RSA BUSINESS-DRIVEN SECURITY™

RSA QUARTERLY FRAUD REPORT

Volume 1, Issue 4
Q4 2018

CONTENTS

EXECUTIVE SUMMARY

The RSA® Quarterly Fraud Report contains fraud attack and consumer fraud data and analysis from the RSA Fraud and Risk Intelligence team. It represents a snapshot of the cyber fraud environment, providing actionable intelligence to consumer-facing organizations of all sizes and types to enable more effective digital risk management.

RSA-OBSERVED FRAUD ATTACK AND CONSUMER TRENDS

For the period starting October 1, 2018 and ending December 31, 2018, RSA observed several global fraud trends across attack vectors and digital channels. The highlights include:

Phishing accounted for 49 percent of all fraud attacks observed by RSA in Q4. Canada, Spain, and the Netherlands were the top three countries most targeted by phishing and represented 71 percent of total attack volume. Most notably, Spain saw a 178% increase in phishing attacks from Q3 due to the launch of new instant transfer services among many of the leading banks in the region.

Total phishing volume increased 12 percent and social media and brand abuse attacks increased 43 percent in 2018.

Total Trojan attacks detected by RSA in 2018 was 22,489, an 8% increase from 2018.

RSA detected 10,390 rogue mobile applications, an 11 percent increase from last quarter and 22 percent of total fraud attacks.

The overall number of fraudulent financial transactions increased 28 percent, with 70 percent originating in the mobile channel.

Card-not-present (CNP) fraud transactions increased 12 percent last quarter, and 80 percent of those originated from a new device.

RSA recovered over 10.7 million unique compromised cards in Q4, a 96 percent increase from the previous quarter.

FEATURE ARTICLE

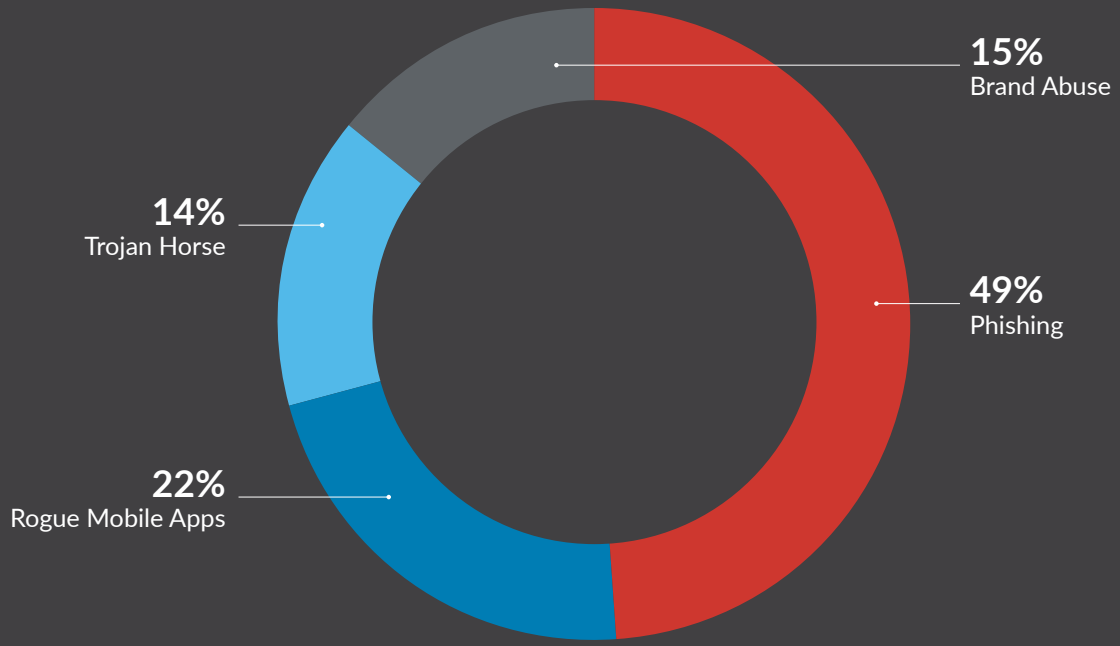
Fraudsters Turn to Telegram Bots for Cybercrime Automation

As part of the social media revolution, the Telegram messaging app has experienced significant growth, adding an average of 350,000 new users daily, and is available in 13 languages facilitating wide adoption globally. The Telegram app allows users to create groups with up to 30,000 members and share files and documents of nearly any type. It even allows bots to be set up for specific tasks. Due to its rich feature set and rapid adoption, Telegram has become a sought-after tool on the fraud scene. Recently, RSA has been tracking a surge in the use of the Telegram bot feature by fraudsters to facilitate and automate their activities. This article explores the different types of fraud Telegram bots available today and the Fraud-as- a-Service offerings that are helping the phenomenon spread.

FRAUD ATTACK TRENDS: Q4 2018

Phishing and malware-based attacks are the most prolific online fraud tactics developed over the past decade. Phishing attacks not only enable online financial fraud but these sneaky threats chip away at our sense of security as they get better at mimicking legitimate links, messages, accounts, individuals and sites. Automated fraud comes in the form of the various active banking Trojan horse malware families in the wild today; these malicious programs do their work quietly and often without detection until it is too late.

By tracking and reporting the volume and regional distribution of these fraud threats, RSA hopes to contribute to the ongoing work of making consumers and organizations more aware of the current state of cybercrime and fueling the conversation about combating it more effectively.



Fraud Attack Trends: Q4 2018

Fraud Attack Type Distribution

In the fourth quarter of 2018, RSA detected 48,148 total fraud attacks worldwide. Phishing attacks accounted for 49 percent of all observed fraud attacks, and overall phishing volume increased 25 percent from Q3. Attacks involving financial malware increased slightly from 12 percent last quarter to 14 percent in Q4. RSA detected 10,390 rogue mobile applications, an 11 percent increase from last quarter and 22 percent of total fraud attacks.

RSA saw YOY increases across all attack vectors as follows:

- Total phishing attacks detected by RSA in 2018 was 67,843, a 12 percent increase from 2017.
- Total Trojan attacks detected by RSA in 2018 was 22,489, an 8 percent increase from 2017.
- Social media and brand abuse attacks detected by RSA in 2018 comprised 22,686 of all fraud attacks, a 43 percent increase from 2017.

