaign. These changes are forced – during this period the messaging protection systems within the operator in question were detecting and blocking each new variant. In effect, the attackers have two, sometimes competing objectives. They need to make the message look legitimate at all points – so misspelling and text replacements that look strange are not a good idea – but at the same time they somehow need to bypass filters in order to deliver the message. All the changes described here were made within one attack (over the course of a few hours) and it is almost certain that each change was made by a human, not an automated program. Sometimes the interval between the changes is very small and therefore the number of messages

being sent is relatively small due to the fact that attackers are testing whether their messages are getting blocked – they do not have visibility on how these messages are being detected and blocked. This indicates that this is a very manually intensive effort on behalf of the attacker.

USE OF CREDIT CARD NUMBERS

There is one more social engineering trick which is used by attackers in order to deceive potential victims and make a message to look as legitimate and trustworthy as possible. You can see that nearly all messages contain the first four or six digits of the credit card number. For a person who is not aware of the credit card number format, this inclusion of part of the code might persuade them that the message has been sent from the bank itself. However, in reality the first four or six digits of the card of a certain bank is public knowledge and can easily be found on the Internet.

There are 16 digits in a credit card number:

```
xxxx xxxx xxxx xxxx
```

The first digit is the Major Industry Identifier. For example, 1 and 2 are used by airlines, 4 and 5 are used by financial institutions, 8 is related to healthcare and telecom. The first six digits including the Major Industry Identifier comprise the Issuer Identifier Number (IIN), which points to the issuing organization. Each bank has a certain IIN which can easily be found. Therefore cybercriminals can pretend that they 'know' the whole card number while in fact they only know the financial institution and the card type ('4' as the first digit indicates out that it is a *Visa* card; '5' a *MasterCard*).

Taking the example above, the card number 4138 09XX XXXX XXXX claims that this is a *Visa* card issued by *Auburn University FCU*. The next nine digits comprise the individual account identification, the last digit is the check digit which is calculated using the Luhn algorithm. These nine digits are the part that only the card holder and the real bank will know – but, by including the right partial number for the right bank, the attackers are able to make the certain message seem more convincing to a potential victim.

EVOLUTION OVER TIME

The statistics described in the previous part were collected between October 2014 and January 2015. However, we have earlier comparison data from 18 months previously – the April/May 2013 period. This is useful to determine whether the bank phishing attacks are changing.

If we look first at the targeted states, we can see that the overall situation hasn't changed significantly. The vast majority of attacks even then were happening in the East Coast of the US, as shown in Figures 8 and 9.

The same is true for the type of banks and financial institutions being targeted. In spring 2013, while the actual bank names were different, the attackers were still targeting localized small banks and credit unions, or using generic terms such as 'Card Service Alerts' in multiple states (Figure 10).

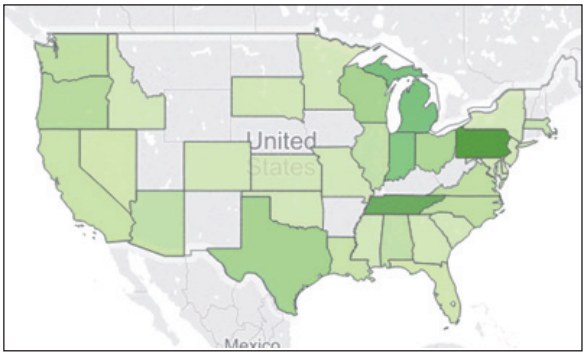

Figure 8: Targeted states April to May 2013.

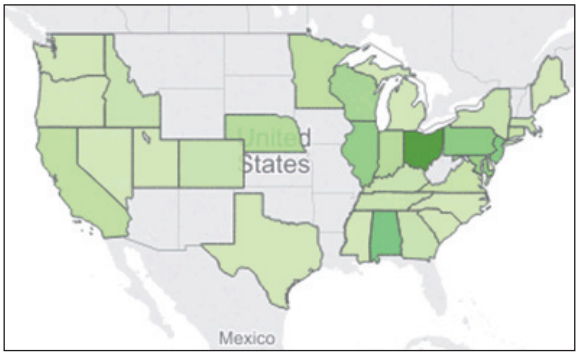

Figure 9: Targeted states October 2014 to January 2015.

