RSA 2011 CYBERCRIME TRENDS REPORT

The Current State of Cybercrime and What to Expect in 2011

Cybercrime continues to show no signs of slowing down. In fact, 2010 marked a year of several new threats and an increased level of sophistication in the attacks witnessed around the globe. As the new decade opens, cybercrime is diverging down a different path as cyber attacks move beyond the financial services industry and malware makes a shift from targeting consumer desktops to employees in the enterprise.

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 2011. 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 350,000 online attacks across 181 countries 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 2011.

Cybercrime Trend 1. Mobile malware and the exploitation of mobile phones to commit fraud

The explosive growth of mobile devices as a general purpose computer "on the go" has made them an attractive target for cybercriminals to exploit. In addition, the use of out-of-band authentication via SMS and phone as an additional layer of security adds to the vulnerabilities in the mobile channel.

Mobile application downloads are increasing at an alarming rate – with the expectation that the number of downloads will more than double in 2011 to 25 billion applications.[1] And as the industry looks to remove barriers to make it as cheap and easy as possible for application developers to meet the demand of mobile users, the proliferation of malware targeted at these applications and devices is inevitable.

Today, consumers are using their mobile devices more than ever before. Beyond downloading applications, they are engaging in mobile banking and payments, checking e-mail, accessing online accounts and storing personal data on their phones.

[1] International Data Corporation (IDC), "Predictions 2011: Welcome to the New Mainstream," December 2010

White Paper

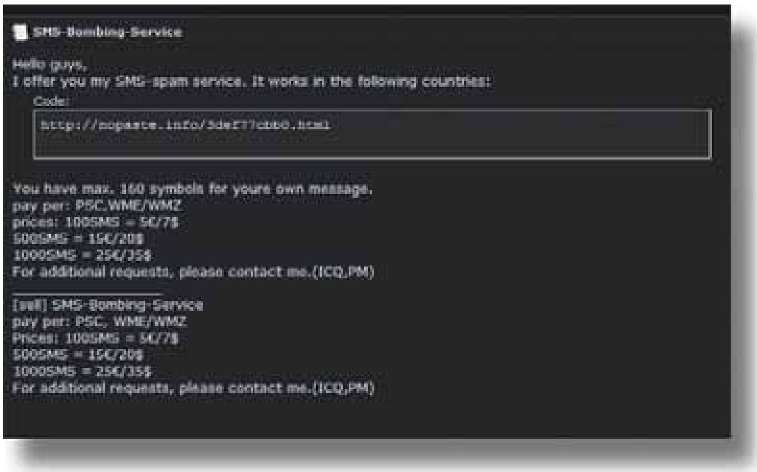
But it is not just consumers and their banks that must consider the risks of mobile malware. The consumerization of IT has laid the bridge for the crossover of consumer technology into the enterprise. Organizations are providing their employees with mobile devices, or employees are using their own personal devices to conduct work-related activities – potentially opening up a backdoor for malware to make its way onto the corporate network.

Beyond the threat of mobile malware, cybercriminals are involved in other exploits of mobile devices in general. For example, many banks use out-of band phone calls or SMS authentication as an extra security measure to validate high-risk transactions. Out-of-band methods became especially popular in 2010 as the threat of man-in-the-browser Trojans grew rapidly.

To circumvent these extra layers of security, cybercriminals have already developed tools to work around them. For example, a cybercriminal can elicit services from other criminals in the fraud underground – at a price of $25[2] – to conduct a telephony denial-of-service attack ("phone flooding") which essentially renders a consumer's mobile device unavailable for incoming phone calls or SMS text messages sent from their bank to confirm a transaction. SMS forwarding services are also becoming mainstream in the fraud underground and enable the one-time passcode sent by a bank via text to a user's mobile phone to be intercepted and forwarded directly to the cybercriminal's phone.

