RSA 2012 CYBERCRIME TRENDS REPORT

The Current State of Cybercrime and What to Expect in 2012

Cybercrime continues to show no signs of slowing down. In fact, 2011 marked a year of new advanced threats and an increased level of sophistication in the attacks witnessed around the globe. As we move into 2012, cybercrime is diverging down a different path as new financial malware variants emerge, cybercriminals find new ways to monetize non-financial data, and the rise of hacktivism-related attacks breathes new life into an old adversary.

The RSA Anti-Fraud Command Center (AFCC) has developed a list of the top cybercrime trends it expects to see evolve over the course of 2012. The RSA Anti-Fraud Command Center is on the forefront of new threat detection and cybercrime intelligence, achieving several milestones including the shutdown of over 550,000 phishing attacks and launching the first commercial anti-phishing and anti-Trojan services in the industry.

In this white paper, RSA will review the current state of cybercrime based on what we witnessed in the last twelve months and provide a series of predictions on what to expect from cybercriminals in 2012.

Trend #1: Trojan Wars Continue, but Zeus will Prevail as the Top Financial Malware

RSA has been observing the Trojan landscape throughout 2011, and Zeus 2.0 has continued to dominate as the leading financial Trojan throughout the year. Indisputably the most widely spread financial malware in the world, Zeus is responsible for around 80% of all attacks against financial institutions today and is estimated to have caused over $1 billion in global losses in the last five years.

One observation noted in the beginning of 2011 was the surge of financial attacks connected to the SpyEye Trojan. Financial cybercrime attributed to SpyEye variants decreased over the course of the year, however, with 19% of attacks attributed to SpyEye in Q1 ’11 to around 4% in Q3 ’11. At this time, SpyEye continues to be the most costly Trojan code sold on the black market, selling for a few thousands of dollars for a basic kit and separate plug-ins averaging $1,000 each. SpyEye also features technical complexity which has been known to be a problem for the average cybercriminal to use effectively.

More recently, the Ice IX Trojan has instead gained momentum. Ice IX was first reported on by RSA in both August and September of 2011 – the first true attempt made by any coder (or team) to develop a new Trojan over the Zeus v2.0’s leaked source code. The coder who allegedly took the job on did promise many features that would make Zeus better, but ended up with a Trojan that was still 98% identical to the old king and not much to boast about when it came to the coding skills exemplified by the malware writer. Nonetheless, the Ice IX Trojan was responsible for 13% of financial cybercrime attacks in Q4 ‘11.

Other Trojan/malware trends expected to continue in 2012 include:

Trojans for mobile platforms

A growing trend in the world of cybercrime codes will further carry Zeus (ZitMo) and SpyEye (SPitMo) over to the various mobile platforms, with the purpose of having these banking Trojans steal data such as SMS codes. "InfoStealers" for the mobile platform are also likely to emerge with Trojans designed to keylog touch-screen input and monitor data traffic through the mobile device.

Privately-owned and geo-specific Trojan development will increase

In 2011, cybercriminals demanded more customized Trojans, built for the types of fraud operations they planned to execute. For example, in 2011, there was an increased development of private Trojans as well as codes adapted to specific geographies. The Shiz Trojan, targeted at Russian banking applications, is just one example.

Banking Trojans will be sold in varying business models

The sophisticated business models used by cybercriminals has allowed tools and services once reserved for the cybercrime elite to be made available on the black market as commodities. The more savvy criminals offer their goods and services to those who may be starting out or are in need of set-up and instructions. Whether selling off-the-shelf botnets, Trojans by the binary, or Zeus recompiles, the underground is loaded with tools to allow any "newbie" cybercriminal to launch an attack.

Typical examples to show how fraud tools have evolved in just a short time – from how they are sold and packaged to the obvious decrease in price as they are commoditized – can be observed below:

Before	**After**
SpyEye – buy full version: $4,000	Buy SpyEye binary with set-up and injections for $600
Zeus – buy full version: $10,000	Buy Zeus recompile, 2 for $380
HTML Injections come with Trojan	Buy customized $50 - $75
Injections crypts – not sold	Buy for $5 each or $50 per month unlimited
Anti-security software – not sold	One time license fee $250 + $10 for upgrades

New black hat tools will counteract security

Cybercriminals are in a perpetual arms race against security professionals and the prevention tools they develop. Taking one recent example as an indication to this trend, "Malware Guard", a botnet-protection tool, was designed to harden a botnet's security and block off any possibly 'hostile' IPs from reaching it (i.e., an IP address originating from a security researcher's lab). The application, made to plug-and-play with the explicit purpose of protecting bot-herders and their infrastructures, is available for sale in the black market for $250.

