FraudAction™ Anti-Fraud Services

RSA

Q3 2017 NEWSLETTER

TABLE OF CONTENTS

Note: Figures and statistics in this report are based on data collected by RSA's Anti-Fraud Command Center (AFCC) in its 24x7x365 battle against phishing and cyber fraud.

RSA

INTRODUCTION

In this issue of the **FraudAction Quarterly Newsletter**, our highlight story focuses on TrickBot's web-injection mechanism. Our quarterly global detection statistics are presented in the **Malware Variants** and **Phishing Attacks** section.

In Case You Missed It lists the reports that were sent out over the last few months, so that you can look up reports that you may have missed. We also have a roundup of FraudAction Webinars You May Have Missed.

Are you familiar with **FraudAction Cyber Intelligence**?

RSA FraudAction Cyber Intelligence (FACI) is a service that provides targeted research and reports on a wide range of cybercrime attacks that facilitate identity theft, emerging threats and fraud trends.

The FraudAction Cyber Intelligence team continuously observes cybercrime threat sources to gather intelligence and deliver it to your organization. Monitoring open-source and closed deep web sources, RSA diligently analyzes intelligence picked up by our sensors and reports it in a swift, easily consumable fashion. With years of experience in the intelligence space, RSA's researchers often directly engage with cybercriminals to uncover further information about specific methods of operation and reveal emerging attack tactics. FACI offers:

- Intelligence on a wide range of underground services that facilitate identity theft and cybercrime, identifying emerging threats and fraud trends.
- Identifying cash out and cross-channel exploits targeting your organization(s) worldwide.
- Uncovering mule accounts and items drops.
- Revealing underground stores selling compromised online banking and payment card accounts.
- Enabling coordination of sting operations to reveal infrastructure sources used by cybercriminals to launch attacks.

Integrating intelligence feeds into Web Threat Detection (WTD) - our intelligence team has made great efforts to improve efficiency and visibility in the detection of a number of crucial fraud activities and indicators, providing them as automated monthly feeds. Now, the FraudAction Intelligence feeds can be easily integrated into the Web Threat Detection analysis server and drive enhanced detection of threats to your organization.

RSA FraudAction 360 offers a complete threat management service that provides proactive detection and mitigation of cyber threats such as phishing, Trojans and mobile rogue apps. Additionally, customers can gain deeper insight into emerging threats with intelligence reports and data feeds that provide deep visibility into the cybercrime underground. The service includes:

- Threat Detection and Alerts: Proactively preventing fraud attempts through early attack detection and real-time alerts identified via a broad partner network and active scanning of tens of millions of URLs.
- Mitigation and Site Shutdown: Reducing the financial impact of cyber threats through rapid shutdown of infection points, command and control sites, and drop zones worldwide.
- Forensics and Credential Recovery: Extensive forensic analysis provides organizations with additional intelligence insights including compromised personal information, email drop accounts, and specific IP information showing where an attack was launched.
- FraudAction Blocking Network. Preventing and blocking access to identified phishing sites and malware infection, drop, and update points.

To keep up with the latest developments and discoveries, follow us on Twitter: @rsafraud
and explore our new re-launched website: rsa.com/en-us/products-services/fraud-prevention

HIGHLIGHT STORY: TRICKBOT SAMPLES UTILIZING WEB INJECTION MECHANISM

INTRODUCTION

Last month, RSA's Anti-Trojan operation released a report on TrickBot following a significant increase in attack volumes targeting our customers. Classified as a Banker Trojan, TrickBot is a modular malware that has the ability to download additional modules and introduce new abilities over time. As such, our analysts have continued to track this Trojan family closely and brings to you their additional findings herein.

TrickBot volumes continue to increase, as can be observed in the Trojan segment below 'Global Distribution of Trojan Families', and several variants have exhibited additional features as part of their modus operandi.

Analysis of recent TrickBot variants revealed the use of a web-injection mechanism by which new pages, located on the Trojan's communication points, were established during the deployment process. This mechanism was inherited from Dyreza, TrickBot's predecessor, and operates in a similar manner.

WEB INJECTIONS

TrickBot utilizes DLL modules, typically named "injectDll64" or "injectDll32" (depending on the OS architecture) which manipulate the browser's behavior according to settings in its configuration files. These are XML files that contain lists of predefined triggers - URL patterns that trigger specific behavior such as stealing data and injecting customized web pages.
The web injections are used in order to extract additional information that is not requested as part of the bank's standard online login process, for example mother's maiden name and bank account number.
In addition to the triggers, a list of C&C (command & control) URLs is included in the configuration files and are used to collect compromised data, send to the compromised machine modified server responses intercepted by TrickBot, etc.

