RSA BUSINESS-DRIVEN SECURITY™

RSA QUARTERLY FRAUD REPORT

Volume 1, Issue 1
Q1 2019

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 January 1, 2019, and ending March 31, 2019, RSA observed several global fraud trends across attack vectors and digital channels. The highlights include:

Phishing accounted for 29 percent of all fraud attacks observed by RSA in Q1. While overall phishing volume increased less than 1 percent quarter over quarter, in terms of overall fraud attacks, phishing decreased sharply due to the exponential growth of attacks from rogue mobile apps.

Fraud attacks from rogue mobile applications increased 300 percent, from 10,390 rogue apps in Q4 to 41,313 in Q1.

Fraud attacks introducing financial malware increased 56 percent, from 6,603 in Q4 to 10,331 in Q1.

Card-not-present (CNP) fraud transactions increased 17 percent last quarter, and 56 percent of those originated from the mobile channel. The average value of a CNP fraud transaction in the U.S. was $403, nearly double that of an average genuine transaction of $213.

RSA recovered over 14.2 million unique compromised cards in Q1, a 33 percent increase from the previous quarter.

FEATURE ARTICLE

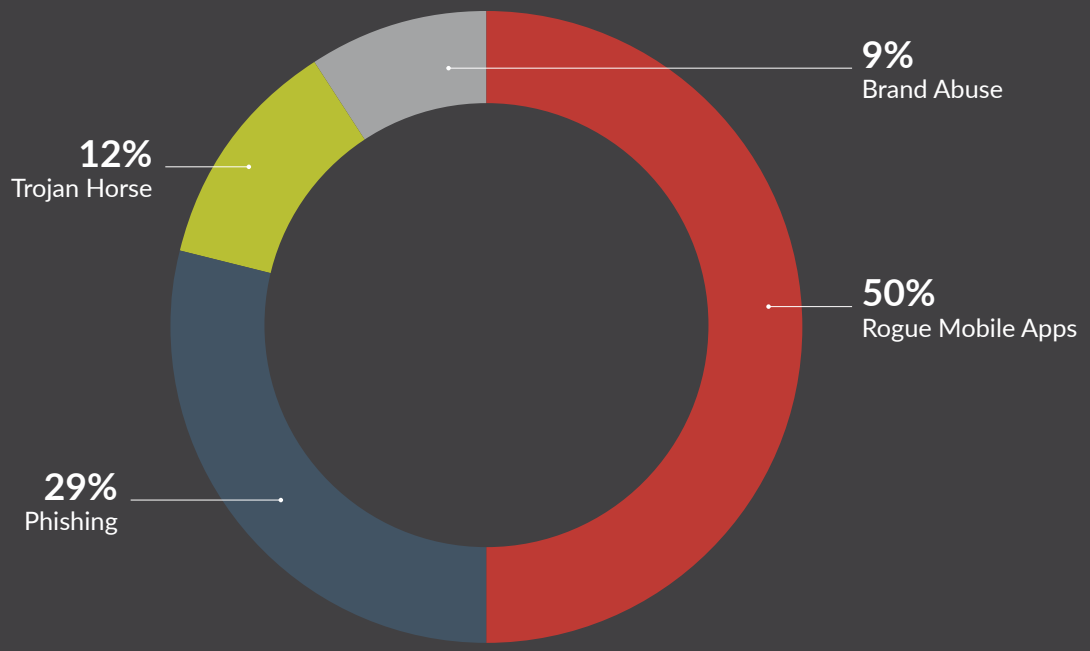
Fraudsters Launch DIY Site to Expand Account Takeover

Account checkers have been around for a long time, but fraud-as-a-service offerings have continued to evolve rapidly in the last couple of years due to the high volume of password breaches. Credential-stuffing tools such as Sentry MBA and SNIPR have been popular among fraudsters; however, their use is restricted by the limited availability of prebuilt configurations, mostly for large websites. RSA recently identified an online studio for developing account checkers capable of attacking nearly any website. In addition to facilitating the development of new checkers, the site has also created a new source of income for fraudsters as the revenue generated from each checker is split between the site owner and the developer. This has introduced new opportunities for fraudsters to attack organizations not traditionally targeted by account takeover.

FRAUD ATTACK TRENDS: Q1 2019

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: Q1 2019

Fraud Attack Type Distribution

In the first quarter of 2019, RSA identified 82,938 total fraud attacks worldwide. RSA detected 41,313 rogue mobile apps in Q1, a 300 percent increase from Q4 2018. This attack vector accounted for half of all observed fraud attacks. Phishing attacks accounted for 29 percent of observed fraud attacks, and overall phishing volume remained relatively the same, increasing less than 1 percent. Attacks involving financial malware increased 56 percent, from 6,603 in Q4 to 10,331 in Q1.