FRAUD ATTACK GLOSSARY

Phishing
Cyber attacks attempting to steal personal information from unwitting end-users under false pretenses either by email, phone call (vishing) or SMS text (smishing).

Trojan Horse
Stealthy malware installed under false pretenses, attempting to steal personal user information.

Brand Abuse
Online content, such as social media, that misuses an organization's brand with the purpose of misleading users.

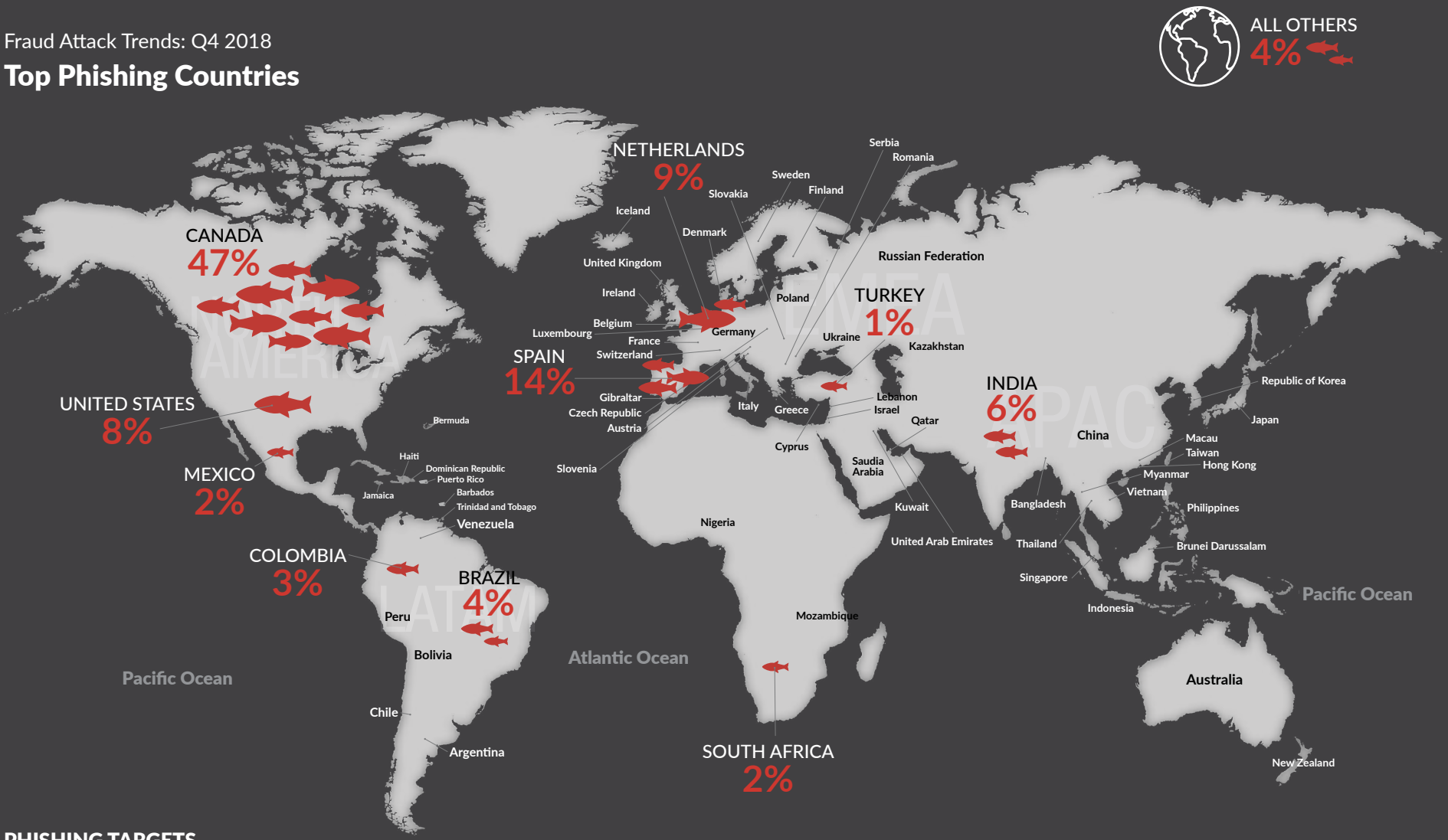
Mobile Application Fraud
Mobile applications using an organization's brand without permission.

IN Q4 2018,
RSA detected

10,390

ROGUE MOBILE APPLICATIONS

Top Phishing Countries



PHISHING TARGETS

Canada, Spain and the Netherlands were the top three countries targeted by phishing representing 70 percent of total attack volume. For the first time in 2018, Turkey appeared on this list, targeted by 1.2 percent of total phishing volume in Q4.

The most significant change was that Spain displaced the United States as the second country most targeted by phishing this quarter, with attack volume more than doubling from 6 percent to 14 percent in Q4. The spike in phishing attacks targeting organizations in Spain can be attributed to the launch of instant transfer services among many prominent financial institutions. This example serves as a reminder of how cybercriminals continue to take advantage of significant events or changes in the market to launch attacks.

