Cybercrime continues to diverge down different paths with each new year that passes. In 2013, cybercriminals are changing the way they organize and targeting new users and new platforms, online transaction-based activities continue to be exploited, and hacktivism-related attacks continue to rise as a way to commit corporate espionage, push political agendas or cause reputational damage.

The RSA Anti-Fraud Command Center (AFCC) has developed a list of the top cybercrime trends it expects to see evolve. The AFCC is on the forefront of threat detection and cybercrime intelligence, protecting global organizations with the shutdown of nearly 800,000 cybercrime attacks and preventing $7.5 billion in fraud losses.

In this white paper, RSA will review the current state of cybercrime based on our experience and insight tracking cybercriminal activity and provide a series of predictions on what to expect from cybercriminals over the next year.

**Trend #1: As the world goes mobile, cybercrime will follow**

Mobile computing levels reached new peaks in 2012. Worldwide smartphone shipments reached 671 million for the year – an increase of almost 42% over 2011. The number of apps available for Apple’s iOS alone topped 775,000. Of the total 40 billion apps that have been downloaded from the iOS app store in the four years since it opened, more than half of those were downloaded in 2012. And that doesn’t even count apps for Android and Windows.

From banking transactions to retail purchases to new behaviors such as mobile showrooming, user adoption of the mobile channel has changed the face of today’s consumer. Inside the workplace, user-driven mobile trends such as bring your own device (BYOD) continue to transform the business landscape as well. As more of our personal and work lives move to the mobile device, cybercriminals continue to develop and refine their schemes to exploit mobile transactions and mobile apps.

**Target: Mobile Transactions**

The number of mobile banking users continues to grow globally. In turn, organizations are adding new functionality to the mobile channel and seeing an increase in mobile transaction volume. According to Gartner, global mobile transaction volume and value is expected to have an average 42% annual growth between 2011 and 2016. As users continue to move more of their daily lives to their mobile device, it is only expected that cybercriminals will do the same and direct more attacks at this growing channel.

---

1. Source: Juniper Research, Smartphone Shipments Exceed 200 Million in Q4 2012, January 2013
2. Gigaom.com, Apple App Store Biggest December Ever: 2B iOS Apps Downloaded, Jan 2013
Vishing (phishing by phone) and smishing (phishing by SMS/text message) are two of the more common attacks we see today that exploit the mobile device. These phishing alternatives are becoming more popular by cybercriminals as witnessed by fraud-as-a-service vendors in the underground readily offering services such as SMS blasting applications and SMS spoofing services. One such SMS-spoofing service, iSPOOF Europe, is an example. Designed to send short messages to potential victims and direct them to fraudulent phone numbers, this service offers the ability to conceal the cybercriminal’s true phone number, replacing it with an alpha-numeric name, for example “ABC BANK CUSTOMER SERVICE.”

SMS spoofing also can be used by criminals to lure unsuspecting mobile users to browse to a malicious URL via a provided hyperlink to update their account or obtain a gift card. These smishing attacks present the victim with a legitimate organization’s name in the “From” field of the text message. The malicious URL is designed to look convincing when it asks for account credentials.

More advanced forms of fraud are emerging in the mobile channel as well. The Citadel Trojan – the most advanced commercial banking Trojan seen to date – was introduced in January 2012. RSA traced a new Citadel variant that exploits the mobile channel and utilizes advanced techniques for cross-channel attacks. The motive behind the variant, known as Citadel-in-the-Mobile (CitMO), is to overcome the hurdle of mobile-based, out-of-band authentication methods (such as one-time passwords) that are provided to customers when they complete wire transfers online.

The attack researched by RSA targeted users by posing as security software for mobile devices (see Figure 1). Once downloaded, the malicious software was equipped with SMS-sniffing functionality designed to hide incoming text messages and turn off phone audio alerts as it intercepts mobile-based passwords from the bank to the victims’ mobile devices. As a result, cybercriminals were able to gain access to a user’s account, intercept or manipulate transactions, and perform account takeover.

**Rogue Mobile Applications**

On Christmas Day, 2012, a record-breaking 328 million mobile applications were downloaded, dramatically closing out a year of record numbers for smartphone activations and application downloads. With numbers like these – and expectations that this trend will continue throughout 2013 – it’s not surprising that mobile apps have drawn significant attention from cybercriminals.