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.

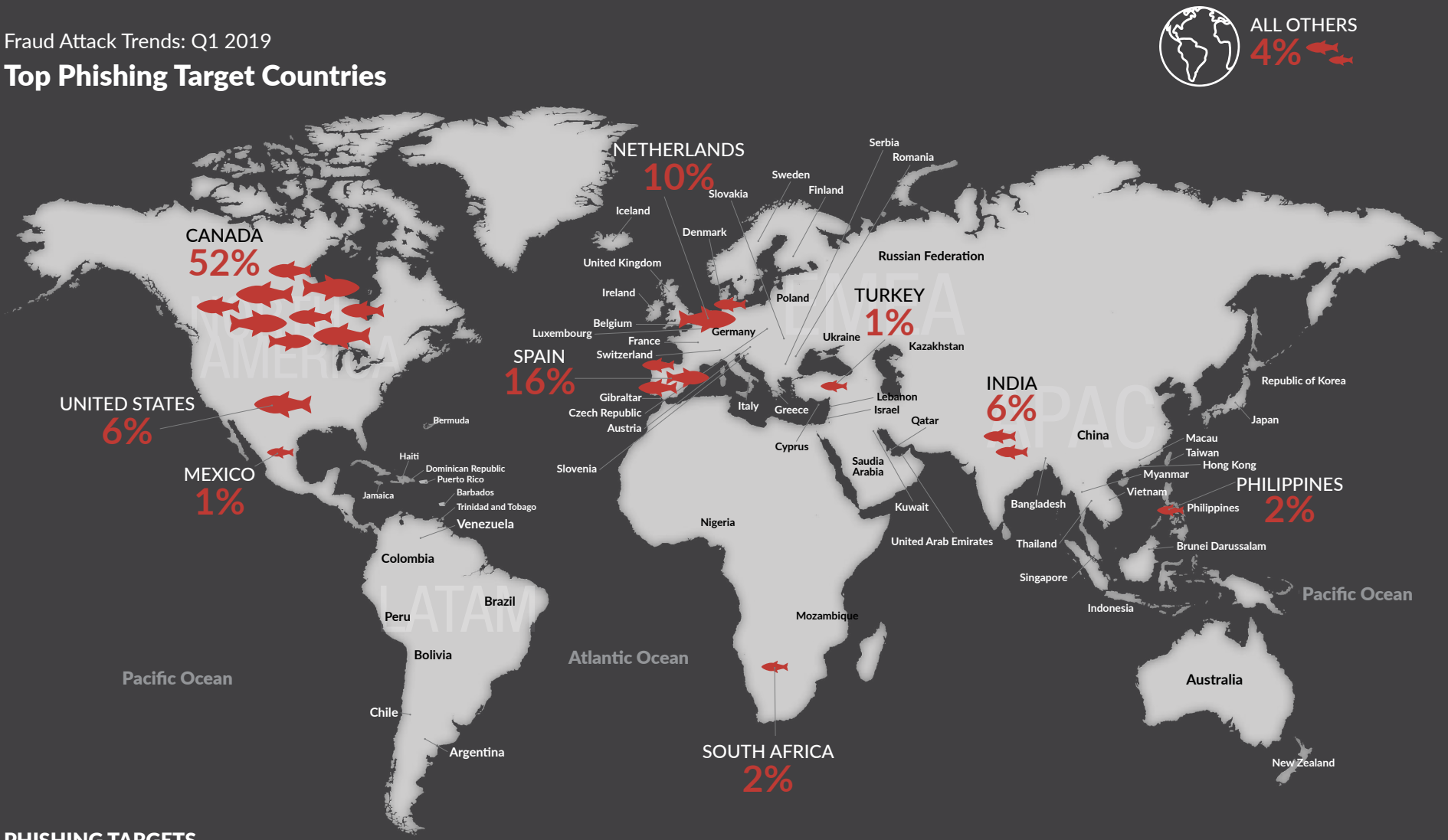
Brand Abuse
Online content, such as social media, that misuses an organization's brand with the purpose of misleading users.