Smishing, or SMS phishing, is another method cybercriminals are using to exploit mobile devices. With smishing, a text message is sent to an individual's mobile device in an attempt to get them to divulge personal information. Smishing is a growing problem for all banking segments including credit unions, regional banks and large nationwide banks. In particular, large nationwide banks have been the hardest hit by smishing as cybercriminals can distribute their SMS spam to a wider base of mobile users who are more than likely to have some form of financial account at one of these institutions. Also, smishing is a fraud tool of choice because it has relevance on a global scale as more consumers access the Internet through a mobile device versus a traditional desktop or laptop PC.

Smishing has become easier to do and a more attractive alternative to phishing. Success rates are higher with a smishing attack compared to a standard phishing attack as consumers are not conditioned to receiving spam on their mobile phone so are more likely to believe the communication is legitimate. Recent research in fact prooves that mobile users are three times more likely to enter their personal information to a phishing site than a desktop user.[3] Furthermore, whereas the majority of phishing e-mails are now stopped by spam filters and often never reach their intended targets, there is no well-developed mechanism for weeding out "spam" text messages.



SMS-Bombing-Service

Hello guys,
I offer you my SMS-spam service. It works in the following countries:

Code:
```
http://nopaste.info/3def77cbb0.html
```

You have max. 160 symbols for youre own message.
pay per: PSC,WME/WMZ
prices: 100SMS = 5€/7$
500SMS = 15€/20$
1000SMS = 25€/35$
For additional requests, please contact me.(ICQ,PM)

[sell] SMS-Bombing-Service
pay per: PSC, WME/WMZ
Prices: 100SMS = 5€/7$
500SMS = 15€/20$
1000SMS = 25€/35$
For additional requests, please contact me.(ICQ,PM)

Figure 1. A cybercriminal advertising his services to help other criminals facilitate smishing campaigns.

[2] RSA FraudAction Research Labs

[3] Trusteer, "Mobile Users Three Times More Vulnerable to Phishing Attack," January 4, 2011

There are many services available today in the fraud underground to help cybercriminals conduct smishing attacks easily and at a low cost. These services enable masses of text messages to be sent instantly from any computer to thousands of mobile phones. In Figure 1, you can see an advertisement posted by one cybercriminal offering his “SMS bombing” services – charging a fixed price per thousand to send a custom text message to mobile users. Cybercriminals can also purchase software that spoofs the sender ID so that the text message appears to come from an e-mail address originating at a legitimate entity.

RSA expects to see a huge growth of malware targeted at mobile devices in 2011. In addition, as banks and other organizations look to leverage the mobile channel to conduct business or as an extra layer of security to combat Web vulnerabilities, we expect to see new and improved services in the fraud underground designed to overcome these roadblocks.

The concept of advanced persistent threats is gaining traction in the business world. The term, which has been traditionally used to describe coordinated attacks against government agencies and the public sector, is now becoming an issue for the private sector.

Cybercrime Trend 2. Malware in the enterprise

Malware is becoming an increasing problem for organizations and government agencies around the world. What has typically been deemed an issue exclusive to consumers and financial institutions has suddenly made a crossover into the enterprise. This is being helped through a number of factors including employee mobility, the use of social networking sites, and user-driven IT. As a result, the corporate network is increasingly being exposed to malware, Trojans, advanced persistent threats (APT) and other attacks that have the potential to lead to a data breach and compromise sensitive data.

The concept of APTs is gaining traction in the business world. The term which has been traditionally used to describe coordinated attacks against government agencies and the public sector is now becoming an issue for the private sector. APTs are particularly concerning after coordinated attacks such as Operation Aurora and GhostNet affected some of the world’s largest organizations.

APT attacks are generally introduced through employees. The second stage of an APT is defined as, “Intrusion into the network that typically starts with spear-phishing e-mails, where the attacker targets specific users within the target company with the intent to infect the employee’s machine and give the attacker a foot in the door.” This is disconcerting when considering research that shows about half of all employees will fall for a good spear phishing ruse[4].

Another factor contributing to the rise of malware in the enterprise is the consumerization of IT and the dual use of computers for personal and business purposes. This opens the door for Trojan infections on corporate-issued endpoints and the opportunity for cybercriminals to capture additional data such as VPN credentials that enable access to corporate applications like webmail accounts and CRM resources. As a result, organizations are facing an increased risk of data loss.

