HIDING IN PLAIN SIGHT -
THE GROWTH OF
CYBERCRIME IN SOCIAL MEDIA
PART 1
## 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 Tutorial on Fraudster Terms ........................................................................................... 5
- Overview of Fraud Activity on Facebook ........................................................................ 6
  - Global View ..................................................................................................................... 8
  - Brazil .................................................................................................................................. 9
  - India and Southeast Asia ............................................................................................. 13
  - Latin America ............................................................................................................... 16
  - West Africa - Ghana and Nigeria ............................................................................. 18
  - France and Other French Speaking Regions .......................................................... 21
- WhatsApp .............................................................................................................................. 23
- Conclusion ............................................................................................................................. 26
- Additional Notes .................................................................................................................. 27
- About RSA .............................................................................................................................. 28
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 1 in a series and presents the results of our research into the phenomenon of cybercrime in social media. 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 220,000 members were investigated for this report. More than 60%, or approximately 133,000 members, were found on Facebook alone.¹
- 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 predominance of Facebook is surprisingly rivaled by other language and community specific platforms.

• WhatsApp appears to be the newest fraud communication channel. Twitter, despite its worldwide popularity and proliferation, is not preferred as a fraud communication channel.

• 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 fully disclosed all information contained in this report to Facebook prior to publication. We would like to recognize Facebook for working with our team to quickly remove the information and responsible parties from their platform. RSA has also notified and provided full access to the data contained within this report to the appropriate law enforcement agencies.

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

While the most active and experienced fraudsters take measures to avoid being identified, a surprising number of actors seem to use their own personal accounts.
numbers and observe fraudsters within the context of the larger social systems they live in.

GEOGRAPHIC DISTRIBUTION OF SOCIAL MEDIA PLATFORMS
As of January 1, 2016, Facebook had 1.6 billion monthly active users. 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
# A Tutorial on Fraudster Terms

In order to follow the activity of fraudsters, it is important to understand their common 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 credit 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 fraudulent transactions or money transfers. 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 e-commerce 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 &quot;rips off&quot; 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.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>53% Carding/carding services</td>
<td></td>
</tr>
<tr>
<td>16% Account takeover</td>
<td></td>
</tr>
<tr>
<td>9% Wire transfer</td>
<td></td>
</tr>
<tr>
<td>8% Malware and hacking tools</td>
<td></td>
</tr>
<tr>
<td>7% Cashout and muling services</td>
<td></td>
</tr>
<tr>
<td>3% Phishing/Spam/Botnet services</td>
<td></td>
</tr>
<tr>
<td>2% DDoS attacks</td>
<td></td>
</tr>
<tr>
<td>2% Mobile</td>
<td></td>
</tr>
</tbody>
</table>

**OVERVIEW OF FRAUD ACTIVITY ON FACEBOOK**

On Facebook, users can create personal ‘profiles’, and gather a list of ‘friends’. They communicate by posting ‘status updates’ on their ‘wall’ (front page of a profile) that may include images, video clips, and links to other content. Another way of communicating is by ‘liking’ and ‘sharing’ a friend’s post or status update, and receive notifications for any updates in a friend’s status or in special interest topics or ‘groups’.

Facebook users can exchange private messages via an integrated instant message application (IM). Users can also create or join interest ‘groups’. Access to a ‘group’ can be set as Public (open to all), Closed (join by request), or Secret (unlisted and invisible to non-members).

Due to the enormous popularity and diverse user base, fraud activity on Facebook thrives in all shapes, forms, and languages. Access to data on Facebook becomes readily available to any user, with just a keyword search and/or a few mouse clicks. Once a person joins one fraud-dedicated group, the
Facebook search algorithm suggests similar groups to join, making it even easier to expand one’s reach and connections in this new worldwide fraud network.

While one would assume that fraud dedicated groups might logically set their privacy settings to “secret” in an attempt to operate stealthily, we found that most groups operate under public or closed setting. Even in the closed groups, a simple join request is all that is required to gain access, without the vouching process or references typically needed to join a fraud forum in the deep web. Facebook launched a new group management app in Q3 2015, and as of February 2016, reached a landmark volume of 1 billion app users³.

Figure 2: A sample of “Suggested Groups” that appear in Facebook once a user expresses a specific interest in carding

While the most active and experienced fraudsters take measures to avoid being identified (for example, using fake or stolen profiles), a surprising number appear to use their own personal accounts. In many cases, these profiles include real names, personal photos, and additional identifying indicators that could help expose them. There is even a sense one gets of impunity, of being too far out of the reach of the long arm of the law.