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

IN Q1 2019,
Fraud attacks increased
300%
FROM ROGUE MOBILE APPLICATIONS

Fraud Attack Trends: Q1 2019

Top Phishing Target Countries



PHISHING TARGETS

Canada, Spain and the Netherlands remain the top three countries targeted by phishing, representing 78 percent of total attack volume. The Philippines appeared on the list, replacing Brazil as a top target with 2 percent of total phishing volume in Q1.

Spain continues to be targeted with a high volume of phishing attributed to the launch of new innovative digital payment services among many prominent financial institutions. This example serves as a reminder of how cybercriminals can exploit digital transformation initiatives to launch attacks.

Top Phishing Hosting Countries

HOSTING COUNTRIES

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

PHISHING HOSTS

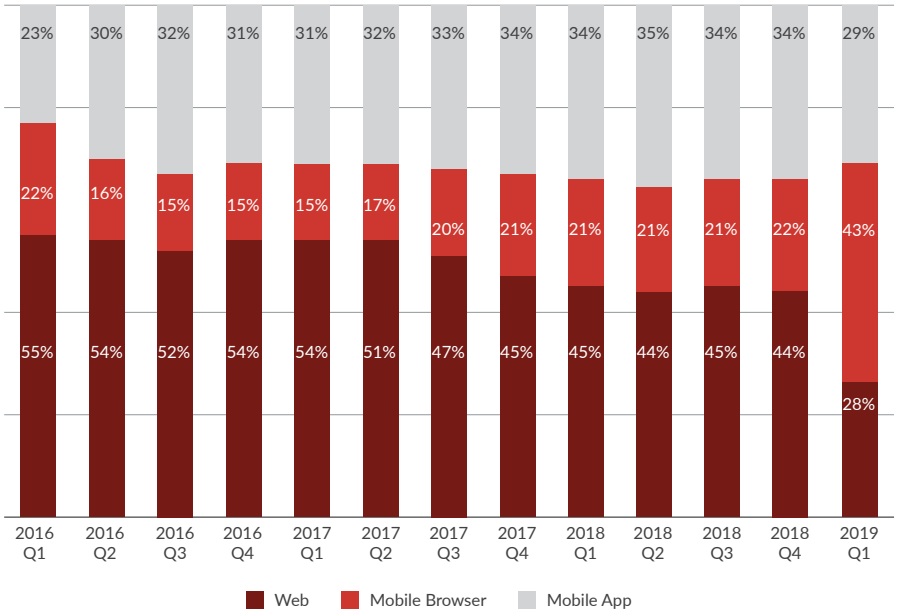
In Q1, we saw China drop from the top ten hosting country list and the UK appeared on the list, although 2 percent of overall phishing attacks were hosted there. The United States remains the top hosting country for phishing attacks.

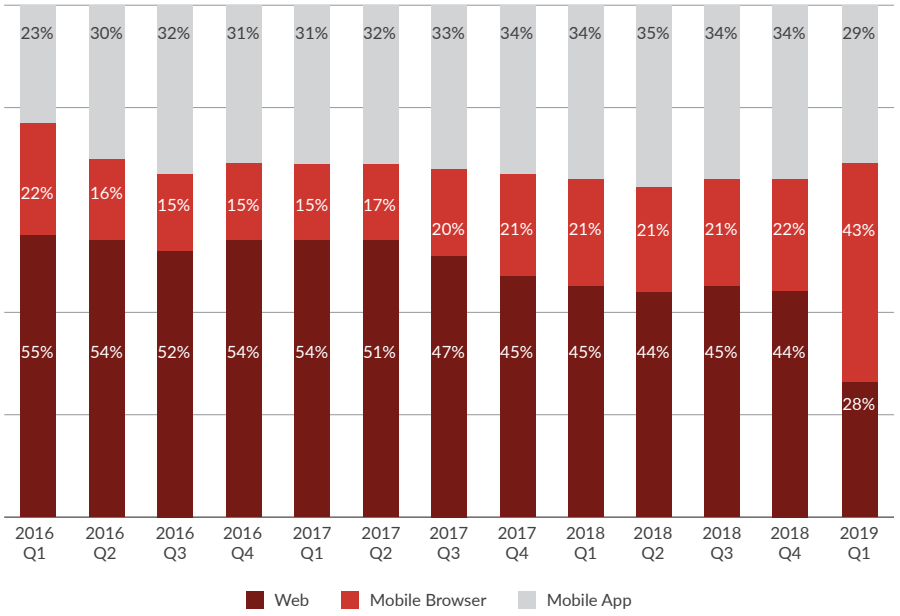
CONSUMER FRAUD TRENDS: Q1 2019

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 digital risk management strategy across customer-facing deployments.

