

WHITE PAPER

2018 CURRENT STATE OF CYBERCRIME

The cybercrime landscape evolves year over year as criminals alter their operating strategies, develop new tools and techniques, and take advantage of changes in consumer and business behavior.

Mobile continues to remain vulnerable to cybercriminals as its popularity as a banking and e-commerce channel grows and more services become available via mobile apps. Cybercriminals are also jumping on the internet of things (IoT) bandwagon by exploiting poor password practices to take over IoT devices for their own purposes. In addition, industry standards and global regulations are driving a digital transformation, yet opening up new points of vulnerability that have the potential to be exploited.

RSA remains at the forefront of fraud detection and cybercrime intelligence, protecting more than one billion consumers around the world from phishing, malware, account takeover, social media threats and other high-impact fraud attacks, and preventing billions of dollars of fraud losses every year. Based on our insight into fraud and cybercrime activity and the latest industry standards and global regulations, we have identified four topics we believe will be significant and directly impact the state of cybercrime in 2018.

[PREDICTION #1] MASS DATA BREACHES WILL CONTRIBUTE TO A SPIKE IN ACCOUNT TAKEOVER

A new market for nonfinancial credentials is emerging in the cybercrime underground, thanks to mass data breaches and phishing attacks exposing billions of usernames and passwords. Relying on the fact that many people use the same username-password combination across multiple accounts, cybercriminals are making money by selling stolen credentials.

Naturally, verified account credentials command a premium, as they can be more readily used to take over other accounts—for example, making fraudulent purchases or money transfers, or hacking Bitcoin and other cryptocurrency wallets—so the business of credential testing services is expanding as well. Yet, other factors contributing to the price of stolen account credentials include the brand, whether there is a credit card on file and how easy it is to resell the goods or services. Today, account credentials may sell for as little as \$0.20 up to \$15 USD.¹

Automated tools, such as Sentry MBA, enable cybercriminals to carry out high-speed username- and password-guessing attacks, sometimes called credential replay attacks. These tools are available at low or no cost, or on a fraud-as-a-service basis. Account takeover success rates can hit up to 5% and produce an acceptable yield of valid credentials to cybercriminals² for their own personal use or downstream sale.

¹ RSA 2018 Cybercriminal Shopping List

² Source: 451 Research, Web Threat Detection Pathfinder Report, 2016

It can be difficult to spot these automated attacks because legacy tools such as web application firewalls (WAFs) are not designed or architected to look for them. More organizations are turning to behavior analytics technologies to assure authenticated users and anonymous guests are interacting with their website in expected ways. These technologies can identify unusual patterns of behavior across both web and mobile applications—for example, the way a user navigates a site or robotic activity, such as thousands of login attempts within only a few minutes.

2018 OUTLOOK

We expect to see more mass data breaches in 2018, leading to a flooded market for stolen credentials. As a result, verifying credentials will become even more of a priority for cybercriminals looking to monetize them. We also anticipate the development of credential checking tools that are programmed to transact immediately following a successful login as a way to try and bypass fraud prevention systems leveraging behavior analytics.

If the value of Bitcoin continues to soar at the rate seen towards the end of 2017, digital wallets containing Bitcoin and other cryptocurrencies will also become an evermore attractive target for cybercriminals wielding stolen credentials.

[PREDICTION #2] CYBERCRIME OPERATIONS WILL EXPAND TO NEW PLATFORMS AND INFRASTRUCTURE

Cybercriminals constantly look for ways to keep their activities up and running. The takedown of two of the largest underground marketplaces for illegal and illicit items in 2017, AlphaBay and Hansa, sent cybercriminals scrambling for alternative ways to secure their operations. Two newly favored options are social media platforms and websites hosted on the blockchain.

SOCIAL MEDIA PLATFORMS

Many cybercriminals are turning to social media, transforming it into what may well be the fastest-growing communication channel for cybercriminals. Using social media allows them to vastly extend their reach to more people. The platforms are global, easy to use and have none of the fees associated with running a forum on the dark web or hosting a website.

During a six-month study of cybercriminals' social media use, RSA saw a 70% growth in the volume of visible fraud activity on social media, much of it occurring in plain sight. Fraud-dedicated groups seem to make little effort to operate stealthily. Even in closed groups, a simple "join" request is all that is needed to gain access, instead of the references or vouching process typically needed to join a forum on the dark web.

