HIDING IN PLAIN SIGHT - THE GROWTH OF CYBERCRIME IN SOCIAL MEDIA
PART 2
# TABLE OF CONTENTS

Executive Summary ............................................................................................................... 1  
The Social Media Revolution and Its Impact on the Fraud World ................................. 2  
Geographic Distribution of Social Media Platforms ...................................................... 4  
A Short Primer of Fraud Terms .......................................................................................... 5  
Cybercrime On Social Media In Russia ........................................................................... 7  
   VKontakte – Leading Platform for Russian Speakers ................................................. 9  
   Odnoklassniki – Classmates Behind the Iron Curtain .......................................... 12  
Cybercrime On Social Media In China ............................................................................. 13  
   QQ (China) – Beyond the Great Firewall of China .............................................. 15  
   Baidu Tieba – A Chinese Paste Bar ....................................................................... 19  
Conclusion ........................................................................................................................ 23  
Attack Map – Who Targets Whom? .............................................................................. 23  
Additional Notes ............................................................................................................. 24  
About FraudAction ......................................................................................................... 24  
About RSA ...................................................................................................................... 25
EXECUTIVE SUMMARY

The use of social media as a cybercrime attack vector is hardly a new concept. For years, fraudsters have used social platforms to target users with phishing attacks, distribute malware, and conduct data mining of intended victims in an attempt to gather personal information.

What has changed, however, is the growing use of social media as a communications channel for fraudsters. Once thought to operate mainly in the deep web behind the mask of anonymous browsers such as Tor, cybercrime forums have rapidly emerged onto social media, and illicit activity is happening in plain sight.

In recent years, the RSA FraudAction™ Intelligence team has observed an exponential growth in the volume and visibility of fraud activities on social networking platforms and embarked on a six month study of the phenomenon, the findings of which are presented in this report. The RSA FraudAction Intelligence team is a full-time research and analysis group that is designed to continuously monitor the Dark Web, the fraud underground, as well as the open web (OSINT) for cybercrime activity.

The goal of the study was to research the structure, format, and entry requirements for joining global cybercrime groups across the most popular social media platforms. We investigated how each platform operates, what restrictions or advantages it offers, and analyzed the statistics of how many special interest groups are out there, and how many members they have.

This report is Part 2 in a series and presents the results of our research into the phenomenon of cybercrime across Chinese and Russian speaking social media platforms. We uncovered and studied hundreds of groups across multiple geographic regions, delving into a number of social networking platforms that are host to extensive fraud activities.

Some of the key findings of this research series are highlighted below:

• More than 500 fraud-dedicated social media groups around the world, with an estimated total of more than
• Most of the fraud-dedicated groups are very public – visible and open to all.
• The types of information openly shared in social media include live compromised financial information such as credit card numbers with PII and authorization codes, cybercrime tutorials, and commercial offerings such as malware and malware tools.
• The worldwide predominance of fraud groups on Facebook is surprisingly rivaled by other language and community specific platforms such as QQ (China) and VKontakte (Russian speaking).
• Fraud groups in some countries focus most fraudulent attacks at the regional level by attacking local retail businesses, banks, and consumer accounts.
• During the period of this study, we detected more than 15,000 compromised credit cards (called ‘CVV2 freebies’ in fraudster lingo) publicized on social media networks.

RSA has made reasonable attempts to contact the respective legitimate parties mentioned in this report prior to publication. RSA has notified and provided this report to the appropriate law enforcement agencies.

The first report in this series can be found here.

THE SOCIAL MEDIA REVOLUTION AND ITS IMPACT ON THE FRAUD WORLD

Every local underground scene has its unique characteristics and intricacies that are usually dictated by the local environment, the majority of fraud markets have more attributes in common than those that set them apart.

