THE CURRENT STATE OF CYBERCRIME 2014

An Inside Look at the Changing Threat Landscape

Web threats and fraud tactics continue to increase in number and sophistication as the profitability of cybercrime transforms the nature of the game. In 2013, phishing alone resulted in $5.9 billion in losses to global organizations, and three in four data breaches were attributed to financial or fraud motives[1]. Cybercriminals have become more organized and adaptive, and continue to develop fraud-as-a-service models which make some of the most innovative and advanced threat and fraud technologies available to a much wider user base.

RSA Research is at the forefront of threat detection and cybercrime intelligence, protecting global organizations with the shutdown of over 800,000 cybercrime attacks. Based on its insight into cybercriminal activity, including analysis of around 300,000 malware variants each week, RSA Research has identified the top cybercrime trends it expects to see evolving over the coming year.

Trend#1: Mobile Threats Become More Sophisticated and Pervasive

The worldwide smartphone market reached a new milestone in 2013 with one billion units shipped in a single year for the first time, up 38% from the 725m units shipped in 2012[2]. In July 2013 Google announced that over a million apps were available in Google Play and more than 60bn had been downloaded[3]. In October 2013, Apple announced similar stats for its App Store[4]. As our personal and work lives increasingly move to — and converge on — our mobile devices, cybercriminals will continue to develop and refine their schemes to capitalize on this trend.

As discussed in last year's report, malicious and high-risk mobile apps have become a significant threat vector as cybercriminals step up their efforts to serve malware and phishing attacks under the guise of legitimate apps. Android is still the most widely used mobile platform in the world which, combined with the open source nature of its operating system, means it is also the platform most targeted by mobile threats. The number of malicious and high-risk Android apps in existence reached almost 1.4m, one million of which were detected in 2013 alone (almost three times the number detected in 2012), with a significant proportion disguised as fake or malicious versions of popular apps[5].

Typically, cybercriminals will use social engineering to persuade a user to install a fake certificate or security software on their mobile phone. HTML injection techniques will be used to send the user to a direct link to download the malicious app. During installation, the app will request various permissions with the aim of gaining super user privileges that will provide full access to the phone's features and may make the app impossible to uninstall.

---

1 Source: Verizon 2013 Data Breach Investigations Report
2 Source: IDC Worldwide Quarterly Mobile Phone Tracker, January 2014
3 Source: Sundar Pichai, speaking at a Google breakfast briefing, July 2013
4 Source: Tim Cook, speaking at Apple's iPad event, October 2013
5 Source: Trend Micro, TrendLabs 2013 Annual Security Roundup

There's also at least one example of a pre-installed malicious app disguised as a fake version of a popular app. In March 2014[6], several variants of a fake Netflix app that steals personal and credit card data were found pre-installed on a number of models of Android phones and tablets from different manufacturers. Although it's not yet clear how the app came to be installed before the devices reached their users, one credible theory is that the malware authors targeted the supply chain, given that a relatively large number of individuals have physical access to Android devices along the way. This contrasts with Apple, which controls the device hardware and operating system from start to finish, making the supply chain much harder, if not impossible, to penetrate.

Unlike the fake Netflix app, the objective of many financially motivated malicious mobile apps is to steal the out-of-band passwords organizations use to provide an additional layer of user authentication. A typical example is a bank sending one-time passwords (or passcodes) by SMS that users must enter to confirm high-risk online transactions such as wire transfers. Fraudsters and cybercriminals have developed SMS sniffers (or SMS hijacking apps) that are designed to work with banking Trojans installed on PCs. The SMS sniffer intercepts the SMS messages and steals the out-of-band password to enable fraudulent transfers from the victim's bank account.

RSA observes that SMS sniffers have become a commodity sale in the criminal underground; and both banking Trojans and the associated SMS sniffers are increasingly available on a fraud-as-a-service basis, leaving the fraudster free to focus on monetizing the operation.

