IBM Security

Security trends in the financial services sector

With money and data both at stake, 2016's leading attack target remains a magnet for cybercrime

IBM X-Force® Research

IBM

Click here to start ►

Contents

Executive overview

The financial services sector has been a magnet for cybercrime for over two decades now, and that was certainly true again in 2016. As revealed in the 2017 IBM X-Force Threat Intelligence Index, the sector was attacked more than any other industry, with the average financial services client organization monitored by IBM Security Services experiencing 65 percent more attacks than the average client organization across all industries (see Figure 1). Moreover, 2016 saw an average 29 percent increase in attacks on financial services organizations—up from 1,310 attacks in 2015[1] to 1,684 in 2016.

Amid these negative findings, there were however some good tidings. The average financial services client we monitored experienced 192 security incidents in 2015[2], but only 94 in 2016. A "security incident" is our most serious classification, so this is indeed welcome news.

Definition of terms

Security event: Activity on a system or network detected by a security device or application.

Attack: A security event that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself.

Security incident: An attack or security event that has been reviewed by IBM security analysts and deemed worthy of deeper investigation.

Figure 1. Average client organization monitored by IBM Security Services, 2016 cross-industry versus financial services comparison. (See sidebar "Definition of terms" for definitions of security event, attack and security incident.)

Contents

Unfortunately, the good news may end here. IBM® X-Force® malware researchers investigating cybercrime trends and financial malware campaigns found that some countries experienced a marked increase in financial cybercrime in 2016. Cyber gangs continued to sharpen their focus on business bank accounts, a trend that began picking up speed in mid-2014, using malware such as Dyre, Dridex, GozNym and TrickBot to target business banking services.

2016 also saw a notable rise in publicly reported Society for Worldwide Interbank Financial Telecommunication (SWIFT) attacks against the messaging system used by thousands of banks and companies to move money around the world.[3] The result was that millions of US dollars were stolen and fraudulently transferred from various global banks using custom malware to remove traces of these transactions.

Combined with other analysis disclosed in this report, these trends and incidents paint a troublesome picture for the financial services sector. Fortunately, financial services organizations can strengthen their cybersecurity immune system with a focus on mitigating notable security pain points such as insider threats and financial malware.

About this report

This IBM X-Force Research report was created by the IBM Managed Security Services Threat Research group, a team of experienced and skilled security analysts working diligently to keep IBM clients informed and prepared for the latest cybersecurity threats. This research team analyzes security data from many internal and external sources, including event data, activity and trends sourced from endpoints managed and monitored by IBM.

Contents

A global view: publicly disclosed financial incidents

IBM X-Force Interactive Security Incidents data is a sampling of notable publicly disclosed incidents.[4] Included are breaches, which are incidents resulting in the exfiltration of data. As Figure 2 shows, there was no shortage of cyberattack-induced financial ruin in 2016. Outages due to distributed denial of service (DDoS) shut down online financial institutions' operations all over the globe. Malware, including ransomware, was responsible for millions in losses. One of the banks targeted in the SWIFT attacks, had USD 81 million stolen from their customers' accounts.[5]

Attackers also turned to an old favorite from their arsenal of phishing techniques, the Business Email Compromise (BEC) scam, to trick unwitting victims out of their money, an issue that hit the victim, but also became an issue for the banks on either side of a multi-million dollar fraud that's hard to cover by existing insurance. Aside from financial losses, many compromises resulted in leaks of highly sensitive financial data. In one bank compromise, 1.4GB of leaked data reportedly included internal corporate files and customer financial data.[6]

With over 200 million records compromised in 2016—a 937 percent increase over the 2015 total of just under 20 million—the financial services sector ranked third among other industries in terms of records breached. In terms of publicly disclosed incidents tracked by IBM X-Force, recent year-over-year totals have remained flat: 22 publicly disclosed incidents in 2014, 21 in 2015, and 22 in 2016.

