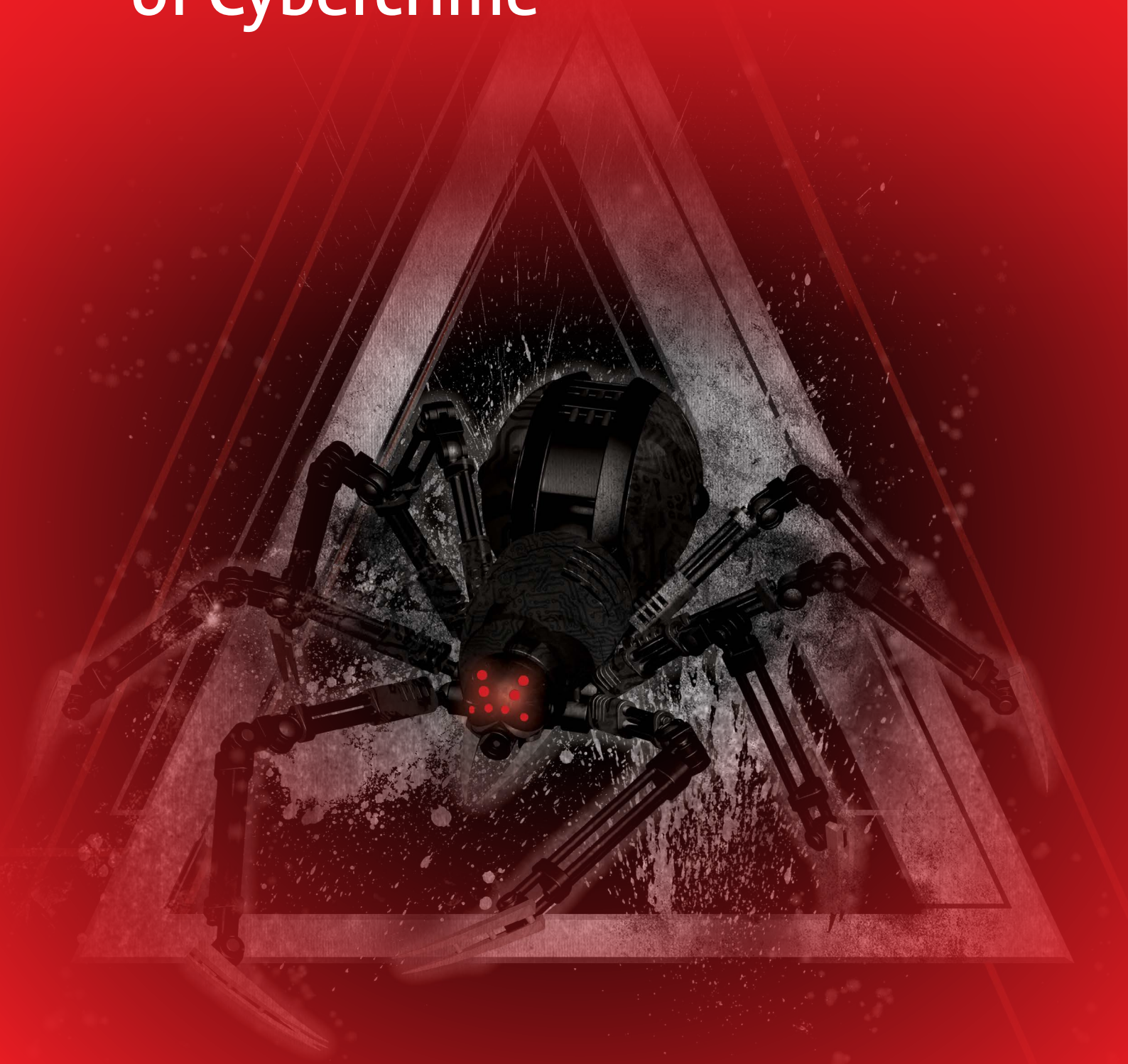
RSA

2016: Current State of Cybercrime



WHITEPAPER

Introduction

There is a truism in today's clickable economy: wherever there is commerce, there is also the risk for cybercrime. Whether a financial institution, an Internet storefront that does business with online shoppers, and now even hospitals with the rising tide of ransomware, cybercrime has no boundaries. In fact, anyone with an email address, an inbox, or a social media account is a target. Most organizations or individuals are not even aware of the bullseye on their back for hackers, cyber thieves, and extortionists until it's already too late to respond or recover from being attacked.