In our view, it is important to examine fraud markets and the actors that operate within them not only as mere statistics, but as living, breathing, and thinking human beings. As individual persons, they are directly influenced by the structure of the environment they live in. The collection of customs, traditions, norms, and ideologies, together with material and economic factors, will act on and influence the majority of individuals in a society. By the same token that the framework influences individual human behavior, those individuals are also capable of changing the social structure they inhabit.

When we look at fraudsters as a social system on a large scale, it is easy to identify their actions or movements en masse; the vast majority of fraudsters simply follow the leader, favoring the ‘tried and true’ methods of both communication and fraud. If one thing is certain about fraudsters, it is that just like water flowing down a mountain, most fraudsters will follow the path of least resistance.

When we say that the fraudster’s behavior is influenced by the structure, we are no longer referring to the fraudster persona and the human being separately. Within each fraudster, the fraud and non-fraud personas co-exist in the same psyche and have a mutual influence on each other.

The introduction of social media and its growth in popularity has drastically changed the way the world communicates. The primary goal of social media is to create communities, and by promoting the exchange of information, encourages contribution to the community by its members. Most social media also suggests new connections with other members of similar interests (social networking), and in this way, communities are created and can grow very rapidly.

All of these basic properties, when combined with a loose policy for verifying the real identity of a user, provide a fertile new ground for fraudsters to sow. Fraud posts began showing up in social media as early as 2011, when
stolen credit cards and e-commerce accounts started being publicized openly on social media platforms. Suddenly, fraudsters were no longer hiding in exclusive underground forums or in the Dark Web.

These new forms of communication provided them with a free turnkey solution that everyone was familiar with, included integrated and free web hosting, multi-language support, a global audience, and a whole range of additional benefits. For a long time, this fraud activity remained largely unnoticed, to the point that some seminal fraud posts can still be found online to this day.

How or why did this activity remain under the radar? Since the primary goal of social media is to create communities, it does so by offering a user suggestions based on the user’s behavior history – a history of their previously expressed preferences, interests, and connections. These suggestions are only seen by the individual user, and not by anyone else. As a result, each user can only see their own personal circle or extended network, but are completely blind to the networks of others that they are not connected with, or to content they have not expressed interest in. This creates large clusters of communities that are only interconnected by a node of individual members that they have in common, but the communities may remain completely detached or unaware of each other’s existence. Put more simply, as a user, one cannot know something exists unless one searches for it or accidentally sees it mentioned on someone else’s page.

Social media as a primary form of communication continued to grow exponentially.

New platforms with varied formats emerged, as platforms that pioneered the revolution kept on growing bigger and bigger. In a large social system where a few individuals manage to influence the structure, the structure in turn influenced a majority of the individuals that composed it. Converging on the same psyche, the non-fraud persona saw its way of communicating socially revolutionized, and thus influenced its other half – the fraud persona.

Initially nesting in the hidden cracks and corners of social media, the level of fraud activity rapidly rose to flood the network with fraud offerings. A vast majority of fraudsters now operate largely in the open. Many of them even use their own personal profiles. There is a parallel world of fraud that hides in plain sight, existing side by side with the rest of us.

As we start reading between the lines, the collateral information that is shared in these social media platforms allows us to look beyond the raw numbers and observe fraudsters within the context of the larger social systems they live in.
GEOGRAPHIC DISTRIBUTION OF SOCIAL MEDIA PLATFORMS

According to Facebook, they had 1.6 billion monthly active users as of January 2016. Facebook is by far the largest social networking platform and the most popular in approximately 75% of the regions in the world. However, there are notable exceptions to the worldwide preference for Facebook in Russia, China, and Japan. The illustration below shows the worldwide distribution of the dominant social networks.

A further breakdown of fraud groups found by language preferences and region is discussed and analyzed in detail in this report series.