INJECTDLL CONFIGURATION FILES

Generally, the injectDLL uses 3 configuration files; dpost, dinj and sinj.

dpost collects generic data such as saved passwords and cookies from browsers and sends it back to the communication point configured in dpost.

dinj is activated once a trigger is identified and captures the browsing data including HTTP headers, cookies and HTML source code that was sent to the legitimate page and returned from it. It then sends it back to the victim with additional or modified data. In the cases observed by our fraud analysts, this additional data often comes in the form of a JavaScript code at the bottom of the HTML source code which allows content manipulation. The dinj C&C/drop typically ends with the string "response.php".

sinj, in a similar manner to dinj, is also activated once a trigger is identified and monitors the traffic adding web-injects according to commands from the C&C.
When browsing to URLs that appear in the trigger list defined in the sinj file, the malware will add **"/!/ping"** at the end of the URL path in the browser's address bar.
At this stage, the user may receive 404 errors which should raise suspicion in the context of an online banking session.
In reality, these requests are sent to a drop/C&C URL structured as **https://xxx.xxx.xxx.xxx/!/ping** (returns a 500 error if accessed directly), however the end-user will see **https://xxx.xxx.xxx.xxx/** in the browser.

When the user submits login credentials, the data is sent to **https://xxx.xxx.xxx.xxx/!?new=1**.
This action prompts the C&C for further commands while the user is stalled with a "**Please wait...**" message instead of showing the legitimate site's authentic response.

While the web-inject page is presented by TrickBot, behind the scenes there is a communication to **https://xxx.xxx.xxx.xxx/!/#####** (**"#####"** representing a 5-digit number). This URL can be directly accessed through the C&C. Usually, the drop/C&C URL comes in form of an IP address with a designated port, for example: 195.133.147.102:443.

Following are the different suffixes added to the sinj C&C URL (https://xxx.xxx.xxx.xxx) and their respective commands:

URL suffix	Commands
/!/ping	Beacon back to C&C
/!?new=1	Detect data submission to the legitimate URL and return additional commands/data if needed
/!/go_skip?time=300	Redirect the user to the legitimate site for login, while suspending traffic manipulation for 300 seconds
/!/#####	Inject web pages
/#####	Provide additional resources for web-injects mentioned above such as CSS, JavaScript files, etc

CONCLUSION

Consumer education is a key factor in the mitigation of cyber-attacks. End-users should be cautious of any out-of-the-ordinary behavior during their online banking sessions, such as 404 errors, delays or abnormal additional information requested.

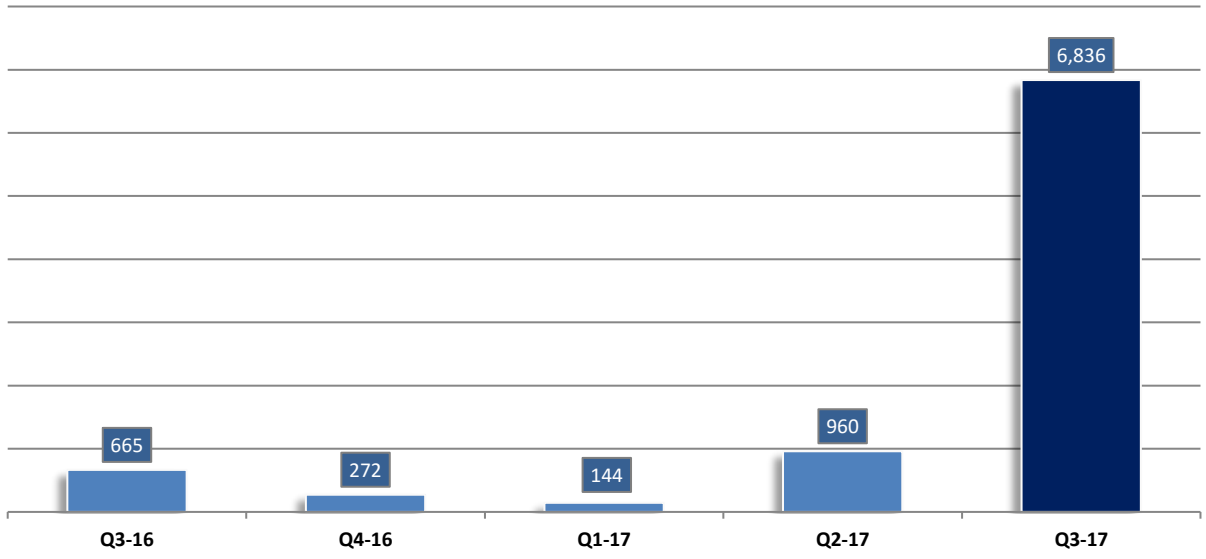
RSA's anti-fraud command center commences shutdown on Trojan's communication channels in order to prevent further infections and data leak. Affected organizations subscribed to RSA's anti-Trojan service receive are alerted when targeted by TrickBot or any other banking malware monitored by FraudAction.

