IBM Security

IBM

IBM X-Force Special Report: 2016 Brazilian Threat Landscape

Mitigating risks to businesses and travelers

IBM Security White Paper

Executive summary

In August 2016, global attention will focus on Brazil. Historically, the sheer volume of attendees at large sporting events makes them an attractive target for criminals: with more than 10,000 athletes and hundreds of thousands of tourists expected in Rio de Janeiro, businesses and travelers will need to keep a sharp eye on their physical and cyber assets.

In this paper, IBM® X-Force® dives deep into several areas—including Brazil's unique security threat landscape—to raise awareness and recommend practices to mitigate threats for businesses and travelers, this summer and beyond. Learn more about protecting your valuable assets, whether from a targeted malware campaign or credit card skimming in a local market.

Cybercrime: Why Brazil?

By Limor Kessem

When it comes to cybercrime, cyber intelligence data indicates that, just as Eastern Europe produces the most sophisticated malware, the Brazilian cybercrime arena is a leader in internet fraud.

Brazil suffers from the second highest number of targets of online banking fraud and financial malware attacks of any country in the world.[1] In 2014, Brazil lost more than USD8 billion (BRL26 billion) to internet crime, which is the top economic crime in the country. In the rest of the world, cybercrime is ranked fourth.[2] Brazil is also 2015's top country in Latin America to suffer from ransomware attacks.[3] In 2015, reports indicated that bank fraud carried out over the internet had cost the top banks in Brazil more than USD615 million (BRL2,221 million).[4]

According to a PwC report, the number of cyber attacks in Brazil jumped 274 percent in 2015 alone, and the resulting financial losses are almost entirely absorbed by the financial sector.[5] Febraban, the Brazilian Banking Federation, says cybercrime causes 95 percent of losses for Brazilian banks.[6]

[1] Robert Muggah and Nathan Thompson, "Brazil's Cybercrime Problem," *Foreign Affairs*, 17 September 2015. https://www.foreignaffairs.com/articles/south-america/2015-09-17/brazils-cybercrime-problem

[2] "Latin American + Caribbean Cyber Security Trends," *Organization of American States, Symantec, et al.*, June 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

[3] "Brasil ocupa 1º lugar dentre os países latino-americanos mais atacados por ransomware," *Writing iMasters*, 3 March 2016. https://macmagazine.com.br/2016/03/17/brasil-ocupa-primeiro-lugar-dentre-os-paises-latino-americanos-mais-atacados-por-ransomware/

[4] "FRAUDE BANCÁRIA É O CRIME QUE MAIS MOVIMENTA A INTERNET," *Blanco Advogados*, 1 July 2016. http://www.blancoadvocacia.com.br/direito-penal/fraude-bancaria-e-o-crime-que-mais-movimenta-a-internet/

[5] "Cresce em 274% o número de ataques cibernéticos no Brasil," *EBC*, 22 February 2016. http://radios.ebc.com.br/revista-brasil/edicao/2016-02/pesquisa-revela-crescimento-de-274-em-numero-de-ataques-ciberneticos

[6] Kate Vinton, "Data Breach Bulletin: Brazilian Banks Lose $3.75 Billion Because Of Boleto Malware," *Forbes*, 7 July 2014. http://www.forbes.com/sites/katevinton/2014/07/07/data-breach-bulletin-brazilian-banks-lose-3-75-billion-because-of-boleto-malware/#1974142650a0

Increases in breaches and their costs

New research from IBM and the Ponemon Institute found that the cost of cybercrime to Brazilian companies is also on the rise. The average cost of a data breach in Brazil increased to BRL4.31 million per incident, compared to BRL3.96 million over the previous year.[1]

While the cost of a data breach in Brazil was significantly lower than the global average, the costs of cybercriminal attacks on companies in the country have steadily increased over the past three years. The report also predicts the probability for future data breaches at companies in Brazil to be the highest amongst countries surveyed at 40 percent.[2]

Based on a survey of Brazilian companies across several industries, the report also includes the following findings:

- The average size of a data breach increased by 8 percent over the past year, with companies experiencing an average of 24,830 breached records per incident.
- The top source of these breaches came from malicious or criminal activity, representing 40 percent of the breaches in the study.
- The cost per breached record increased significantly in the study, from BRL175 to BRL225.