Against this dynamic and challenging environment, there are several key issues that are even now proliferating across the digital flight path. Each has the ability to disrupt business as usual and each has the power to take over identities, and in extreme cases, even threaten someone's life. From mobile threats and ransomware to the role of biometrics in reducing fraud, a myriad of threats exist across the cyber landscape and the commoditization of cybercrime is making it easier and cheaper to launch attacks on a global scale.

As attackers are well-organized and well-informed, take advantage of the latest fraud-as-a-service innovations and capitalize on shared intelligence in the deep web, organizations must be prepared to do the same. Being attentive will not keep you out of the crosshairs of a bad actor's line of sight or out of the headlines. This paper will examine the current state of cybercrime and explore how organizations and individuals can marshal to respond to the industrialized cybercrime threat.

From mobile devices to routers, hackers are always in search of non-PC platforms (and likely less protected) to compromise. As mobile continues to eat the world, so will the attacks waged against mobile devices, mobile services, and mobile users.

Mobile Eats the World

From mobile devices to routers, hackers are always in search of non-PC platforms (and likely less protected) to compromise. As mobile continues to eat the world, so will the attacks waged against mobile devices, mobile services, and mobile users.

Mobile transactions are growing rapidly, but fraud is outpacing it as cybercriminals are migrating to less protected, "soft" channels. In 2015, RSA saw that 45% of all transactions originated from the mobile channel while 61% of fraud attempts were made from a mobile device. As organizations continue to roll out more mobile services to customers and employees begin to depend on them in order to do business on their behalf, the mobile channel has become rife with cybercrime.

Mobile is eating the world and becoming the dominant channel for instant communication and the expressway for banking and commerce worldwide. In fact, by 2020, it is estimated that 80% of adults on earth will have a smartphone[1]. Mobile devices helped influenced more than $1 trillion in total purchases in 2015 between online and offline transactions[2], and revenue from mobile e-commerce sales are projected to reach $516 billion by 2017[3].

As organizations transform the way they interact with customers, this has not gone unnoticed by cybercriminals as evidenced by the rise in fraud attempts originating from the mobile channel, increasing 173% increase between 2013 and 2015 compared to a mere one percent in the Web channel[4].

Mobile is not the only platform at risk, however. Other non-PC based platforms have been targeted including routers which were subject to malware that allowed attackers to gain nearly undetectable remote control to launch attacks against other routers and systems on the same network.

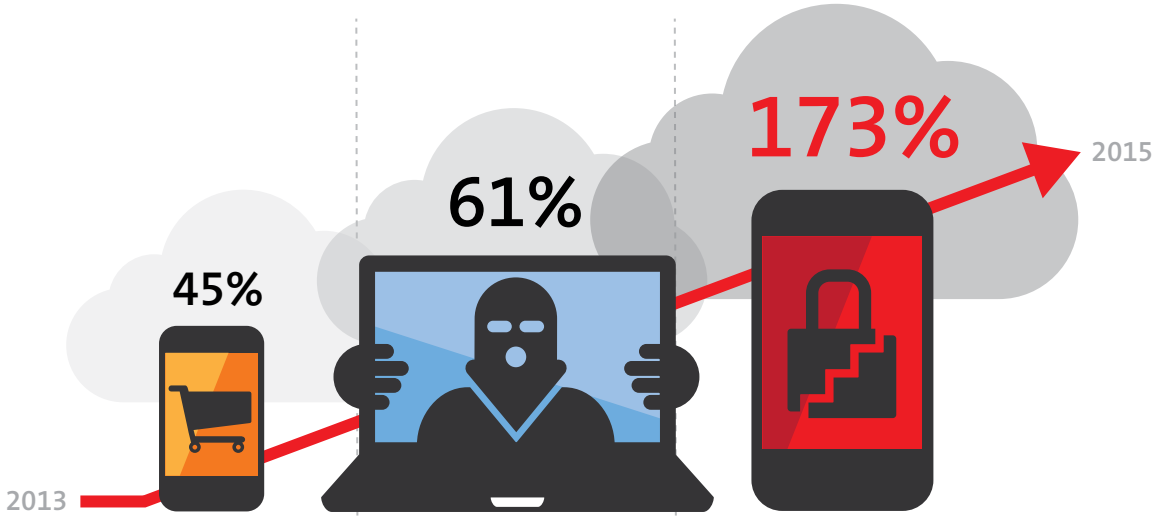
1 GSMA
2 Forrester Research, "U.S. Cross-Channel Retail Forecast, 2015 To 2020"
3 Statista, "Mobile Retail Commerce Revenue Worldwide"
4 RSA Adaptive Authentication Services

To assure the integrity of the mobile channel, there is a growing interest in the use biometrics. For mobile-based authentication, a recent RSA survey showed over 90 percent of banks are currently exploring the use of biometrics in their mobile apps or intend to explore them within the next six to twelve months.

