RSA BUSINESS-DRIVEN SECURITY™

RSA QUARTERLY FRAUD REPORT

Volume 2, Issue 2
Q2 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 April 1, 2019, and ending June 30, 2019, RSA observed several global fraud trends across attack vectors and digital channels. The highlights include:

Phishing accounted for 37 percent of all fraud attacks observed by RSA in Q2. Overall, phishing volume has increased 6 percent since last year.

While Canada remained the top targeted country in Q2, overall attack volume decreased 33 percent from last quarter. However, India and South Africa saw a significant increase in overall attack volume. Quarter over quarter, phishing attacks targeting India increased 54 percent while attacks targeting South Africa increased almost 200 percent.

Fraud attacks from rogue mobile applications increased 191 percent in the first half of 2019.

Fraud attacks introducing financial malware increased 80 percent in the first half of 2019.

Forty-seven percent of card-not-present (CNP) fraud transactions originated from the mobile channel. The average value of a CNP fraud transaction in the U.S. was $352, nearly 50 percent higher than that of an average genuine transaction of $220.

RSA recovered over 6.8 million unique compromised cards in Q2. This is a significant decrease from the previous quarter, but not surprising as there tends to be a large increase in carding activity right before and after the winter holidays.

FEATURE ARTICLE

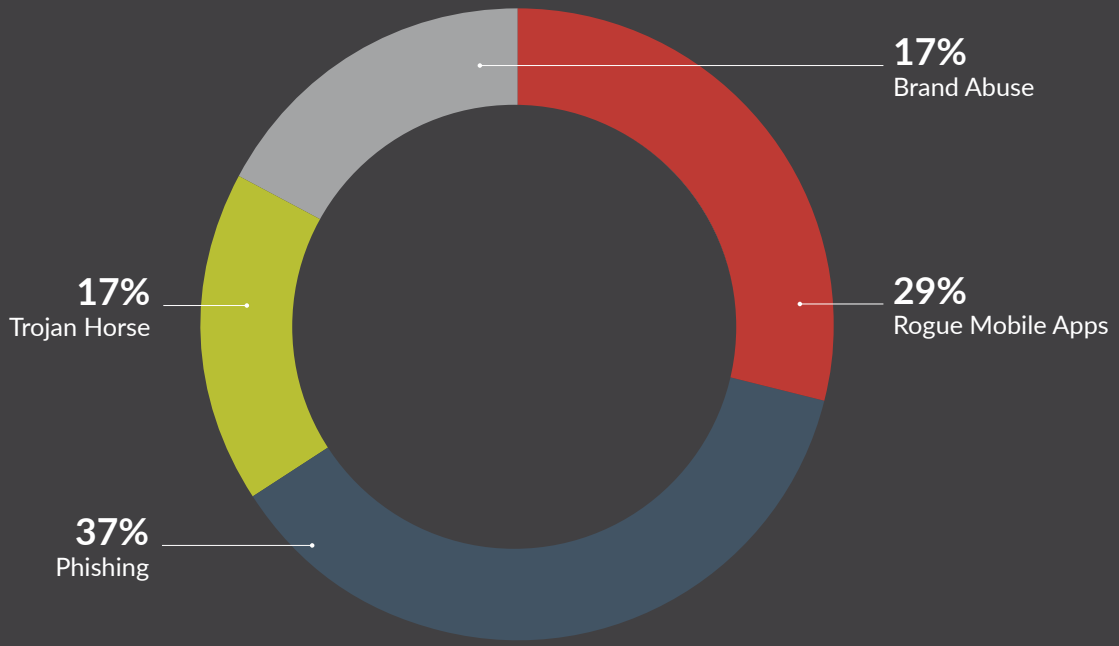
Ramnit Malware Makes a Return with New Tricks

Fraudsters don't always have to create new malware from scratch; they can just bring back old strains in the form of new variations, changing how they work and how they are delivered. Ramnit is a great example of how fraudsters can adapt malware over long periods to pose an increasingly sophisticated threat, as well as to circumvent defenses that have been put up to fight it. This article explores the evolution of Ramnit and its recent changes in functionality, targets and methods of distribution.