More Trojan-assisted manual attacks

Due to stronger security, blocking scripts (such as man-in-the-browser), and locking the communication of the bank's servers with the online banking customer, Trojan developers are resorting to remote-control-assisted manual attacks using the victim's own device. This type of fraud is lengthier and requires hands-on action by the cybercriminal; it is thus linked with the more lucrative nature of attacks on corporate accounts.

In terms of attack methods and the improvement of existing mechanisms, cybercriminals are commonly using two distinct Trojan-assisted manual attack methods to commit financial fraud.

- **Automated Attack Scheme – Man-in-the-browser Scripts with Mule Panel Relay**
  Man-in-the-browser (MITB) scripts have long been implemented in almost every banking Trojan with the purpose of automating transactions from compromised bank accounts. Cybercriminals can typically apply MITB scripts in two ways. The first way is to modify a money transfer after the genuine user has initiated the transaction. The second way happens as soon as the user logs into the bank account.

In the second instance, the Trojan does not wait for the user to perform a transaction, but rather initiates it and attempts to automate the siphoning of money out of the account. This attack method sees higher success rates when used on bank accounts that do not require any additional transaction protection elements such as out-of-band authentication.

– **Manual Attack Scheme – Remote-Control-Enhanced MiTM Fraud**
Bank websites on which Trojan scripts no longer successfully execute or where the bank's server's communication has been locked once the session has been activated have pushed cybercriminals away from automated fraud transactions and back into the manual attacks. The move to manual attacks has considerably slowed-down the transaction rate and cannot compare to the speed of automated MITB attacks. Nonetheless, it appears that cybercriminals had no other choice if they hoped to see successful wires.

This attack scheme is expected to carry through into 2012 along with the regular automated MITB scripts presently used by banking Trojans. It would also be logical to see malware authors attempt to develop a new type of code to bypass the hurdles which have impeded the use of automated MITB transactions.

In 2012, RSA also expects to see financial Trojans increasingly be used to infiltrate corporate resources, allowing cybercriminal gangs access to critical information and infrastructure (see Trend #2).

Trend #2: Cybercriminals will Find New Ways to Monetize Non-Financial Data

Cybercriminals continue to understand the value of non-financial data harvested by their Trojans and are already actively looking for ways to monetize this information. Not only is victims' information being traded in the underground, but access to victims' computers is increasingly being offered for sale, as well. Some examples of non-financial data for sale in the underground today are as follows:

Utility Statements

Exemplifying interest in non-financial data include cybercriminals seeking access to billing statements of consumer's utility accounts, including accounts with gas and electricity providers, as well as telecommunication providers. Perpetrators likely collect these details in order to trace additional personally identifiable information (PII) or facilitate other forms of identity theft such as the opening of new bank accounts or obtaining personal loans.

Medical Records

Numerous instances of fraudsters seeking "fresh" medical records were also traced possibly for such cash out operations as selling patient databases to law firms or to commit insurance billing fraud (see Figure 1).

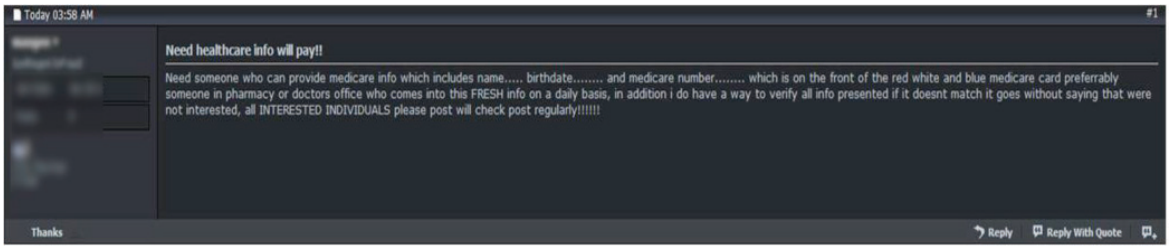


Figure 1: A post in the underground seeking health information of Medicare patients.

To the Highest Bidder – Troves of Personal Details

Currently, the three types of non-financial information most widely traded in the underground consist of spam mailing lists, dates of birth (DOB), and unfiltered Trojan logs.