A study conducted by RSA in April 2010 revealed the vast extent of potential exposure to malware and data loss within some of the world’s largest organizations. Based on RSA’s visibility into a significant volume of data captured by malware from our efforts in shutting down Trojan infection, update and drop points, we attempted to quantify the risk malware poses to the enterprise.

Based on the results of the data analyzed, it is clear that there are a high number of corporate machines being used for work purposes that are infected with malware. RSA found that just among the Fortune 500, 88 percent demonstrated botnet activity associated with their domains and 60 percent had e-mail addresses compromised by malware.

The risk against the enterprise is further complicated by the continued debate of social networking sites. Many organizations continue to struggle with striking the right balance between whether to allow employees access to these sites and how they leverage the

[4] Wombat Security Technologies

sites for their own marketing and promotional purposes. Research that shows more than one in five Facebook users have active malware or viruses on their computer[5] begets the question: Is it a personal or work-issued device?

RSA expects to see an increase in malware intruding on corporate networks in 2011 via APT-like attacks that target employees within the organization. The spread of malware will also be facilitated as consumer technology is introduced into the enterprise and more organizations embrace the use of social networking.

Cybercrime Trend 3. The Trojan Wars: Competition among malware developers in the black market will lead to new features and shorter development cycles

The Zeus Trojan is widely recognized as the “de facto” malware in the world of online banking fraud – estimated to be responsible for about 90 percent of banking fraud worldwide. Since becoming commercially available in the black market, Zeus is almost a commodity, with numerous malware authors developing their own best of breed version of the Trojan.

The Zeus Trojan is widely recognized as the “de facto” malware in the world of online banking fraud – estimated to be responsible for about 90 percent of banking fraud worldwide. Since becoming commercially available in the black market, Zeus is almost a commodity, with numerous malware authors developing their own best of breed version of the Trojan.

Recently, the announcement made by the authors of the Zeus and SpyEye Trojans of the merging of their two Trojans made waves in the cybercriminal underground. The merger announcement came in light of extensive arrests made in late September, 2010 in connection with Zeus Trojan attacks. As the new hybrid Trojan has yet to be released and offered commercially in the cybercriminal underground, Zeus currently maintains its reign among commercial malware. However, this may mark an ‘in-limbo’, as SpyEye’s author, Harderman (aka Gribodemon), is more likely to invest his efforts in perfecting the new hybrid rather than updating the legacy Zeus releases.

The author of Zeus, known as Slavik, has granted Harderman the Zeus Trojan’s complete code, and Harderman, in turn, has announced that Zeus will serve as the basis of the new Super Trojan. Harderman further stated that to enhance the Trojan’s functionalities, each of SpyEye’s modules will be available for purchase as a separate plug-in for the merged Trojan.

Harderman has already announced his plans to implement in the new Trojan a ring-0, or kernel mode, rootkit (thus far only seen in Sinowal), as well as add remote desktop access, granting access to each infected computer’s desktop GUI. Admitting that the Zeus Trojan’s HTML infections were superior to his own, Harderman has announced he will study these to enable their implementation in the new hybrid Trojan. Should Harderman act on his plans, this already spells *evolution* in the type of commercially-available malware likely to be sold in the underground in 2011.

SpyEye Trojan

In 2010, the emergence of the SpyEye Trojan took form along with its sophisticated plug-ins and features. SpyEye was rapidly and continuously updated throughout 2010, with several major updates being released within the course of just six months.

The first update (released in late January 2010) featured a configuration tool and a builder, both inspired by Zeus. It also offered a first-of-its-kind Automatic Mass Registration module, which facilitates conducting multiple fraudulent registrations to e-wallet services that require registration with payment card data. The module searches SpyEye’s logs for credit cards, and according to a card’s billing address, pairs each card with a bot from the same country, or even the same U.S. state. The module then registers a new e-wallet account. By accessing the e-wallet service from a matching geo-IP location, the transaction is less likely to be flagged as high-risk. HTML injections were added shortly following these updates.