Figure 1: Global distribution map of social networking platforms

![Global distribution map of social networking platforms](https://www.statista.com)
A SHORT PRIMER OF FRAUD TERMS

In order to follow the activities of fraudsters, we need to familiarize ourselves with some of their jargon. The following are some of the most popular activities in the fraud landscape, and the current terms used both by fraudsters and the info-sec community.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC</td>
<td>Credit Card</td>
</tr>
<tr>
<td>CC Shop</td>
<td>Online fraud vendor that sells stolen CC data, cards, related tools, services, and information.</td>
</tr>
<tr>
<td>CC Checker</td>
<td>An application or a website that offers a service that checks if credit card data is still active or valid.</td>
</tr>
<tr>
<td>Carding</td>
<td>The act of purchasing merchandise with stolen credit cards or credit card data.</td>
</tr>
<tr>
<td>Cashout</td>
<td>The act of monetizing the funds, credit, services, or goods that were obtained in fraud activities.</td>
</tr>
<tr>
<td>Drop</td>
<td>A bank account controlled by a fraudster that is used to receive funds from fraud transactions. A physical address / location where merchandise can be sent to be picked up by the fraudster or their collaborators.</td>
</tr>
<tr>
<td>PII</td>
<td>Personal identification information – any and all information that can be used in identifying an individual for authorization of accounts and transactions.</td>
</tr>
<tr>
<td>Fullz/CVV2</td>
<td>A full set of stolen credit card data, including the card owner’s PII. Commonly obtained via Phishing or Trojan attacks, and used in online or ecommerce transactions.</td>
</tr>
<tr>
<td>Dumps/dumpz</td>
<td>Magnetic stripe data that can be used to clone a physical credit card using an MSR device and plastic credit card blanks.</td>
</tr>
<tr>
<td>Skimming</td>
<td>The act of copying the magnetic stripe data of a credit card, debit card, or ATM card, for later use in cloning such a card. The main source for Dumps.</td>
</tr>
<tr>
<td>Logins</td>
<td>Login information to compromised customer accounts.</td>
</tr>
<tr>
<td>Ripper</td>
<td>A fraudster who “rips off” other fraudsters by promising to provide goods or services, accepting payment, and disappearing without delivering the goods.</td>
</tr>
<tr>
<td>Freebies</td>
<td>Compromised PII, logins, and CC data that are publicized for free. Used to attract customers for a service or merchandise that a fraudster is selling - a „try before you buy“ sample. Also used by fraudsters who wish to brag.</td>
</tr>
<tr>
<td>Show-off</td>
<td>Publicizing a successful fraud transaction to demonstrate a fraudster’s ability, skill, or simply to boost their ego. Commonly includes images of the merchandise that was carded or stolen, or images of the transaction approval or confirmation.</td>
</tr>
</tbody>
</table>
The bar graph below represents the most popular fraud topics found in the study according to their appearance as keywords in the group names and/or searches for items posted in those groups. Activity related to carding, cashout, and the sale of stolen credentials is the predominant topics discussed within the groups, accounting for nearly 90% of activity.

- **53% Carding/carding services**
- **16% Account takeover**
- **9% Wire transfer**
- **8% Malware and hacking tools**
- **7% Cashout and muling services**
- **3% Phishing/Spam/Botnet services**
- **2% DDoS attacks**
- **2% Mobile**
CYBERCRIME ON SOCIAL MEDIA IN RUSSIA

Fraud-dedicated groups on social media in Russia operate primarily on two platforms: VKontakte (VK) and Odnoklassniki (OK). RSA’s analysts discovered approximately 60,000 members listed in the fraud-dedicated groups across these two platforms.

One of the most common activities in the Russian speaking groups is sharing of information on how to carry out fraud including tutorials, proven methods for sale, Fraud-as-a-service offerings, as well as general discussions on new and novel methods.

Contrary to what we observed in previous years, Russian fraudsters no longer appear to be cautious about attacking local retail businesses, banks, and ATMs. As illustrated in the image below, much of the fraud activity in this region is focused on cashout methods and services, carding methods, fund transfers, e-wallets and online exchange services, account takeover, selling compromised account logins, and shell corporations often used in money laundering.