GLOBAL VIEW

In the course of this investigation, it appears that fraudsters on Facebook predominately come from regions of the globe where a high volume of transnational organized crime and corruption is often reported. Therefore, it is not surprising to see openly marketed offerings such as counterfeit currency and drug trafficking, that are much more serious than those directly related to cyber-fraud.

On a global level, carding stands out as the most popular fraud activity on Facebook. This includes buying and selling stolen credit cards (‘CVV2’ is far more popular than ‘dumps’), carding as a service, buying and selling carded items, carding tutorials as a service, buying/selling/exchanging carding methods, or the usual carding bragging and sharing live CVV2 data as ‘freebies’.

Figure 3: Malware tools and botnets openly publicized on Facebook
Brazil is the largest South American economy and ranks second worldwide in online banking fraud and financial malware. It is therefore no surprise to find that Brazilian fraudsters have a very formidable presence in Facebook groups.

The most common activities on Facebook among fraud groups operating in Brazil include:

- ‘Carding-as-a-Service’
- CVV2/Fullz for sale
- Counterfeit currency
- Account takeover – compromised online consumer accounts and bank accounts
- Sale of mobile phone ‘top-up’ (prepaid air time recharge)
- Fake/forged document scans

In Brazil, the RSA FraudAction Intelligence team analyzed 24 out of 120 fraud-dedicated groups identified on Facebook, with approximately 24,300 unique members. The top four groups contained over 17,000, or about 70%, of all members.
The activities detected from Brazilian fraudsters on Facebook mirror that of the underground in the fact that they are self-contained regionally - Brazilian fraudsters target Brazilian businesses and consumers.

The Brazilian fraud community has a number of unique terms that are used in their posts. The following is a basic glossary of some of those terms:

<table>
<thead>
<tr>
<th>Term</th>
<th>Origin and Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>lotter</td>
<td>derived from caloteiro - a 'ripper'</td>
</tr>
<tr>
<td>notas fake</td>
<td>fake notes - counterfeit currency</td>
</tr>
<tr>
<td>aprovações</td>
<td>approvals or approved purchase transactions – ‘carding’</td>
</tr>
<tr>
<td>info cc</td>
<td>credit card information – 'fullz'</td>
</tr>
<tr>
<td>esquemas</td>
<td>derived from schemes - carding methods</td>
</tr>
</tbody>
</table>

*Figure 5: Typical Brazil community post uses movie poster themes to publicize fraud offerings*
Figure 6: Additional movie poster style advertising carding and other offerings

Figure 7: A Brazilian fraudster advertises a credit card checker site on Facebook

Figure 8: Selling counterfeit currency
Figure 9: Selling compromised credit card information

Brazilian Fraud Group 101 is mostly focused on selling gaming accounts which explains its isolation from other fraud groups who are very active in carding.

Brazilian Fraud Group 104 has most active fraud vendors and buyers as well as the most members who are present in other fraud groups.

These five groups are the most active and represent the main hubs of fraud activity on Facebook in Brazil.

Brazilian Fraud Group 112 has the highest number of members by count, but 70% are inactive lurkers, most likely “newbies.”

Figure 10: Relational clustering map illustrating a sample of the Brazilian fraud group landscape on Facebook. Individual members are represented by the dots, and unique groups are represented by different colors.

The graph above is a cloud or clustering representation of the affiliations between unique Facebook 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 that is ‘where the action is’. 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.

INDIA AND SOUTHEAST ASIA
The Indian fraud community on Facebook carries out their business mostly in English, often mixed with local languages written in Western characters. In addition to India, we observed fraud activity on Facebook across Southeast Asia including Indonesia, Vietnam, Malaysia, Pakistan and the Philippines.

In India and Southeast Asia, the RSA FraudAction Intelligence team analyzed 59 out of 159 fraud-dedicated groups identified on Facebook, with approximately 56,200 unique members among them. The top four groups contained over 29,000, or about 51%, of all members.

![Figure 11: Facebook group post in India selling local eWallet accounts with balance listed in Rupees. Several posts within these fraud groups contain mixed English and other language in the message.](image)
Figure 12: Offering carding services

Figure 13: Public Facebook fraud group in the India and Southeast Asia. Once again, mixed languages are prominent, including non-Western characters in one of the replies.
Fraudsters from India and Southeast Asia are clearly divided into two very large clusters. Although fraudsters operating within India (shown in orange) are larger in numbers, they are scattered throughout this graph, and simultaneously affiliated with many of the medium size and smaller groups (shown at the top of the graph). We also see fraudsters from Pakistan (green) and Vietnam (blue) concentrated in this area of the graph.