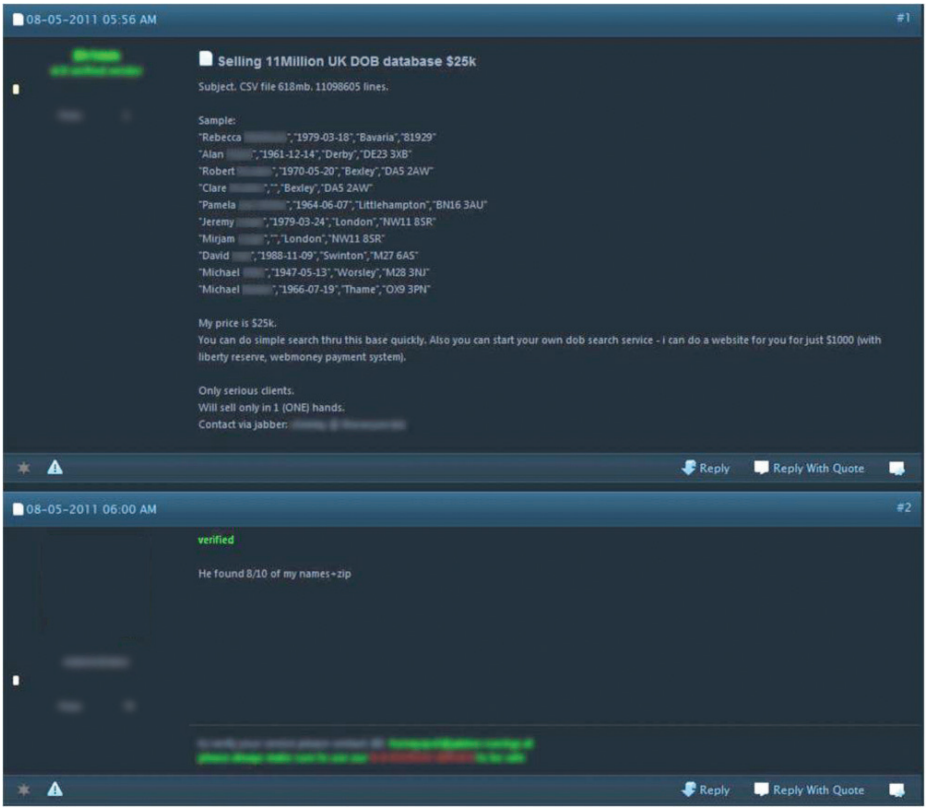
As spamming campaigns are still the most pervasive method of spreading malware, the trading of such lists speaks to the growing demand for 'spammable' email addresses. Cybercriminals can buy spam mailing lists that are pre-filtered by country, enabling more effective, regionally-targeted spam campaigns. For example, a cybercriminal looking to spam German banking customers can buy a pre-filtered list of email addresses belonging to German citizens. And just as in the real world, cybercriminals will pay more for quality. One fraud vendor in the underground had a list of 100,000 German email addresses at a price

tag of $350 USD, with separate lists targeting the US, UK, Spain, Italy and Australia. However, a more sophisticated vendor guarantees the quality of his spam list based on campaigns that elicited a recipient's reply. The price: 500 responses for $600 USD.

Since PII, such as date of birth (DOB), is often used as a secondary form of confirming an individual's identity as part of the authentication process (both online and in the Call Center), DOBs have become a widely demanded commodity in the underground. DOBs are often sold along with an individual's Social Security number (SSN) to defraud US-based merchants, financial institutions and service providers.

For several years now, DOB and SSN lookup stores have been quite common in the underground, with a few credit report stores and vendors also available for cybercriminals seeking additional background information on a potential identity theft victim. Expanding into the non-U.S. market, Figure 2 shows an example of a DOB database of UK residents being offered for sale in the underground. The going rate for such PII is between $1 and $3 USD (see Figure 2).

Figure 2: A cybercriminal seeks to sell a database of personal information on 11 million UK consumers



Hacked User Accounts

Other types of non-financial online accounts traded in the underground consist of gaming accounts, such as "Steam" and Xbox Live accounts, as well as online courier service accounts, such as those provided through Fedex, DHL, and UPS.