[1] "Custo médio das violações de dados ultrapassa R$ 4 milhões no Brasil," *ComputerWorld*, 15 June 2016. http://computerworld.com.br/custo-das-violacoes-de-dados-ultrapassa-r-4-milhoes-no-brasil

[2] "2016 Cost of Data Breach Study: Brazil," *Ponemon Institute*, June 2016. https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-2077&S_PKG=ov49556

Technological factors that put Brazil at risk

Let's go over some of the technological factors that contribute to cybercrime gaining momentum in Brazil:

- Large population, many internet users, low security awareness—and enterprising cybercriminals.[1, 2]
- Creation of fake bank accounts. Establishing a false identity has become easier in the digital age, and cybercriminals have taken advantage of this. False ID cards have become simple to acquire, and many criminals have been found to open bank accounts in the names of recently deceased individuals. This causes another problem…
- Money mules not needed! With easy access to banking credentials, cybercriminals don't need to hire outside agents or work with underground money mule networks. They can open and use fake bank accounts to move the money.

[1] "Brazil Internet Users," *Internet Live Stats*, accessed 26 June 2016. http://www.internetlivestats.com/internet-users/brazil/

[2] Fabio Fettuccia Cardoso, "Brasil está atrasado em estratégias de combate a crimes cibernéticos," *Jusbrasil*, 13 April 2016. http://fabiofettuccia.jusbrasil.com.br/noticias/180688777/brasil-esta-atrasado-em-estrategias-de-combate-a-crimes-ciberneticos

Cultural factors that put Brazil at risk

Some of the cultural factors that have enabled cybercrime to continually gain momentum in Brazil are:

- As internet connectivity and services become available in more parts of the country, many Brazilians are accessing online services only for the first time. For these early-stage users, security is often not top of mind nor is training usually available, increasing their chances of becoming victims of cybercrime as soon as they go online.[1] The risk rises as users in Brazil favor access to their online banking account through their mobile devices, which can often be even less secure.[2, 3]
- Consumer behavior in Brazil makes it harder for banks to tell the difference between fraud and legitimate transactions. Users who log in from a variety of publicly available computers or devices at places such as libraries and internet cafes make it difficult to determine fraudulent activity based on device information alone.

[1] "Troubleshooting Brazilian Technophilia", *Transformaciones*, 6 April 2016. https://clastransformaciones.wordpress.com/2016/04/06/troubleshooting-brazilian-technophilia/

[2] Micali, Bruno, "Mobile é o principal meio de brasileiros acessarem conta bancária," *TecMundo*, 24 June 2016. http://www.tecmundo.com.br/celular/106557-mobile-principal-meio-brasileiros-acessarem-conta-bancaria.htm

The Brazilian malware landscape

Cybercrime in Brazil is beyond doubt one of the country's greatest challenges, with cybercriminals adapting their attacks to the landscape they operate in.

The most prolific types of cybercrime attacks in Brazil are facilitated by malware,[1] and Brazilian cybercriminals tend to operate at lower sophistication levels compared to cybercriminals creating malware in Eastern Europe. However, this trend is beginning to change, and Brazilian criminals are collaborating with Russian-speaking cybercrime actors to create better malware. Here are the top malware threats employed in Brazil against banking and payment users online:

- Trojans with customizable Delphi-based source code: Delphi malware code is the most popular in Brazil, based on historic usage and the fact that it is easier to understand and customize for developers of varying skill levels.
- Image-based phishing scams: Cybercriminals set up a static image overlay that looks like the bank's site, with the exception of the login fields. They present this image on full screen in order to steal the victim's online banking credentials.
- Remote overlay Trojans: The scam leverages a remote control connection to the infected endpoint, combined with the persistence of a transposed screen, or overlay, that blocks the user from accessing the actual web browser. Simultaneously, the criminal performs a fraudulent transaction while the user is "stuck" at the overlay.

[1] Robert Muggah and Nathan Thompson, "Brazil's Cybercrime Problem," *Foreign Affairs*, 17 September 2015. https://www.foreignaffairs.com/articles/south-america/2015-09-17/brazils-cybercrime-problem

The Brazilian malware landscape (continued)

- Fake browsers to steal credentials: When a victim navigates to an online banking website, malware crashes the internet browser and relaunches a new, fake one instead. The fake browser is controlled by the criminal who uses it to harvest the victim's online banking credentials.
- Malicious Boleto browser extensions: Malicious extensions are used as add-ons that infect the most popular internet browsers. These can alter transaction details on the fly for a popular payment method used in South America, the Boleto payment.
- Malicious proxy-changers: The most popular attack vector in Brazil over the past six years, this class of malware for the most part tampers with the victim's Proxy Auto-Config (PAC) file. This is a file used by the browser to automatically choose the correct proxy server that will fetch a requested URL. By poisoning this file, the browser sends victims to a phishing page set up by the criminal.
- Abuse of legitimate tools such as Microsoft Windows default wares: Brazilian cybercriminals often use legitimate tools and Windows default wares to stop or delete security software from infected endpoints, so that it does not interfere with their malware.