Fraudsters from Indonesia (shown in red, bottom right) are rather isolated from the rest of the fraud groups in Southeast Asia and found primarily in five large groups. Although there are significant ties with the main cluster in the upper left, the directionality of the links, as shown by the color of the lines, indicates that these are mostly fraudsters from India that are active in Indonesian communities, and not the other way around.

**Figure 14:** Relational clustering map of India and Southeast Asia fraudsters and groups on Facebook. The most active fraud groups within this region can be found in India and Indonesia.
LATIN AMERICA (SPANISH)
Spanish speaking countries in Latin America have many active fraud communities on Facebook as represented by number of members. As Spanish is the shared language among many regions, it makes it more difficult to pinpoint fraudsters to a specific country, although Mexico was observed to play a key role as the apparent hub of these groups based on the geographic location of the companies they attack, such as local mobile phone service providers and retailers.

Most of the carding activity in this region centers on the exchange of ‘bines’ (BINs), as opposed to carding methods or full credit cards offered as ‘freebies’. Fraudsters in Latin America assume that if a certain BIN was used for successful carding at a particular merchant, using another card from the same BIN will dramatically increase the chances of continued success. As such, special lists pairing ‘bines’ with merchants are commonly bought and sold in the Spanish speaking fraud groups on Facebook.

In Spanish speaking countries in Latin America, the RSA FraudAction Intelligence team analyzed 12 out of 112 fraud-dedicated groups identified on Facebook, with approximately 23,000 unique members. The top four groups contained over 21,700, or nearly 95%, of all members.

Fraudsters in Spanish speaking Latin America are organized in three large groups (shown on the left in violet), with two main groups sharing a large number of members in a third one. Due to the fact that all of the countries in the region share a common language, boundaries are blurred, and assigning a particular location becomes a matter of identifying linguistic cues from each individual fraudster. We discovered that fraudsters in this region also maintain ties with groups in other regions such as Brazil and Southeast Asia, and these groups appear in orange at the far right of the graph.

Figure 15: A Facebook post found in one fraud group in Latin America says, “Travels at 40%. Take advantage now. Lodging only.”
Fraudsters in Spanish speaking Latin America mainly organized in three core groups, and two of those groups share a large number of members with the third (center).

Fraudsters in Spanish-speaking groups within Latin America are also found to have ties with groups from Brazil and Southeast Asia.

**Figure 16:** Relational clustering map of fraudsters and groups on Facebook in Latin America. A majority of fraud groups are believed to originate in Mexico, and fraudsters in this region maintain ties to fraud groups in Brazil and Southeast Asia.
WEST AFRICA - GHANA AND NIGERIA

Fraudsters in West Africa appear to be much less diligent about protecting their privacy when compared with other regions in the fraud groups across Facebook. A great number of fraudsters from Ghana and Nigeria carry out fraudulent activities through what appear to be their own personal profiles. Many of the fraudsters in this region are facilitated by accomplices located in the US and UK who (judging by their Facebook profiles) also appear to originate from the region of West Africa.

It is interesting to note that many fraudsters in this region portray themselves as deeply religious, and seem to believe that their activities are a legitimate way of earning a living, often posting prayers of thanks for “good work” or “producing a good yield.” This mindset does not come as a surprise - most fraudsters in West Africa appear to be in the 18-30 year old demographic, and are most likely a generation raised by the same swindlers who invented the infamous “Nigerian 419” scams.

There is also a more sinister side to the criminal world in West Africa - drug trafficking, advance fee and internet fraud, and human trafficking are the most common trans-national activities carried out either in their own region or in other parts of the world.

Activities of the organized criminal groups in West Africa can be grouped into three broad categories:

- **Illicit goods** - drug trafficking, stolen property, counterfeiting
- **Illicit services** - human trafficking, cybercrime/fraud, commercial vices (sex and pornography)
- **Infiltration of business or government** - extortion and racketeering, money laundering, corruption

In West Africa, specifically Ghana and Nigeria, the FraudAction Intelligence team analyzed 5 out of the 105 fraud-dedicated groups identified on Facebook, with approximately 5,000 unique members.

---

The two largest Facebook groups in West Africa serve mostly as marketplaces for selling and sharing stolen card data.

Figure 17: West African FB post – recruiting accomplices

The three smaller groups located in West Africa are mostly dedicated to fraud-as-a-service and mule activities such as sending and receiving money transfers.