Whereas gaming accounts may be bought by cybercriminals who second as gaming enthusiasts, or may be resold to non-fraudster fans, courier service accounts can facilitate e-commerce fraud perpetrators in getting merchandise reshipped to their country of residence (a fraud scheme that usually involves 'item drops,' or reshipping mules). Since many U.S. and European-based online merchants ship to a limited roster of countries, an account with a leading international courier service can help bypass this hurdle.

Access to Infected Victim Computers

In 2011, an increasing number of underground credit card shops (specializing in the sale of compromised credit card data) offered remote access to users' infected systems, sold by the unit. In exchange for a couple of dollars, a fraudster can receive a data set that allows him to access an infected computer (using the remote desktop access of his choosing).

A related service, called “loads” or “installs” in underground terminology, is also offered in the underground. In exchange for a fee, cybercriminals help their peers infect new victims with malware or Trojans. A “load” or “install” is a confirmed new infection of a user’s system, payable by the unit or per infection batch. Cybercriminals that operate these services run dedicated websites to offer and manage their “infections-for-sale” operations, enabling them to both buy and sell botnet web traffic.

It is no longer just financial data for sale in the black market. Information stolen as a result of a Trojan infection or hacking can be monetized in an ever-multiplying number of ways. RSA believes that cybercriminals will strive to monetize a new variety of personally identifiable information and growing assortment of hacked accounts in 2012 and be forced to innovate to compete against increasingly sophisticated authentication measures, such as advanced knowledge-based authentication system and cutting-edge out-of-band authentication technologies.

Trend #3: Fraud-as-a-service Vendors Will Bring New Innovations

The fraud underground is a vivid marketplace where different types of vendors create tools, share methods for making money, and find ways to sell anything they can create and monetize per the market’s demand. Fraud-as-a-service (FaaS) is the one area of the underground economy which has seen the most consistent innovation throughout 2011. Comparable to legitimate hosted software service (SaaS) providers, those who create and provide the fraud supply chain with the latest Trojan codes and plug-ins offer their work and associated services to those who require turnkey solutions, set-up, instructions and support.

The most dominant FaaS offerings in 2011 were the more elaborate sets of compromised credit cards (dubbed “dumps” in underground forums) and account logins (both offered through CC Shops). Another hot commodity was card checking tools, relays and services (often embedded into existing CC Shops), Trojans in different constructions (sold by the binary, sold second hand, sold as readymade botnets, sold as ‘cracked’ versions or genuine complete kits), and CC Shop platforms designed to enable cybercriminals to sell large amounts of compromised data.

Fraud-as-a-service will continue to evolve in all directions, making it easier to find, buy and pay for “off the shelf” services that continue to make it easier for cybercriminals to commit fraud. RSA expects a series of new technologies, services, and business models to emerge in the underground as FaaS continues to grow throughout 2012.

Trend #4: Out-of-band Methods Will Force Cybercriminals to Innovate

Strong authentication at login has become necessary to protect online financial accounts. However, cybercriminals are consistently developing new attack methods that can bypass login authentication – and even two-factor authentication systems. Some attacks that have continued to evolve throughout 2011 are man-in-the-browser Trojans and SMS forwarding.

Transaction protection has become a critical part of protecting financial transactions from account takeover and reducing financial fraud. In fact, global regulations – from the United States to India to China – stress layered online security with a focus on protecting transactions, both financial and non-financial. For example, the updated FFIEC Guidance released in 2011 in the United States specifically requires banks to implement risk-based fraud detection and monitoring systems which enable out-of-band authentication for high-risk transactions.

Man-in-the-browser Trojans

Man-in-the-browser (MITB) Trojans first emerged in 2007 as a way for cybercriminals to overcome two-factor authentication – specifically one-time passwords. A MITB Trojan works by intercepting data as it passes over a secure communication between a user and an online application. In just a short time, MITB Trojans have advanced so quickly that most of the available kits for sale on the black market come programmed with functionality to fully automate the process from infection to cash out.

Zeus/SpyEye is the most common Trojan variant used for conducting man-in-the-browser attacks. Most variants are able to identify and intercept different types of Internet traffic in real-time and is mainly exploited to conduct automated attacks, such as using an array of the victim’s personal and device identifiers. Zeus/SpyEye can also facilitate manual hijacking of a victim’s active online session.

SMS Forwarding

Some financial institutions have implemented out-of-band SMS authentication as an additional layer of security for confirming high-risk transactions. Referred to by some as a "man-in-the-mobile" attack, SMS forwarding shows the rapid evolution of Trojan development.