[5] PrevX

In February 2010, a host-ban option was added, in effect preventing users from accessing predefined URLs, for example, the URL of the bank from which the Trojan has just stolen money – in an effort to conceal the account's new balance. SpyEye's third release was enhanced with the famous "Kill Zeus" feature which disabled older versions of the Zeus Trojan installed on users' systems. Finally, the fourth SpyEye release was fortified with an anti-piracy lock for preventing the copying and reselling of the malware, as well as a balance grabber and support of Firefox HTML injections.

Zeus Trojan

In retrospect, the arms race between SpyEye and Zeus seemed to have accelerated just before their announced merger: Zeus 2.0 was introduced in April 2010, while Zeus 2.1 was traced in August, just three short months later.

Zeus 2.0 made the Trojan 'compatible' with the latest versions of Windows and the Firefox browser, enabled multiple instances of the Trojan to run on the same infected machine, and added an FTP grabber, among other new functionalities. One of the most important changes in Zeus 2.0 was the naming convention used by the Trojan to name its files and directories.

Zeus 2.1 came furnished with a revolutionary digital signature mechanism – marking the first instance of this technology being used for malware as opposed to legitimate software. The digital signature on each file and update downloaded by the Trojan is now verified, and the latest version also keeps most of its strings in encoded form. These methodologies were clearly implemented to thwart reverse-engineering efforts by law enforcement and security researchers, and lower the feasibility of turf wars between competing cybercriminals over the same botnet.

Also new to Zeus 2.1 is the Trojan's ability to record data in numerous languages; data which was previously recorded by the Trojan as question marks, as well as the Trojan's record-keeping of the exact city, state and zip code of each machine. The latter feature enhances proxy-matching capabilities with compromised accounts and payment cards.

Stuxnet will undoubtedly spark a new type of arms race in the world – an arms race conducted with malware that targets physical infrastructure, unlike other forms of malware whose ultimate objective is to steal money.

The profusion and intense release rate of new Trojan upgrades, plug-ins and features observed throughout 2010 is likely to persist in commercially-available malware kits during 2011. As RSA traced numerous mule-management tools throughout 2010, mule management applications for managing automated transfers within man-in-the-browser Trojans are likely to continue to increase next year in quantity and sophistication, as well. With each new rung driven into the evolution ladder, security measures will become higher and tighter, spurring even more sophistication on the part of malware authors to avoid existing detection mechanisms. As a result, we will likely see shorter development cycles and accelerated releases of newer crimeware versions in the year to come.

In addition, the merger of Zeus and SpyEye, while not yet complete or available for purchase, will in effect provide one malware author with a monopoly on malware-for-sale kits. It is highly likely that today's vacuum will soon be occupied by new malware authors who seek a share of the profits that are currently only reaped by Harderman and 'licensed' resellers of the Zeus Trojan. This means that we are likely to see new malware kits being offered for sale in the underground throughout 2011.

Cybercrime Trend 4. An increase in privately developed Trojans, designed to conduct highly specialized attacks, will continue to proliferate in the wild

If you say “cyber attack against critical infrastructure,” the first word that comes to mind for most is Stuxnet – the specialized Trojan spread through a USB that was designed to target systems that run critical infrastructure. Stuxnet was unique in that it was one of the first pieces of malware of its kind to be devised for the purpose of attacking physical infrastructure. Stuxnet will undoubtedly spark a new type of arms race in the world—an arms race conducted with malware that targets physical infrastructure, unlike other forms of malware, Trojans, adware and worms, which simply partake in an economic supply chain whose ultimate objective is to steal money.

Experts agree that Stuxnet required immense resources to develop—resources equivalent to those of a nation state. Though privately developed and operated “banker Trojans” do not require nearly the same level of expertise on a wide range of fields, nor the same timeframe or manpower that researchers say would have been required to author the Stuxnet Trojan, banker Trojans do generally require a small team of at least two to three experts. The more sophisticated Trojans, such as those that perform MITB attacks, generally require a rootkit expert, an operating systems expert, and a web expert. In 2010, we saw the proliferation of a large number of privately developed and operated Trojans, authored to attack a specific set of targets, mostly a specific set of financial institutions’ websites.