Figure 2: The most popular activities mentioned in fraud-dedicated groups in Russian social media
Figure 3: Distribution of members in the Russian fraud groups on the VK social platform

The graph above is a cloud or clustering representation of the affiliations between unique group identities (members) and the fraud-dedicated groups to which they belong. Where a single region is described, the different clouds represent different fraud activities or special interest communities. Where we describe more than a single region, the clouds represent the geographic communities of fraudsters.

Connections between individual members are indicated by lines that take on the specific color of the main group or community where the individual originates. Though the groups at the edges of this graph have the largest volume of members, it is the smaller groups in the center that are of more interest as they have the most active members.

The clouds that appear to be distinctly separate from the rest, and have fewer connections to other clouds, indicate that the majority of fraudsters in that cloud are affiliated to one or two groups at most. In the Russian-speaking fraud groups across social media, this could indicate the widespread use of fake profiles where each fraudster maintains more than one profile to avoid detection. This would be consistent with the sophisticated OPSEC for which Russian fraudsters are known.
VKONTAKTE – LEADING PLATFORM FOR RUSSIAN SPEAKERS

VKontakte (VK.com), boasting an estimated **350 million** registered users, is the most popular social network in Russia (and the second largest social network in Europe) and the second most visited web portal in the Russian speaking regions – second only to Yandex. VK, which literally means “in touch”, is fashioned much like Facebook (using the same theme colors and a very similar graphic layout) – including news feeds, ‘walls,’ ‘likes,’ and private chats. Like Facebook, VK is also organized by profiles, groups, and pages. In VK, groups are referred to as communities and divided into open group, closed group, page, and event. Access to all Russian social networks requires providing a valid phone number upon registration.

Most of the groups seen on VK are open, and although they don’t reach the membership count that similar Facebook groups might have, they allow all visitors to post on the group wall or leave comments, even when they are not registered members. However, in closed groups, the content can only be seen by approved members (including posting or commenting). There are also secret groups where a new user must be invited by a member or administrator in the secret group.

Many personal profiles of fraudsters on VK provide clues to their nature right within their names, and it is apparent that they are fraud-related; examples include *obnal = cashout or zaliv = transfer*. The profiles are used most of the time as a way to connect fraudster to their peers or advertise their services. One can also find fraud-related discussions in personal profiles (postings on their profile ‘wall’).

The VK admin is well aware of the different types of fraud in its community and tries to fight the phenomenon by shutting down pages, groups, and profiles. However, many fraudsters continue to use fraud-related terms like *cashout, carding, and selling CCs* in naming their groups and profiles (although some fraudsters may use English characters to write Russian words and vice versa, or special characters mixed with letters to try and evade automated detection engines).
Figure 4: Example of a card drop group on VK

Figure 5: “Dump and PIN” group
**Figure 6:** VK notification of a fraud group that was blocked due to involvement in credit card fraud

**Figure 7:** Open group in VK that offers carding and "obnal" (or cashout)
Odnoklassniki (OK) is the second most popular social network in Russia speaking communities, claiming more than 200 million registered users and 45 million daily unique visitors. This social network is a part of the Mail.ru web email portal.

Members have profile pages where they share photos, videos, thoughts, and other types of information. OK also has sections for groups, videos, games, music, photos and more. Members can be ‘friends’ with each other, as well as carry out private chats.

![Fraud group in Odnoklassniki](image)

**Figure 8: Fraud group in Odnoklassniki**
CYPHERCRIME ON SOCIAL MEDIA IN CHINA

Fraud-dedicated groups on social media in China operate primarily on the two most popular web platforms - QQ and Baidu Tieba. This can partly be explained by the isolation due to censorship, blocked web portals and services restricted by the government that prevents the population in China from accessing many websites and services in the Western world.