Top Hosting Countries

HOSTING COUNTRIES

1.	United States	6.	Germany
2.	India	7.	Malaysia
3.	Russia	8.	Netherlands
4.	Canada	9.	Poland
5.	France	10.	China

PHISHING HOSTS

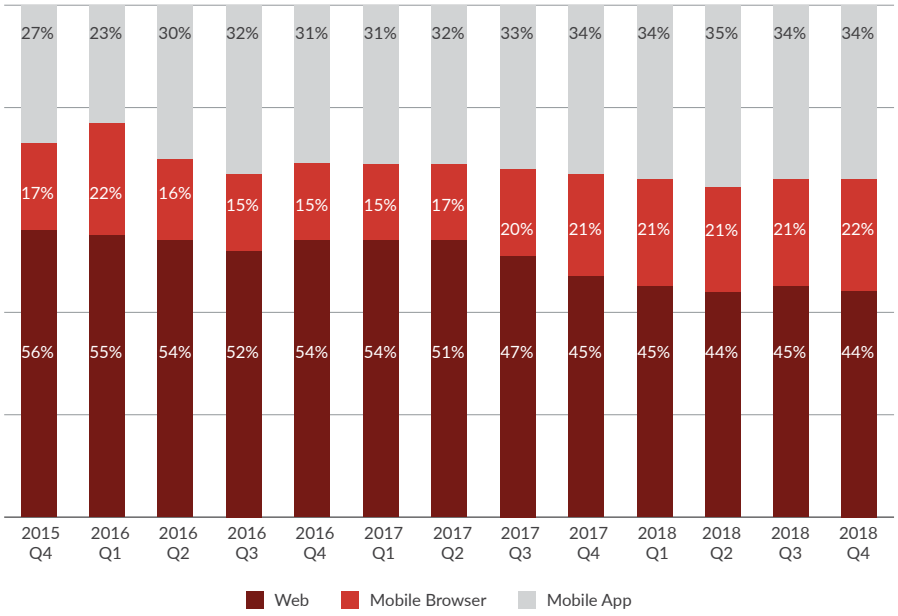
In Q4, we saw Italy drop from the top ten hosting country list and Poland appeared on the list, although only a small fraction of overall phishing attacks were hosted there (two percent). The United States remains the top country, hosting 50 percent of phishing attacks last quarter.

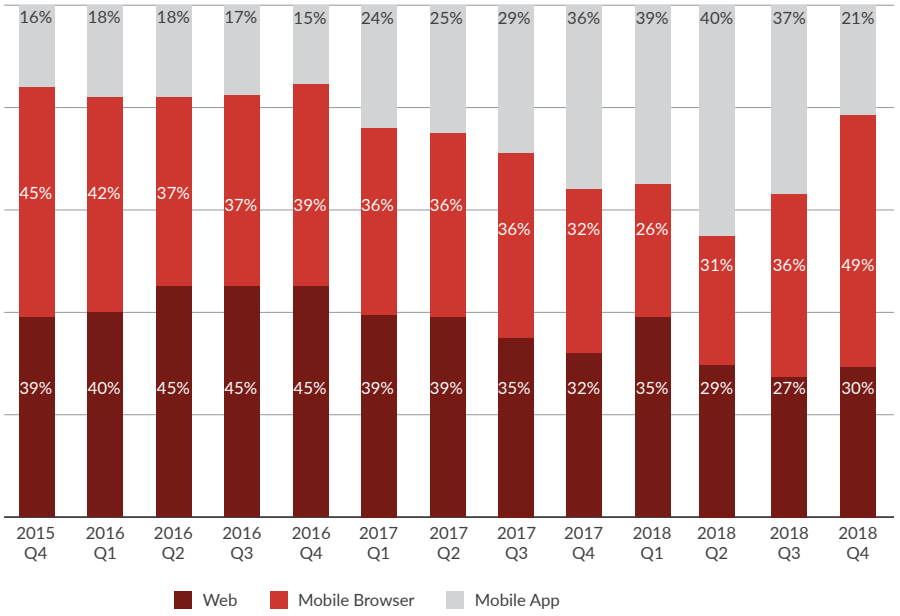
CONSUMER FRAUD TRENDS: Q4 2018

The RSA Fraud and Risk Intelligence team analyzes consumer fraud data and informs the security and risk-management decisions for major organizations while serving the public interest by identifying, preventing and reducing financial cyber fraud attacks on consumers. Observing consumer fraud trends over time can support decision-makers on how to build or refine their omnichannel fraud prevention strategy and which channels are more vulnerable to fraud attacks.

These data points are intended to broadly frame the current consumer fraud atmosphere, and identify relevant trends, by tracking broad indicators of online fraud across both financial and e-commerce focus areas.

Transaction and Fraud Transaction Distribution by Channel





Source: RSA Fraud & Risk Intelligence Service, October 2015-December 2018

TRANSACTION METHOD

In the fourth quarter of 2018, mobile browsers and applications accounted for 56 percent of overall transactions observed by RSA, representing little change in channel distribution from the previous quarter. While the mobile channel witnessed significant growth in transaction volume over the past three years, specifically with mobile applications, it appears mobile banking adoption has started to level off.

FRAUD TRANSACTION METHOD

In Q4, the overall number of fraudulent financial transactions increased 28 percent, with 70 percent originating in the mobile channel. The significant shift occurred in how fraud was distributed across the mobile channel. Fraud from mobile browsers increased significantly from 36 percent in Q3 to 49 percent in Q4 while fraud transactions from mobile apps fell from 37 percent to 21 percent. It is unclear whether this shift in mobile fraud is a "one off" or part of a longer term trend. RSA will continue to monitor the impact.

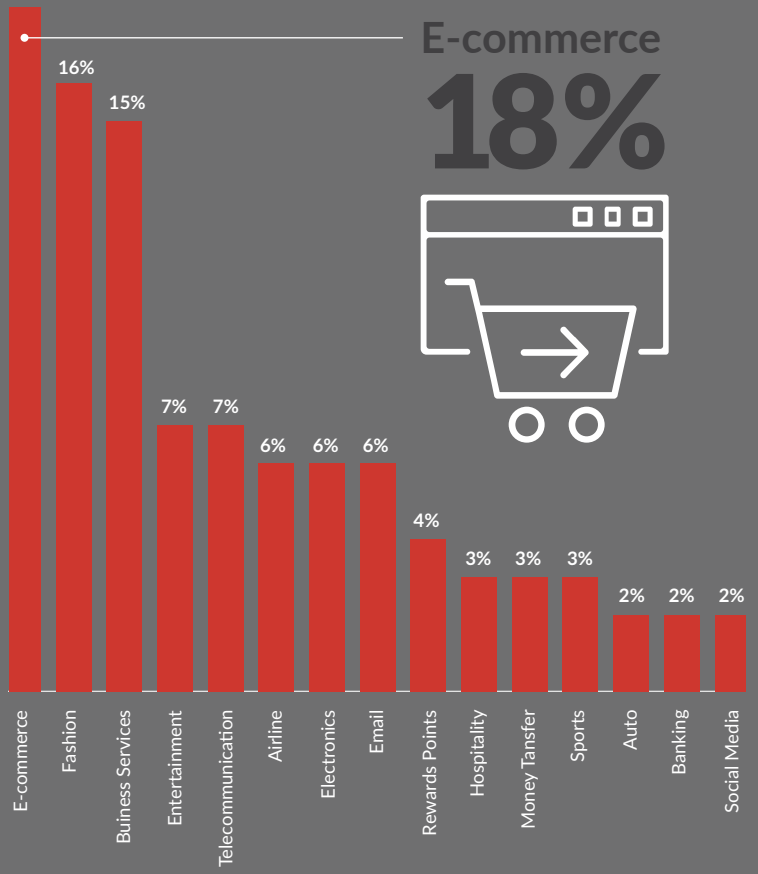
Year over year, fraud transactions from the mobile channel increased 27 percent showing the growing preference among fraudsters to initiate unauthorized transactions through this channel.