The Lamp Trojan, in addition to collecting financial information from more than two dozen U.S. financial institutions, may also be specifically interested in industrial espionage.

For example, the **Qakbot Trojan** proliferated greatly throughout 2010 and was the first Trojan observed by RSA to exclusively target business and corporate accounts, as opposed to the more commonly-targeted personal bank accounts. Qakbot gained wide media attention when it famously infected the computer network of the UK’s National Health Service. The Trojan demonstrates a wide range of sophisticated behaviors, such as its ability to replicate itself over shared directories within local area networks (LANs), for example, LANs used by a small department or team within corporate organizations. This enables Qakbot to compromise even more corporate-based computers, whose users are more likely to access corporate online banking accounts.

Syscron (aka Carberp) is another private, highly-targeted Trojan with two main variants: The first, and by far the more pervasive one, targets only a handful of European-based banks, as well as a Russian webmail service provider. The second variant, which is far less pervasive, targets about two dozen banks, the majority of which are U.S.-based, along with a handful of European-based banks.

The **Nimkey Trojan** (aka Chilkat), also released into the wild in 2010, was most notably implicated in the theft of 1.6 million EU emission allowances (EUAs), valued at nearly 20 million Euros. EUAs are used to trade CO2 emissions within the 27-nation bloc, and studying Nimkey’s URL trigger list clearly shows that the Trojan targeted nearly all the participating countries EUA trading platforms (in addition to financial institutions).

Bancos, a variant of Brazilian Banker, was specifically coded to target eight South American banks, as well as two South American webmail services. The Trojan has a “cautious” installer, which first reviews a user’s browsing history to ascertain whether the user is in fact a customer of one of the targeted banks. If the computer is of no interest to the Trojan, its executable file remains packed and uninstalled, in a dormant state that is undetectable by anti-virus programs.

The **Lamp Trojan**, which according to some researchers may have been developed in China, contains an MS-Office Suite “Document Grabber,” – a specific command designed for the sole purpose of collecting Microsoft Office Suite documents. This is an unusual feature among private Trojans which typically focus on collecting financial and banking-related information. This implies that Lamp collects Word files, Excel spreadsheets, and PowerPoint presentations. Lamp may be one of the only examples of a Trojan that, in addition to collecting financial information from more than two dozen U.S. financial institutions, may be specifically interested in industrial espionage.

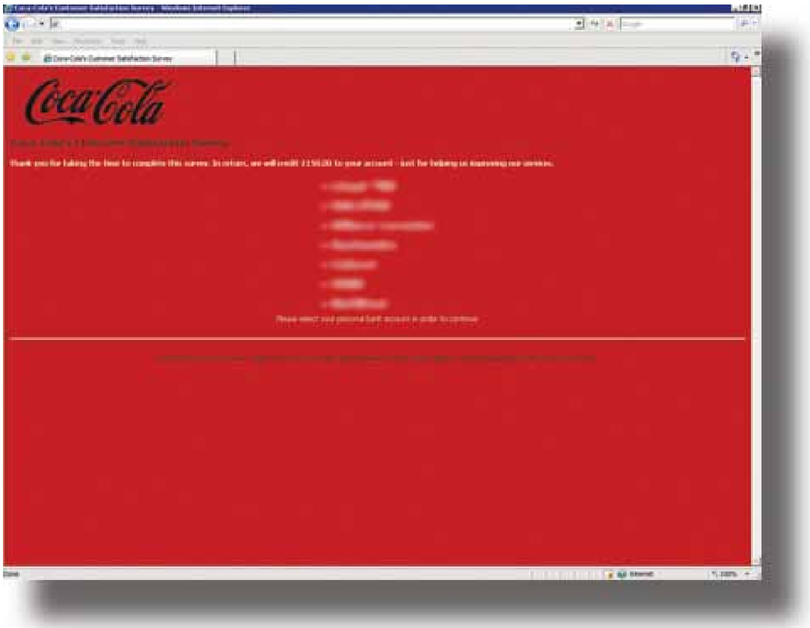
Other privately-developed, sophisticated Trojans that were initially released in 2009 and gained wider territory in the wild through 2010 include **Mimicker**, **Silon**, and **Bugat**. RSA expects to see more of these specialized Trojans created by closed crime rings in 2011. Privately developed and operated Trojans enjoy the advantage of creating less 'noise' on the web, as their operators carefully select their distribution channels. By virtue of having a smaller distribution, these Trojans are less likely to be traced and researched by anti-virus providers allowing them to stay under the radar for longer periods of time. Hence, the appeal of privately developed Trojans is likely to increase in 2011.