Contents

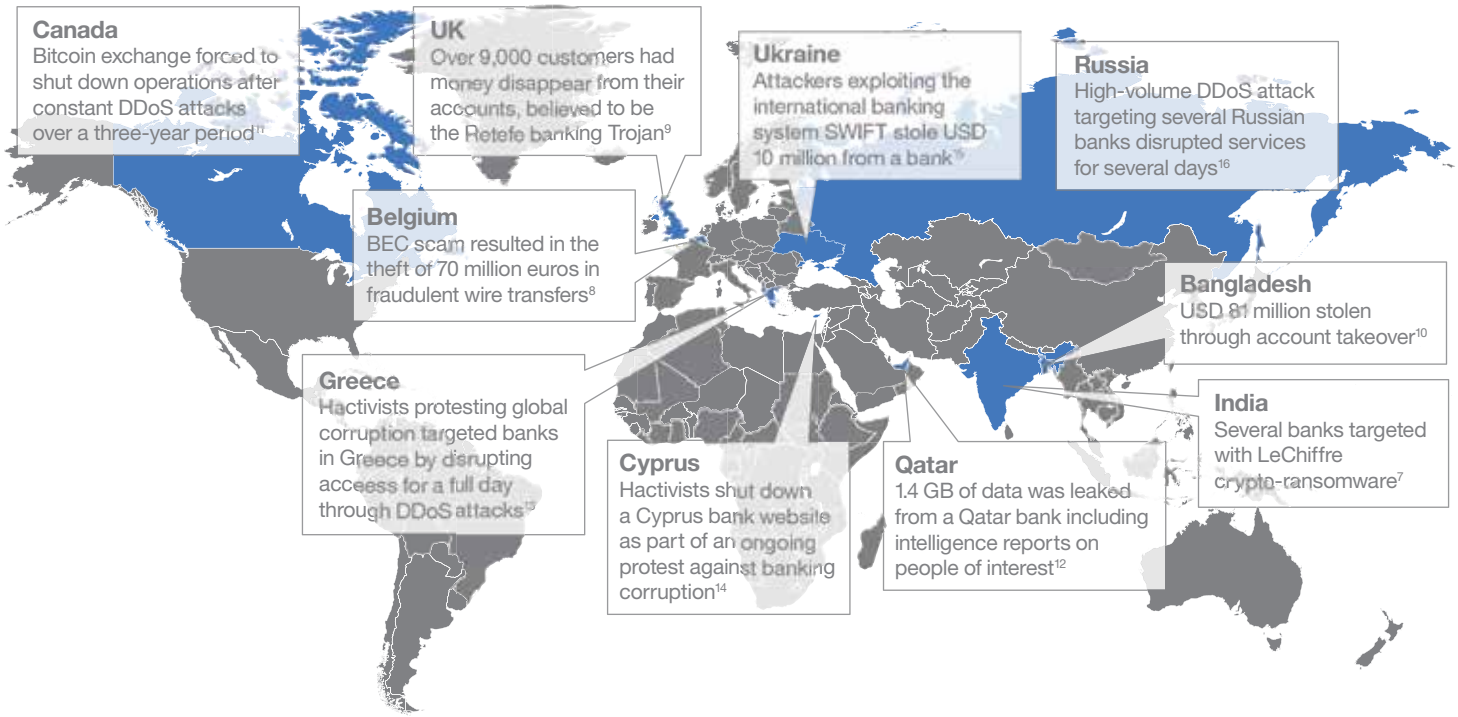

Figure 2. Notable 2016 publicly disclosed financial services security incidents. Source: IBM X-Force Interactive Security Incidents data.

Contents

Where are the "bad guys"? Insiders versus outsiders

Security executives and their teams deal with numerous attacks every year. To prioritize defenses and budgets they continually keep tabs on where threats are coming from. Are they mostly external attacks, or do insiders make up a large part of their organization's overall attack surface?

To discover whether an attack is coming from inside or outside the organization, security investigation teams first identify the source and destination IPs as internal or external, then further investigate the associated attack pattern to determine malicious or inadvertent intent. IBM Managed Security Services (MSS) 2016 data for the financial services sector (see Figure 3) reveals more insider than outsider attacks (58 percent to 42 percent) affected organizations, and within the insider group, many more inadvertent actors (53 percent) were the culprits than malicious insiders acting against the organization (5 percent).