Compromised Credentials by Type

Globally, more than 4.5 billion records were compromised in the first half of 2018 alone. Most of these records end up for sale in the dark web, and they vary in price depending on a number of factors such as how "fresh" they are (e.g., how recently they were compromised) and the type of account.

RSA conducted extensive research across some of the most popular dark web stores to learn more about the average selling price of stolen credentials across various types of consumer accounts and which ones are most lucrative. A breakdown of average price in the dark web based on account type is below:

Account Type	Price Range
Retail: Major retailers, fashion, entertainment, home goods, auto	$0.20 - $6.00
Social: Social media, emails, dating sites, instant messaging	$1.00 - $10.00
Hospitality: Airlines, hotels, and travel	$0.70 - $10.50
Financial: Bank accounts, money transfer services, credit cards	$0.50 - $15.50
Technology: Telecommunications, mobile devices and electronics, business services	$0.40 - $4.50



The specific type of compromised credentials that are most popular within dark web stores are e-commerce accounts which represents 18 percent of accounts for sale and includes most major online retailers that sell a variety of goods and services. This is followed closely by fashion and business services as well as telecommunications and entertainment accounts. Reward points accounts represent 4 percent, however, airline and hospitality accounts are often tied to reward points. Therefore, rewards points accounts more likely represent 13 percent of stolen credentials for sale.

Average Credit Card Transaction and Fraud Transaction Values

(E-Commerce, by Region)

The average value of a fraudulent transaction will likely always be higher than that of a genuine transaction, since fraudsters regularly use stolen credit cards to make quick, high-value purchases since these goods are easy to resell for a profit. There are, however, insights to be gained in the differences between the spending levels related to genuine and fraud transactions.

In the fourth quarter, the most drastic difference between the value of genuine and fraud transactions was observed in Australia, where the average value of a fraud transaction was $387 USD, a 22 percent increase from Q3. Despite the holiday shopping season, the UK saw a 30 percent decrease in the average fraud transaction value in Q4. The United States and the rest of the EU saw little change in overall fraud transaction value.

REGION	TRANSACTION VALUE	FRAUD TRANSACTION VALUE	DIFFERENCE $
European Union	$154	$396	$262
Americas	$218	$418	$200
UK	$159	$247	$88
Australia/New Zealand	$166	$387	$221

Source: RSA Fraud & Risk Intelligence Service, October 2018-December 2018

Device Age vs. Account Age

ANALYSIS

"Device Age" refers to how long the RSA Fraud Platform has "known" or "trusted" a given device (laptop, smart phone, etc.). "Account Age" refers to how long the RSA Fraud Platform has "known" or "trusted" a given account (login, etc.). This data demonstrates the importance of accurate device identification to minimize false positives and customer friction during a login or transaction event.

E-COMMERCE

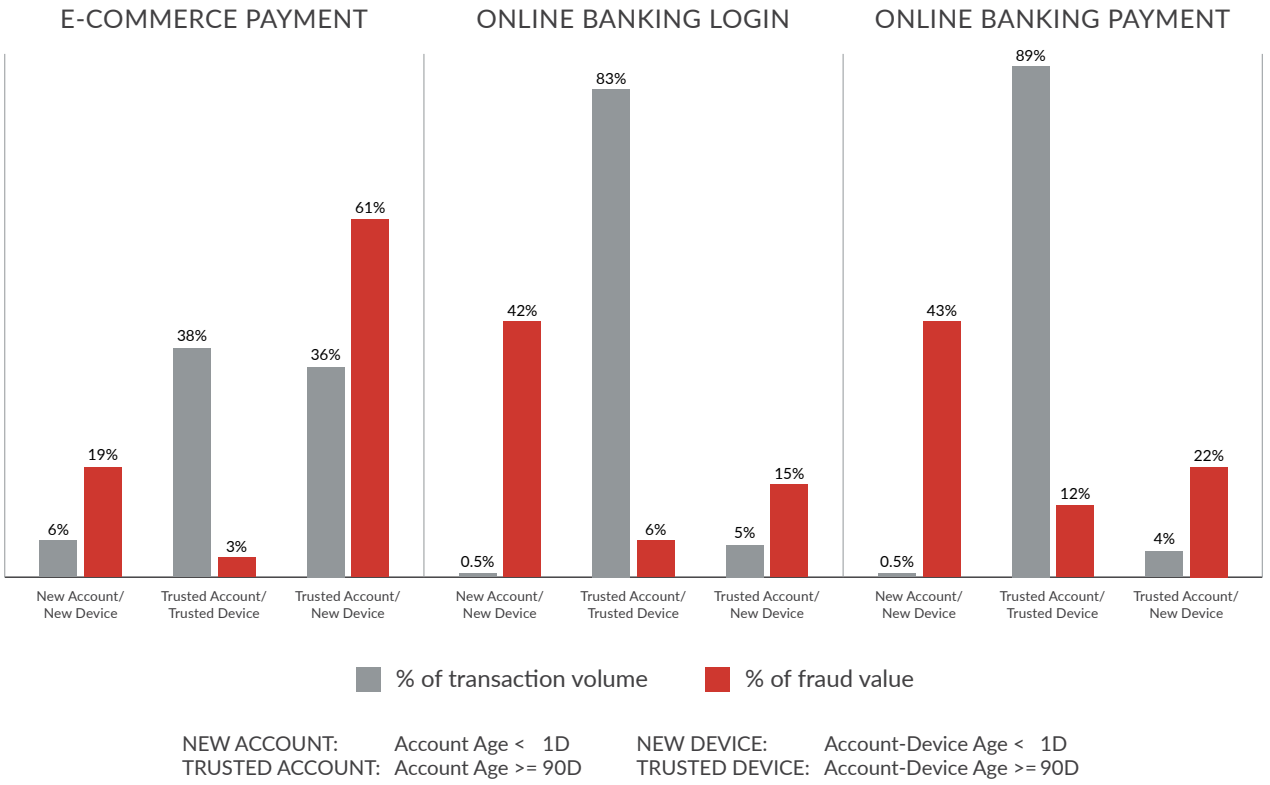
In the fourth quarter, RSA saw a 12 percent increase in card-not-present (CNP) fraud transactions, and 80 percent of those originated from a new device. Seventy-four percent of CNP fraud transaction value originated from trusted accounts indicating account takeover or credential replay attacks where fraudsters use stolen credentials gathered from a data breach to login or "take over" other accounts owned by a victim.