Ransomware and cyber espionage will continue to proliferate, putting critical data, and even lives, at risk.

Biometric authentication is not just the talk of proof-of-concepts or patent pending ideas. It is real and quickly gaining popularity among consumers. Some financial institutions have even started to deploy it along risk-based authentication to allow customers to access services like balance checking, fund transfers, cardless ATM withdrawals and payment verification.

The combination of biometric technology integrated with risk-based authentication services is enabling a new generation of authentication services to replace passwords and PINs while meeting the needs of end users to deliver security in a way that is simple and seamless. RSA anticipates a growth in deployment of risk-based authentication services coupled with biometrics in the next one to three years as organizations look to minimize fraud losses as they move more services to the mobile channel.



Ransomware and Cyber Espionage Proliferate

Ransomware and cyber espionage will continue to proliferate, putting critical data, and even lives, at risk.

Ransomware — the virtual equivalent of real world extortion — is increasingly the subject of both media coverage and incidence with an average payment of $500 to the "ransomeers" to release your data. The reason ransomware has become so popular for attackers all converges around the same thing: it makes money — easily, singularly, and in almost every case, payment is guaranteed as organizations and individuals respond to fear.

The U.S. Federal Bureau of Investigation and other law enforcement agencies have even advised organizations and individuals to pay the ransom or risk not getting their data back. One particular strain of Cryptowall ransomware was estimated to have cost victims over $325 million in 2015[5].

5 Cyber Threat Alliance

But when lives are at risk, the issue or ransomware – to pay or not to pay – is pressing. This was the case when one California hospital paid a ransom of $17,000 to attackers to recover access to its computer systems and therein patient records. Another hospital soon announced it was operating under an "internal state of emergency" after a ransomware attack held their computer systems hostage.

Additional high-profile, maximum impact targets for ransomware abound. These include reports that someone opened a phishing email at Israel's Electricity Authority which provides utility services for the country. As a result, not only was that individual's computer infected with ransomware, but so too were other computers in the Authority's network. While the electric grid was itself not "taken down," the fact that ransomware was used to describe the attack generated concern among providers of critical infrastructure globally.

Cybercrime will become further commoditized. From the types of data targeted for compromise to new fraud-as-a-service models, fraudsters are continually undergoing evolution. Even the ways they communicate are changing.

Complicating the ransomware matter even further is that virtually no machine or operating system is immune from infection. There has been ransomware distributed across mobile devices, Linux ransomware that targets web servers and, most recently, Apple saw its MACs breached by the recent discovery of "KeRanger" ransomware.

The takeaway from these extortion-based infections, and subsequent payment to criminals, will likely lead to increased attacks on critical infrastructure – bigger targets translates to bigger rewards. Due to the sensitivity, level of accessibility required for patient care, and ultimately, the potential to directly threaten human life, healthcare systems will be particularly impacted by ransomware.

Regardless of whether ransomware is deployed by organized cybercriminals or propagated by more opportunistic attackers leveraging an as-a-service vendor, ransomware will become more intrusive over the coming year. To counteract the spread of ransomware, organizations should deploy a security monitoring solution that uses behavioral-based analytics that focuses on detecting these active threats by analyzing the behavior of every process executed on the endpoint as well as the network activity into and out of the enterprise.

Organizations will start to move to security monitoring solutions that leverage behavioral-based analytics as they are far more effective by looking for a set of suspicious indicators rather than relying on static indicators or signatures. Such tools can be deployed to detect, understand, and block the execution of ransomware on any endpoint to prevent further spread across the corporate network and overall reduce the dwell time of the attack.

The Commoditization of Fraud Requires Intelligent Response

Cybercrime will become further commoditized. From the types of data targeted for compromise to new fraud-as-a-service models, fraudsters are continually undergoing evolution. Even the ways they communicate are changing.

The ease of external agent attacks resulting from commoditized malware leaves nearly every provider of any type of service vulnerable. The proliferation of ransomware as discussed is just one example, and even these attacks have been reduced to a fraud-as-a-service offering.