Read more about these trends in this IBM article on the malware landscape.

Brazilian malware on the global threats map

Malware is prolific in Brazil,[1] and the same types of malcode are spread far and wide on user endpoints throughout the country:

- The "Janela" category, which means "window" in Portuguese, includes all attack types that overlay fake windows on the user's desktop.
- "CPLware" includes all the attacks that leverage .CPL files to usher malware into target endpoints—similar to the purpose of malware loaders such as Upatre, only simpler. The .CPL file format is used for disguising malicious files as they are delivered to unsuspecting victims via spam email. The essential function of .CPL files is that once they are double-clicked, they can automatically load an application—in this case, malware—without being an .exe file, which would be much more suspicious. The most prolific family in this category is called "Banload."
- "Remoto" refers to attack types that use remote admin tools to take over user endpoints and initiate fraudulent transactions from them.

[1] "Global Security Map," *CyberDefcon*, Accessed 12 July 2016. http://globalsecuritymap.com/#br

Top malware families worldwide in 2016, year to date

Data on malware in Brazil mostly reveals attack volume per *category*, rather than distinct malware families in the classic sense. Brazilian endpoints often contract malware such as "Janela," "Remoto" and variations of Boleto payment malware extensions. The typically Brazilian malware is so prolific that it ranks in the top 10 on the global malware chart, as shown in Figure 1.

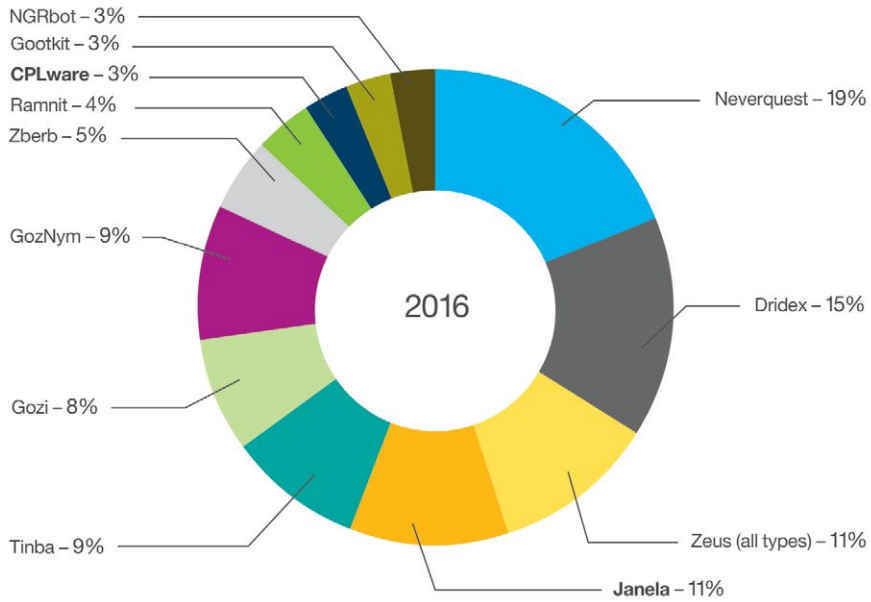

Figure 1: Top malware families in 2016 year to date - Global perspective (Brazilian malware families indicated in bold)

Top malware families in Latin America in 2016, year to date

In Latin America, the “Janela” category comprises more than half of all malware, as shown in Figure 2. This is significantly more than the global occurrence. It is followed closely by “Remoto” malware.