Furthermore, SMS sniffers are being developed with more sophisticated features. In November 2013, RSA researchers identified an SMS hijacking app targeting Android devices that offered new capabilities. Known as the iBanking Mobile Bot, it was offered for sale in a Russian-speaking underground community for $4,000–$5,000. Some of the functionality of the iBanking bot include:

Function	Comment
HTTP and SMS control	Send commands to the bot over HTTP or via SMS from a designated phone number.
Intercept all incoming SMS	Send stolen SMS messages to the attacker's web panel and the drop phone number.
Send SMS from the victim's phone to any number, without victim's awareness	Form of telephony fraud (monetization of mobile bots).
Intercept (forward) all incoming calls	Can enable hijacking of phone calls which will likely result in diverting security calls from the bank.
Steal device-related information	Phone number, ICCID, IMEI, IMSI, model, OS, network carrier, IP, geolocation, etc.
Steal contact list (names and numbers)	Can possibly be used in an infection campaign.
Capture audio using device microphone	Attacker can listen to and intercept the victim's private conversations.
Persistence	Reminiscent of Obad, the app attempts to social engineer the victim into giving it super-user privileges, making it impossible to remove the app. (The bot can also send an SMS notifying the operator of an attempt to remove the app.)

The iBanking mobile bot is capable of gaining access to:

1. All images stored on the device
2. A full list of the installed applications
3. The geo-location coordinates using the device's GPS to pinpoint the exact location of the device

6 Source: various, including http://www.cio.co.uk/news/security/pre-installed-malware-turns-up-on-new-smartphones/

These additions would help cybercriminals plan better Trojan-facilitated fraud scenarios, including more credible impersonation and identity theft possibilities.

2014 OUTLOOK: Mobile Threats

Malicious and high-risk apps are overwhelmingly programmed for Android devices. Although a few do exist for other platforms and more have been promised, Android's popularity and open platform make it likely to remain the focus of malicious app developers for some time yet.

The effectiveness of SMS sniffers means that, over the longer term, banks and other organizations will need to find less vulnerable ways to deliver out-of-band passwords. Alternatively, they will need to implement authentication solutions that don't rely on active user intervention, such as risk-based behavioral analysis and multi-factor authentication methods that take advantage of smart device features, such as the camera, speaker or geolocation capability, as discussed in Trend#4.

Trend#2: Bitcoin's Popularity Makes it a Target for Theft and New Fraud Currencies Emerge Forcing Cybercrime Activity Further Underground

Compared with other crypto- or cyber-currencies available today, Bitcoin is relatively trusted and popular. Its value is based purely on supply and demand, and is subject to considerable fluctuation. In May 2013 a Bitcoin was worth around $100; towards the end of the year its value peaked at over $1,000 — until the Chinese and Russian governments banned Bitcoin transactions over fears of money laundering, funding terrorism or tax evasion. Its value currently hovers at around $435 (April 2014).

Since its introduction in 2009, Bitcoin has gradually become more widely accepted in the mainstream. For example:

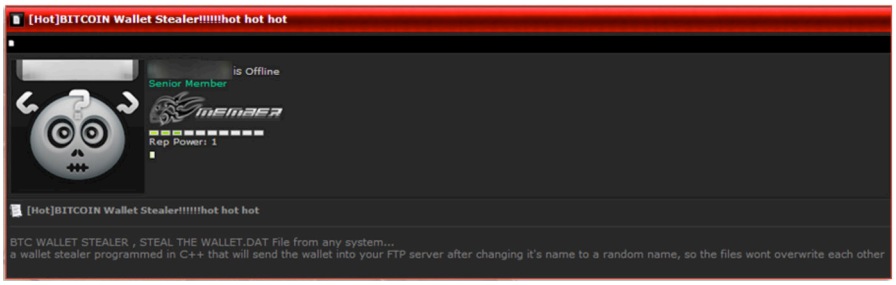
- Gaming outlets, and retailers including Overstock and Zynga, accept it as a valid payment method.
- In August 2013, the German government recognized it as a legal private currency and even imposed a tax on it.

The comparative anonymity of Bitcoin makes it similar to cash, inasmuch as it's difficult to associate Bitcoins with the holder or the receiver. Bitcoin therefore appeals to criminals and fraudsters as a payment method among themselves. This anonymity also makes the currency a target for theft, as there's little hope of tracing and recovering stolen Bitcoins. It's not surprising, therefore, that software has been developed to steal Bitcoin wallets (see Figure 1), and that Bitcoin holders are subject to classic phishing and social engineering attacks, including 419 scams.