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, January 2016-March 2019

TRANSACTION METHOD

In the first quarter of 2019, mobile browsers and applications accounted for 56 percent of overall transactions observed by RSA, representing no change in channel distribution from the previous quarter. While the mobile channel witnessed significant growth in transaction volume over the past three years, mobile banking adoption has started to level off.

FRAUD TRANSACTION METHOD

In Q1, the overall number of fraudulent financial transactions reported decreased 25 percent, with 72 percent originating in the mobile channel. Fraud from mobile browsers decreased slightly from 49 percent last quarter to 43 percent, while fraud from mobile apps increased slightly from 21 percent to 29 percent. The average value of a fraudulent financial transaction in the mobile channel was $1,058.

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 because 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 Q1, the most drastic difference between the value of genuine and fraud transactions was observed in North America, where the average value of a fraud transaction was $403, nearly double that of a genuine transaction. The average value of a fraud transaction in Australia decreased 31 percent, from $387 last quarter to $267 in Q1.

REGION	TRANSACTION VALUE	FRAUD TRANSACTION VALUE	DIFFERENCE $
European Union	$158	$360	$202
Americas	$213	$403	$190
UK	$178	$217	$39
Australia/New Zealand	$171	$267	$96

Source: RSA Fraud & Risk Intelligence Service, January 2019-March 2019

Device Age vs. Account Age

ANALYSIS

"Device Age" refers to how long the RSA Fraud Platform has "known" or "trusted" a given device (laptop, smartphone, 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

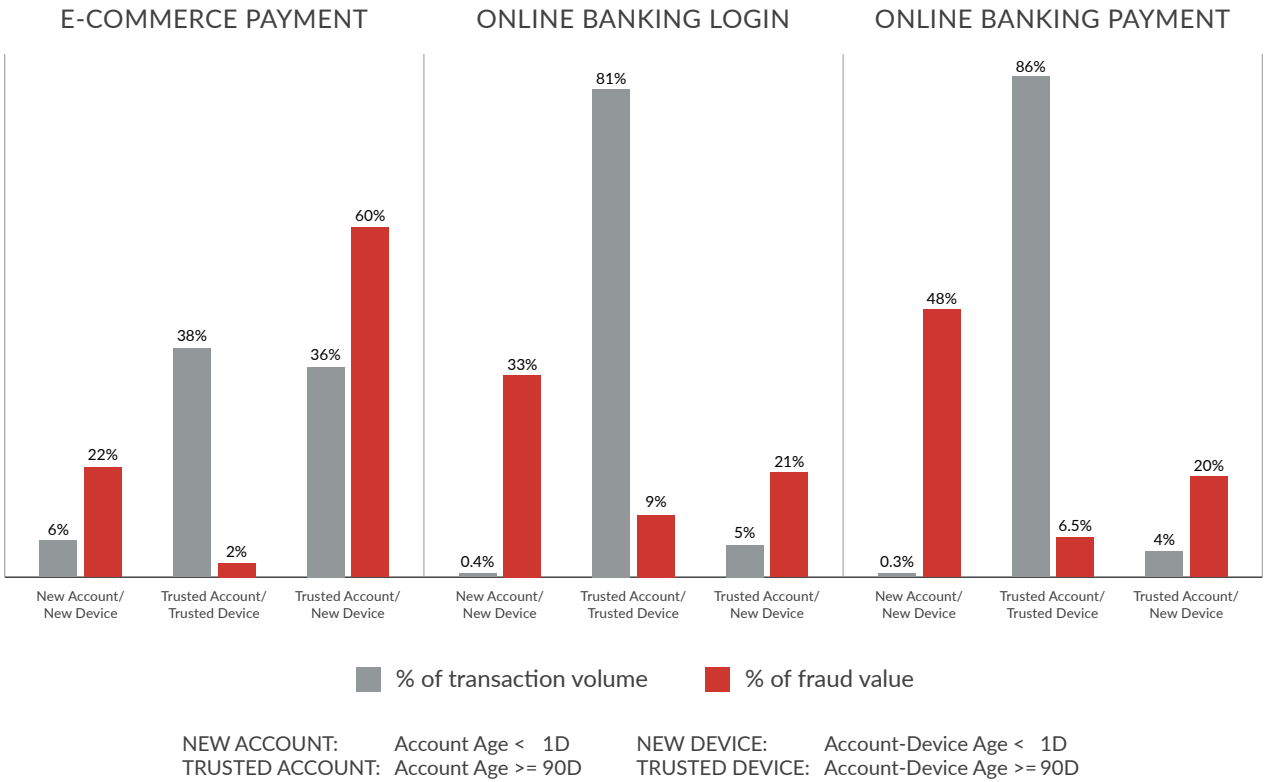
In Q1, RSA saw a 17 percent increase in card-not-present (CNP) fraud transactions. Sixty percent of fraud transaction value originated from a new device but trusted account indicating account takeover activity continues to be a preferred and successful attack vector for cybercriminals.