Cybercrime Trend 5. Evolution of phishing attacks and the organizations they target

While phishing attacks are one of the oldest tools in the cybercriminal's arsenal, their longevity has not prevented them from continuing to evolve. In 2009, we saw the launch of the first chat-in-the-middle phishing attack. In 2010, other types of phishing attacks emerged including attacks that simultaneously target the brands of multiple entities and attacks that intercept transaction confirmation codes sent to consumers' mobile phones as part of out-of-band authentication.

Phishing attacks that simultaneously target consumers of multiple entities, using different social engineering schemes, were very popular in 2010. Several of these attacks were distributed under the guise of important notices from tax collection agencies of various countries including the U.S., UK, Australia, South Africa, and India. These attacks presented users with a list of bank logos, prompting them to click on their bank's logo in order to log into their account and claim a tax refund. Yet instead of logging in to their account, users would log in to a phishing page where their online banking credentials would be captured.

Figure 2: After taking the survey, users were prompted to enter their online banking credentials in order to have their reward credited to their account .


Coca-Cola's Customer Satisfaction Survey - Windows Internet Explorer
Coca-Cola's Customer Satisfaction Survey
Coca-Cola

Thank you for taking the time to complete this survey. In return, we will credit [illegible] to your account - Just for helping us improving our services.

Please select your personal bank account in order to continue.

In another phishing scam that targeted multiple entities, online users were baited into entering their online banking credentials by an e-mail that masqueraded as a customer satisfaction survey. The phishing attack promised responders a monetary reward for their participation in the survey. After taking the survey, users were prompted to enter their online banking credentials in order to have their reward credited to their account (see Figure 2).

To validate online banking transactions in real-time, many banks across the globe deploy one-time passwords that are sent to a customer's mobile phone via an SMS text message. In 2010, RSA observed cybercriminals' attempts to bypass this security measure using phishing attacks that requested users to enter their online banking credentials. Next, users would be presented with a ‘delay page’ that showed a “please wait” message where they would be directed to a page that would prompt them to enter the one-time password sent to their mobile phones.

The act of phishing requires minimal set up fees and little technical knowledge. Cybercriminals are likely to continue developing their phishing kits in 2011, with functionality that includes targeting multiple organizations with a single attack and intercepting one-time passwords.

Conclusion

Cybercrime is a near and present threat for all organizations today. While primarily focused on the consumer and financial services industry for many years, cybercrime definitively made the shift into the enterprise in 2010. Cybercriminals are working everyday to create better technology that will lead to larger payoffs. They are switching their methods and hitting diversified targets to yield better information. As experienced by one organization: It took cybercriminals just four *hours* to overcome a countermeasure that had taken them four *months* to develop[6].

Managing risk against the threat of cybercrime is certainly not easy an easy task. One of the most important lines of defense is intelligence and awareness of the potential risks. Industry and governments have been making great strides to embrace information sharing among competitors and partners, but most importantly, the general public. In 2010, we witnessed many major arrests across the globe which can be directly attributed to improvements in international collaboration between law enforcement agencies. As we move into 2011, these continued efforts will play an integral role in the fight against cybercrime.

[6] http://www.thinq.co.uk/2010/10/25/how-bank-hackers-beat-barclays/#

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.

CYBERC WP 0111