On Facebook—the single most popular channel—active groups in all regions of the world are openly sharing live, compromised financial information (such as credit card numbers with PII and authorization codes), cybercrime tutorials, malware and hacking tools, and cashout and muling services. Some cybercriminals even sell stolen credit card data and hacking kits from their own personal profiles. Figure 1 demonstrates the most popular fraud topics posted and discussed in these groups.

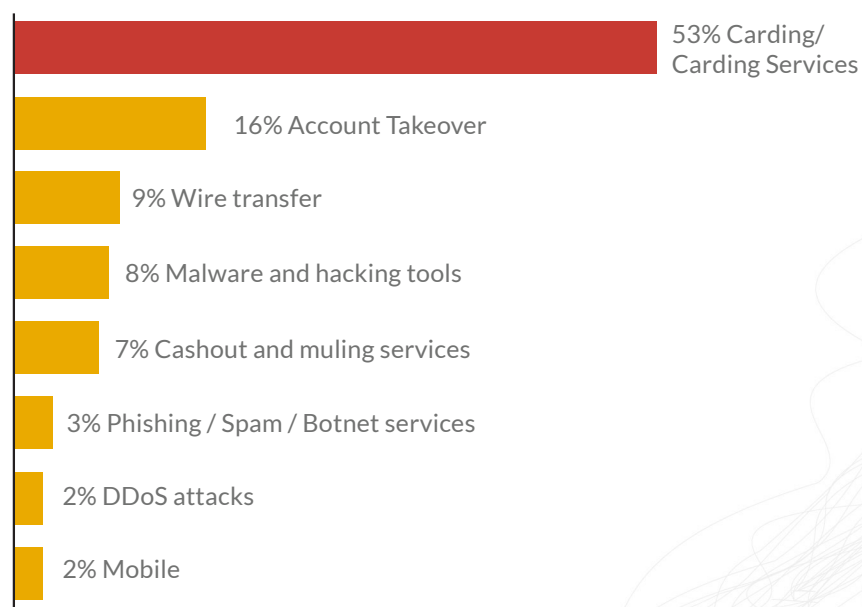


Figure 1: Most Popular Fraud-Related Posts on Facebook

BLOCKCHAIN HOSTING

A new phenomenon among cybercriminals is an increased interest in hosting their websites on the blockchain. Some even register domains using a blockchain-based DNS. The advantage of using the blockchain-based DNS feature is that the website can retain its blockchain-based domain, rendering it bulletproof against any attempts to reroute the domain or prevent access to the website by a centralized entity. As a result, cybercriminals are making significant steps towards the adoption of this technology and utilizing the benefits of this platform to guarantee the sustainability of their operations.

Figure 2 shows one example of a prominent credit card store in the dark market making the transition to blockchain hosting.

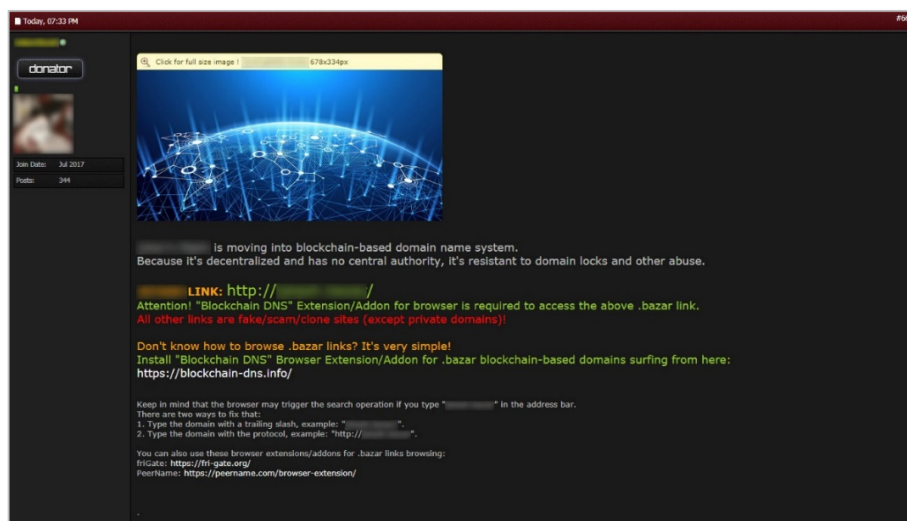


Figure 2

INTERNET OF THINGS (IOT) DEVICES

IoT devices—including doorbells, fridges, activity trackers, smart watches, home heating systems and medical devices—are becoming part of everyday business and consumer life. These devices are an increasingly attractive target for cybercriminals, who are taking them over with ransomware and adding them to their infrastructures.