FRAUD ATTACK TRENDS: Q2 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: Q2 2019

Fraud Attack Type Distribution

In the second quarter of 2019, RSA identified 57,406 total fraud attacks worldwide. RSA detected 21,389 phishing attacks, representing 37 percent of all fraud attacks identified and a 10 percent decrease from last quarter. Fraud and brand abuse attacks on social media represented 17 percent of all fraud attacks in Q2 and increased 34 percent from last quarter, from 7,348 in Q1 to 9,882 in Q2.

The total number of global fraud attacks detected by RSA increased 63 percent in 1H 2019 as compared to 2H 2018. The breakdown, by attack type, for the first half of the year is listed below:

Phishing	Social Media Attacks	Financial Malware	Rogue Mobile Apps
6%	37%	80%	191%

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.

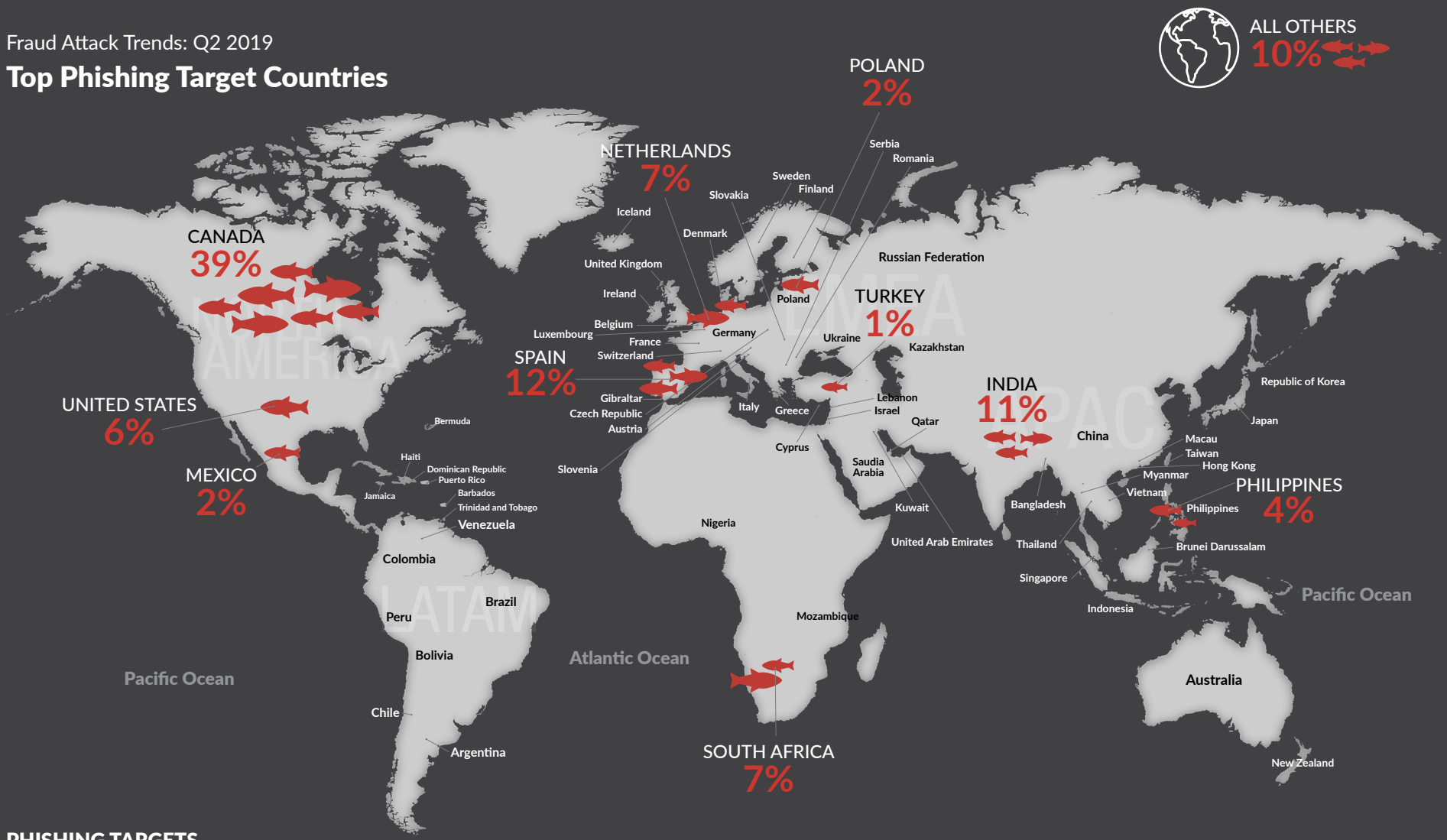
IN THE FIRST HALF OF 2019,
Fraud attacks increased