ONLINE BANKING: LOGIN

While less than 1 percent of logins were attempted from a combination of a new account and new device, this scenario accounted for 32 percent of total fraud volume observed in Q1. This is indicative of fraudsters attempting to leverage stolen identities to create mule accounts as part of the "cash-out" process.

ONLINE BANKING: PAYMENT

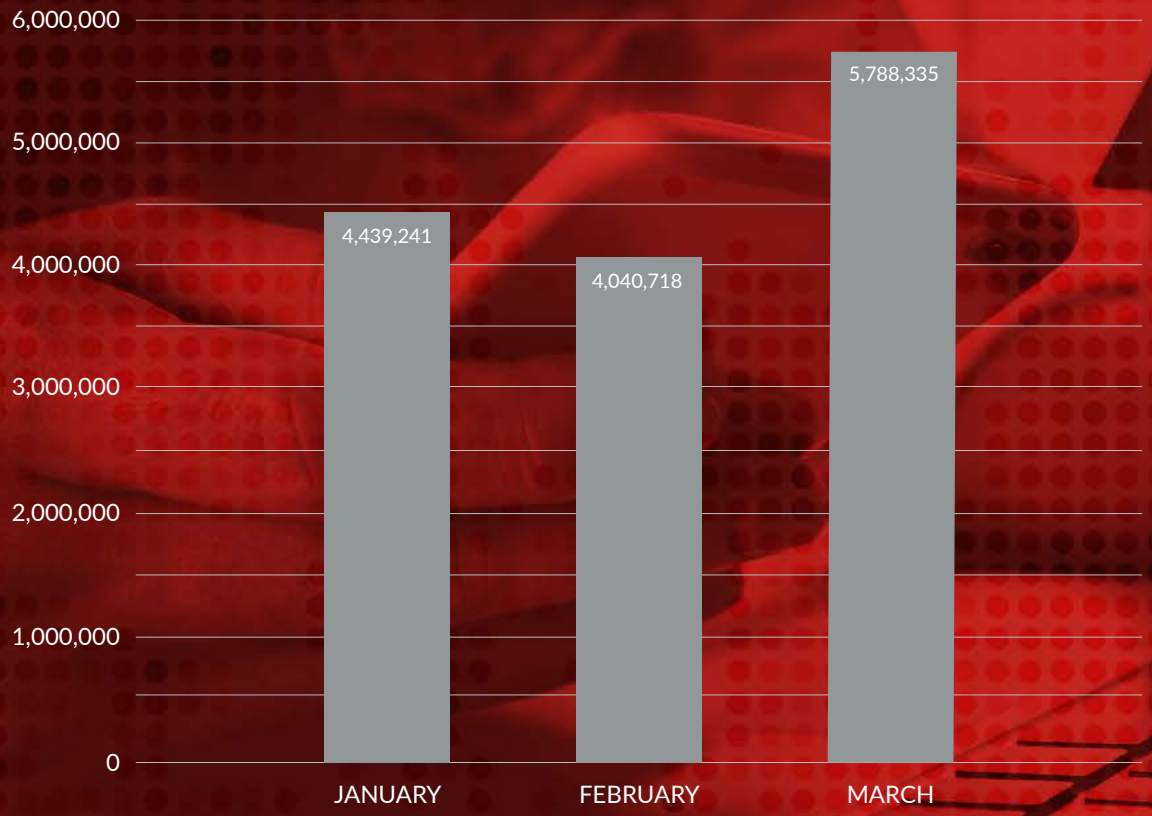
Similar to fraud patterns at login, less than 1 percent of legitimate payment transactions were attempted from a new account and new device, yet it made up 48 percent of total fraud value, a slight increase from 43 percent in Q4. This is indicative of an increase in account takeover where fraudsters 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, January 2019-March 2019

Compromised Credit Cards Discovered/Recovered by RSA



Source: RSA Fraud & Risk Intelligence Service, January 2019-March 2019

ANALYSIS

In Q1 2019, RSA recovered over 14.2 million unique compromised cards and card previews from reliable online fraud stores and other sources. This represents a 33 percent increase in cards recovered by RSA from the previous quarter.