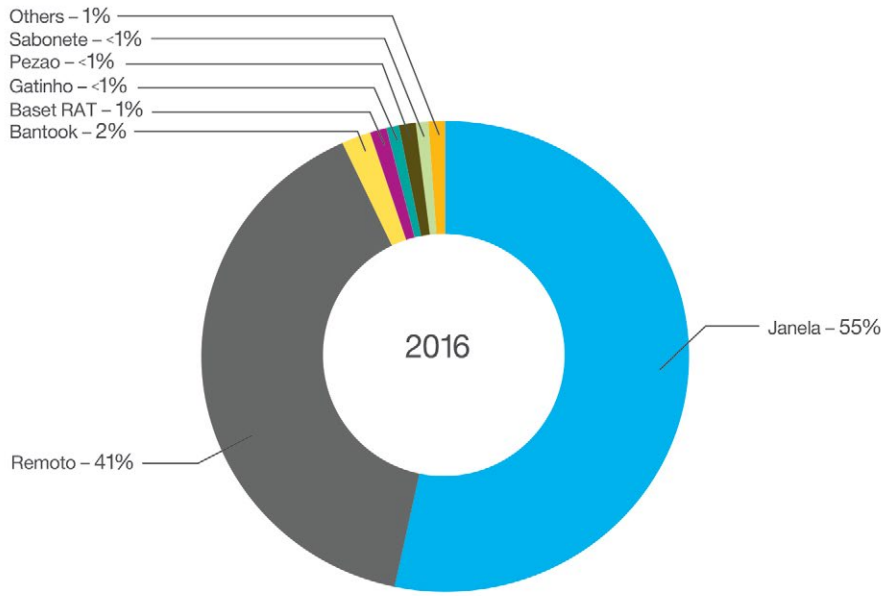

Figure 2: Top malware families in 2016 year to date - Latin American perspective

Malware threat forecast

When it comes to malware, Brazil may have its tested-and-true favorites, but it definitely doesn't remain naïve or unchanged. Locally attacking cybercriminals go through the same evolution that applies to other threat landscapes in the world: they become more advanced over time to continually beat security controls.

To that end, Brazilian cybercriminals add obfuscation, encryption and evasion techniques to their malware. They buy malicious code from criminals in the Russian-speaking underground, and find ways to deliver their malcode using modern methods, such as exploit kits and sophisticated social engineering.

IBM X-Force Research expects to see continued development of threats that affect Brazil, and overall, the move of more sophisticated banking Trojans into the country.

Malware trends to watch out for

One trend to watch out for is attacks on enterprise users. IBM X-Force anticipates digital extortion and business email compromise (BEC) fraud will hit Brazil and aim at the high-value users in companies, or the companies themselves.

Ransomware is also expected to gain momentum in Brazil, a trend that seems to wait only for an opportune moment and an anonymized payment method in the local marketplace. In that sense, Brazilian users have a certain grace period because cryptocurrency adoption is relatively low, with only 17 bitcoin nodes in the country per 10 million people,[1] and individuals may not necessarily have the funds to send prepaid vouchers to an attacker.

In the near term, we do not expect to see significant change in the malware landscape itself, since developing new types of code does not happen frequently in the region. We do, however, definitely foresee an increase in attacks launched to infect online services users with malware, and to phish both visitors' and locals' payment card and account credentials. The phishing is likely to leverage typical Brazilian malware and may customize its look and feel to resemble event-specific web pages.

[1] "BitCoin Adoption by Country, *OpenHeatMap*, Accessed 12 July 2016. http://www.openheatmap.com/view.html?map=BibbonsGomphotheriidaeJewely

Other potential cyber attacks

by Michelle Alvarez

Today's constantly evolving attack vectors and increasingly sophisticated methods for cybercriminals to avoid detection get a lot of attention. But that doesn't mean the criminals have abandoned methods that have long been successful in their quest to separate victims from their money. Headlines may focus on data breaches at large enterprises that steal customer information, attacks on healthcare institutions that result in lucrative insurance fraud, or hactivist actions against governments that seek political gain, but the individual user—and the individual banking account—remains at risk from clever tricks and scams.

For the cybercriminal targeting large events, there may be no particular reason to give up on these time-tested and often very profitable methods of fraud and theft. In fact, with huge numbers of unsuspecting visitors in the country, there's one compelling reason—profit—for trying every method available. And for the individual computer or smartphone user, there is every reason to be careful.

Distributed-denial-of-service attacks

Beyond malware campaigns, many tried and true attack vectors will be recycled to take advantage of global attention, including distributed-denial-of-service (DDoS) attacks.