80%

FROM FINANCIAL MALWARE

Fraud Attack Trends: Q2 2019

Top Phishing Target Countries



PHISHING TARGETS

Canada, Spain and India were the top three countries targeted by phishing, representing 61 percent of total attack volume. Poland appeared on the list replacing Turkey as a top target with 2 percent of total phishing volume in Q2.

While Canada remained the top targeted country in Q2, overall attack volume decreased 33 percent from Q1. However, India and South Africa saw a significant increase in overall attack volume. Phishing attacks targeting India increased 54 percent while attacks targeting South Africa increased almost 200 percent in Q2.

Top Phishing Hosting Countries

HOSTING COUNTRIES

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

PHISHING HOSTS

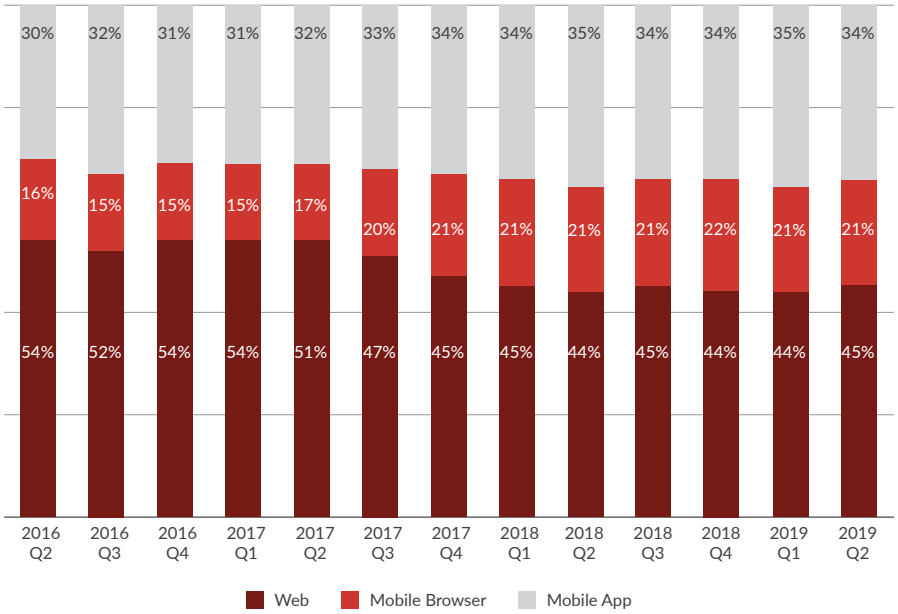
In Q2, we saw Poland drop from the top 10 hosting country list and Australia appeared on the list, hosting slightly more than 3 percent of overall phishing attacks. The United States remains the top hosting country for phishing attacks.