In addition, a number of online Bitcoin exchanges have reported attacks by hackers suspected of creating fraudulent transactions by exploiting a flaw in the Bitcoin protocol in order to steal Bitcoins. An attack forced, Mt Gox, the largest and oldest Bitcoin exchange, to close in February 2014 and file for bankruptcy in the face of massive losses. Some 850,000 Bitcoins were reported to have gone missing, representing about 7% of all the Bitcoins in existence at the time — although Mt Gox did subsequently discover 200,000 of those missing Bitcoins in an old wallet.

Another major development last year that had a major effect on cybercrime business was the Liberty Reserve takedown in May 2013 and the confiscation of all accounts by law enforcement. Liberty Reserve was the preferred method of payment and cashout among cybercriminals and caused ripples as black market operators were forced to find new payment systems. Perfect Money and Bitcoin were considered as alternatives to Liberty Reserve, but lacked the anonymity required for dark business.

Figure 1: A sample posting in the underground advertising Bitcoin wallet stealers.



This has led to the growing adoption of forum-specific currencies which allow users to safely transact within their own community, under the supervision of a forum administrator, avoiding the use of the more public currency options such as Perfect Money and Bitcoin. In some instances, different forums shared the same currency further widening the use and adoption of these platforms. RSA Research analysts have been tracking several of these forum-specific currencies. One of the more popular platforms is the United Payment System currency which appears to be shared by four different Russian language forums, thereby allowing members from different forums to transact with each other.

Another currency being tracked in the underground is called LessPay. The operators of the service claim to be *"the next Liberty Reserve"*. Inside the forums, the service boasts anonymity, user safety, and the absence of account blocking. Adding and cashing out funds from a LessPay account can be conducted through a variety of exchanges and for just a small commission or fee. While still relatively new and immature, it has recently become the premier payment method in one of the biggest underground credit card stores.

2014 OUTLOOK: Bitcoin and Virtual Currencies

The closure of Mt Gox and other exchanges in the wake of attacks may ultimately push Bitcoin operators and exchanges to accept some sort of independent oversight at some point in the future. In the meantime, as long as it continues to be used as a payment method, Bitcoin wallets will be a target for theft and attacks. At the same time, the number of private currency systems will continue to grow and mature in the underground. By moving from less public to forum-specific currency systems, it will make it even more difficult for law enforcement to track cybercrime activity.

Trend#3: Malware Gets More Sophisticated, APT Attacks Remain Unabated and POS Malware Attacks Become Common

Fraudsters and cybercriminals are finding sophisticated new ways to make botnets stealthier and more durable, and to shield the data stolen during attacks. At the same time, they're also generating significant returns from unsophisticated hit-and-run POS malware attacks. Cyber-espionage attacks continue to occur with tactics that are largely unchanged and new players in the space being identified.

Stealthier, more durable botnets

Botnets are used by fraudsters, cybercriminals and hacktivists to host their infrastructure and launch attacks such as DDoS to bring down the websites of banks, government agencies and other high-profile organizations. The large number of zombie computers in a typical botnet means an attack will move around, making it difficult to find the source and shut the attack down. Even so, cybercriminals are developing even more robust botnets that can remain active for longer before being discovered.

– Botnets are being created that behave as similarly as possible to legitimate software and take considerable time and effort to detect. This has changed the way defenders focus their efforts, such as detecting when an infected computer communicates with a domain that's been used for cybercrime in the past.

– Hosting a botnet's command-and-control center in a Tor-based network (where each node adds a layer of encryption as traffic passes) obfuscates the server's location and makes it much harder to take it down.

– Cybercriminals are building more resilient peer-to-peer botnets, populated by bots that talk to each other, with no central control point. If one bot (or peer) in a peer-to-peer botnet goes down, another will take over, extending the life of the botnet using business continuity techniques.

– An alternative business continuity–led approach involves controlling a botnet from a mobile device using SMS messages. For example, some have speculated that the cyber attack on South Korean banks in early 2013 may have been a multi-vector attack that involved Android phones located in China, Korea or both[7]. With this type of botnet, if the primary command-and-control center gets shut down, the cybercriminal can redirect the botnet to an alternative center via SMS.

Attackers shield stolen data

The cybercrime world is like an arms race: cybercriminals pursue a course of action until the defenders work out how to combat it, at which point the cybercriminals change tack. An example of this is the use of password-protected zip files by APT attackers to exfiltrate stolen data. The challenge for the defender is to crack the password on the zip file to see what was taken. Because attackers tend to work from a script or within a structured framework, they will often reuse a password, enabling the defender to link attacks and open subsequent zip files with ease.