Figure 9: The most popular activities mentioned in fraud-dedicated groups in Chinese speaking social communities

While cashout methods are a popular topic, members within Chinese-speaking fraud communities are actively interested in hacking tools and methods, as well as computer and video games and gaming activities, credits and licensing.

In most fraud posts across the various platforms in China, including underground forums, open web forums, or social networks like Baidu Tieba, fraudsters use their QQ number for identifying themselves when making direct contact.

The fraudsters use the main chat feature of the group to advertise using bots. Sometimes, there are questions in a group which are often found in traditional Dark Web markets. Many advertisements offer images to show proof of ability. Examples include pictures of card skimmers and screenshots of carding.

Group members can also upload files to share with the group such as tutorial videos or malware APKs (Android apps). Files and media are uploaded as messages in the main chat, but are also displayed as a list of all uploaded files in a separate tab. Fraud-as-a-service vendors often upload password protected files such as “EMV function plus.zip”, and then sell the password to interested customers.
Groups dedicated to the trading of hacking software. Its members are largely unrelated to other groups.

Groups dedicated to cashout, with members in orange dedicated to credit card and wire transfer fraud.

One of many smaller, more dedicated fraud communities. Members in this group are focused on phishing-related activity.

Groups dedicated to malware, with members in pink focused on mobile malware and those in blue dedicated to PC malware.

**Figure 10: Distribution of members across fraud groups in China based on types of fraud activity**

While fraudsters from other regions organize themselves by language or location, most Chinese-speaking groups are organized by type of activity, and this is reflected in the network graph above.

As usual, groups with larger member bases are the ones where CVV2 ‘freebies’ are shared. Represented in red, violet, and grey, they tend to stay in the center of the graph, as they also have many members in common. Activities such as carding, bank and e-wallet logins trading, and ATM skimming software trading are also seen in these groups.
QQ (CHINA) – BEYOND THE GREAT FIREWALL OF CHINA

Tencent QQ (QQ.com, QZone.QQ.com) is the top IM chat platform in China. It can be accessed through a proprietary computer application or the QQ mobile app, as well as via the QQ website. QQ.com is a web portal that offers many services, including the social media website Qzone, micro blogging, online gaming, a news portal, and more. It is also available in an international version (English). QQ claimed 829 million users as of January 2015.

In our study of QQ, RSA fraud analysts studied 25 out of 276 fraud-dedicated groups identified on the platform. The top ten groups contained an average of 2,000 members each, with many of those individuals serving as members in more than one group.

Qzone functions as a social network much like Facebook. Users can create groups for discussion on any topic. Each user and group is identified by a QQ number.

Fraud activities in QQ are organized in groups, and each QQ group is divided into two sections:
- Main chat
- Media upload section (files of any extension, videos, images, archives, etc.)

Users can also access groups via the Qzone website (Qzone.QQ.com), where they can view group information as well as file and media uploads. There is also a posting section for each group (functions like a message board, this feature is NOT available in the proprietary QQ program) where group members can publish posts, and other members can comment and ‘like.’ Note that the main chat of a group is NOT available through Qzone.

There are public groups and closed groups. Users can access public groups without requesting to join, but are not allowed to comment unless they are registered and accepted into a group. Joining a group is by request only and requires approval by the group admin. Some groups require users to provide additional information, or reasons for wanting to join.

Groups can be searched by keywords or by a QQ number, and can be sorted according to activity or by the total number of members. The fraud group names are most often indicative of their activity or offerings so they can be searched using the relevant keywords. Some groups are specific to certain people, and users are unable to request to join, but may find them in search results.
The number of members in a group is limited by quotas. Once a group reaches 75% of its limit, the group admins can request an upgrade to the next quota level. When a group reaches the quota, you receive a message that no one can join. A QQ fraud group typically contains 500 members or more.

Groups in QQ use either the Chinese equivalents of the terms (Chinese names for the well-known American retail and financial entities or for fraud terms like dumps, credit cards, etc.) or they may use proper English words.