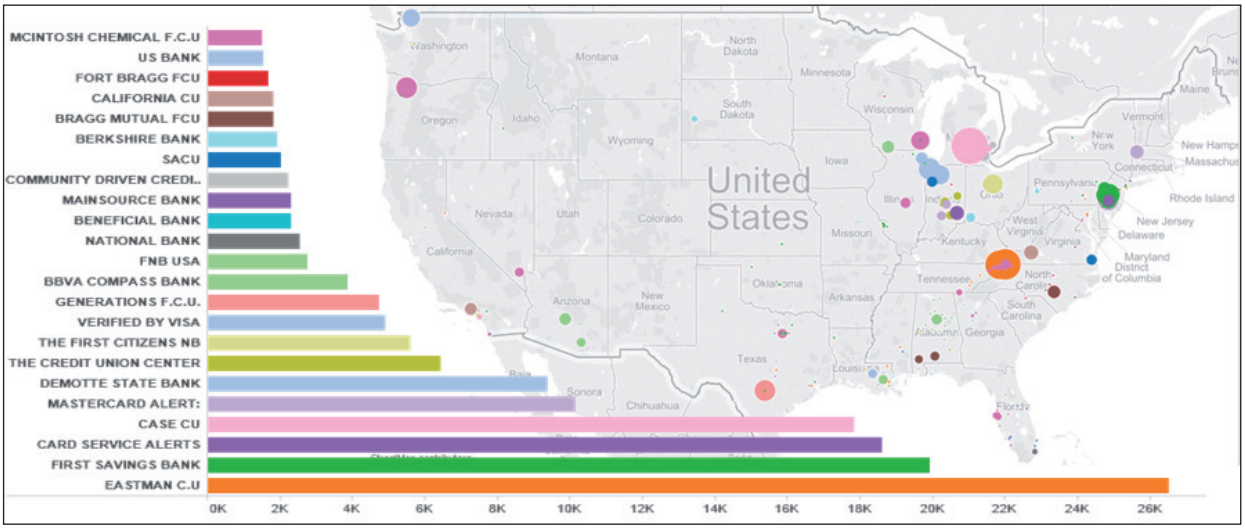

Figure 10: Types of banks and financial institutions being targeted in 2013.

The word clouds shown in Figures 11 and 12 visualize the most popular words which were used by the attackers in 2013 and in more recent attacks. In general, the two clouds are somewhat similar but there are some differences. The main and the most important difference is that the length of the most common words seems to have become smaller. The reason is that the more recent period of this type of scam can be characterized as the period when the attackers are trying to shorten the length of words used in an attempt to avoid defences and are using special symbols or punctuation marks in order to avoid filters rather than, for example, replacing the letter 'i' with 'l', as occurred in the past. In the later period, there is also a greater variety of words.

We can actually see this change if we plot the average length of words per time period (see Figures 13 and 14), which shows that the length of words is now shorter than it was in the past. One major reason for this is due to much less use of the word 'deactivated' and its variants.

Finally, if we look at days of operation (see Figures 15 and 16), we can see some significant changes. In 2013, the greatest number of attacks took place on working days, but in 2014/2015 the attackers decided to switch to send much more

Figure 11: Most popular words used by the attackers from April to May 2013.

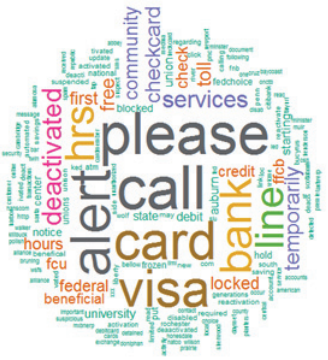

Figure 12: Most popular words used by the attackers from October 2014 to January 2015.