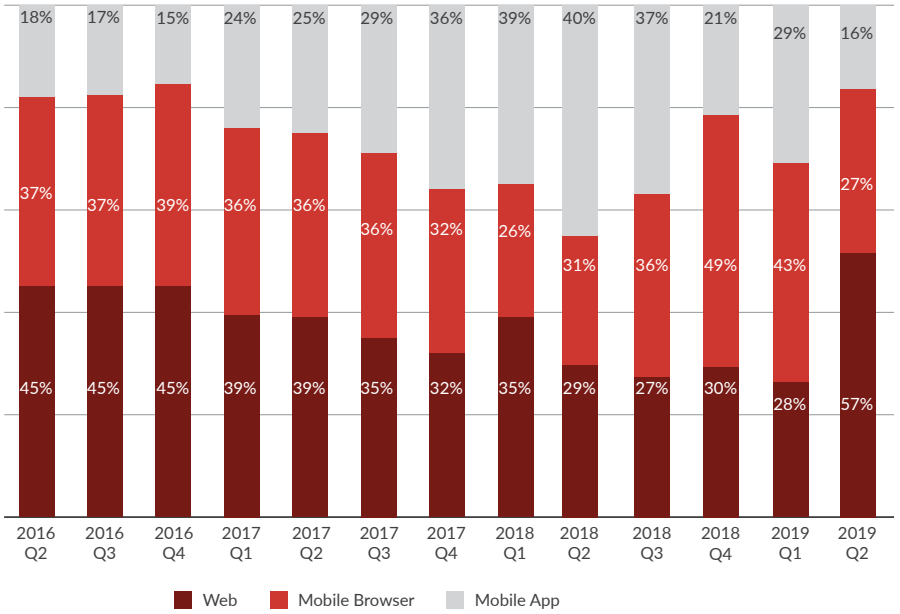
CONSUMER FRAUD TRENDS: Q2 2019

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, April 2019-June 2019

TRANSACTION METHOD

In the first quarter of 2019, mobile browsers and applications accounted for 55 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.

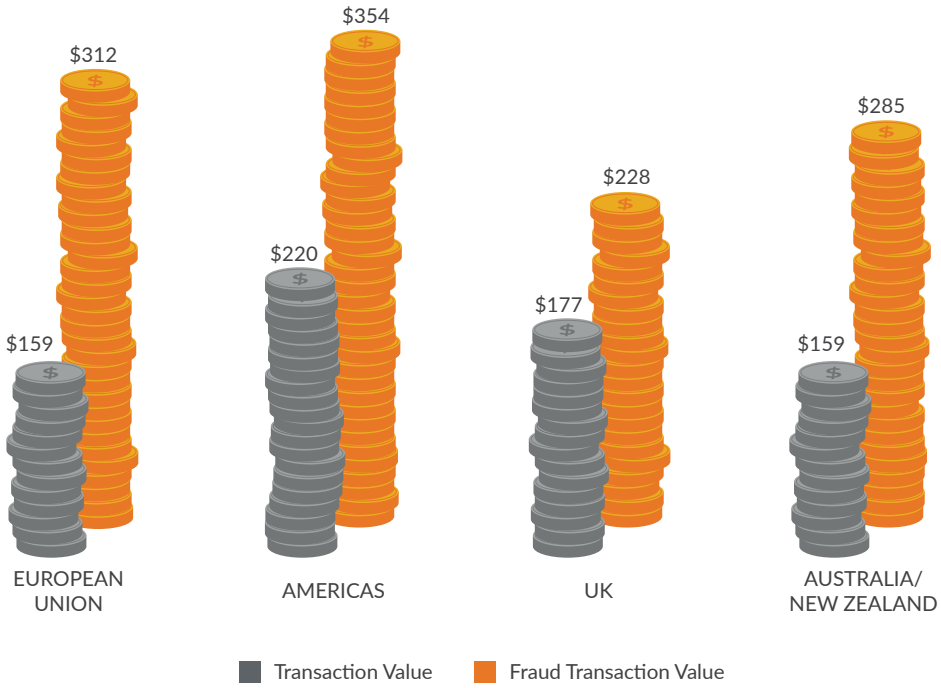
FRAUD TRANSACTION METHOD

In Q2, there was a significant shift in fraud transactions across channels. In Q2, only 43 percent of fraud transactions originated in the mobile channel compared to 72 percent in the previous quarter. Fraud in the web channel increased significantly from 28 percent to 57 percent in Q2. This is the first time in three years that fraud in the web channel outpaced the mobile channel. RSA will continue to monitor this to see if it is simply an anomaly or an ongoing trend.