Once the attacker realizes they've been rumbled, they'll change something about their process in order to regain the upper hand — for example, switching from zip files to rar files (which are more difficult to crack), or using asymmetric encryption algorithms that are harder for defenders to reverse engineer. This results in the defender losing the ability to identify the stolen data and establish relationships between attacks, until he or she manages to crack the next one.

Cyber espionage attacks

Cyber espionage attacks have continued unabated in the last year, with attack methodology largely centering around spear phishing attacks, in which specific internal personnel are targeted with documents containing malicious Trojans to allow the attacker to establish a foothold in the network. Also popular last year were "Watering Hole"[8] attacks, or strategic web compromise, in which the attacker compromises a website that is of business interest to a target and uses it as an exploit platform to intrude into the target network. Attacker malware varies in sophistication, but simple methods continue to be successful for the most part.

While the frequency of reported incidents appears to have increased, this is likely due to a move towards intelligence-driven detection, rather than an actual increase in attacks. Additionally, new nation-state players such as the "Hangover"[9] campaign out of India and the "Snake"[10] campaign in Russia have made recent headlines and caused a shift in viewing cyber espionage as a threat originating from specific regions to a more global one.

---

7 Source: RSA Firstwatch blog "Tales From the Darkside: Mobile Malware Brings Down Korean Banks", March 2013 (https://community.emc.com/community/connect/rsaxchange/netwitness/blog/2013/03/21/tales-from-the-darkside-mobile-malware-brings-down-korean-banks)

8 https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/

9 http://normanshark.com/wp-content/uploads/2013/08/NS-Unveiling-an-Indian-Cyberattack-Infrastructure_FINAL_Web.pdf

10 http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf

Hit-and-run POS malware attacks

Hit-and-run attacks are carried out against retailers using point-of-sale (POS) malware, much of which is based on the free-to-use leaked code for Dexter and Alina malware. ChewBacca, which was uncovered by RSA in January 2014 (see Figure 2), and BlackPOS are other well-known examples of POS malware. This type of malware infects POS terminals, scraping the terminals' memory for the payment card and personal data — customers' names, card numbers, expiration dates and card verification value (CVV) information — that can be used to clone cards.

POS malware does this by searching for simple regular expressions for card magnetic stripe data. When a card number is found, it is extracted and logged. Even when a retailer is compliant with PCI DSS, unless data is encrypted or tokenized at the moment of capture at the POS terminal, there's a short window of opportunity during which it can be stolen in readable form.

This type of POS malware was used during the very high-profile attack against several large retailers late last year that affected tens of millions of card holders. The cost to financial institutions has so far been estimated at over $200m, and that only takes into consideration expenses for actions such as notification and card reissuance. That still does not account for fraudulent purchases making it a figure that is likely to increase in the long term. These attacks have mainly been confined to countries such as the U.S., where EMV technology is not yet in widespread use.

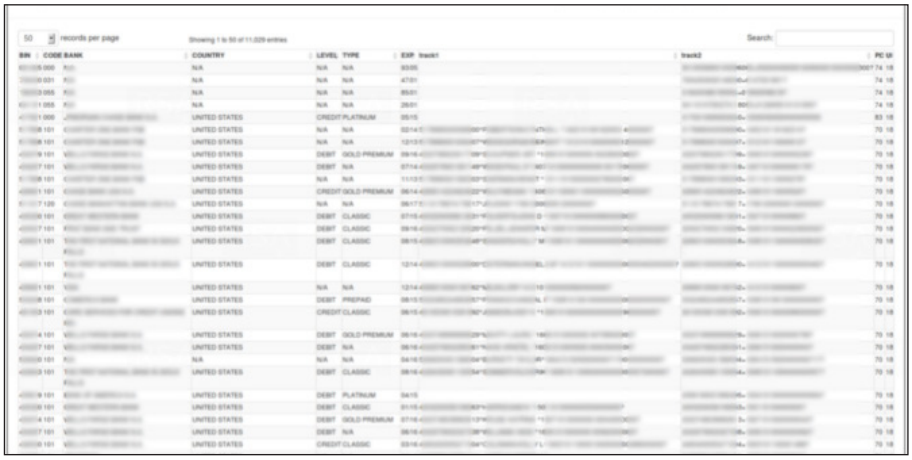


Figure 2: A server-side report from the Chewbacca malware which displays credit card details including Track 1 and 2, expiration date, and issuer.