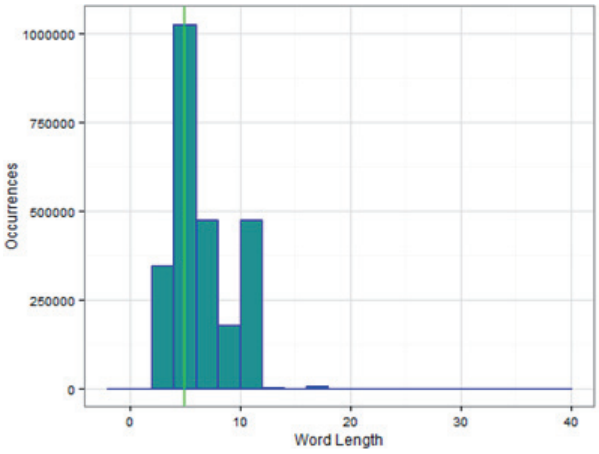

Figure 13: Average length of words April to May 2013.

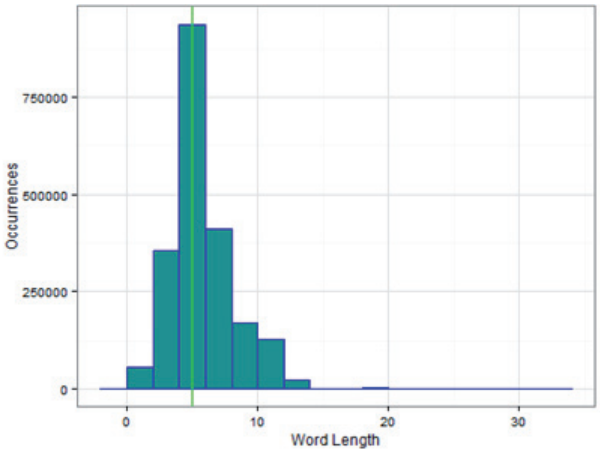

Figure 14: Average length of words October 2014 to January 2015.

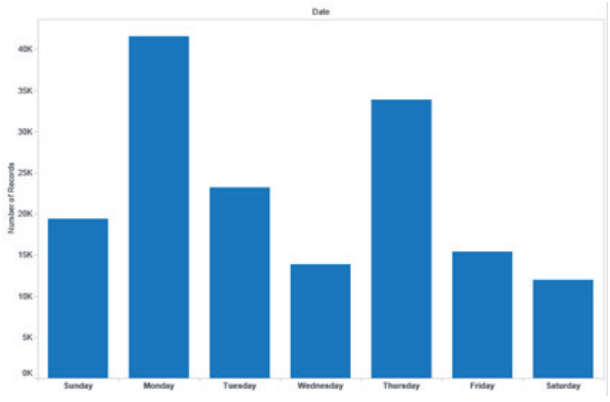

Figure 15: Days of operation April to May 2013.

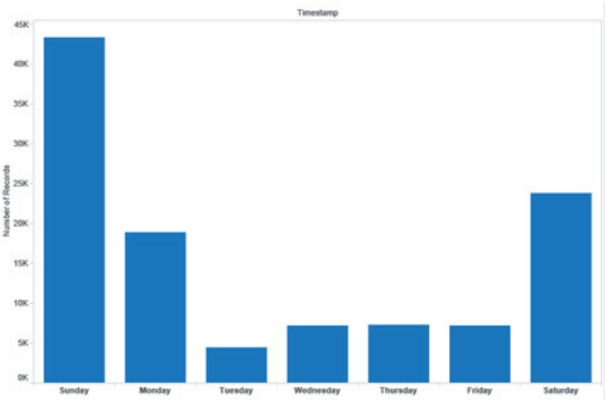

Figure 16: Days of operation October 2014 to January 2015.

over weekends. There are various potential reasons for this, whether to increase the conversion rate, or to avoid defences. On the conversion rate side, one reason may be that smaller banks are more likely to be closed at the weekend and thus less likely to respond with warnings to their customers to ignore these phishing attacks. Another reason is that people may feel that a text message pointing to an automated system over a weekend is more 'normal'.