Among the top five targeted industries—retail, healthcare, manufacturing, financial services, and information and communications—the 2017 IBM X-Force Threat Intelligence Index reveals that in 2016 the financial services industry experienced the highest level of threat from inadvertent actors. It's useful to think of an inadvertent actor as a compromised system carrying out attacks without the user being aware of it, as in the "Subvert Access Control" attack type described in more detail below. Often it happens when a desktop client is compromised via malicious email attachments, clickjacking or phishing, or vulnerable computer services that have been attacked from another internal networked system.

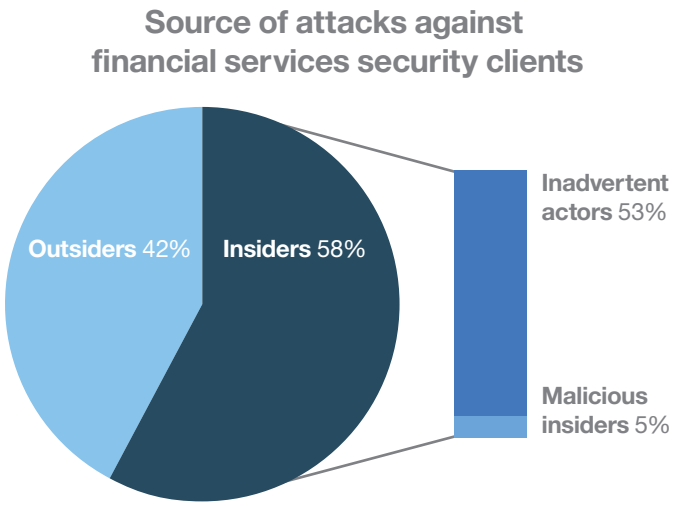

Figure 3. In 2016, insiders were responsible for more financial services sector attacks than outsiders.

Contents

Prevalent methods of attack in financial services monitored clients

To classify and better understand the types of threats that affect financial entities, X-Force has grouped 2016 observed attack types according to the standard set by the MITRE Corporation's CAPEC™ (Common Attack Pattern Enumeration and Classification) effort (see Figure 4). As described by MITRE, their system "organizes attack patterns hierarchically based on mechanisms that are frequently employed in exploiting a vulnerability." The only exception is the "Indicator" category, which describes conditions and context of threats and attack patterns.