The continued growth of card data for sale in black market storefronts is not surprising. Renowned cybersecurity blogger Brian Krebs recently reported on the growing demand for CNP data in carding markets ("E-Retail Hacks More Lucrative Than Ever, Krebs on Security, April 2019). Ironically, this coincides with the rollout of the first EMV 3D Secure compliance deadlines from the major card networks. RSA observed a 17 percent increase in CNP fraud transactions in Q1, further supporting this trend.

FEATURE ARTICLE

Fraudsters Launch DIY Site to Expand Account Takeover

Account checkers have been around for a long time, but fraud-as-a-service offerings have continued to evolve rapidly in the last couple of years due to the high volume of password breaches. Credential stuffing tools such as Sentry MBA and SNIPR have been popular among fraudsters, however, their use is restricted by the limited availability of pre-built configurations, mostly for large websites. RSA recently identified an online studio for developing account checkers capable of attacking nearly any website. In addition to facilitating the development of new checkers, the site has also created a new source of income for fraudsters as the revenue generated from each checker is split between the site owner and the developer. This has introduced new opportunities for fraudsters to attack organizations not traditionally targeted by account takeover.

ACCOUNT CHECKING OVERVIEW

Account checkers are automated tools used by fraudsters to test username-password combinations and check their validity. Most checkers are relatively simple; they receive a list of credentials in a pre-determined format as their input, then iterate through them to determine which ones work. The more advanced checkers can also receive a list of SOCKS5 proxies to mask their checking activity. Most checkers use the CURL library (a popular code library for interacting with remote servers) for their login attempts and then read the response from the site to determine if the login was successful. In case of success, certain checkers may also retrieve information pertaining to the account, such as the credit card associated with it, billing address, and the orders list.

For years, account checkers were relatively rare as fraudsters focused on exploiting compromised credit cards. The number of credit card checkers, which similarly to account checkers test if a credit card is valid, outgrew the number of

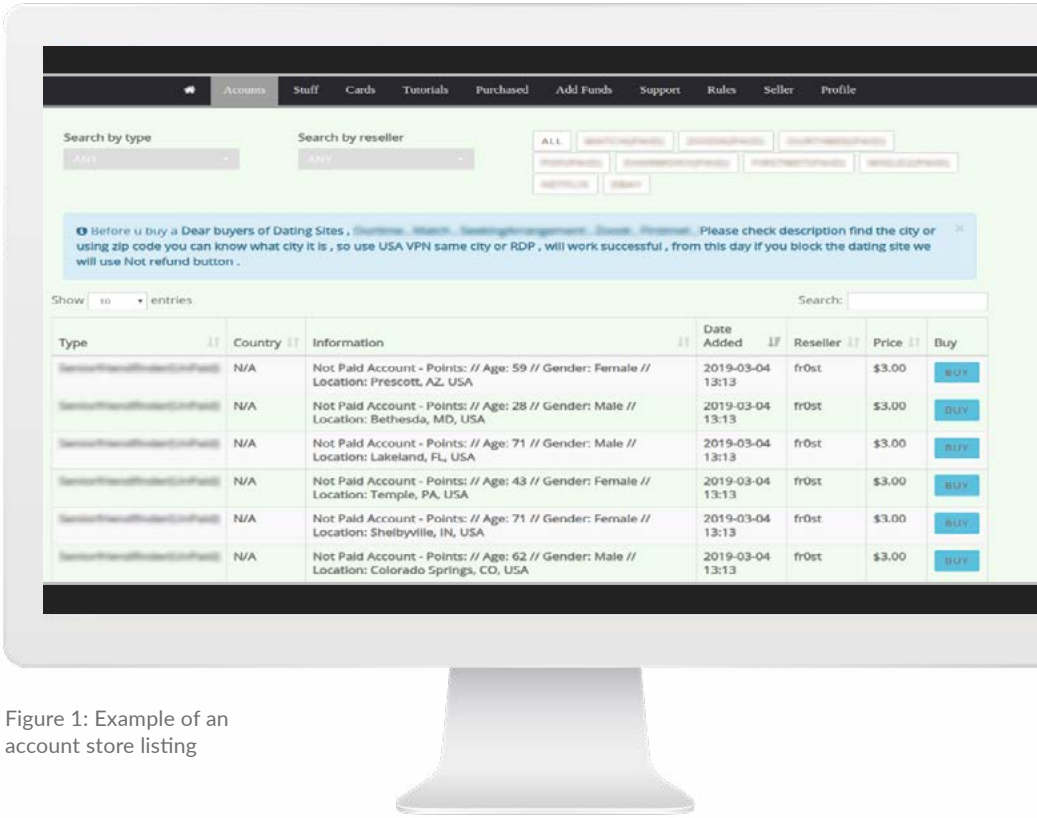


Figure 1: Example of an account store listing

account checkers. The few account checkers that were available focused on very large online services such as eBay and PayPal, which were at the time highly targeted by phishing and other attack methods.