Large events that attract a lot of attention are a natural target for hacktivist groups, who may look to disrupt activities and sponsors to gain attention for their cause. For example, during the 2014 World Cup in Brazil, the hacktivist group Anonymous claimed responsibility for cyber attacks on websites of the Brazilian government and major sponsors of the World Cup.[1]

The concern is not only specific to Brazil—it includes businesses worldwide that are sponsors of these global-scale events. Organizations and businesses that are involved with these global competitions are advised to employ a mitigation strategy/defense against potential attacks, and pay particular attention to DDoS attacks. There are multiple ways to help proactively prevent DDoS attacks.

Read more in this IBM article on hacktivism.

[1] Jack Simpson, "World Cup 2014: 'Hacktivist' group Anonymous plan cyber-attack on World Cup sponsors," *The Independent*, 1 June 2014. http://www.independent.co.uk/news/world/americas/world-cup-2014-hacktivist-group-anonymous-plan-cyber-attack-on-world-cup-sponsors-9467786.html

Phishing scams, malicious sites and fake apps

The 2012 Summer Olympic Games saw its fair share of Olympics-related scams. According to F-Secure, one scam involved a PDF masquerading as the London 2012 Olympics schedule.[1] The file exploited a two-year-old vulnerability (CVE-2010-2883) in older versions of Adobe Reader and Acrobat. In this scam, the PDF acted as a dropper, downloading other executables onto the compromised computer to launch other attacks. In another example, during the 2014 World Cup, there were phishing attempts containing Trojans that arrived in the guise of spam mailings promising lottery-won World Cup tickets.[2]

Prior to the 2012 Olympic Games, the US Department of Homeland Security issued a bulletin warning of malicious sites appearing on search results pages designed to trick users into downloading malware.[3] Sites may also offer exclusive footage but use fake videos and codecs to distribute malware.

Users should also be wary of event-themed mobile applications. In 2012, Russian websites claiming to be legitimate app stores offered a fraudulent version of the "London 2012 – Official Mobile Game" containing malware.[4]

[1] "Targeted Attack: London 2012 Olympics," *F-Secure Labs*, 28 May 2012. https://www.f-secure.com/weblog/archives/00002370.html

[2] Ava Fedorov, "Brazil faced almost 90,000 cyber attacks during World Cup," *SC Magazine*, 30 July 2014. http://www.scmagazineuk.com/brazil-faced-almost-90000-cyber-attacks-during-world-cup/article/363664/

[3] "Strategic Outlook: 2012 Summer Olympic Games," *US Department of Homeland Security*, 2012. http://info.publicintelligence.net/NCCIC-Olympics2012.pdf

[4] "Scammers Prey on London 2012 Mobile Game Players," *ThreatTrack Security Labs*, 27 July 2012. https://blog.threattrack.com/scammers-prey-on-london-2012-mobile-game-players/

Point-of-sale hazards

By Charles Henderson and David Byrne

As fans converge on Brazil, criminals are acutely aware that many of the attendees come from high income brackets. This temporary collection of wealthy targets is likely very enticing. Robbing travelers is a global and ancient custom, and while payment cards can be much simpler than cash, they are still vulnerable. When you hand your card to a clerk, how do you know that the data is safe? The truth is that consumers don't really know. No one can gauge the security of a modern cash register or mobile payment device just by looking at it, and even the friendliest merchants will quickly kick you out for trying your own security testing.

The Payment Card Industry Data Security Standard (PCI-DSS) was created to merge the separate standards of five of the world's largest payment card companies with the ultimate goal of keeping people using their cards. The regulations must be balanced with merchant requirements for a streamlined payment experience for their customers. Regulations in and of themselves are not a solution for payment card fraud.

Recommendations for merchants

Threats usually aren't obvious—they can be hidden deep inside your hardware and software. Here are some of the ways you can protect both your business and your customers:

- Don't confuse security with regulatory compliance. There's certainly overlap, but aim higher than just convincing your assessor that you're compliant.
- Implement penetration testing procedures for your point-of-sale (PoS) environment to identify misconfigurations and other potential problems.
- Routinely check for skimmers, both software- and hardware-based. Software skimmers are specialized malware packages that monitor PoS memory for plaintext card data. Hardware skimmers are even more devious. Criminals have designed miniature monitoring devices that fit inside normal card readers, so when a customer or clerk swipes a card, the monitoring device reads the magnetic stripe at the same time as the legitimate reader.
- Consider engaging a penetration testing team to manually test your PoS solution.
- Utilize mobile device management (MDM) software to monitor device security state for mobile payment stations.