In fact, mobile apps have become the new threat vector, as cybercriminals seize the opportunity to serve malware and phising attacks under the guise of legitimate apps. Android, the world’s most widely used mobile platform, is also the most targeted by mobile threats due to the nature of its open source. To demonstrate, the number of malicious and high-risk Android app samples detected in 2012 was 350,000, showing a significant increase from the 1,000 samples identified in 2011.

Although the appeal of the mobile channel and its applications for cybercriminals stem from mobile’s ties to financial transactions and payments, crime associated

---

4 Flurry Blog, Peter Farago, January 2, 2013
5 TrendLabs 2012 Mobile Threat and Security Report
with unauthorized “rogue” applications is not limited to banking and extends to retail, gaming, entertainment – and virtually any business that offers a mobile application. From rogue third-party ATM locators that sell for USD$1 to entertainment apps that serve up malicious links in fake ads, mobile app fraud takes on many forms, making it difficult for users to identify.

**Bring Your Own Device (Byod)**

While company-issued mobile devices are common in the workplace, it is clear that IT departments are under increasing pressure to allow the use of employees’ personal mobile devices to access sensitive corporate data and applications. Yet, many of these organizations are not prepared for the impacts of this user-driven BYOD trend.

According to a recent survey by the SANS Institute⁶, while an increasing number of organizations allow BYOD for remote access to corporate systems, a full 62% of respondents state that their organization is still using password-only authentication to secure access from mobile devices.

While data protection and compliance are top reasons for organizations to implement mobile access security for BYOD, the inadequate use of strong authentication methodologies, and a lack of tracking and central control around the devices – such as mobile device management (MDM) – remain at issue. These factors leave the devices – and the organizations that allow BYOD – highly vulnerable to malware and data theft through hostile applications and unauthorized access.

*In 2013, as organizations continue to move towards greater readiness and acceptance of the shift to mobile and its related practices, they will continue to struggle with important security and policy issues. As mobile vulnerabilities increase, so do opportunities for cybercrime, and while not as prevalent as it is online, fraud will continue to intensify in the mobile channel through socially engineered attacks on users and mobile apps will increasingly be exploited as a means to launch phishing and Trojan attacks.*

**Trend #2: The Privatization of Financial Banking Trojans and Other Malware**

Cybercriminals are slowly bringing malware development deeper into the underground and Trojans that have generally been popular due to their commercial availability in the open black market are suddenly less available for sale. Cybercriminals’ fear of infiltration by undercover agents and subsequent prosecution by law enforcement as well as changes in international law are causing Trojan development to become more privatized.

Yet, development has not slowed down by any means. For cybercriminals that rely on commercial malware offerings, this past year showed Trojan development increase more than in any previous time period – beginning with the introduction of Citadel and ending with the return of the Carberp Trojan to the commercial scene. While the Zeus Trojan continues to be the most prolific malware used in financial attacks, a look at other major players reveals a few interesting changes in the landscape.

**Zeus and Zeus-Based Trojans**

Zeus – already the most popular banking Trojan in use – became even more accessible in mid-2011 after its source code was exposed publicly. Suspicions that Zeus’ original coder, “Slavik” participated in the development of Zeus v2.1.0.10 have persisted in 2012. Security researchers, in fact, have proven that Slavik has not retired, and believe that he continues to play a low-key role in the Russian-speaking cybercrime scene.

Other variants of Zeus were developed during 2012 including the Ice IX Trojan which proved to be a poorly programmed variation that gained momentum in the underground due to the great demand for support services by botmasters operating Zeus. In February 2012, the Ice IX developer announced another upgrade to the Trojan – then disappeared two months later, leaving buyers stranded without support or bug fixes and suspending the sale of Ice IX to new buyers.

The most successful Zeus offshoot to-date also surfaced in 2012. Citadel, a banking Trojan that was introduced to the underground in January, has evolved into the most sophisticated Trojan business model the world of commercial malware has ever known.