The criminal developers behind the Zeus Trojan, for example, have modified its attack code to stage a remote takeover of smartphones, which in turn allows them to launch a man-in-the-mobile attack. This typically starts through an infection on a user's computer where the Trojan mimics a message from the bank requesting the user to supply a mobile telephone number and make and model of the device to 'set up' the new security method. An SMS/text message is then sent to a user's mobile device asking them to download a digital certificate or application in order to complete the process. Whenever a transaction requires an out-of-band SMS to complete, the Trojan intercepts the code and forwards it on to a device controlled by the attacker. SilentBanker and Gozi are two other financial Trojan variants known to be programmed with such plug-ins.

Protecting multiple points across any activity – from login to transaction – is critical to managing fraud risk. Out-of band authentication – whether via SMS text or phone call – is the strongest step-up authentication method available as it completely bypasses the online channel. However, cybercriminals are already starting to innovate very sophisticated attacks in an attempt to bypass out-of-band authentication systems.

Account takeover continues to be an issue for financial institutions around the world. In the U.S. alone, these types of attacks are expected to cost the financial services industry over $210 million in losses in 2011[1]. As more banks continue to utilize out-of-band systems for confirming high-risk transactions, cybercriminals will build the tools to bypass them. As we head into 2012, RSA expects that transaction protection will become a top priority for financial institutions as account takeover attacks grow in sophistication. RSA also expects to see a rise in mobile malware targeted at bypassing out-of-band authentication systems.

Trend #5: The Rise of Hacktivism

Hacktivism was further popularized in 2011 as groups such as Anonymous, LulzSec, and AntiSec took on governments and major global corporations through highly-publicized hacking incidents. The goals of hacktivism are most often driven by a politically charged agenda with the intent to cause fear, intimidation, or public humiliation.

In rethinking information security, understanding the adversary, including their motivations, capabilities, and objectives, is critical in how organizations protect themselves. For example, the profit-motivated cybercriminal has the ultimate goal of making money from any data they can steal – although most often, personal and financial data is the target. On the other end of the adversary spectrum, state-sponsored attacks also seek very specific types of data such as intellectual property or trade secrets.

Hacktivists fall somewhere in the middle of the profit-motivated and non-profit motivated criminal because the organizations and information they target and their motivation can vary so widely. The advanced skill sets and autonomy displayed by hacktivist groups, however, give them their own unique position among the spectrum of adversaries considered to be a threat today. A general profile of these anti-establishment vigilantes follows:

- **Motivations:** Ego, populist agenda, self-declared moral code, front for other organizations
- **Methods:** Bribery, recruitment of insiders, malware and hacking tools that target a specific systems or set of data, denial-of-service tools
- **Target:** Large corporations, governments, supply chains, security infrastructure providers, or media outlets that oppose their agenda or moral code
- **Inherent Risk:** Varies depending on the nature of protected information and the public profile of potential targets

There is no doubt that 2011 was the "Year of the Hack." While the threat of APTs and cybercrime attacks are relevant for all enterprises to consider, the threat of public exposure via hacktivism will propel top-down interest into security by executives. Hacktivism will persist throughout 2012 and drive enterprises to re-evaluate their security posture. RSA

1 Aite Group, "Banks and Businesses in the Crosshairs: Cybercrime and Its Impact," September 2011

expects to see organizations move towards intelligence-driven security operations focused on developing knowledge of threats in order to detect attacks in closer to real-time and focus investment in malware analysis, incident response and next generation technologies to address hacktivism.

Trend #6: Better Information Sharing will Lead to More Crackdowns on Cyber Gangs and Botnet Operators

In 2011, it was a pivotal year in terms of information sharing across international law enforcement agencies. To name just a few high-impact international initiatives, Interpol and Europol jointly established a new, secure information-exchange platform, enabling the safe sharing of crime-related data in real-time, training workshops and residencies were held by the Interpol to train the cyber-police force of dozens of countries, and extensive cooperation between agencies in Europe with the FBI led to the apprehension of several multi-million dollar cybercrime rings.

Cybercrime victims are often targeted by botmasters operating from within a country other than their own. Perpetrators' infrastructures are usually dispersed over numerous locations, with bulletproof hosting services purchased in one country, domain registrations performed by providers in another country, and money mules often recruited using bogus job ads appealing to residents of the target country. Furthermore, the botnets used to disguise an attack's "mother ship" web servers, more often than not comprise machines scattered around the globe. In addition, commercially-available Trojan kits, sold in fraudster forums, are coded by malware authors of diverse nationalities.