MALWARE STATISTICS

The following charts map out the global Trojan malware activity recorded by RSA over the last five quarters.

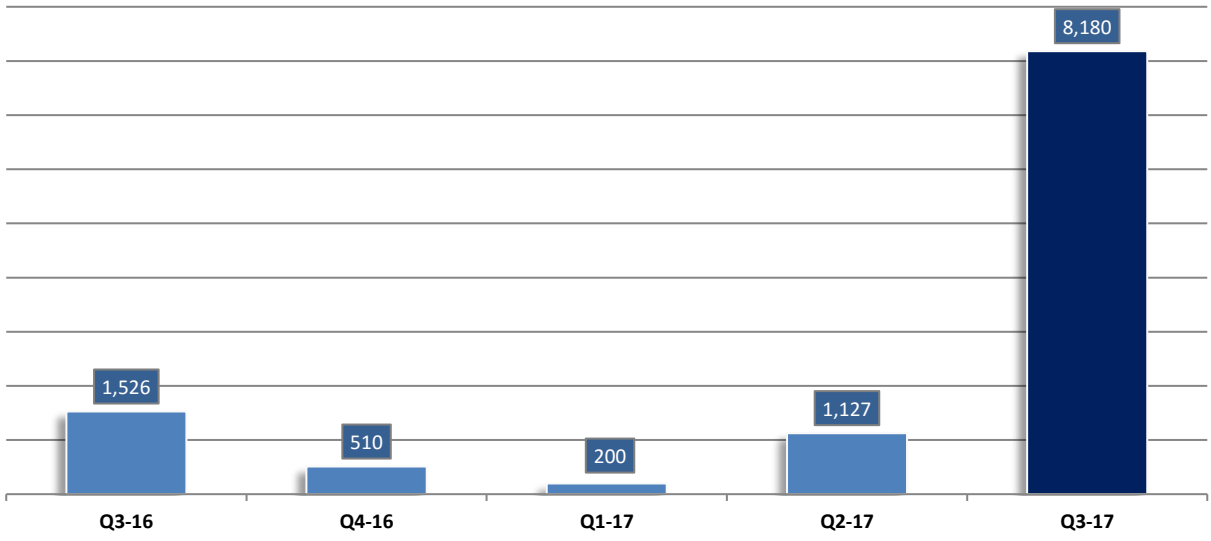
VARIANTS PER QUARTER

The graph below shows the count of unique banking Trojan variants detected by RSA over time.



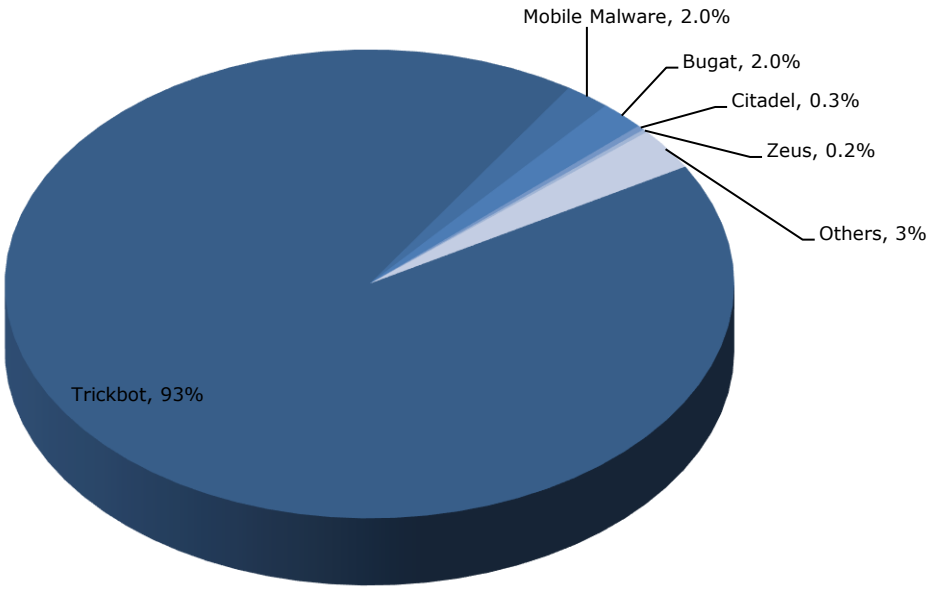
UNIQUE TROJAN COMMUNICATION POINTS - URLS PER QUARTER

A count of communication points (URLs) used for *infection*, *update* or as *drop points* in Trojan attacks worldwide. Each Trojan attack may use multiple communication points, therefore, the number of unique Trojan-related communication points will always be *significantly higher* than the number of unique variants detected.