The average value of a fraudulent financial transaction in the mobile channel was $735.

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 Q2, the most drastic difference between the value of genuine and fraud transactions was observed in Europe, where the average value of a fraud transaction was $312, nearly double that of a genuine transaction. In the UK, for the last several quarters, there has been little difference in the average value of a genuine vs. fraudulent transaction as compared to other regions.

REGION	TRANSACTION VALUE	FRAUD TRANSACTION VALUE	DIFFERENCE $
European Union	$159	$312	$153
Americas	$220	$344	$124
UK	$177	$228	$51
Australia/New Zealand	$159	$285	$126

Source: RSA Fraud & Risk Intelligence Service, April 2019-June 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

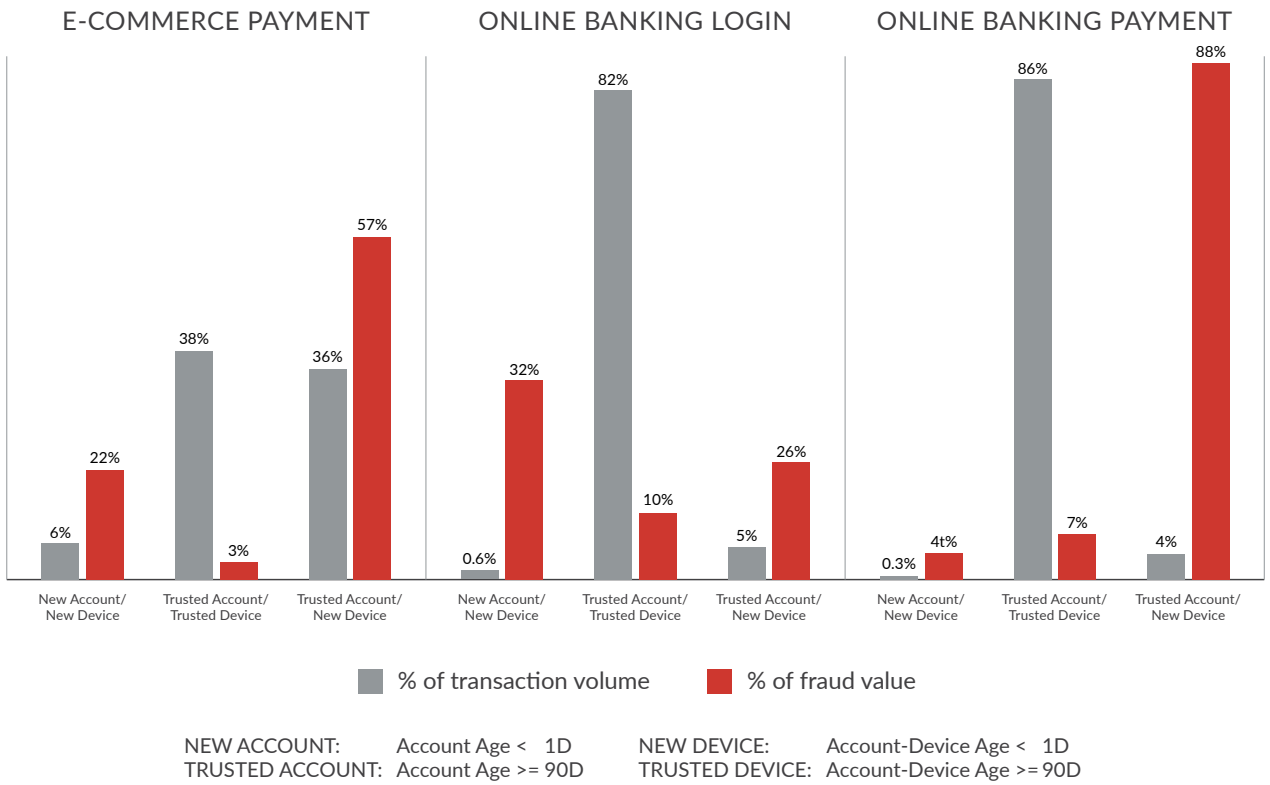
In Q2, 57 percent of fraud transaction value originated from a new device but trusted account, indicating account takeover activity continues to be a preferred and successful attack vector for cybercriminals.