The tendency for these connected devices to use default passwords makes it all too easy to compromise them. “It’s only a fridge,” one might think; but in fact, it’s a device that can become part of a botnet and used to launch a DDoS attack or host a phishing website.

2018 OUTLOOK

Use of social media platforms by cybercriminals is a phenomenon that shows no sign of diminishing, despite action by the platform operators to remove posts, profiles and groups engaged in illicit activities. While Facebook will remain popular with cybercriminals, we expect to see increased growth in new social media platforms as a fraud communication channel. Cybercriminals will also continue to extend and expand their infrastructure leveraging the blockchain and IoT devices, and as a result, there will be an increase in related fraud-as-a-service offerings.

Mirai Botnet

Mirai is one of the best-known examples of the exploitation of IoT devices to host cybercriminal infrastructure. The Mirai botnet seeks out poorly secured IoT devices and uses a table of more than 60 common factory default usernames and passwords to log in to them. It then infects them with malware, rendering them part of the botnet.

Mirai is known to have exploited IP cameras, routers and DVRs—a list that will grow as more devices are sold and new connected devices enter the market.

[PREDICTION #3] OMNICHANNEL EXPANSION, OPEN APIs AND FASTER PAYMENTS WILL PRESENT NEW VULNERABILITIES TO EXPLOIT FOR FRAUD

As consumer transactions migrate to the mobile channel, so does fraud. Meanwhile, the dawning of the open API economy and growing adoption of faster payment mechanisms are driving innovation, but also increasing potential fraud exposure.

MOBILE FRAUD

Today, mobile fraud is outpacing web fraud. More than 60% of fraud originates from mobile devices. It used to be mobile browsers that were fraud heavy, but now 80% of mobile fraud comes from mobile apps.³

It's a natural shift for cybercriminals, given that many banks and retailers continue to extend the range of services their mobile apps support. Once a cybercriminal has taken over an individual's mobile banking app, they are able to carry out actions such as setting up new payees and initiating transfers. RSA data shows that fraudulent transactions from the mobile channel are more than double the value of genuine transactions, as shown in Figure 3.

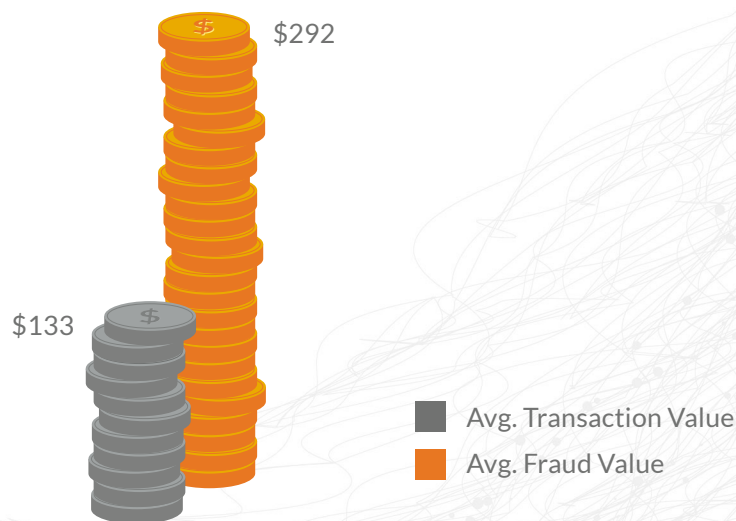


Figure 3

OPEN API ECONOMY

Under pressure to remain competitive in a strong FinTech market, financial institutions are leveraging the open API economy and opening up their systems. In some cases, it's an obligation. For example, the EU's Payment Services Directive II (PSD2) requires banks that do business in Europe to open access for data aggregators and payment services. There are similar initiatives and regulations in the United States and Asia as well.

³ RSA Adaptive Authentication Data Science Analysis, 2017

In practice, this means a consumer can connect their bank account to other services, such as a credit rating agency or utility. They then benefit from the convenience of a single sign-on from their bank account to view their credit score or pay their electricity bill, in addition to carrying out banking transactions. They may also be able to view their bank account information through third-party applications.