Figure 18: Relational clustering map of fraudsters and groups on Facebook in West Africa. The larger groups act as marketplaces for the sale and trade of stolen credit cards and account logins.
Fraudsters from the West African countries of Ghana and Nigeria are mostly concentrated in two large groups, with a few smaller groups as satellites. The larger groups (represented in purple and green) work mostly as marketplaces for CVV2/fullz, logins, and the sharing of ‘freebies’. The smaller groups in the bottom (orange, light blue, dark green) are more exclusive offshoots of the big groups and are primarily dedicated to fraud-as-a-service type activity such as ‘carding as a service’ and handling money and bank wire transfers.

Figure 19: A Facebook member in West Africa seeking accomplices with access to Canadian banks
FRANCE AND FRENCH SPEAKING REGIONS
The French speaking fraud community extends beyond the borders of France to other French speaking nations in Europe and communities in North Africa.

The majority of the attacks we identified targeted French businesses (e-commerce websites, banks, local prepaid credit cards, etc.). A large proportion of the activity in French speaking fraud groups on Facebook is dedicated to computer games and gaming fraud (trading in gaming accounts, monetizing fraud transactions through the gaming platforms, and trading or selling the most popular video games today). There are also lots of ‘freebies’ offered in the French fraud groups (accounts, tutorials, CCs, tools). Some members of the French fraud groups also attack targets in the U.S. and UK.

The topics discussed most often in French speaking fraud groups include:
- Gaming fraud
- Carding
- Banking fraud
- Fake documents
- Hacking
- Drugs
- Malware

In France and French speaking regions, the RSA FraudAction Intelligence team analyzed 19 out of the 120 fraud-dedicated groups detected on Facebook, with approximately 25,100 unique members. The top three French speaking groups we researched contained over 18,300, or 73%, of all members.

A large proportion of fraud activity in French speaking groups is focused on gaming fraud.
Fraudsters in France and other French speaking regions tend to organize in medium-sized Facebook groups. These groups contain a large proportion of fraudsters from North African countries such as Morocco, Algeria, and Tunisia. In some groups, we witnessed the mixing of languages, with items in both French and Arabic posted within the same group.

Most of the groups act as dedicated marketplaces for carding, selling CVV2/Fullz, and bank logins (the large cluster on the left, in purple, blue, and green), as well as the sharing of ‘freebies’. Special interest groups such as the group on the right side (orange) dedicated to gaming fraud, still show significant links to the credit card and banking fraud communities.

**Figure 21:** Relational clustering map of French speaking fraudsters and groups on Facebook. Unlike other regions, there is no single dominant group. Instead, fraudsters tend to organize in small or medium-sized groups.
WHATSAPP

As of February 2016, the wildly popular WhatsApp mobile messaging platform announced it had surpassed over one billion active monthly users. WhatsApp allows users to send each other instant messages, including images, audio, and video, and more recently, to make VOIP phone calls via the app. By default, users also see an instant confirmation when the other party receives and reads a message (this feature can be disabled by the user).

WhatsApp also allows users to create groups, such as a group for friends and family, and all members of that group receive messages that are posted by any member of that group.

In the newest trend of cybercrime in social media, many fraudsters use the platforms’ groups to recruit members into their Whatsapp groups. The “Group” feature enables anybody to create a decentralized chat room, where the group’s creator (admin) can add up to 200 members. These groups are completely off the grid and unlisted.

Figure 22: “The Anonymous Carders 2K16” group on WhatsApp offering a fraud tutorial
Figure 23: A fraudster shows confirmation of a carding transaction in a group on WhatsApp

Figure 24: A listing of fraud groups and individuals on WhatsApp
Figure 25: A fraudster on Facebook posts a call for members to join his carding group on WhatsApp

Figure 26: A typical conversation among fraudsters on WhatsApp
CONCLUSION

So where is the mention of fraudsters operating on Facebook in the United States and Europe? Although fraud activity is prominent in the United States and Europe, fraudsters in these regions appear to continue to operate in the underground and not on social media.

One of the most prominent takeaways is when you view cybercrime on social media from 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, such as the Brazilian cybercrime economy, 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 27: Fraudsters that attack the U.S. and UK](image)

(Blue = target countries, Red = attackers)

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 on Facebook in these regions is a clear indication that fraudsters are on alert and intelligence sharing and prosecution is working.

*In part two of this special report series, we examine cybercrime in the common social media platforms in Russia and China.*
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 RSA 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’s solutions help organizations execute advanced cyber defense strategies that reduce the risks of operating in a digital world. Through visibility and analytics, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud, and cybercrime. For more information on RSA, please visit rsa.com.