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 Q2. This is indicative of the creation of mule accounts to be used as part of the "cash out" process.

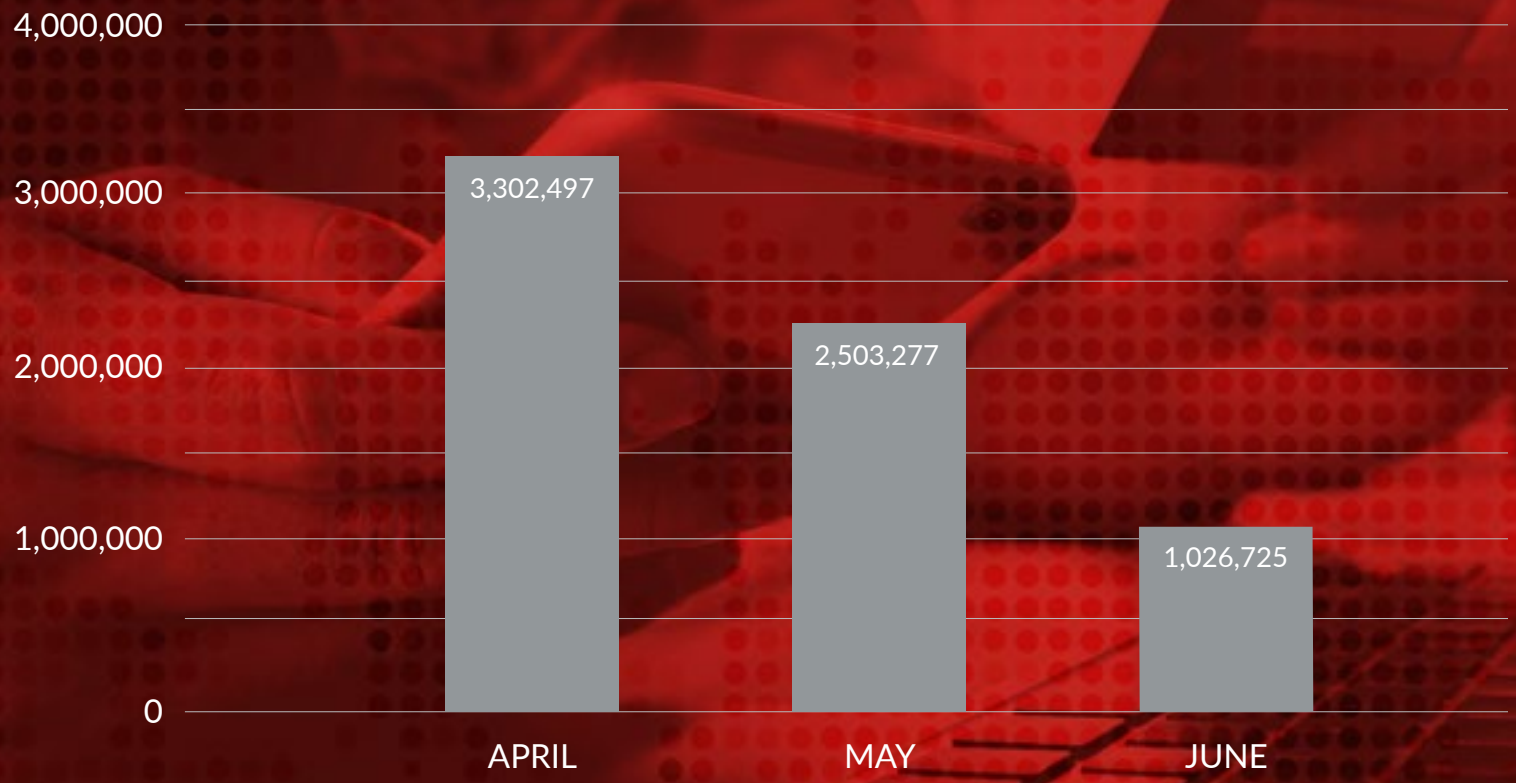
ONLINE BANKING: PAYMENT

In Q2, 88 percent of payment fraud attempts originated from a trusted account and new device, a significant increase from only 20 percent last quarter. This is indicative of a flood of recent account takeover attacks where fraudsters are attempting to use compromised financial information to initiate payments from victims' accounts. It also highlights the importance of a layered fraud prevention approach, specifically the use of risk-based transaction monitoring solutions that are capable of identifying fraud attempts beyond login and at the point of transfer.



Source: RSA Fraud & Risk Intelligence Service, April 2019-June 2019

Compromised Credit Cards Discovered/Recovered by RSA



Source: RSA Fraud & Risk Intelligence Service, April 2019-June 2019

ANALYSIS

In Q2 2019, RSA recovered over 6.8 million unique compromised cards and card previews from reliable online fraud stores and other sources. This represents a 52 percent decrease in cards recovered by RSA from the previous quarter.

The significant decrease in stolen cards for sale in fraud forums is not surprising for this time of year. It is typical to see an increase in card fraud leading up to and following the holiday shopping season.

FEATURE ARTICLE

Ramnit isn't the only malware to evolve and adapt to exploit current trends, and it won't be the last.

Ramnit Malware Makes a Return with New Tricks

RSA threat analysts saw financial malware attacks increase 80 percent in the first half of 2019, and one of the culprits turns out to be an old favorite for fraudsters: the Ramnit Trojan. First detected in 2010, this banking Trojan has reappeared in new guises every few years to target financial institutions and their customers. Europol led a coordinated takedown effort in Europe in 2015, but Ramnit developers have continued to evolve its capabilities since that time.