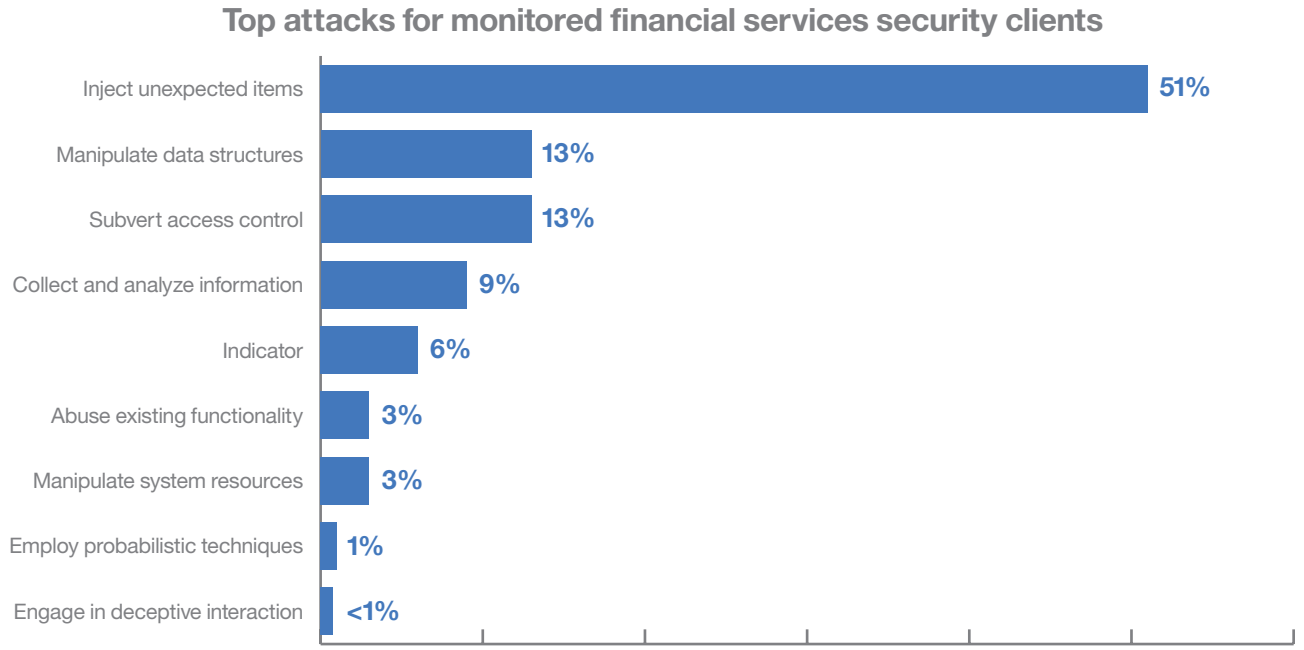

Figure 4. Injection-type attacks were the clear leader in the financial services sector in 2016. Source: IBM Managed Security Services data, January 1 – December 31, 2016.

Further details on each attack type appear in the following sections.

Inject unexpected items

According to IBM MSS analysis of 2016 data, the number one attack vector, involving the use of malicious input data to attempt to control or disrupt a system, targeted 51 percent of the financial services clients monitored by IBM X-Force. That figure was notably higher than the cross-industry average of 42 percent.

Command injections, which include operating system command injection (OS CMDi) and SQLi, belong in this category. OS CMDi is also known as "shell command injection," after which the now infamous and widely prevalent Shellshock vulnerability is named. Shellshock activity, which surged across all industries before its two-year anniversary in September 2016, accounted for just over a quarter of all attacks targeting financial services organizations in 2016.

SQLi and OS CMDi are perhaps the most popular attack vectors within this sector because successful exploitation of these vulnerabilities can provide attackers with the ability to read, modify and destroy sensitive data. The personally identifiable information (PII) in the databases of financial institutions is highly valued by hackers because they can sell it for a handsome profit or hold it hostage, demanding that the financial institution pay a ransom to get it back or prevent its public disclosure.

Manipulate data structures

The number two attack vector involved attacks in which the attacker attempted to gain unauthorized access through the manipulation of system data structures. As CAPEC™ states, "Often, vulnerabilities [such as buffer overflow vulnerabilities], and therefore exploitability of these data structures, exist due to ambiguity and assumption in their design and prescribed handling."[17] The great majority of the attacks in this category targeted buffer overflow vulnerabilities.

On a positive note, while the cross-industry client average for attacks in this category is 32 percent, the figure in the financial services sector, 13 percent, is substantially lower. That might be because attackers view this attack vector as less potentially successful against financial services targets.

Subvert access control

The number three attack vector, accounting for 13 percent of attacks—substantially higher than the cross-industry average of three percent—involved attacks attempting to subvert access control through the "exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage identity and authentication."[18]

Most of the attacks we observed in this category involved the exploitation of vulnerabilities in the target's client-server communication channel for authentication and data integrity by leveraging the implicit trust a server places in what it believes to be a valid client.

Man-in-the-middle (MITM) attacks, in which attackers attempt to intercept and relay messages between two parties (people or systems), falls under this category. This technique could allow an attacker to steal the information going back and forth or insert malicious code into the connection. Some mobile banking apps have been found to mishandle the way they transmit data, making them vulnerable to MITM attacks.[19]

Collect and analyze information

Attacks focused on the collection and theft of information made up nearly nine percent of attacks targeting client devices. Most of these involved fingerprinting, often viewed as a kind of reconnaissance that gathers information on potential targets to discover their existing weaknesses. Essentially, an attacker compares output from a target system to known "fingerprints" that uniquely identify specific details about the target, such as the type or version of its operating system or an application. Attackers can use the information to identify known vulnerabilities in the target organization's IT infrastructure and better prepare their tactical plans.