The QQ portal attempts to block certain fraud keywords from being searched. To counter the blocking efforts, fraudsters substitute Chinese characters that resemble the fraud terms. Fraudsters on QQ generally post ‘CC freebies’ as images instead of plain text, and this helps to evade automated security searches and blocking by the portal.

Often, a fraud group profile picture provides more real information about the group than the actual name or the descriptive text. The name may appear to be innocent, but the image conveys what fraud activity or offering is inside. For example, a group named “chanting flowers” uses the real Chinese word for “cashout” as its group profile image. Many of the fraud groups on QQ also contain contact information in the profile image to let users know how they can be contacted to join or to be approved.

The table below shows examples of word or character substitutions that are used in group names on QQ:

<table>
<thead>
<tr>
<th>PHRASE</th>
<th>FRAUD GROUP PICTOGRAM</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>nèi liào - domestic stuff</td>
<td>内料</td>
<td>Chinese banks, CVV or dumps</td>
</tr>
<tr>
<td>wài liào - foreign stuff</td>
<td>外料</td>
<td>foreign banks, CVV or dumps</td>
</tr>
<tr>
<td>tàoxiàn - cashout</td>
<td>套现</td>
<td>monetizing, cash out</td>
</tr>
<tr>
<td>yínháng kǎ - debit card</td>
<td>银行卡</td>
<td>debit card</td>
</tr>
<tr>
<td>dúpīn - drugs</td>
<td>毒品</td>
<td>drugs</td>
</tr>
<tr>
<td>huābei - chanting flowers</td>
<td>花呗</td>
<td>cash out</td>
</tr>
</tbody>
</table>
Figure 11: Cloned bank credit card

Figure 12: Offering skimming and carding supplies and services
Figure 13: Yileyoo control panel

Figure 14: Preview of a credit card shop used to attract buyers
BAIDU TIEBA – A CHINESE PASTE BAR

Baidu Tieba (tieba.baidu.com) whose literal meaning is “Baidu paste bar,” is China’s largest online community, hosted by the largest Chinese search engine and web portal in the world - Baidu (Baidu.com). It functions as a social network and a platform for forums. Forums (referred to as “bars”) are automatically generated by the user whenever there is a keyword search for a forum name that does not yet exist. Users can post messages, files, pictures, and videos as in any standard online forum. As of 2014, there were more than eight million bars or forums on Baidu.

Fraud communications in Baidu Tieba are found in the form of fraud posts and advertisements in Tieba forums with fraud-related names or legitimate names that can be interpreted as being fraud-related keywords. Examples include bank, “mastercard,” cashout, cloning and skimmers.

In our study of Baidu Tieba, our team identified and analyzed 14 fraud-dedicated groups. The top three groups had a membership count of over 26,000 members.
The Chinese fraudsters post offerings for sale, or notices seeking collaborators or advice, and provide their contact details (a QQ number in most cases) or request that their peers leave contact information in the comments. Much like other social networks, Tieba includes a feature that offers links with automatic suggestions for related forums.

The Baidu portal fights fraud groups by temporarily blocking forums that are used primarily for fraud. For example, a “mastercard” forum and “debit card” forum were blocked due to legal considerations. They also delete some fraud posts from forums, but are frequently only caught after a number of days that the posts are up.

To counter the portal’s security measures, fraudsters in Tieba often replace some of the Chinese characters in fraud terms to Pinyin, so that they cannot be detected by automatic monitoring. Another evasion technique is to omit a character in 2-character-long fraud words. A few examples of the modified words or pictograms are presented below.