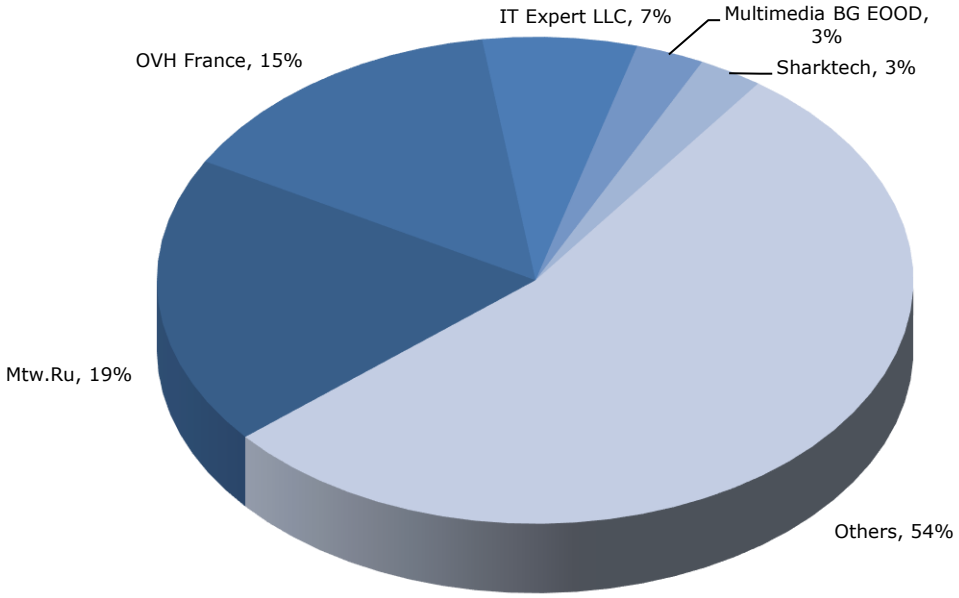
GLOBAL DISTRIBUTION OF TROJAN FAMILIES

The chart below shows the distribution of various Trojan families responsible for attacks on entities worldwide in the reported quarter, as detected by the RSA Anti-Fraud Command Center (AFCC).



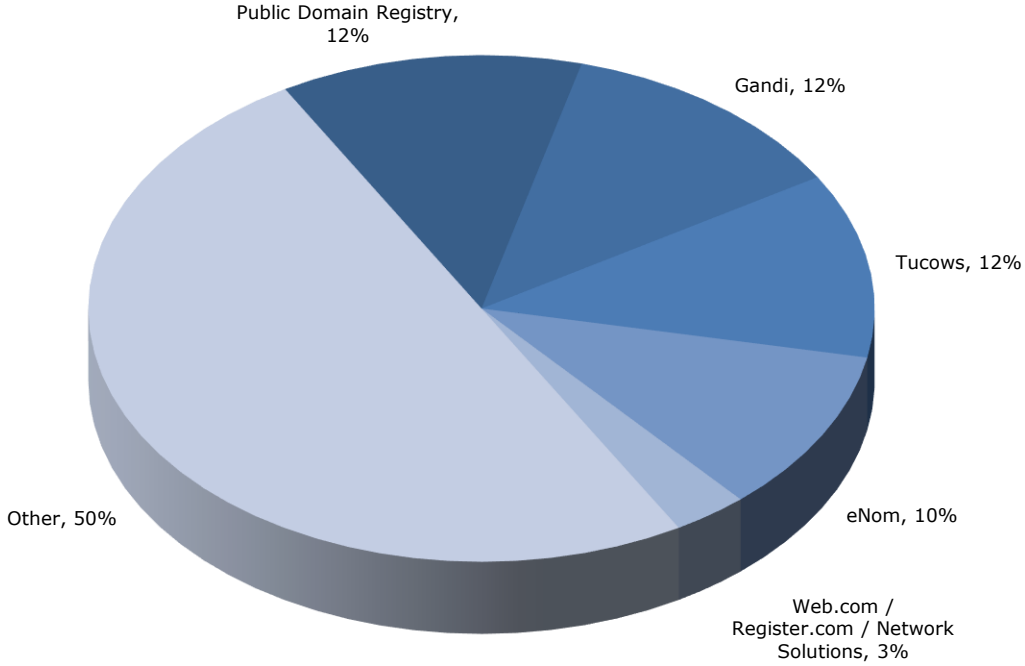
TOP TROJAN-HOSTING ISP

The chart below shows a proportional view of the ISPs to have hosted the largest number of Trojan communication resources in **Q3 2017**.