ONLINE BANKING: LOGIN

While only half of a percent of legitimate logins were attempted from a combination of a new account and a new device, this scenario accounted for 42 percent of total fraud volume observed in Q4. This pattern often indicates fraudsters attempting to leverage stolen identities to create mule accounts as part of the "cash out" process. For organizations, new account protection is a high risk scenario and often associated with synthetic identity fraud.

ONLINE BANKING: PAYMENT

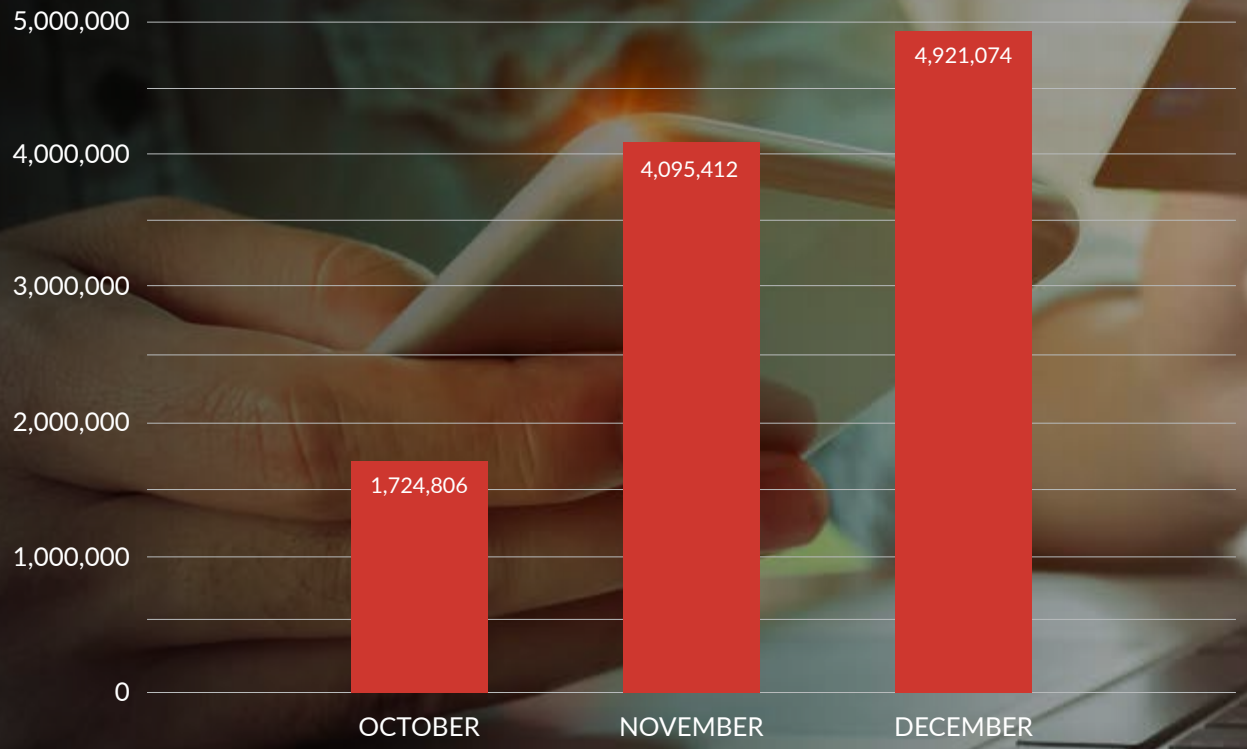
Similar to fraud patterns at login, less than one percent of legitimate payment transactions were attempted from a new account and new device, yet it made up 43 percent of total fraud value, nearly doubling from 21 percent in Q1. This is indicative of an increase in account takeover where fraudsters are attempting to use compromised financial information to initiate payments from victims' accounts.



NEW ACCOUNT: Account Age < 1D
TRUSTED ACCOUNT: Account Age >= 90D
NEW DEVICE: Account-Device Age < 1D
TRUSTED DEVICE: Account-Device Age >= 90D

Source: RSA Fraud & Risk Intelligence Service, October 2018-December 2018

Compromised Credit Cards Discovered/Recovered by RSA



Source: RSA Fraud & Risk Intelligence Service, October 2018-December 2018

ANALYSIS

In Q4 2018, RSA recovered over 10.7 million unique compromised cards and card previews from reliable online fraud stores and other sources. This represents a 96 percent increase in cards recovered by RSA from the previous quarter.

One cause for the increase can be correlated to the increase in phishing attacks witnessed in Q3 which is common as fraudsters seek to gather fresh credentials to sell in anticipation of the holiday shopping season. In turn, it is not unusual to see the spike in compromised cards for sale as fraudsters look to unload much of their newly harvested stock and will often advertise their own Black Friday or Cyber Monday "specials" through forum advertisements and posts.