The intangible, ephemeral nature of online fraud schemes, which can be easily launched from one location while targeting scores of others, has made the cooperation and information sharing between international law enforcement agencies integral to fighting cybercrime.

Increased Collaboration

In 2011, increased cooperation among international law enforcement agencies, combined with assistance from the private sector and academic researchers, resulted in several high-profile arrests and the takedown of criminal operations that were attributed to hundreds of millions of dollars in losses. Some examples include:

- **Operation Trident Tribunal.** This investigation into a scareware scam, initiated by the FBI's Seattle office, culminated in "Operation Trident Tribunal"– a crackdown on a Kiev-based crime ring by the Security Service of Ukraine, as well as agencies in Germany, Latvia, and Cyprus. The gang's criminal operations infected the systems of nearly one million users and robbed consumers of more than $72 million.
- **Operation Ghost Click.** This investigation by the FBI led to the arrest of several Estonian-based cybercriminals in connection with a fraudulent DNS-rerouting scheme that enabled the gang to rake in $14 million in fraudulent advertising revenue. The list of investigation partners included NASA's Office of Inspector General (OIG), the Estonian Police and Border Guard Board, the National High Tech Crime Unit of the Dutch National Police Agency, and Georgia Tech University.

Cyber Security Training

In July 2011, Interpol held its very first international Cyber Security Training Workshop in Singapore, to share knowledge and demonstrate practical techniques for tackling cybercrime with specialist law enforcement personnel from 20 countries. The two-day training event comprised best practices for gathering online forensics and botnet analysis, among other topics, with professional expertise contributed by both public and private sector specialists.

Another event was held in Dublin in the form of a two-week program (July through August 2011), marking the first joint Interpol and academia training program, called the Interpol Cybercrime Summer School Training Course. The program focused on fighting the latest advanced threats including mobile phone forensics, VoIP and WiFI-related investigations, as well as other general practices, such as money mule investigations, the detection and analysis of malware and the extraction of forensic data.

Legislation to Improve Information Sharing

As the debilitating effects of cybercrime gain awareness among the general user public, lawmakers are taking initiatives to improve the oversight of research and mitigation efforts. For example, on December 15, 2011, members of the House Homeland Security Committee in the U.S. introduced a bill called "PrECISE Act," a proposal for Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness. The bill would set up a single entity that would streamline information sharing between the private and public sectors. In light of reports of extensive intrusions that according to one former FBI agent[2] caused intellectual property valued at $500 billion to be stolen in 2010, the bill is believed to gain unequivocal support from lawmakers.

Increased Cyber Security Spend

A wave of advanced cyber threats, along with greater vulnerabilities introduced by the pervasive use of new technologies such as mobile devices and cloud computing, is helping to drive increased spending on cyber security within the private and public sector. According to a study[3] by management consulting firm PwC, global spending on cyber security was expected to exceed $60 billion in 2011. In addition, the study estimates spending on cyber security to grow ten percent year over year over the next three to five years.

The risks posed by cybercrime to the public and private sectors' intellectual property, combined with the growing threats to critical infrastructure, is already accelerating orchestrated efforts by global lawmakers to uproot today's advanced threats and secure tomorrow's online environment. More legislation, improved collaboration and training, and increased cyber security spending are critical to building a foundation for a trusted digital world.

In 2012, RSA expects to see international cybercrime training and information sharing initiatives increase across the globe, signifying not only enhanced cooperation between law enforcement agencies, but also marking a tighter rapport between the private sector, public sector, and academia in their joint efforts to mitigate and crack down on cybercrime. As a result of improved information exchange and training, RSA expects to see a record year for cybercrime gang busts and botnet takedowns.

Conclusion

Every minute, 232 computers are infected by malware. The lightning speed at which cybercriminals develop attacks and new malware code is making it harder for global organizations to manage fraud risk. One of the most important lines of defense is intelligence and awareness of the potential risks. As we move into 2012, the combined efforts by law enforcement and industry to improve information sharing and collaboration along with the move towards intelligence-driven security will help drive response to cyber threats in near real-time and further narrow the window of opportunity for cybercriminals.

About RSA

RSA is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.

2 http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html

3 PwC, "Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry," December 2011.

CYBERC12 WP 0112

www.rsa.com