Recommendations for travelers

As in any travel, the watchword for visitors conducting financial transactions is “caution.” Here are a few best practices you should follow:

- Consumer liability for fraudulent transactions depends on the country in which the fraud occurred. If you’re unsure about your liability for fraud, contact the bank that issued your payment card.
- Travel with at least two payment cards, ideally from separate banks.
- Check with your issuing bank to see if you need to notify them about travel.
- Be thoughtful about where you use a payment card. If in doubt, use cash.
- If you’re using a cash machine, try to find one in an area with better physical security, such as a bank or hotel lobby.
- Check cash machines for card skimmers—grab the plastic casing around the card slot and give it a few good pulls. It should never be loose on a legitimate device.
- Review your card statements for anomalous activity, but don’t focus just on high-price purchases. Many criminals will first attempt a very low purchase amount to verify the accuracy of the stolen data.

Conclusion

Regardless of whether you are attending or watching from home, the key to protecting your personal data is vigilance. Be aware of your physical and digital surroundings, taking care to validate that applications and websites are actually meeting their intended purpose and not masking nefarious activity. Regularly check bank statements for anomalies and be aware of your liability for fraudulent transactions if traveling to a foreign country.

For businesses involved in the economy of these events, having an incident response plan and regularly practicing it is always a good idea. If you're involved in retail transactions, investigate your PoS systems for signs of compromise, either physical or digital. With the ongoing threat of phishing, malware and digital extortion, businesses as well as individuals are best advised to maintain watchfulness.

To read more security research and insights from IBM X-Force, visit the X-Force Research hub.

Authors and contributors

Author	
Charles Henderson	**Global Head of Security Testing and Threats** With more than 20 years of experience in the information security industry, Charles Henderson and the teams he has managed have specialized in network, application, physical and device penetration testing, as well as vulnerability research. His team's clients range from the largest on the Fortune lists to small and midsized companies interested in improving their security posture. He has been a featured speaker at various conferences (including Black Hat, DEFCON, RSA, SOURCE, OWASP AppSec USA and Europe, SXSW and Merchant Risk Council) around the world on various subjects relating to security testing and incident response.
David Byrne	**Security Testing** David Byrne is a Senior Managing Consultant in the IBM Security Services Global Center of Competence (CoC). The CoC is a team of subject matter experts who deliver services projects through leveraging market leading solutions and innovative approaches across all security areas to protect your business. David has worked in IT since 1996 and in information security since 2000. He started his career in security operations at Fortune 100 companies, but has been a security consultant for the last nine years. He specializes in application security testing, with secondary focuses on network security and incident response. David has presented at many security conferences around the world, including Black Hat, DEFCON, RSA, and OWASP AppSec USA and Europe. He has also published a number of vulnerability advisories from his testing and research.

Authors (continued)

Author	
Limor Kessem	**Senior Cybersecurity Evangelist** Limor is one of the top cyber-intelligence experts at IBM. She is a regular blogger on SecurityIntelligence.com and a highly appreciated speaker on New York Metro InfraGard webcasts. She has spoken at security events worldwide, conducts live webinars on all things fraud and cybercrime, and writes a large variety of threat intelligence publications. Limor is considered an authority on emerging cybercrime threats.
Michelle Alvarez	**Threat Researcher and Editor** With more than 10 years of industry experience to her role, Michelle is responsible for researching and analyzing security trends and developing and editing security and threat mitigation thought leadership papers. She has been a regular contributor to the IBM X-Force Threat Research Paper Series and the SecurityIntelligence.com blog.

Additional contributors	
Diana Kelley	**Executive Security Advisor**
Pamela Cobb	**Portfolio Manager, IBM X-Force**

About IBM X-Force

Advanced threats are everywhere. Help minimize your risk with insights from the experts at IBM.

The IBM X-Force research team studies and monitors the latest threat trends including vulnerabilities, exploits, active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, IBM X-Force also delivers security content to help protect IBM customers from these threats.

IBM Security Services: Protect your enterprise while reducing cost and complexity.

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimize your security program, stop advanced threats, protect data, and safeguard cloud and mobile. Should you experience an IT security breach, IBM X-Force Incident Response Services can provide real-time on-site support, including intelligence gathering, containment, eradication, recovery and compliance management.

For more information

To learn more about IBM X-Force, please visit: **ibm.com**/security/xforce/

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2016

WGW03235-USEN-01