FEATURE ARTICLE

Fraudsters Turn to Telegram Bots for Cybercrime Automation

As part of the mobile and social media revolution, the Telegram messaging app has experienced significant growth, adding 350,000 new users daily. The platform has been widely adopted globally and is available in 13 languages. The Telegram app allows users to create groups with up to 30,000 members and share files and documents of nearly any type. It even allows bots to be set up for specific tasks. Due to its rich feature set and rapid adoption, Telegram has become a sought-after tool on the fraud scene.

Until recently, fraudsters mainly utilized Telegram groups and channels to organize their communities. Groups can be best described as chat rooms in which all members can read, comment and post. This is where fraudsters advertise, connect and share knowledge and compromised information, much like the role forums play on the dark web. Channels, on the other hand, are groups in which only the administrator is authorized to post and regular members have access to view, similar to blogs. Fraudsters mainly use Telegram channels to advertise fraud services and products in bulk.

Telegram bots are a new popular feature allowing third party apps to run within the platform. Bots enable users to enhance the messaging experience. Legitimate uses of Telegram bots include automatic file converters, daily weather or horoscope notifications, management of to-do lists and more.

Recently, RSA has witnessed a surge in the use of the Telegram bot feature by fraudsters to facilitate and automate their activities. Some provide automated tools for common actions conducted by fraudsters, whereas others provide actual fraud services via online stores. Below, we will explore examples of the different types of fraud Telegram bots available today as well as Fraud-as- a-Service offerings that are helping this phenomenon spread.

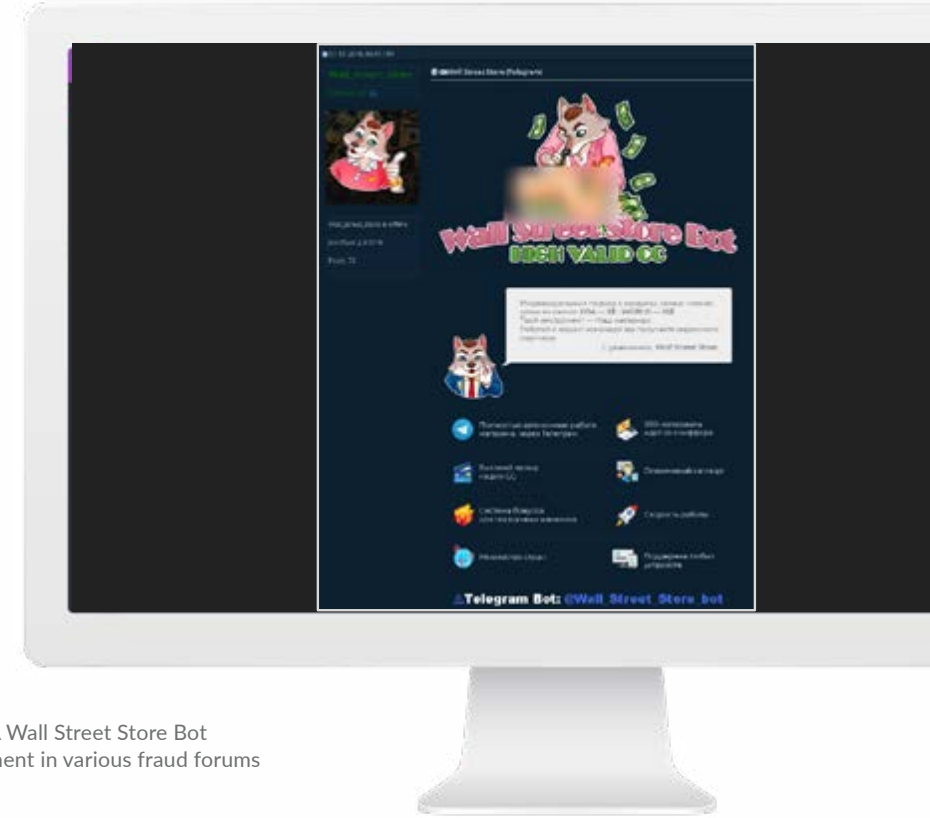


Figure 1: A Wall Street Store Bot advertisement in various fraud forums

TELEGRAM BOTS

@WALL_STREET_STORE_BOT

Wall Street Store Bot is a credit card store on Telegram which started off as a command-only bot and has since added user-friendly buttons that allow fraudsters to receive information on balance, purchase history and more. The most valuable is the "Available Cards" button which allows fraudsters to download a file, either HTML-based, PC-compatible or a text-based, mobile-compatible version, containing all cards available on the store. The card details are displayed in a table with filter options, similar to what we typically see in traditional credit card stores. Customers copy the card IDs they are interested in and enter them in the bot chat to complete the purchase.

Like any respected credit card store, Wall Street Store Bot also includes a credit card checker, an auto-refund system, a user ranking system to encourage purchases and a user-specific Bitcoin wallet to add funds.

In addition to the bot itself, the store operates a separate 24/7 support channel in English and Russian, which is used both as a customer service platform and a channel to post news and updates about the store and its available card database.

@BANKERROBOT

Banker Robot is the official bot of the highly-popular **@PerfectCarders** channel in the Brazilian Portuguese-speaking fraud community. It is a general purpose bot which allows easy access to tools and information often required by fraudsters in their day-to-day activities. When typing the /tools command, the user is presented with various free automated services, including the retrieval of proxy/Socks5/RDP lists, generators of fake PII and banking information. Additional lookups include BINs, IP addresses and ZIP codes, current values of cryptocurrencies and validation of credit card numbers.

@MRBANKERBOT

MrBanker Bot is another bot from the makers of @PerfectCarders, and its main features include the sale of credit cards and access to "Spectrum Checker," the official credit card checker of the channel. A weekly subscription goes for R$60 (~$16USD) or a monthly subscription for R$250 (~$65USD).