<table>
<thead>
<tr>
<th>ORIGINAL PICTOGRAM</th>
<th>FRAUD GROUP PICTOGRAM</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>国内料 - guónèi liào</td>
<td>内 - nèi</td>
<td>domestic stuff</td>
</tr>
<tr>
<td>出售 - chūshòu</td>
<td>出 - chū</td>
<td>selling</td>
</tr>
<tr>
<td>复制 - fùzhì</td>
<td>复 - fù</td>
<td>cloning</td>
</tr>
<tr>
<td>支付宝 - zhīfùbǎo</td>
<td>支付 - bao</td>
<td>alipay</td>
</tr>
</tbody>
</table>

Figure 16: “ID + Name + Card Number, so you can withdraw money!!!”
Figure 17: Bank ATM skimmer copying device collecting POS data

Figure 18: An advertisement seeking accomplices for bank transfers; shown is a sample transfer receipt for 79800 CNY, or about 12,000 USD
Figure 19: “Fresh 101” – Advertising stolen credit card data with service code 101. Can be used internationally, and does not require a PIN. Offering a wide range of CC data from all over the world.
CONCLUSION
So where is the mention of fraudsters operating on social media in the United States and Europe? Although fraud activity is prominent, fraudsters who operate within these regions prefer to stay hidden in the underground and are not found on social media.

One of the most prominent takeaways is when cybercrime on social media is viewed on a global map between the targeted countries and their attackers. While some fraud groups mainly operate and target victims in the regions they are located, the majority of attacks still target the U.S. and UK regions.

The image below illustrates the relationships between fraud communities and their intended targets.

Figure 20: Collaborative links between fraudsters in different regions of the world

Interestingly, many fraud communities tend to target victims within their own countries. The map below shows the top countries where fraudsters prefer to commit fraud at the regional level by attacking local retail businesses, banks, and consumer accounts.

Figure 21: Countries with fraud groups who mostly target victims within their own region
In recent years, international cooperation among law enforcement agencies in the United States and Europe has yielded many high-profile and much publicized cybercrime gang busts and apprehensions. Prosecution has been aggressive, carrying heavy penalties and jail sentences in many cases. The research presented in this report might cause those who have questioned the value of intelligence sharing and impact of cybercriminal prosecution to reconsider. The overall lack of fraud groups in the U.S. and many parts of Europe is a clear indication that fraudsters are on alert and intelligence sharing and prosecution is working.

**ADDITIONAL NOTES**

- RSA researchers utilized network visualization software to help gain a better understanding of the network structures and inter-relationships between the social media groups and the fraud group members in this study.
- The graphic representations helped us demonstrate the relative sizes of the groups, as well as the key connections and overlapping memberships between groups.
- To make the relational network graphs more readable, some of the less relevant elements in each graph have been filtered out.

**ABOUT FRAUDACTION**

RSA FraudAction is a managed threat intelligence service which provides global organizations with 24x7 protection and shutdown against phishing, malware, rogue mobile apps and other cyber attacks that impact their business. Supported by 150 analysts in RSA’s Anti-Fraud Command Center, the RSA FraudAction service analyzes millions of potential threats every day and has enabled the shutdown of more than one million cyber attacks. For more information, contact FAS.Inquiries@RSA.com.

**CONTENT AND LIABILITY DISCLAIMER**

This Research Paper is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. EMC has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. EMC shall not be responsible for any errors or omissions contained on this Research Paper, and reserves the right to make changes anytime without notice. Mention of non-EMC products or services is provided for informational purposes only and constitutes neither an endorsement nor a recommendation by EMC. All EMC and third-party information provided in this Research Paper is provided on an “as is” basis.
EMC DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, WITH REGARD TO ANY INFORMATION (INCLUDING ANY SOFTWARE, PRODUCTS, OR SERVICES) PROVIDED IN THIS RESEARCH PAPER, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

In no event shall EMC be liable for any damages whatsoever, and in particular EMC shall not be liable for direct, special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue or loss of use, cost of replacement goods, loss or damage to data arising out of the use or inability to use any EMC website, any EMC product or service. This includes damages arising from use of or in reliance on the documents or information present on this Research Paper, even if EMC has been advised of the possibility of such damages.

ABOUT RSA
RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud and cybercrime.
For more information, go to rsa.com.