Referral abuse malware

Some common breeds of malware were on the rise for inciting referral abuse in 2013. The malware is custom-designed to target corporations that pay cash to affiliate referrers for each installation of the target's software. This type of customized malware is written specifically to install software on a victim PC under a referrer's identity, make the infected machine click on ads that pay pennies per click, and direct it to purchase "likes" on social media.

In August 2013, RSA Research discovered a variant of the Zbot Trojan being used in referral abuse[11]. The typical charter of Zbot has been to attempt to swipe passwords, but this variant was also programmed to check for availability of Instagram usernames – likely in an effort to create an army of fake Instagram users that can be sold as followers to help individual users or businesses create an image of popularity. The same Zbot variant was also capable of SEO poisoning to help boost keyword rankings, likely in an effort to push its own content to the top of search engine results. These rank-abuse promoted pages often contain malicious content to spread additional malware.

11 https://blogs.rsa.com/new-zbot-variant-builds-instagram-army/

2014 OUTLOOK: Malware Continues to Spawn New Waves of Attacks

From POS malware to referral abuse, cybercriminals are continually in search of new approaches to monetize their bots. At the same time they seek to spawn new attacks, they are also creating more bulletproof infrastructure on the backend. They are moving their infrastructure to P2P and Tor-based networks to evade detection. They are changing the methods they use to mask stolen data, making it more difficult for researchers to reverse engineer and understand the methods being used behind prominent cyber attacks. Advancements in cybercrime technology and infrastructure will only continue. For example, given the computing power contained in a smartphone and criminals' willingness to adopt new technology, it is likely we will witness more mobile-phone-based botnets and command-and-control centers over the coming year.

Also, with the scale of several high-profile data breaches, we are likely to see a shift in the U.S. market towards adoption of EMV payment cards. It will be slow, but 2014 will be a pivotal year in making the move. Regulations such as PCI-DSS will be re-evaluated and lead to stricter guidance for retailers to implement encryption or tokenization at the point of sale. Until there is a major industry change, there is little reason to expect criminals to stop using POS malware–based attacks against retailers, given the enormous returns that are possible from this relatively unsophisticated, easy-to-obtain malware.

Trend#4: User Authentication Will be Redefined by Mobile

The password problem has long been an issue for organizations with any online presence, especially those with consumer-facing portals, where the number of digital identities requiring protection reaches into the millions. Consumers create multiple digital identities requiring them to remember multiple passwords. This can lead users to create weak passwords, write them down on paper, or re-use them across multiple sites. In fact, one in five online users recycles the same password for every online account[12].

Major password breaches made headlines throughout 2013, compromising tens of millions of passwords, user IDs, email addresses and other personal information. In many cases, passwords were stored in plain text. But even where advanced protection methods such as hashing and salting were used, password-guessing software was employed by hackers to readily crack them. In fact, according to the 2013 Verizon Data Breach Investigations Report, over 75% of attacks leveraged weak or stolen credentials.

The resulting brand damage and outrage on the part of consumers caused by these large-scale breaches have led many organizations to rethink their password policies. It is not uncommon for organizations to require users to create a complex password which consists of numerical characters and special symbols. Even the average length of acceptable passwords has gone from six to eight or even ten characters.

However, creating strong passwords doesn't solve the problem as consumers and organizations must also contend with malware threats, most of which today are equipped with keylogging functionality designed to steal password credentials and other data. Not to mention the risk of social engineering, where the malware presents the user with legitimate-looking screens asking for credential information (such as one-time passcodes). Therefore, the strength of a password is of no significance if it is captured by a data-stealing Trojan.

12 Kaspersky Lab Infographic, March 2013

The password debate is only further complicated when you consider the increased use of mobile services. Consumers are bringing more of their daily lives to their mobile device — from conducting financial transactions and making purchases to managing their personal health and wellness. Organizations are being forced to accommodate the demands by employees, partners, and other stakeholders to incorporate Bring Your Own Device (BYOD) polices that would enable more remote access services from mobile devices. As more users start using mobile devices for personal and professional business, strong passwords simply don't meet usability requirements. Passwords that may be easy to enter on a physical keyboard are difficult to enter on a mobile touch screen.