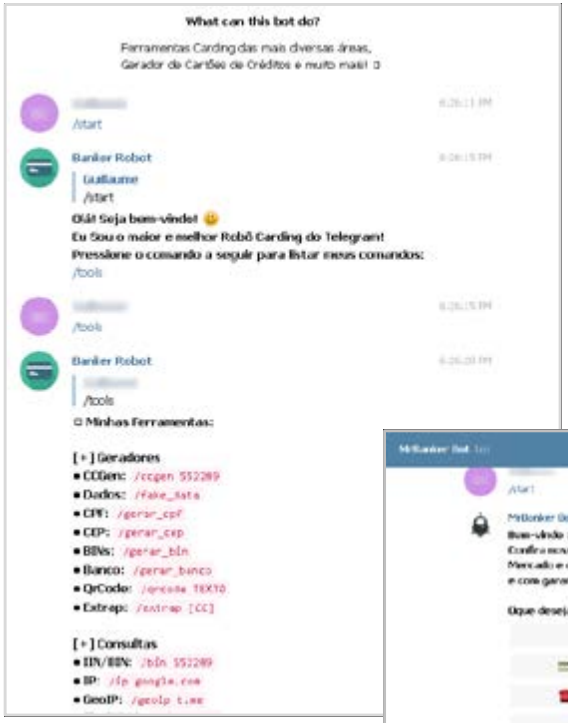


Figure 3: Banker Robot (Telegram web version)

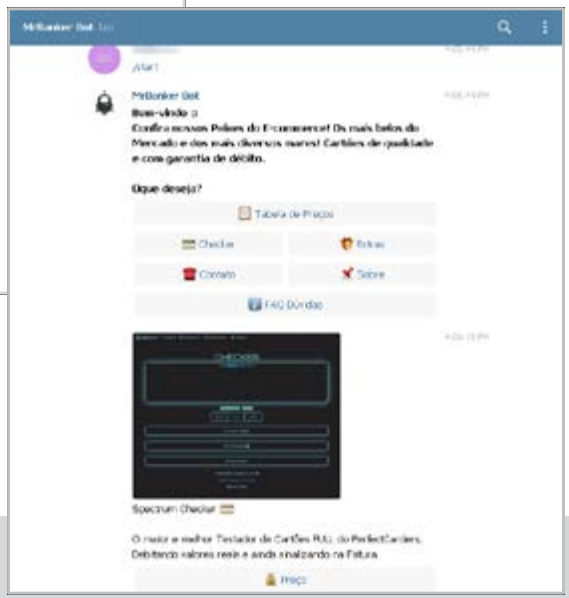


Figure 4: MrBanker Bot (Telegram web version)

Figure 2: Example of an export file presenting the available cards for sale

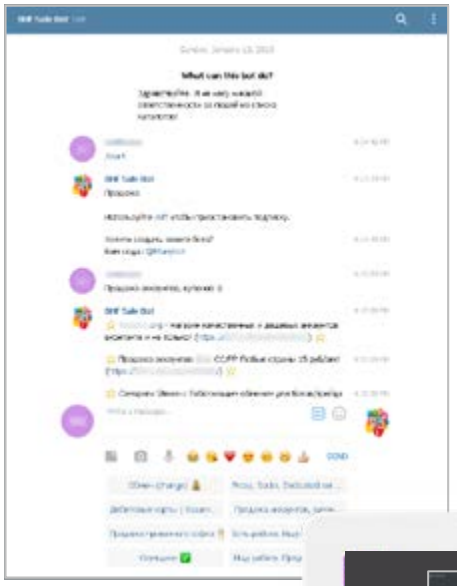
Due to its rich feature set and rapid adoption, Telegram has become a sought-after tool on the fraud scene.

@SALEBHFBOT

The BHF Sale Bot first appeared in February 2018 and is geared to allow easy searches for listings on the prominent Russian hacking forum BHF. The search categories include:

- Exchange
- Debit Cards, Wallets, Sim
- Sale of Private Software
- Proxy, Socks, Dedicated Servers, VPN
- Selling Accounts, Coupons
- Looking for a Specialist
- Looking for Work

Figure 5: BHF Sale Bot (Telegram web version)



ROSKOMNADZOR SERVICE (@RSKMBOT)

Roskomnadzor is a renting service for Telegram bots and online webstores, offered by Russian-speaking fraudsters to the fraud community.

The service has an official website and a number of Telegram channels for customer service, technical support and news and updates (which even provides coupons!), and is frequently advertised in highly-regarded fraud forums and marketplaces. Orders are made via a dedicated Telegram bot where customers can choose a plan out of the following options:

"White Thematic" for $6 per month

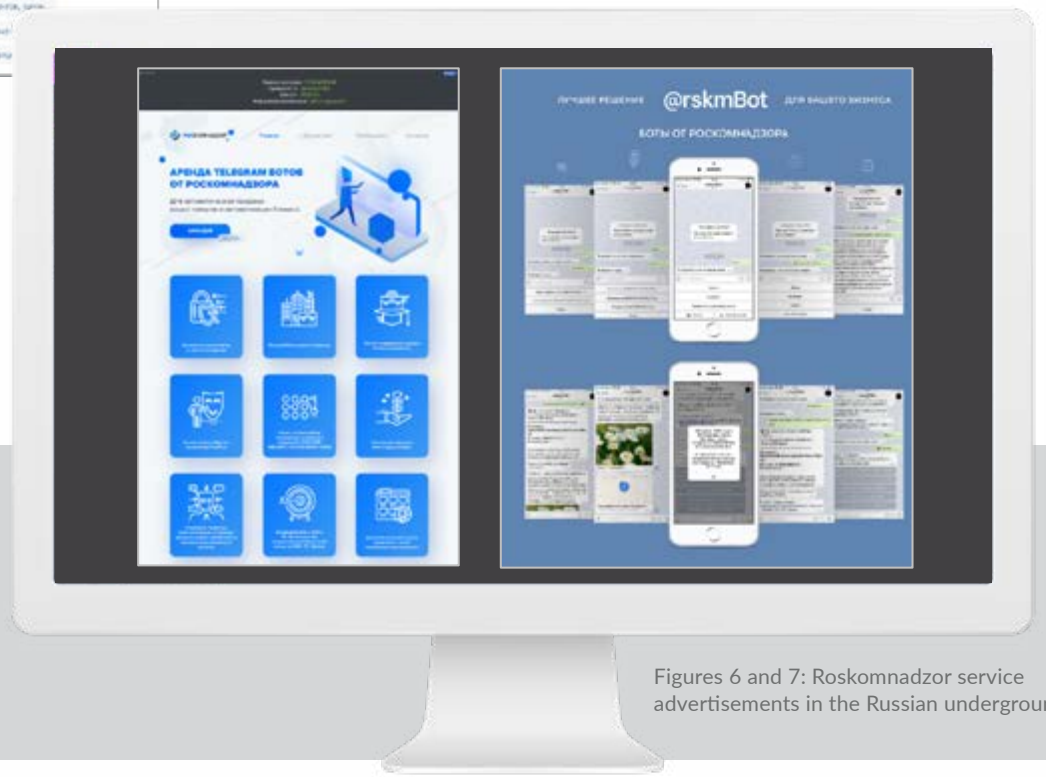
Permitted Items: accounts of any type, credit cards, IDs, virtual wallets, counterfeit or stolen documents (e.g. passports, certificates, insurance)