Fraudsters don't always have to create new malware from scratch; they can just bring back old strains in the form of new variations, changing how they work and how they are delivered. Ramnit is a great example of how fraudsters can adapt malware over long periods to pose an increasingly sophisticated threat, as well as to circumvent defenses that have been put up to fight it.

RAMNIT TROJAN TODAY: WHAT, WHO, HOW

Ramnit was originally designed to attack bank accounts by infecting PCs and using them as proxy servers for malicious activity, but analysts in the RSA Anti-Fraud Command Center have recently detected several major changes in what Ramnit does, who it targets and how it spreads.

- **What it does:** Previously, Ramnit operated as a botnet, infecting computers, turning them into bots and using them to spread itself to other computers. But based on RSA-observed activity in the last year, the malware's current objective is to steal credentials via web injects that trick people into providing confidential information.
- **Who it targets:** While Ramnit is best known for focusing on the banking industry in North America and Europe, RSA has recently seen it targeting Japanese entities.
- **How it spreads:** Ramnit was originally distributed using worm capabilities, but it is now distributed via executable files that are downloaded and executed by an unwitting user. RSA has specifically found it distributed by malspam (malware spam via email), with victims downloading it by, for example, clicking on an ad on an insecure website.

A DEEPER DIVE INTO RAMNIT'S MODE OF OPERATION

According to findings of the RSA Anti-Fraud Command Center, Ramnit steals credentials via web injects by running an executable file containing concealed malicious code. When executed by the unsuspecting victim, the file creates new processes into which a set of core modules is injected to send information to a remote command and control (C&C) server. Among those core modules is one that downloads browser injections containing JavaScript code and a list of target websites. These browser injections introduce JavaScript or HTML code into the target websites, with the goal of manipulating the webpage to steal credentials or other sensitive information. Ramnit then uses a second C&C server to receive and store the stolen data.