---

RSA has reported significantly on the advanced features and new developments available for Citadel since January 2012. Recent developments with Citadel and the team behind it have taken this Trojan deeper underground, and although it is still considered commercial malware, it is much less available and can only be purchased by new buyers if they are “vouched” for by other cybercriminals. This move is likely intended to keep the Trojan from being too widely spread thus making sampling of the malware more difficult for researchers and keeping Citadel strains from being detected.

SpyEye
The SpyEye Trojan has been disappearing gradually, particularly since May 2012 when its developer (“Gribodemon/Harderman”) took an indefinite leave from the highly exclusive Russian-speaking forums where it was posted, “Spy’s author, he’s no longer with us. He’s in Malaysia. So there will be a new SpyEye complied soon. For fans and amateurs.” A prominent banking Trojan, SpyEye automates the theft of confidential information and wages attacks through man-in-the-browser tactics.

Bugat v2
Bugat v2 continues to have consistent presence on the global Trojan attack scene, accounting for an average of 14% of all financial Trojan attacks researched by RSA last year. Privately operated, Bugat v2 (also known as Feodo and Sodast) targets financial institutions – mostly online brokerage firms – with the purpose of stealing credentials that could lead to fraudulent cash-out options. This Trojan was discovered and sampled first in the wild in August 2010. Its variants send stolen credentials to Russian-based drop servers.

Gozi and the Gozi Prinimalka Blitzkrieg
In late September 2012, RSA uncovered information about a malware attack spree planned by Russian-speaking cybercriminals – and specifically designed to target 30 US-based banks. A post published by an underground actor known to RSA provided extensive details on the gang which was planning the attack spree and their goal to recruit 100 botmasters to carry out the operation. Clues left by the gang’s spokesperson lead to RSA’s discovery of the malware to be used in the attacks – a variation of the Gozi Trojan dubbed Gozi Prinimalka – which has already been used in previous attacks to steal millions from financial institutions. This new variant included several updated features including a VM cloner to duplicate a user’s PC settings that would allow a botmaster to take on the genuine IP address when accessing a bank’s website.

Carberp
The Carberp Trojan, also known as Syscron, is semi-private malware that has been sold in the underground for more than two years. Carberp infects a PC with the purpose of stealing credentials for bank account takeovers and fraudulent wire transfers. In December 2012, the Carberp Trojan returned to the commercial malware scene, with sales in underground forums to new and existing buyers and price tags that extend up to US$40,000 for a full kit. The price quoted for Carberp is four times the top asking price ever paid for Zeus or SpyEye kits in the underground.

The Trend Towards Privatization
The latest proof to support the privatization of malware was the discovery of Zeus v2.0.9.4 Evolution, malware based on Zeus with a personal touch. Evolution has its own admin panel, most of which is written in English, but also contains significant Russian-language elements (for instance in charts, in the FAQ page, and in the cash-out options it uses – some of which are Russian-based).

Aside from its credit card grabber plugin, the Trojan also possesses a DDoS tool which can enable the botmaster to recruit infected PCs for attacks on online targets. Using a banking Trojan’s botnet for DDoS attacks is one of the ways botmasters can monetize their botnets, charging hourly fees for the DDoS while they work on siphoning money out of infected users’ bank accounts.

---
7 To see all the latest RSA Trojan research, visit the RSA FraudAction Research Labs blog at http://blogs.rsa.com/author/rsafarl/.
In many cases "Anonymous" denied any ties to hacktivists claiming to be part of its ranks.

At this time, Evolution most likely is being maintained by a malware developer (or a small group of developers) who keep it operational and who have programmed its new admin panel GUI. As in most Trojan operations, it is very possible that Zeus Evolution may become commercial malware in the near future.

While 2012 was punctuated with increased development of Trojans and variants based on the exposed Zeus code, the ready stream of commercial malware for new-user purchase and operation was disrupted as the best-known developers started to take their projects further underground to avoid the risk of being caught by law enforcement. RSA expects to see commercially available malware to continue the shift towards privatized operations, thus ultimately making it more challenging for law enforcement to track and crack cybercrime operations and for organizations and the security industry to gain insight into Trojan activity.

Trend #3: Hacktivism and the Ever-Targeted Enterprise

Hacktivism exploded in 2012, and became the number one cyber outlet of choice for the public expression of controversial opinions – political and economic – as well as a means for protesting ideological conflicts. Today's hacktivist groups predominantly are non-related teams (or individual hackers) who attack entities – alleged "culprits" – according to their own political, religious, social, and/or economic agendas.