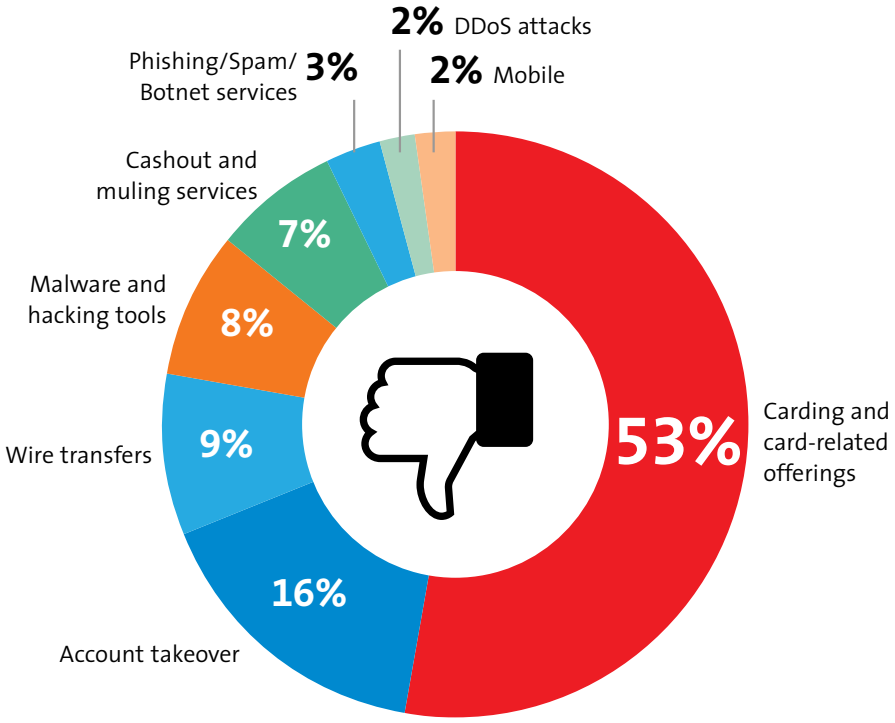
However, for some cybercriminals who enjoy the chase but are unsure to what to do with the data they have captured from these attacks, there is now a solution. The black market is no longer just a storefront for selling stolen credit cards. Any type of credential or account access that exists can be found for a price. E-commerce, email and social media accounts are up for bid, typically ranging from $2 to $10. There is even demand for the most unlikely types of data such as healthcare records and patient medical history.

Even the ways cybercriminals sell, communicate and exchange information is changing. Recently, RSA uncovered the broad use of open forums, specifically social media, being leveraged by cybercriminals to communicate and as general global havens for cybercrime.

In a six month study, RSA uncovered more than 500 fraud-dedicated social media groups around the world with an estimated total of more than 220,000 members. More than 60 percent, or approximately 133,000 members, were found on Facebook alone. The types of information openly shared in social media include live compromised financial information such as credit card numbers with PII and authorization codes, cybercrime tutorials, malware and hacking tools, and cash out and muling services. On a global level, carding stands out as the most popular fraud activity, comprising 53% of the posts RSA observed.

Beyond a single enterprise view, tracking cybercrime developments that are global, cross-industry, cross-channel, and cross-device is imperative for organizations concerned with identifying and confronting new threats and attacks. Fraud intelligence services have evolved beyond static reports and automated feeds, offering far more comprehensive insight into the threat landscape and attack-related data as it relates to a specific brand or business operation. Organizations are recognizing the value of these services and improving fraud detection through direct integration of threat intelligence sources collected in the dark web with existing security controls.

Cybercriminals are using social media to sell and share data. Over 50% of all fraud activity is related to carding and associated fraud-as-a-service offerings.



Card-Not-Present Fraud Will Spike

The side effects of EMV will start to be felt by retailers as card-not-present fraud rises and reaches over $7 billion in the U.S. by 2020. New methods of authentication for e-commerce transactions will be required to curb the losses.

With EMV chip cards gradually replacing the magnetic stripe, cybercriminals are rushing to gain the most they can financially before the U.S. goes almost completely over to them. As a result, ATMs and other POS terminals across the country are under attack from so-called skimming devices.

The side effects of EMV will start to be felt by retailers as card-not-present fraud rises and reaches over $7 billion in the U.S. by 2020. New methods of authentication for e-commerce transactions will be required to curb the losses.