Prohibited Items: the bot's control panel, extremist material, explosives, weapons, drugs, radioactive substances, gambling equipment, and more

"Black Thematic" for $80 + 1% of the turnover per month

Permitted Items: the sale of any goods is allowed including hardware (such as skimmers), illegal substances and more

Prohibited Items: the bot's control panel and extremist material



Figures 6 and 7: Roskomnadzor service advertisements in the Russian underground

RSA has witnessed a surge in the use of the Telegram bot feature by fraudsters to facilitate and automate their activities.

Advantages of the service include:

- Free replacement in case of blocking
- Personal "bulletproof" server
- Full traffic encryption (for anonymity)
- Detailed statistics on the number of users, goods sold, and categories
- Coupons and discounts
- Uninterrupted server availability
- Integrated cryptocurrency payment reception system
- Intuitive design of the control panel
- Online webstore with a domain as a gift when renting a Telegram bot

The service also offers a demo store bot (@Lease24Bot) and a demo webstore for potential customers to interact with and try out their functionalities.

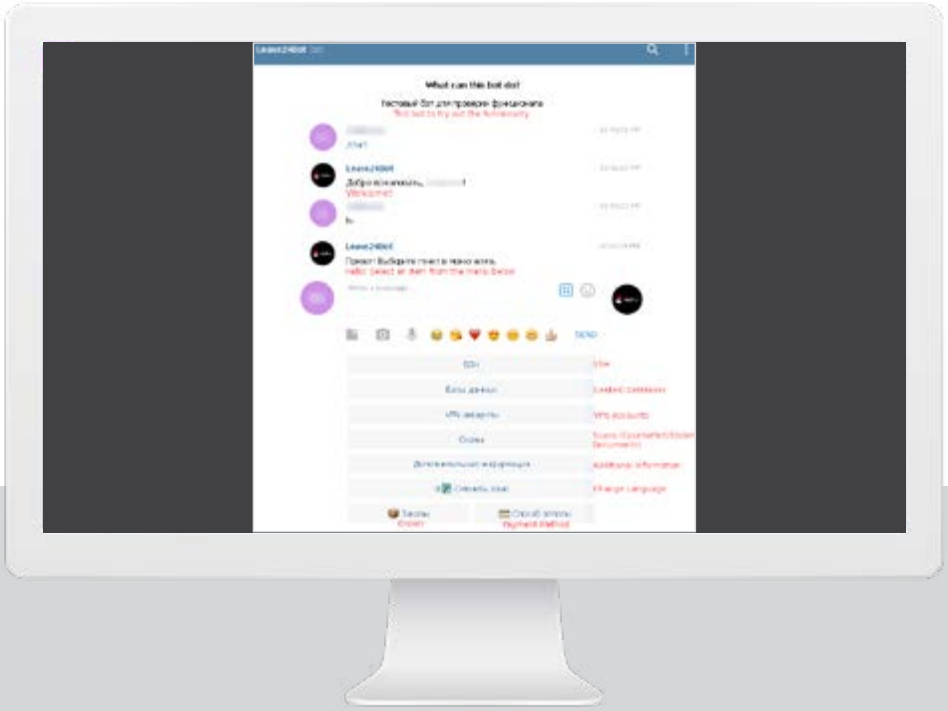


FIGURE 8: Lease24Bot – demo bot for Roskomnadzor

CONCLUSION

RSA first reported on the growth of global cybercrime on social media back in 2016 which studied over 500 fraud groups across Facebook. In 2018, RSA released a follow-on report highlighting the spread of cybercrime to other social media platforms, including Telegram. This trend continues to evolve, with Telegram gaining momentum and preference as a "one stop shop" for fraudsters. (NOTE: to access RSA's previous research on this topic, please refer to the Additional Resources section below)

The use of Telegram bots not only demonstrates the continued growth of social media and other popular platforms by cybercriminals for illicit activity, but also the use of advanced technologies such as AI to automate their businesses.

Telegram bot stores possess several significant benefits for fraudsters. Not only do they eliminate the need to register a host and domain, all the typical security challenges that may impact a website, DDoS attacks perhaps most notably, become irrelevant. The use of the Telegram platform also eliminates fraudsters' need to protect and hide their website from law enforcement.

While the implementation of Telegram bots in the fraud context is relatively new, we expect this trend to gain more momentum in 2019. RSA's intelligence analysts will continue to monitor this and other social media platforms and advise the public accordingly as new fraud threats emerge.

Additional Resources

"Hiding in Plain Sight: The Growth of Cybercrime in Social Media," published by RSA, February 2016

"Cybercrime in Social Media Grows 70 Percent in Six Months," published by RSA, December 2016

"The Social Media Fraud Revolution," published by RSA, May 2018

ABOUT THE RSA® FRAUD & RISK INTELLIGENCE SUITE

The RSA Fraud & Risk Intelligence Suite helps organizations manage fraud and digital risk across multichannel environments without impacting customers or transactions. The suite offers risk-based authentication and behavior analytics solutions for web, mobile and e-commerce as well as fraud intelligence services to allow organizations to protect their customers across the entire digital journey. The Fraud & Risk Intelligence Suite is deployed at over 5,000 global organizations and protects over 1.5 billion consumers.

RSA