One change that is not evident overall is whether the group intends to stop. While there has been a small decline between the two periods, it has been less than the general drop that the rest of North America has experienced [12].

CONCLUSION

Within North America, mobile messaging attacks are declining as operators introduce new and better forms of in-network filtering. The overall attack volumes are dropping due to faster/quicker detection techniques. However, some other criminals groups have moved on or stopped completely – making these bank phishing messages a notably persistent type.

This persistence translates into more complexity, with the average word size decreasing and sending patterns changing. It is clear now that this criminal group will always remain present while favourable economics are in place: i.e. if the cost to defeat defences is less than the number of victims multiplied by the amount stolen from each victim.

In general, the recommendations for consumers and the industry are:

- If you're just an average phone user, ignore the messages – a bank will never contact you like this; report the messages to banks and carriers.
- If you represent a mobile operator, these messages can and should be blocked to protect your customers; put protection in place.
- If you represent a bank, monitor and get intelligence so you can know if an attack happens; raise alerts and spread the word to your customers when it does.

Even though there have been important successes in the battle against mobile messaging abuse, there are no signs at the moment that these attackers are going to completely stop their activities. However, the industry is constantly progressing, and given the successes against other groups, and with greater intelligence then it is conceivable that this group may be significantly disrupted. In the past, very few of these attacks would have been blocked, whereas now we are in a position to force evolution due to attacks being blocked. This forced evolution, and the change in attacks being sent over email or voice, is a sure sign that the problem is being tackled and progress is being made. What remains in the interim is for mobile phone users to continue to be wary if they receive these messages, and for the industry to pool intelligence and co-operation in dealing with these criminals.

REFERENCES

[1] Kumparak, G. The Day SMS Began To Die. Techcrunch. October 2011. http://techcrunch.com/2011/10/12/ding-dong-the-witch-is-dead/.

[2] The SMS is Dying a Slow and Lingering Death. siliconANGLE. http://siliconangle.com/blog/2013/04/29/the-sms-is-dying-a-slow-and-lingering-death/.

[3] Spence, E. Where Will All The SMS Messages Go When Texting Dies? Forbes. http://www.forbes.com/sites/ewanspence/2014/01/14/where-will-all-the-sms-messages-go-when-texting-dies/.

[4] Evans, B. WhatsApp sails past SMS, but where does messaging go next? http://ben-evans.com/benedictevans/2015/1/11/whatsapp-sails-past-sms-but-where-does-messaging-go-next.

[5] McGloin, S. Attacking the CASL. AdaptiveMobile. http://www.adaptivemobile.com/blog/attacking-the-casl.

[6] McDaid, C. Big Spam Hunting. AdaptiveMobile. http://www.adaptivemobile.com/blog/big-spam-hunting.

[7] Mendes, C. Spammers' SMS Boom Focused on the Indian Real Estate Syndrome. AdaptiveMobile. http://www.adaptivemobile.com/blog/spammers_sms_boom_focused_on_the_indian_real_estate_syndrome.

[8] Bank Scam Audio Recording. https://www.youtube.com/watch?v=jeNk9O3Nz00.

[9] https://twitter.com/DanversPolice/status/541957769344331776.

[10] https://twitter.com/BBB_CVA/status/566334669030178817.

[11] Krebs, B. Hacked Hotel Phones Fueled Bank Phishing Scams. Krebs On Security. http://krebsonsecurity.com/2015/02/hacked-hotel-phones-fueled-bank-phishing-scams/.

[12] McDaid, C. Big Spam Hunting. AdaptiveMobile. http://www.adaptivemobile.com/blog/big-spam-hunting.