In many cases, hacktivists choose to cluster their activity under the names of collectives, particularly the more prominent ones such as "Anonymous". Their association, in most cases, is arbitrary with no legitimate connection, and often is motivated by the notoriety of the collective. This is particularly true for claims associated with "Anonymous," since this loosely organized collective is the most well-known hacktivist group, and by far the most popular.

The al-Qassam Cyber Fighters, a self-proclaimed group of Muslim hacktivists, is also making a big name for itself in what it has dubbed Operation Ababil, attacking dozens of U.S. banks with repeated distributed denial-of-service (DDoS) attacks. The group recently boasted publicly in a statement that they estimate the “approximate cost on U.S. banks per each DDoS minute” to be $30,000.

Another change coming to bear is the cross-over impact between the financially-motivated cybercriminal and the hacktivist. We have witnessed the weaponization of financial Trojans such as Zeus variants being used in APT-style attacks and the use of the Citadel financial Trojan which has the ability to map corporate networks. Hacktivists are also finding a business opportunity and supplemental revenue stream in the underground, as financially motivated criminals seek to buy the information stolen in hacktivist attacks and use it to commit fraud (see Figure 2).

Figure 2: A conversation among cybercriminals after a major hacktivist attack that involved the theft of millions of credit cards. (Source: RSA Anti-Fraud Command Center)

---

In many cases "Anonymous" denied any ties to hacktivists claiming to be part of its ranks.
Top attack methods in the hacktivists’ arsenal include:

– **Distributed denial-of-service (DDoS)** – Leverages multiple compromised systems – usually infected with a Trojan or other form of malware – to flood a targeted system, usually one or more web servers of a website, with an onslaught of meaningless electronic “traffic” meant to render the target’s website inaccessible. In January 2013, Anonymous petitioned the U.S. government to decriminalize DDoS attacks and make them a legal form of protesting.

– **Doxing** – Gathering and exposing valuable personal information of public figures such as politicians and celebrities to the benefit of the hacktivist, usually in an attempt to cause the individual to take notice of the issue at hand – and react or take action in a way that favors the hacktivists’ ideology. The term is derived from “documents” or “docx.” Recent doxing victims include First Lady Michelle Obama and U.S. Vice President Joe Biden.

– **Hacking and exposure** – Gaining unauthorized access to – and publicly exposing in plain view on the Internet – large amounts of confidential data with the goal of causing monetary and reputational damages to the targeted entity.

DDoS attacks are the hacktivists’ cyber attack weapon of choice for a number of reasons. First, they do not require actual hacking knowledge or skill. Many “off-the-shelf” tools are available right on the Internet at little or no cost. And second, these attacks can be just as damaging as they are simple. By flooding a website and making it inaccessible, businesses stand to lose revenue and suffer brand and/or reputational damage.

It’s no surprise that hacktivism will continue to be top-of-mind in 2013. What RSA observes as evolving is how these groups organize, their attack methods, and their motives. The wave of DDoS attacks unleashed by hacktivists against many of the world’s major financial institutions in late 2012 – and which continue today – is a good example. The precise reason for the attacks is still unclear. However, some point to political retaliation while others believe it is a guise to hide fraudulent wire transfers.

*Beyond the ongoing onslaught of DDoS attacks and other hacktivist threats, RSA expects to see an increased number of financial Trojans being used in cyber espionage and hacktivist attacks and the sale of more data stolen from hacktivists available for sale in global fraud forums.*

**Trend #4: Account Takeover and Increasing Use of Manual-Assisted Cyber Attacks**

Man-in-the-browser and man-in-the-middle Trojan attacks continue to be used as a weapon of choice for cybercriminals to conduct account takeover. Aite Group estimates that account takeover was responsible for US$455 million in global losses to financial institutions in 2012 and expects that number to increase to US$794 million by 2016.

A man-in-the-browser attack is designed to intercept data as it passes over a secure communication between a user and an online application. A Trojan embeds in a user’s browser application and can be programmed to trigger when a user accesses specific online sites, such as an online banking site. Once activated, a man-in-the-browser Trojan can intercept and manipulate any information a user submits online in real-time.