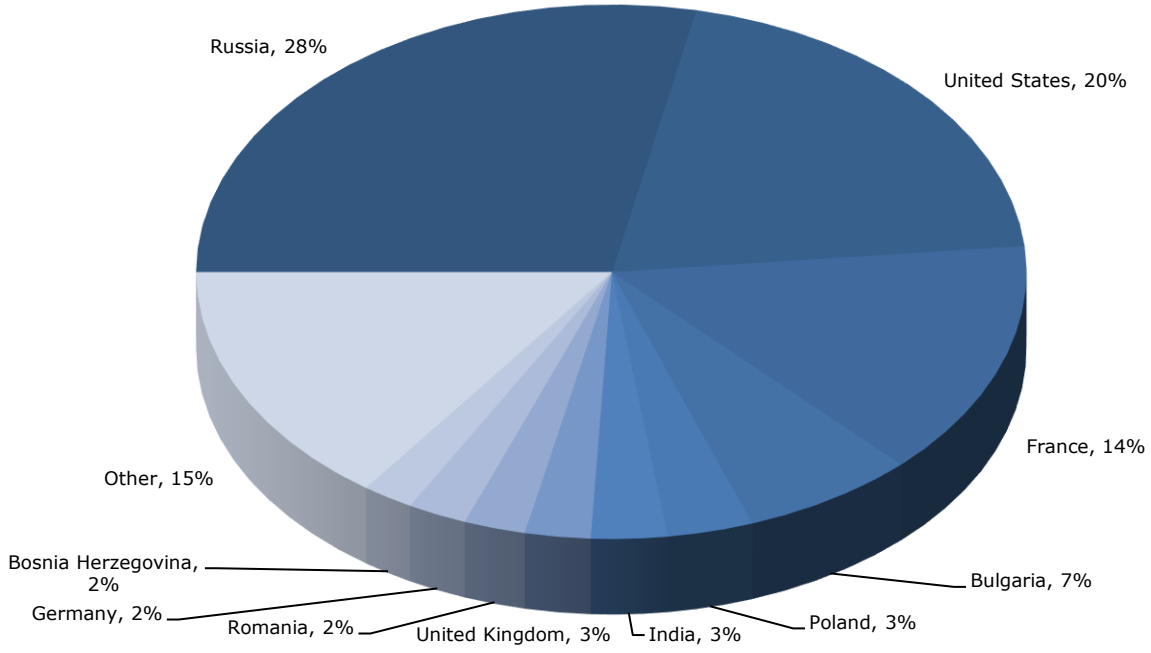
TOP REGISTRARS OF TROJAN DOMAINS

The chart below shows a proportional view of the registrars with which the largest numbers of Trojan communication domains were registered through **Q3 2017**. Trojan botmasters normally purchase one or more domains to host their communication resources.