As the last G20 country to move to EMV, the U.S. is at an advantage – and a disadvantage. The good news is that both issuers and retailers can draw on lessons learned in other countries that experienced the drastic shift of fraud from the POS terminal to card-not-present (CNP) transactions when EMV was rolled out. For example, Canada saw their liability shift enacted in April 2011 and experienced a 38% increase in CNP fraud over the next three years[6].

However, the bad news is that EMV technology is hardly new and has been widely used across Europe and Asia for the past decade. This has provided cybercriminals with a ten year head start in developing mechanisms to work around the chip. EMV counterfeiting software is widely available in some underground forums, ranging in price from $500 to $2,000. In addition, with more consumers now transacting from mobile devices, it is no longer just the Web channel that must be secured.

As the opportunity for in-person fraud diminishes, CNP fraud is projected to dramatically increase, reaching over $7 billion in the U.S. by 2020[7]. Other estimates have CNP fraud expected to be nearly four times greater than point-of-sale card fraud by 2018, eclipsing an astonishing $19 billion in losses[8].

The 3D Secure protocol was developed many years ago to help improve security by reducing fraudulent use of payment transactions online. However, despite its positive objectives, adoption of the protocol failed to take off as many retailers chose to opt out and accept the risk of chargebacks vs. cart abandonment. The password-based system proved too inconvenient for consumers and incapable of addressing the scope of today's advanced threats. As a result, EMVCo announced in January 2015 it was taking the reins on developing the next-generation of 3D Secure for consumer authentication.

With the much anticipated modifications to the 3D Secure protocol and projected spike in CNP fraud as a result of EMV rollout in the U.S., it is expected that issuers will start to adopt the same risk-based technologies similar to what was deployed for online banking to secure e-commerce transactions. Merchants will also become more inclined to opt in to 3D Secure to minimize chargebacks as a result of the liability shift and improved user experience expected from the modifications to the protocol.

The Internet of Things: From Fiction to Reality

The Internet of Things is moving from fiction to reality, though slowly. Risks will remain mostly unknown, but another major hack will make headlines and create another Big Data quandary.

A refrigerator used to wage DDoS attacks as part of a botnet. A home alarm system used to host a phishing attack. Hackable baby monitors exposing your family to strangers half a world away. While it sounds like the plot of a science fiction movie, it is the reality of today's Internet of Things (IoT).

While emerging as well as traditional hardware and software vendors attempt to wrap their heads around varied and sundry IoT mechanisms (both for execution as well as reporting), it should come as little surprise that cybercriminals are now planning to steal data collected through those same IoT devices. To date, the most high-profile examples of IoT hacking have been controlled hacks in the automotive industry, but it also inspired the recall of more than 1.4 million vehicles.

6 Canadian Bankers Association
7 Aite Group, "3D Secure: The Force for CNP Fraud Prevention Awakens," January 2016
8 Javelin Strategy & Research

These "controlled hacks" demonstrate that when it comes to the Internet of Things, cyber attacks are not just possible, but also inevitable. This is just the tip of the iceberg. From Microsoft Kinect to Nest to smart streetlights that listen to conversations occurring just below them, in time the Internet of Things will not only be pervasive, but also intrusive.

Like many innovations that seek to make our lives easier, the Internet of Things represents both opportunity as well as risk. It also raises the age old question of how much privacy we are willing to trade off for convenience. With more than six billion connected devices worldwide expected by the end of 2016[9], there is no doubt that cybercriminals will attempt to exploit a myriad of weaknesses, although full-scale attacks are still premature. However, we do expect to see more controlled hacks raise headlines and awareness of the vulnerability we face from living in an interconnected world.

Conclusion

Although each of the issues above are unique in terms of how they originate, who they target and their impact on business and consumers alike, they do share something in common: collectively, they comprise a threat horizon that continues to accelerate and expand with no end in sight.

Fraud prevention approaches now require solutions which can extend to mobile and cloud environments, make greater use of behavioral analytics, and take advantage of integrated threat intelligence capabilities to protect users and data. Even if attacks can't be stopped completely, it is possible to change how we detect and respond to an attack to minimize the potential for loss or damage.

Cybercriminals have long shared their knowledge and expertise in order to drive their success, and defenders must take the same approach — after all, a team is stronger than the individuals in it. RSA is pleased to note a generally increased propensity to share intelligence about threats and attacks with peers, government agencies, and the security industry in order to increase knowledge across the board.