However, in recent years RSA has observed a shift in the underground where more fraudsters are focusing on account takeover. This change can be attributed to several factors. First, advanced security methods deployed by financial institutions has created huge barriers for committing fraud driving less sophisticated criminals to other attack vectors. If in the past a fraudster committed e-commerce fraud by using a compromised credit card and the

"guest checkout" option, today many use account takeover of existing customer accounts in order to reduce the risk of being flagged for fraud. Also, many of the accounts are used as infrastructure for further defrauding individuals and organizations. For example, compromised accounts for dating sites are used for romance scams, while compomrised accounts of registrars and hosting companies are used to set up phishing websites.

Another manifestation of this shift towards account takeover is the growing popularity of account stores. Similar to credit card stores, they are fully automated websites that enable fraudsters to purchase compromised accounts.

ACCOUNT CHECKER STUDIO

Traditional account checking websites offer a list of checkers for hundreds of different websites. While this often includes the largest and most popular websites, their use is restricted by the limited availability of pre-built configurations.

RSA has recently discovered an account checker site that also includes an account studio that enables fraudsters to develop their own checkers for websites that do not already appear in the pool of checkers available. The site splits the income from the checker with its developer, providing an incentive for fraudsters to use the studio and increase the pool's selection.

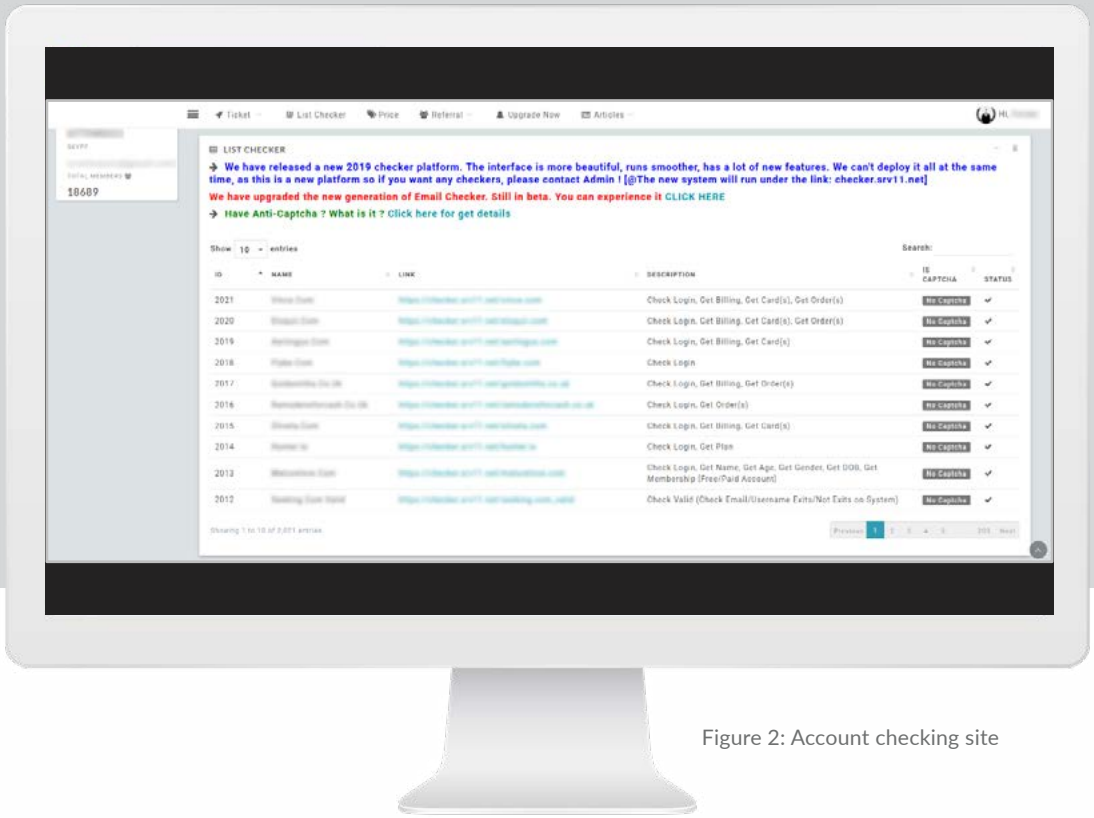


Figure 2: Account checking site

The studio provides a user interface for designing a new checker, enabling the user to define the different steps for checking an account.