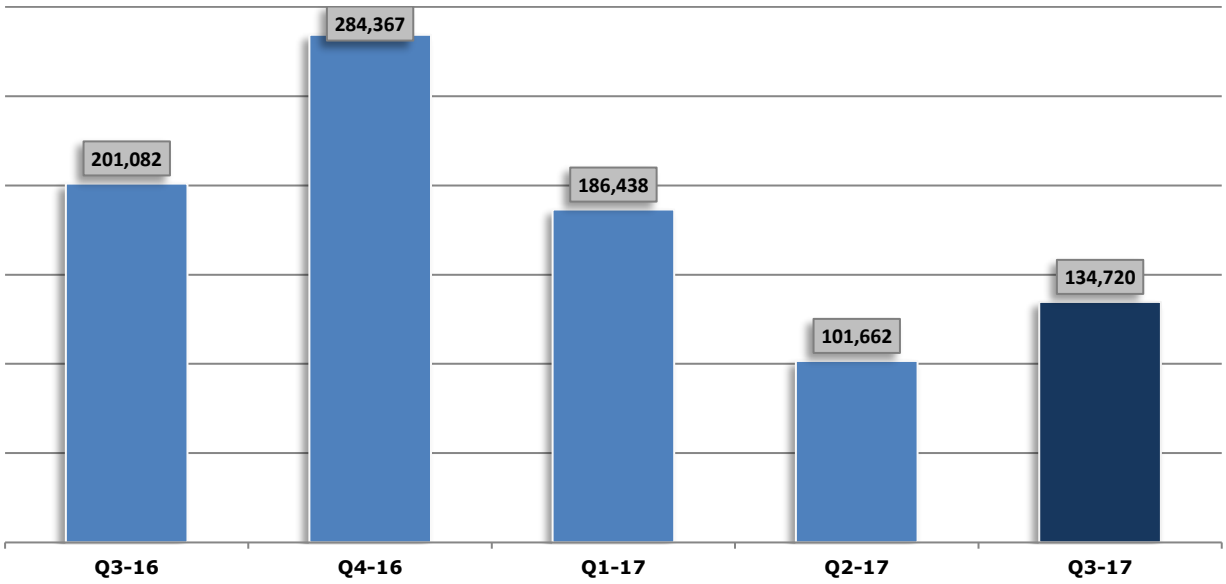
TOP TROJAN-HOSTING COUNTRIES

The chart below shows a proportional view of the ISPs to have hosted the largest number of Trojan communication resources through **Q3 2017**.

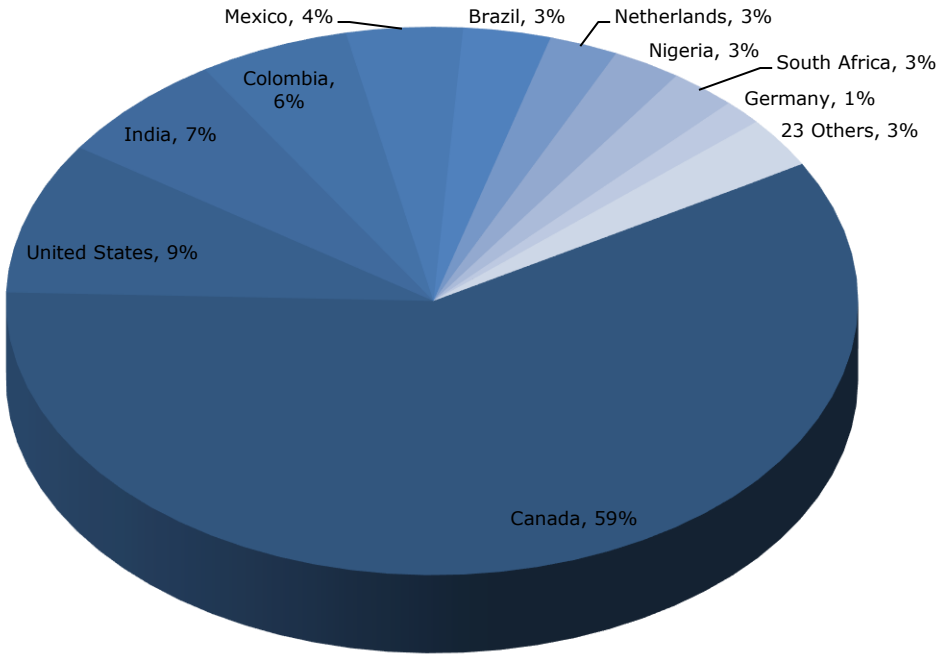


PHISHING STATISTICS

In **Q3** of **2017**, RSA recorded a total of 134,720 Phishing attacks in the global market.