The technology and skills required to launch a man-in-the-browser attack are not particularly new or advanced. However, RSA has seen a dramatic shift towards more manual-assisted attacks in 2012, such as man-in-the-middle, as financial institutions have increasingly started to leverage out-of-band authentication and behavioral analytic tools that are capable of detecting automated attacks.

A man-in-the-middle attack works much the same way as man-in-the-browser except the interception is not automated, but rather it is the actual attacker inserting himself into the transaction and serving up communications directly to the end user (i.e., socially engineered pages that state the bank’s website is under maintenance in order to allow the attacker time to conduct a fraudulent transaction).

The use of remote access tools (RAT) are standard plug-ins available in most banking Trojans today. Depending on the financial Trojan, a plug-in typically costs just a few hundred dollars in the black market. An example of a remote access tool researched by RSA called “World Bank Center” was an interface developed for use by multiple botmasters and botnets to facilitate real-time interaction with infected users and streamline fraudulent transactions. Cybercriminals using World Bank Center perform account takeover through a man-in-the-middle attack. As soon as an infected user accesses his bank account, a

---

9 Aite Group, “Citadel and Gozi and Zeus – Oh My!” November 2012
cybercriminal can easily and quickly keep their victims engaged by pushing interactive HTML injections to the user, most often to gather additional information (see Figure 3) or to stall the user while the botmaster sets up to attempt a transaction.

RSA expects to see a perpetual increase in the use of manual-assisted attack methods, such as man-in-the-middle attacks, in order to evade detection. Managing fraud losses from account takeover will continue to be a major issue that financial institutions will struggle to address. As a result, there will be increased investment in transactional-level security and behavioral analytics tools capable of detecting anomalies such as clickstream patterns, HTML injection, and proxy injection.

Trend #5: Cybercriminals Will Leverage Big Data Principles to Increase Effectiveness of Attacks

Just as many real-world organizations have started to apply the principles of Big Data to maximize the value of the volume of data they collect, cybercriminals have also started to move in that direction. From a cybercriminal’s perspective, managing data accumulated by botnets of infected PCs can create immense amounts of useless data on drop zone servers and clog infrastructure. Malware developers have been working on different parsing solutions and implementing the use of databases into their command & control administration panels in order to distill only the most pertinent data.

One such tool built into the Citadel Trojan’s administration panel enables data filtering and charting of botnet activity statistics. For example, it can provide data on the most popular software installed on infected machines, as well as anti-virus systems providing cybercriminals with knowledge about security tools that could pose a problem on infected bots (see Figure 4).
Another plugin known as IntelegentBot was offered to cybercriminals operating botnets to help them sort through pertinent stolen data. The web-based platform is accessible by username and password and would require each new user to connect their Trojan databases to the tool. IntelegentBot uses regular expressions to search for specific words which would typically be used to look up bank triggers (URLs/names). A separate screen allows for searching only credit card data and sifting it out of the complete database. The increasing use of data analytics and parsers by cybercriminals and botmasters shows a new level of sophistication in malware development. Beyond just helping to organize only the relevant stolen data, cybercriminals are also now able to use this technology to make business decisions as to where they should invest their money on exploit kits and other black hat tools. RSA expects to see cybercriminals increase their use of tools that are capable of performing Big Data type analytics to learn more about infected victims and increase the effectiveness of their Trojan attacks.

Conclusion

It goes without saying that cybercrime gets more sophisticated every year. In some cases, we are in the very early stages of future threats as we see with mobile where defenses are still nascent. In other cases, we are seeing the result of dynamic defense-in-depth strategies that have thwarted off threats and forced cybercriminals to move back to more manual-assisted attacks.

With a flurry of chatter about evolving threats, so little attention is being paid to the changing IT environment itself. Many disruptive technologies – from cloud computing and social media to mobile device management – are transforming the face of information security. But the most significant movement today is the rapid adoption of leveraging Big Data principles to improve detection of cyber threats and fraud. These disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they leverage new platforms and intelligence to do so. Across identities, applications, and networks – both physical and cloud environments – we can expect organizations will continue to work towards making existing tools more effective, embrace intelligence-driven security programs, and improve the way they use behavioral analytics to identify and respond to emerging cyber threats.