The studio provides a user interface for designing a new checker, enabling the user to define the different steps for checking an account. Each step consists of POST and GET page requests that are sent by the browser while communicating with the website. The user can also set up specific headers that are sent with each step in case the website the credentials are being checked against requires them for login.

In addition, the studio allows its users to request custom checkers to be developed, and even grants them credits if their requests are fulfilled.

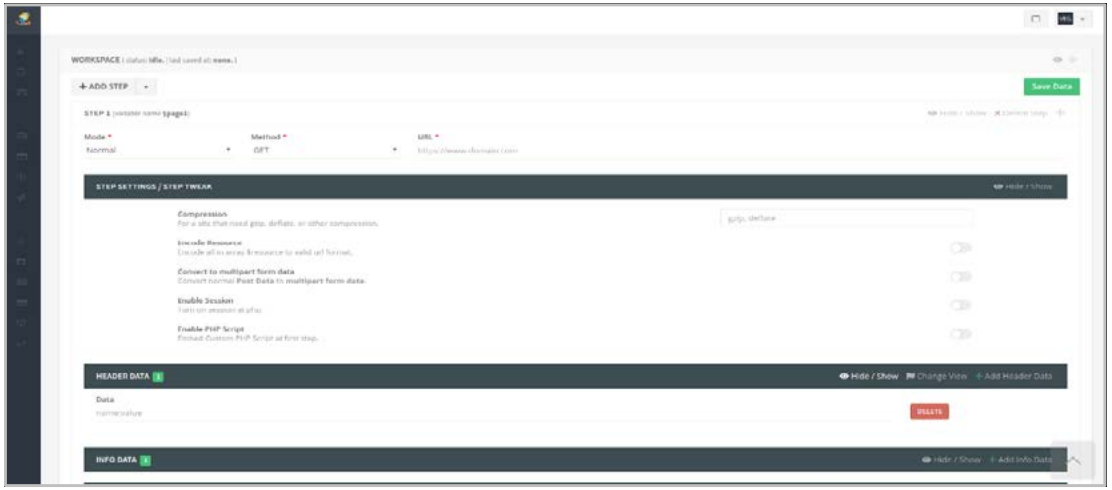


Figure 3: Page request definition

Once the different steps are defined, the checker is ready to be used; it will return TRUE on a valid account and FALSE on an invalid account.

The developers have a designated dashboard on the website through which they can track the performance of their checkers. For example, they can see how many users were exposed to their checker, how many checks were actually performed and how much money they've earned from those account checks.

CONCLUSION

While other account checking sites are limited by the amount of work their operators put in, this new studio opens up the creation of account checkers to the broader fraud community. As a result, the number and diversity of websites that have dedicated checkers available in the dark web has grown exponentially. With over 500 checkers in its pool of websites to choose from currently, RSA expects this number will grow even more as the site gains more popularity. As such, organizations, regardless of size or industry, should expect a growth in automated credential stuffing and account takeover attacks.

It can be difficult to spot automated attacks because legacy tools are not designed or architected to look for them. Account checkers are based on scripts that follow a specific set of page requests, and they generate patterns that may be identified when analyzing activity logs. These patterns can help block subsequent login attempts conducted by the same checker. In addition, since many checkers use proxy servers, these patterns should not be based solely on IP addresses, but rather on specific headers or unique characteristics that may occur during the login process.

The adoption of technologies that leverage behavior analytics can assure authenticated users and anonymous guests are interacting with applications in expected ways. Behavior analytics can identify unusual patterns of behavior across both web and mobile applications – for example, the way a user navigates a site or robotic activity such as thousands of login attempts within only a few minutes.

The old username/password combination is simply no longer sufficient as a form of consumer authentication. The use of multi-factor, adaptive authentication and transaction risk analysis to watch for signs of fraud based on device, user behavior and other indicators is another critical layer to prevent the onslaught of account takeover in the event of a successful login attempt.

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

RSA