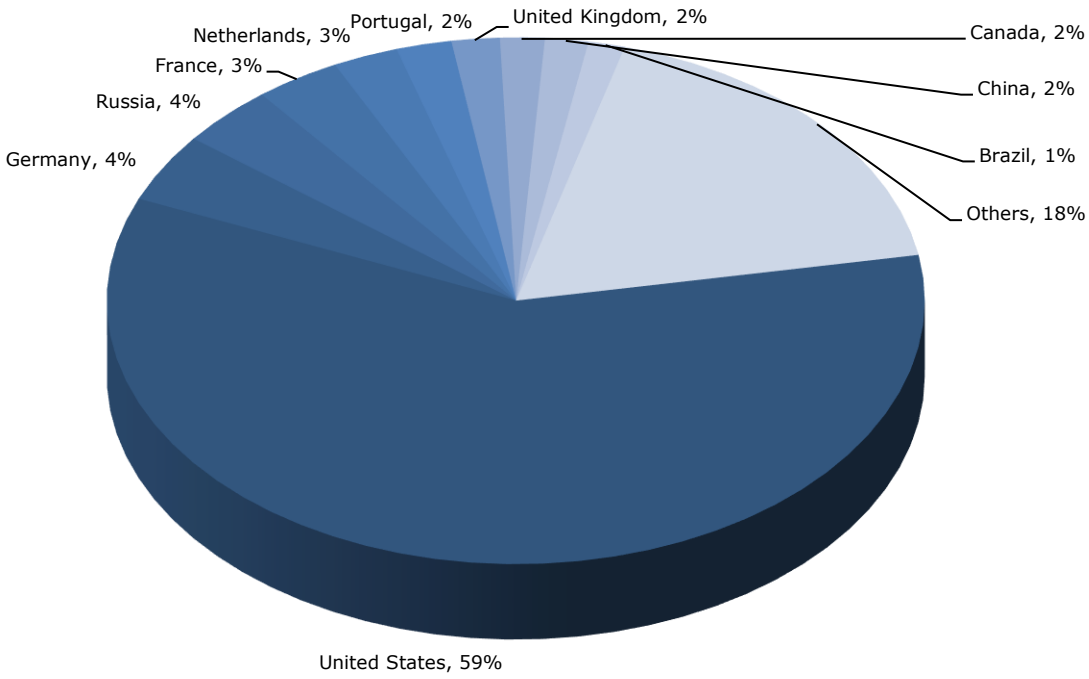


GLOBAL PHISHING ATTACK DISTRIBUTION

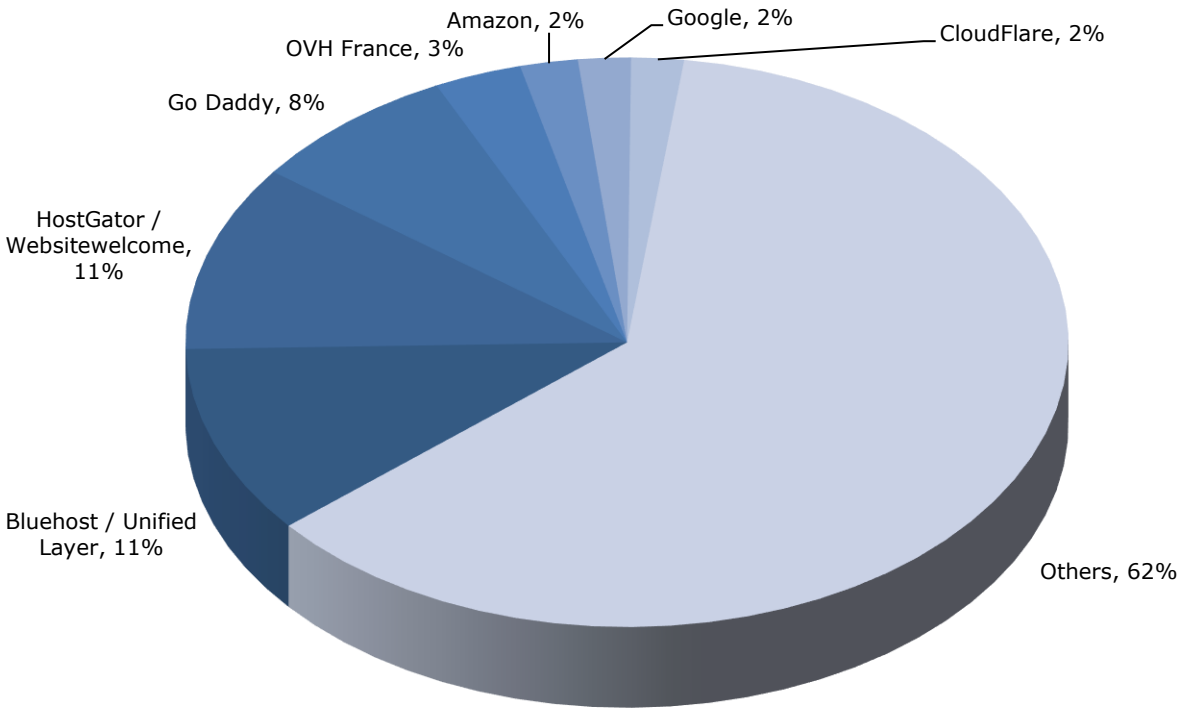


RSA

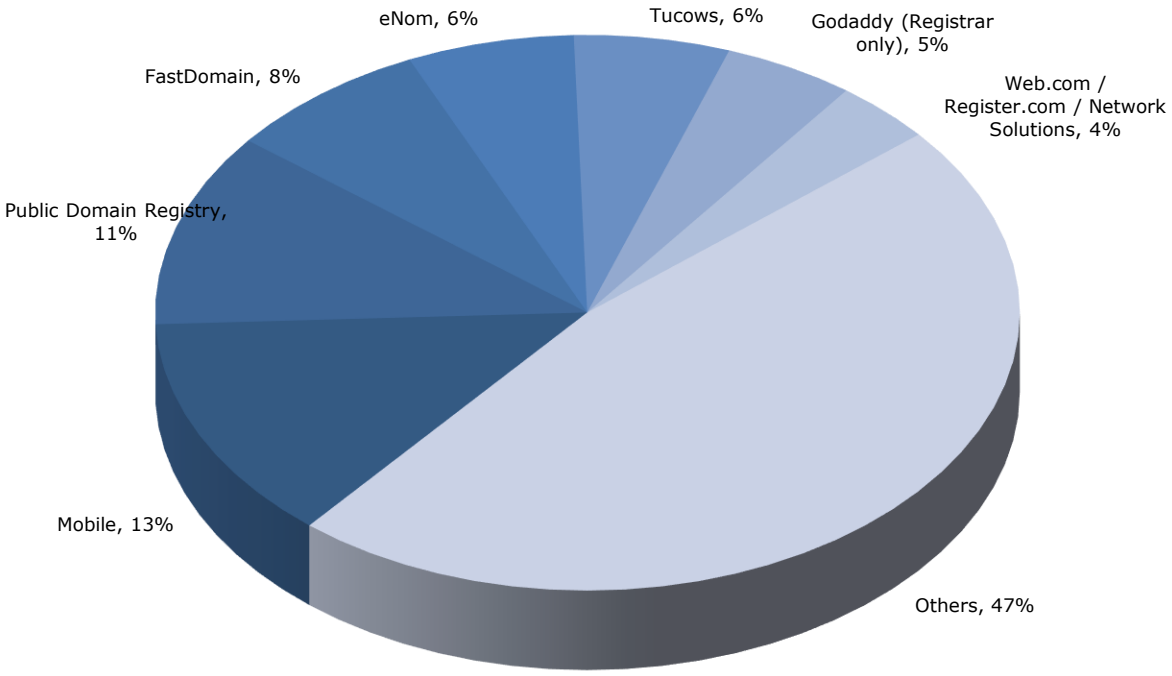
TOP COUNTRIES HOSTING PHISHING



TOP ISPS HOSTING PHISHING



TOP REGISTRARS HOSTING PHISHING



IN CASE YOU MISSED IT

THREAT REPORTS

A summary of reports sent out to customers in recent months.

Report File name	Synopsis
TR170906 TrickBot - The Malware Built to Trick Your Personal Data Out	RSA Trojan researchers shed light on TrickBot's modus operandi
TR170614 Marcher and BankBot Mobile Banking Malware Gain Momentum	An insightful overview of two popular mobile malware families – Marcher and BankBot
TR170605 Mobile Applications Used by Fraudsters	Cybercriminals use applications to facilitate fraud on the mobile channel, allowing them to expand their exploit options

FRAUDACTION WEBINARS

"20 On Fraud Webinar: Fraud-as-a-Service Websites: Scamming in Plain Sight"

While the development of real websites for fraud-as-a-service offerings is not new, their recent prevalence is striking. These professional websites give cybercriminals absolute independence to peddle their fraudulent wares and control each and every aspect of their operation.

From cash-out and account takeover services to digital currency exchange, fraud-as-a-service websites are offering a wide variety of cybercrime goods and services that have been traditionally thought to be reserved for underground marketplaces and forums.

View the webcast replay here

"20 On Fraud Webinar: The Chinese Fraud Underground: An Inside Look"

Despite its perceived isolation, the Chinese cybercriminal underground is flourishing. Fraud ads are rampant with a variety of fraud-as-a-service offerings used to target organizations and consumers around the globe. In this session, get an inside look at the most common interests and practices unique to local fraudsters and why Chinese forums have come to be one of the fastest growing fraud markets in the Dark Web.

View the webcast replay here

"20 On Fraud Webinar: Money Mule Operations in the Dark Web"

Money mules are a common fraud-as-a-service offering in the Dark Web and absolutely critical in enabling the cash out process. Whether in the form of humans or accounts, mules are one of the most difficult parts of the fraud supply chain to detect. Insight into known mule accounts has helped many banks prevent losses from fraudulent transfer requests to other banks, and also shut down accounts that may have been set up to prevent the flow of fraudulent transfers through their own organization

In this webinar, we provide an inside look at money mule operations in the underground, presented by RSA's self-proclaimed "mule hunter." View the webcast replay here

ABOUT RSA

RSA, a Dell Technologies business, offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, go to rsa.com.

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.