These and other factors are pushing organizations to redefine traditional user authentication. Beyond consumer use cases, organizations are grappling to offer the same flexibility to their mobile workforce by providing the convenience of technologies they are already familiar with and use in their daily life (e.g. online banking). But the struggle to extend these capabilities securely is complicated by both technological and usability challenges. From the technological perspective, organizations must address issues such as the lack of central control within cloud-based applications, lack of security in mobile app development, and the inability to authenticate from multiple devices. From the usability perspective, there is a shortage of strong authentication options in the market built for mobile devices, coupled with the paradigm of balancing security and mobile users' demands for convenience.

As mobile devices continue to become more pervasive, this opens up the ability to use a rich set of factors for deeper authentication through a smartphone or tablet. Using cost-effective technologies built into those mobile devices, such as the camera, speaker, accelerometer, fingerprint sensor and geo-location to enhance authentication also enables a more convenient user experience. There is a wide range of user authentication technologies that have potential on mobile devices, based biometrics such as fingerprint, face or voice print, iris structure, ear shape and heartbeat analysis, as well as "behaviometrics" like keystroke analysis and handwriting.

2014 OUTLOOK: User Authentication Redefined

The industry is at a major crossroad in user authentication. Besides the volume of password breaches and resulting consequences to targeted organizations, the growth in use of mobile devices for both personal and business use cases is pushing organizations to redefine user authentication and find new ways to secure access beyond traditional username and password. RSA expects that traditional authentication services will be designed for ultimate user convenience on mobile devices and will be driven by enhanced identity management, adaptive analytics, and policy enforcement engines. New unified authentication solutions and services will be developed over the next one to three years to support a range of multi-factor strong authentication methods that are built in to the smart device, including biological and behavioral biometrics, enabling user choice of devices while maintaining control over access to sensitive data. RSA also anticipates that consumers will become more identity-aware and will take action to safeguard their privacy by leveraging tools to manage their own security.

Conclusion

Through constant innovation, cybercriminals are developing increasingly sophisticated malware — including mobile malware — and botnet management techniques, alongside fraud-as-a-service models that make many types of malware much more widely available. At the same time, a lot of criminal and fraudulent activity still relies on relatively unsophisticated malware, such as POS malware, and classic phishing attacks that continue to yield good returns.

Organizations are therefore challenged on many fronts in their efforts to protect their data and that of their customers, partners and suppliers from cyber threats. More mobile workforces and customer bases, and extended supply chains, throw into relief the pivotal role of user authentication, and the resulting need for more sophisticated approaches to securing access than conventional controls based on usernames and passwords. The shift towards software-defined networks, cloud infrastructures and BYOD adds further complexity.

Together these trends are driving the need for intelligence-driven security and identity management systems that can operate in mobile and cloud environments, enable greater use of behavioral analytics, and take advantage of smart device capabilities to protect users and data from hackers, fraudsters and cybercriminals.

There's also a pressing requirement for anti-malware that's able to spot — and block — zero-day threats. However, organizations recognize that good security isn't just about preventing attacks and breaches. It's also about accepting that attacks are inevitable, and implementing tools and techniques that provide the actionable intelligence to enable rapid detection and remediation. In essence, the more an organization is able to narrow the window of opportunity for an attacker, the better they can minimize damage and losses.

There also continues to be an increased focus on sharing intelligence about threats and attacks with peers, government agencies and the security industry, to increase knowledge across the board. The security industry will be redefined by intelligence and knowledge sharing which will be critical to help drive improvements in best-practice approaches to combating cyber threats.

About RSA

RSA, The Security Division of EMC, is the premier provider of intelligence-driven security solutions. RSA helps the world's leading organizations solve their most complex and sensitive security challenges: managing organizational risk, safeguarding mobile access and collaboration, preventing online fraud, and defending against advanced threats.

Combining agile controls for identity and access management, fraud detection, and data protection, robust Security Analytics and industry-leading GRC capabilities, and expert consulting and advisory services, RSA brings visibility and trust to millions of user identities, the data they create, the transactions they perform, and the IT infrastructure they rely on. For more information, please visit www.RSA.com and www.EMC.com.

CYBERTR WP 0414

www.emc.com/rsa

EMC²

RSA