Indicator

Note that "Indicator" is not a CAPEC™ mechanism of attack. A cyberthreat indicator consists of certain observable conditions as well as contextual information about the condition or pattern. These events, which accounted for six percent of all attacks, could indicate either an attempted or a successful attack on the target system. A large percentage of the attacks involved targeted systems experiencing 100 or more external pings in a short time, which might indicate a compromised internal host. If compromised, a host could be attacking other targets or communicating with other compromised hosts until detected and stopped.

Abuse existing functionality

Three percent of attacks involved attempts to abuse or manipulate “one or more functions of an application in order to achieve a malicious objective not originally intended by the application, or to deplete a resource to the point that the target’s functionality is affected.”[20] Successful attacks in this category could allow the attacker to obtain sensitive information or cause a denial of service, as well as execute arbitrary code on the target.

Manipulate system resources

Attacks attempting to manipulate some aspect of a system’s resource state or availability accounted for three percent of all attacks. Resources include files, applications, libraries and infrastructure, and configuration information. Successful attacks in this category could allow the attacker to cause a denial of service, infect a machine to become a botnet command-and-control (C&C) server, or execute arbitrary code on the target.

Employ probabilistic techniques

One percent of attacks involved an attacker using what CAPEC™ describes as “probabilistic techniques to explore and overcome security properties of the target.”[21] Most of the activity involved brute-force password attacks, a tactic in which an intruder tries to guess a username and password combination to gain unauthorized access to a system or data. Most of the attacks observed by X-Force targeted the Secure Shell (SSH) service. Users favor SSH because it can provide secure remote access. The downside is that it can provide attackers with shell account access across the network.

Engage in deceptive interaction

Less than one percent of attacks made attempts to convince a victim to perform an action through spoofing, such as in a clickjacking attack. In this type of attack, the attacker attempts to hijack the victim's click actions and possibly launch further attacks against the victim.

Contents

Recommendations and mitigations

Never neglect training and refreshing employee awareness

Foster awareness regarding BEC scams and other phishing scams through education. A variety of approaches—video, webinars, in-person instruction—can be used to educate employees. Programs that simulate phishing attacks could test employees at regular intervals. Encourage employees to report suspicious emails for further investigation.

Apply a cognitive approach to detecting phishing sites

The financial services industry experienced a relatively high percentage of attacks from inadvertent actors or those that unwittingly introduced threats to the target organization's environment. Falling victim to spear phishing is one of the inadvertent actor's biggest weaknesses. They have the power to lure employees to either download malware, opening the first door to the attackers, or lead them to a fake website where their corporate credentials will be stolen.

According to IBM X-Force data, 70 percent of credentials are stolen in the first hour of a phishing attack.[22] In order to react to a phishing attack quickly and accurately, machine learning and cognitive computing need to be incorporated to help boost the speed and scale of phishing detection and protection. A cognitive engine capable of helping detect relevant phishing attacks as they emerge and then alerting customers about it is now available in IBM Trusteer Rapport®.

The new cognitive engine analyzes unstructured data from suspicious websites, including links, images, forms, text, scripts, DOM data and URLs. It can accurately identify a wide variety of phishing pages, including those that only present users with an image to elude content analysis and those that deliver dynamic content to the page to evade web crawlers. By analyzing text, wording and logos used on a site, it can further point out the targeted brand(s) with accuracy and discern whether the use of a logo is legitimate or suspicious.

Further reduce exposure to insider threats

Mitigating phishing attempts is key to reducing the threat from inadvertent actors. However, to further reduce exposure to insider threats, financial services organizations must combine data security and identity and access management solutions to protect their sensitive data and govern the access of all legitimate users.

Contents

The more users have access to sensitive information, the greater the chance that someone will put it at risk, either maliciously or mistakenly. Companies must ensure they are limiting access to only those users who absolutely need it, and that controls stay current as the user population changes and evolves over time. Similarly, the more easily accessed the information is, and the more places it resides, the greater the chances that an insider, or an outsider with stolen credentials, will be able to gain access to it for the wrong reasons.

Solutions that include an identity manager and account-provisioning component, such as IBM Security Privileged Identity Manager, can help an organization centrally manage and audit the use of privileged IDs across different scenarios. Solutions like IBM Security Guardium® can help ensure that sensitive data is appropriately protected.