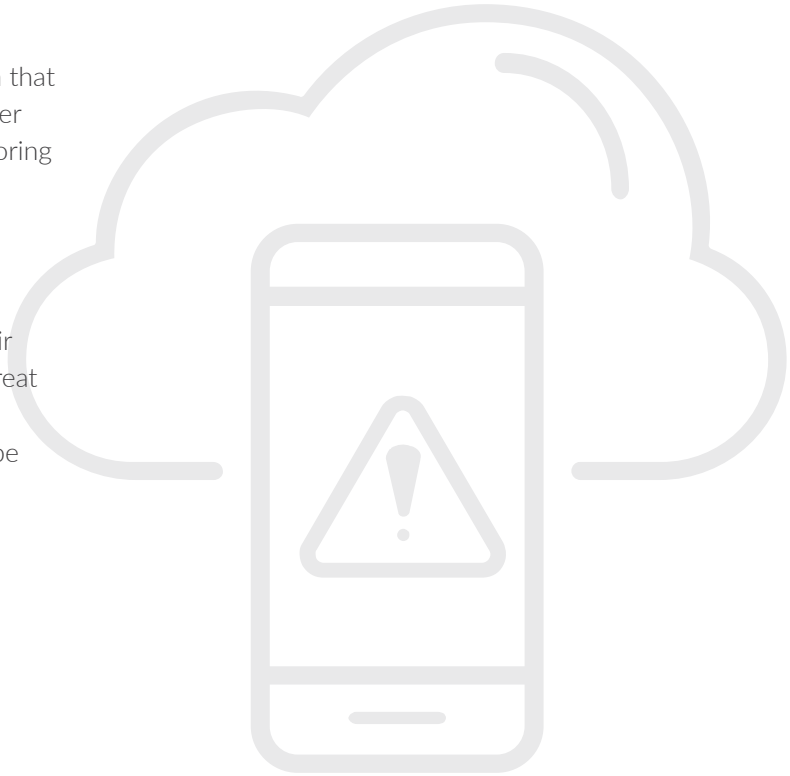
NEW SIGNS OF FRAUDSTER COOPERATION AND COLLABORATION

It isn't only the behavior of Ramnit that has changed recently; it's also the behavior of the Ramnit developers. At a time when more and more fraudsters are taking advantage of an as-a-service model for carrying out cyber attacks, the group behind Ramnit has always operated outside that model. They solely own and control the malware and have not made its source code available as a service—enabling them to tightly control distribution and targets. But could that be changing?

The answer may lie in a recent cooperative effort involving Ramnit and AZORult, a widespread, commonly used malware family. The cooperative activity consists of AZORult downloading Ramnit and then Ramnit, in turn, providing the ability to install other malware on infected machines. The cooperation both improves distribution and makes it possible to fine-tune the malware to meet specific fraudster goals.

While the cooperation between Ramnit and AZORult may make it easier to spread Ramnit, it does not mean that Ramnit has become a commercialized malware at this point. All indications are that its campaigns remain controlled by the same closed gang that has always controlled it. Nor does it mean that Ramnit is about to become commercialized. Nevertheless, the appearance of cooperation with another group after nearly a decade of independent operation is worth noting and warrants continued monitoring to see what else, if anything, develops.

The appearance of cooperation with another group after nearly a decade of independent operation is worth noting and warrants continued monitoring to see what else, if anything, develops.



CONCLUSION

Ramnit isn't the only malware to evolve and adapt to exploit current trends, and it won't be the last. Remember, it wasn't that long ago that RSA saw fraudsters turning to Telegram bots to automate their efforts and distributing BankBot malware via rogue WhatsApp apps. Similarly, Ramnit has posed a threat for nearly a decade by constantly shifting its attention to new targets and means of attack that seem promising. Combating malware that has survived by continually evolving requires that organizations be just as proactive and determined in their own efforts to fight back.

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