This is a significant shift from the past, when banking information was held in closed systems. This shift is expected to drive innovation by giving consumers easier access to their money and more flexibility in moving it around while helping to expand the market for digital wallets and other electronic payment systems. However, it also opens up new potential for fraud exposure if proper security is lacking.

As an individual's bank account becomes their one-stop shop for a range of services, it can be used in the same way by a cybercriminal who gains access to it. The risk is borne by the bank (or other organization), which must up its consumer authentication game to ensure appropriate protection of customers' money and data.

FASTER PAYMENTS

Last year saw advances in the speed with which consumers and businesses can make payments—a trend expected to continue. It is a watershed moment for the payments industry in particular, and the banking system as a whole, as instant, same-day, real-time and person-to-person (P2P) payment services take off.

A successful example of such services is the U.K.'s Faster Payments Service (FPS), rolled out around ten years ago, which has seen rapid adoption and is changing the way consumers transact and pay bills. In 2017, FPS processed 1.7 billion payments and over 1.4 trillion euros in payment transfers, and today accounts for more than one in six non-card- and non-cash-based payments.⁴ Similar services now being implemented in the U.S., Australia and New Zealand are finding favor with increasingly digitally engaged consumers.

The fraud risk with faster payments is that there's little or no time to review, recall or stop a payment once initiated. For instant and same-day payments, therefore, proper authentication is critical to prevent fraud. Given that customers use these services precisely because they are quick and seamless, banks and other service providers must determine risk correctly and strike the right balance between effective security and a frictionless customer experience.

2018 OUTLOOK

As banks, payment providers and retailers extend services to mobile and other digital channels, they face new challenges and vulnerabilities that could

open their customers and their businesses up to increased fraud and new types of attacks. Organizations need to evaluate their omnichannel strategies to provide effective protection and fraud detection across multiple channels, without losing sight of customer expectations for speed and convenience.

Organizations should be prepared to ask their customer authentication providers hard questions about how well-suited their solutions are for multichannel environments and, in particular, how they address mobile users' needs. Authentication providers should also be able to demonstrate a clear understanding of how new and emerging regulations and standards impact an organization's business strategy.

[PREDICTION #4] ISSUERS AND MERCHANTS WILL PREPARE TO ADOPT 3D SECURE 2.0

E-commerce fraud results in a whopping \$660,000 in losses per hour.⁵ The huge impact of these losses on banks and card issuers, as well as on merchants, is set to drive strong adoption of the 3D Secure 2.0 protocol (also known as EMV® 3D Secure).

This prediction is more than a hunch. Research commissioned by RSA revealed that 57% of merchants plan to adopt 3D Secure 2.0. These companies see the potential of the more powerful and data-rich version of the protocol to help them deliver even better fraud protection to their customers.

With global e-commerce sales set to top \$3.5 trillion,⁶ there is no doubt that cybercriminals will also be keen to take advantage of this growing channel. The 3D Secure 2.0 standard is designed to deliver even greater fraud protection, while putting the customer experience at the center of payment authentication.

2018 OUTLOOK

Risk-based authentication will be a key enabler driving adoption of 3D Secure 2.0 and has consistently proven to result in higher approvals and lower fraud. As global deadlines for adoption loom, issuers and merchants will start their readiness preparation throughout 2018 to ensure a smooth migration, and there will likely be a handful of early adopters to help lead the way. Issuers will also likely plan their 3D Secure 2.0 strategy in accordance with local regulations such as the EU's PSD2 directive.

CONCLUSION

Organizations are challenged on many fronts in their efforts to protect their customers and their businesses against fraud. The growing popularity of mobile for retail, banking and other services makes it especially vulnerable to cybercriminals and requires organizations to ensure an effective approach to security across all digital channels.

Although major dark web marketplaces have been shut down, cybercriminals are staying in business by adapting to other platforms, ranging from familiar social media channels to more specialized blockchain infrastructures. They are also developing new tools to take advantage of advances in payment services that are designed to make life easier for genuine customers.

Fraud-prevention approaches now require solutions that can extend to mobile and cloud environments, make greater use of behavioral analytics, take advantage of integrated threat intelligence capabilities, and most importantly, be designed with customer experience in mind. While it is impossible to stop every fraud attack, it is possible to change how organizations detect and respond to them in order to minimize potential loss or damage.

⁵ Source: RSA, Mind-Blowing Cost of Cybercrime Every 60 Seconds, October 2017

⁶ Source: Aite Group, The Force for CNP Fraud Awakens, March 2016