Solutions such as IBM Surveillance Insight for Financial Services that adopt a proactive approach towards managing risk of non-compliant employee behavior are essential. Solutions able to ingest unstructured data—such as chat transcripts, email communications and voice recordings—and combine it with structured trade transaction data create a more robust unified surveillance system.

Augment cyber security intelligence capabilities

Security intelligence, a must across all industry sectors, is especially important in the financial services sector. It’s critical that organizations understand the attack vectors to which they are most vulnerable. Having this knowledge can help financial services companies stay one step ahead of criminals and bolster internal and external detection and protection mechanisms.

But how do security operations teams keep pace with the myriad of threats and ever-growing number of attacks targeting their organizations? Keeping up with threat intelligence is a vital part of risk awareness. With that, the speed of threat data far exceeds human capability. Even the most skilled security professionals can have difficulty sifting through the sheer volume of security incidents and available threat data. A solution that combines cognitive capabilities and analytics, such as IBM QRadar® Advisor with Watson®, augments a security analyst's ability to identify and understand sophisticated threats by tapping into unlimited amounts of unstructured data from blogs, websites, research papers and the like, and correlating it with relevant security incidents.

Contents

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. Security Intelligence Operations and Consulting Services can assess your security posture and maturity against best practices in security. With IBM X-Force Incident Response and Intelligence Services, IBM experts proactively hunt and respond to threats, and apply the latest threat intelligence before breaches occur. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that can help you improve your security posture—often at a fraction of the cost of in-house security resources.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors billions of security events per day in more than 130 countries, and holds more than 3,500 security patents.

Contents

About the author

Michelle Alvarez, a Threat Researcher and Editor for IBM Managed Security Services, brings 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 joined IBM through the Internet Security Services (ISS) acquisition in 2006. At ISS she served as an analyst and contributed to the development of the X-Force Database, one of the world's most comprehensive threats and vulnerabilities database. For many years, Michelle played an important operational role within the Information Technology-Information Sharing and Analysis Center (IT-ISAC), a non-profit, limited liability corporation formed by members within the information technology sector. She is a regular contributor to the IBM-sponsored security blog, SecurityIntelligence.com, and has her master’s degree in information technology.

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

For more information on security services, visit: **ibm.com**/security/services

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog

Contents

[1] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SE912353USEN

[2] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SE912353USEN

[3] http://money.cnn.com/2016/05/20/news/swift-bank-attack-global-ecuador/

[4] http://www-03.ibm.com/security/xforce/xfisi/

[5] https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

[6] http://www.bankinfosecurity.com/qatar-national-bank-suffers-massive-breach-a-9068

[7] http://news.softpedia.com/news/lechiffre-ransomware-hits-three-indian-banks-causes-millions-in-damages-499350.shtml

[8] http://www.net-security.org/secworld.php?id=19370

[9] http://www.independent.co.uk/news/business/news/tesco-bank-accounts-suspended-transactions-access-frozen-hack-money-la-a7402006.html

[10] http://thehackernews.com/2016/04/bank-firewall-security.html

[11] https://www.hackread.com/bitcoin-exchange-ddos-attacks/

[12] http://www.databreachtoday.com/qatar-national-bank-suffers-massive-breach-a-9068

[13] https://www.hackread.com/anonymous-ddos-attack-bank-greece-website-down/

[14] https://www.hackread.com/oplcarus-hacktivists-ddos-central-bank-of-cyprus/

[15] http://thehackernews.com/2016/06/ukrainian-bank-swift-hack.html

[16] http://www.theregister.co.uk/2016/11/11/russian_banks_ddos/

[17] https://capec.mitre.org/data/definitions/255.html

[18] https://capec.mitre.org/data/definitions/225.html

[19] http://news.softpedia.com/news/76-ios-apps-including-medical-and-banking-tools-are-exposing-data-to-hackers-512693.shtml

[20] https://capec.mitre.org/data/definitions/210.html

[21] https://capec.mitre.org/data/definitions/223.html

[22] https://securityintelligence.com/hey-phishing-you-old-foe-catch-this-cognitive-drift/

Contents

IBM Security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
April 2017

IBM

SEL03129-USEN-00