

AN OFFERING FROM BDO'S CYBERSECURITY PRACTICE

BDO CYBER THREAT INSIGHTS

2018 3rd Quarter Report

SPECIAL FOCUS:
RECENT CYBER EVENTS
IN THE FINANCIAL
INSTITUTIONS INDUSTRY

In this issue

PREFACE

1

Cryptocoin's Crash

1

The Erosion of Info-Security

2

GLOBAL EVENTS AND TRENDS

3

BEC and Social Engineering Attacks – A Case Study

3

Disgruntled Employee Steals Sensitive Data from NSO

4

Faxploit – Attack Vector Leverages Exploit in Fax Machine Protocol

6

Lazarus Group - North Korean APT Deploys its First MacOS Malware

6

New Andariel Reconnaissance Tactic Leverages 0-Day Exploit in ActiveX

7

SPECIAL FOCUS / THE FINANCIAL INSTITUTIONS AND BANKING INDUSTRY

8

Ongoing Cybersecurity Insurance Dispute: Hackers Stole \$2.4 Million in Two Attacks on National Bank of Blacksburg

9

Japanese Crypto Exchange Zaif Loses \$60 Million in Attack

10

Bancor Cryptocurrency Market Hacked, \$23 Million Stolen

11

Attack on Indian Cosmos Cooperative Bank Results in \$13.5 Million Stolen

12

Russian Threat Group "MoneyTaker" Steals \$1 Million from Russian Bank via AWS CBR System

14

Adopt a Threat-Based Cybersecurity Model in 2019

15

BDO CYBERSECURITY SERVICES

16

CYBERSECURITY LEADERSHIP TEAM

17

Preface

Throughout the first half of 2018, several major incidents have had a profound impact across the cybersphere, and we are beginning to see their full ramifications.

CRYPTOCOIN'S CRASH

One of the most significant trends that has shaped the online environment is the meteoric rise and recent crash of cryptocurrency, which has impacted the global economy in a way that's reminiscent of the dot-com crash in the early 2000s.

At its height, cryptocurrency led by the likes of Bitcoin, Ethereum and Litecoin represented the first real promise of large scale financial decentralization. Starting as a fringe concept, it was on the verge of becoming a mainstream and legitimate fiat, until its promise fell flat. In fact, many have¹ called crypto's 80 percent dive worse than the dot-com crash.

That being said, criminal actors still exploited the situation. North Korea took a prominent role and has evolved from a fairly minor nation-state cyber entity to a formidable criminal actor. This, in conjunction with the ever-growing proliferation of advanced persistent threat groups (APTs) and advanced attack tools in China and Russia, has prompted governments and law enforcement agencies to seek measures to curb this tide of rapidly evolving threats. We have seen the results of this effort in recent months. This includes the arrest of the head of the Russian criminal group FIN7, and the indictment of the North Korean hacker allegedly behind major attacks including WannaCry.²

Another such effort was Operation Darkness Falls, an FBI-led international operation that took down multiple top Darknet vendors. This was the latest of notable law enforcement activity against Darknet illegal trade, which has been one of the key channels of cryptocurrency use. Consequently, throughout 2018, Darknet activity has experienced a significant scale-turn, with many actors abandoning Darknet markets and either moving to private Darknet forums or to clear-web platforms³ such as Telegraph.

Furthermore, due to diminishing returns following the crash of many cryptocurrencies, cryptomining attacks, aka cryptojacking, are no longer as cost effective as they were in mid-2018.⁴ While still relatively widespread⁵, in Q3 many actors appeared to have shifted their focus back to more traditional and lucrative criminal venues such as ransomware⁶ and Business Email Compromise schemes⁷—now with the added benefits of new funds, tools and experience.

1 <https://www.bloomberg.com/news/articles/2018-09-12/crypto-s-crash-just-surpassed-dot-com-levels-as-losses-reach-80>

2 <https://www.washingtontimes.com/news/2018/sep/14/north-korea-disputes-existence-park-jin-hyok-suspe/>

3 <https://www.intsights.com/dark-side-of-asia-research-report>

4 <https://arxiv.org/pdf/1808.09474.pdf>

5 <https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Ilicit-CryptoMining-Whitepaper.pdf>

6 <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018>

<https://www.bleepingcomputer.com/news/security/ryuk-ransomware-crew-makes-640-000-in-recent-activity-surge/>

7 <https://www.infosecurity-magazine.com/news/account-takeover-attacks-result-in/>

THE EROSION OF INFO-SECURITY

Another continued trend is the erosion of basic recommended info-sec behavior amongst individuals, companies and organizations. Cynical net-neutrality laws, consolidation of personal data among a handful of companies, growing dependency on interconnected devices (IoT)⁸, and the constant barrage of online threats and data breaches, have all fatigued the general population on this matter.

Moreover, a recent report⁹ found that more than 90 percent of U.S. retailers' websites are noncompliant with the industry security standard, Payment Card Industry Data Security Standard (PCI DSS). For example, it was recently reported¹⁰ that customers of online retailer Newegg had their cards skimmed for a full month, and a U.S. government payment service exposed records of more than 14 million customers because of a website error.¹¹

In response, many individuals are giving up on obtaining full control of their digital presence; accepting 'transparency' in return for convenience. Beyond the ethical privacy implications of this issue, the immediate ramifications are that malicious actors increasingly leverage the complacency of employees and organizations to execute seemingly basic attacks with potentially severe outcomes.

8 <https://www.infosecurity-magazine.com/news/blackiot-aims-to-disrupt-the-power/>

9 <https://www.infosecurity-magazine.com/news/over-90-of-us-retailers-fail-pci/>

10 <https://arstechnica.com/information-technology/2018/09/newegg-hit-by-credit-card-stealing-code-injected-into-shopping-code/>

11 <https://www.infosecurity-magazine.com/news/government-payment-service-exposes/>



Global Events and Trends

A number of notable cybersecurity trends and events specific to the financial services and banking industry are presented below from the third quarter, illustrating the various threats companies and organizations from all sectors face. The first events demonstrate long-established threats that continue to plague companies and organizations, while the last two showcase the continual exploration of new and innovative attack methods by malicious actors.

The Business Email Compromise (BEC)'s Global Rise

This year has seen a sharp increase in Business Email Compromise attacks (BEC), which are growing to be one of the most preferred attack vectors used by cybercriminals. These types of attacks, often involving criminals spoofing domains, impersonating brands, corporate identities, executives or company clients, are proving advantageous to threat actors. They are lucrative, often require little technical effort or investment, and are often quite sophisticated.

According to the FBI, most BEC victims use wire transfers or checks as common methods of transferring funds for business purposes. Criminals use the method most commonly associated with their victim's normal business practices. The FBI also reported that between December 2016 and May 2018, there was a 136 percent increase in identified global exposed losses from BEC scams. Incidents have been reported in all 50 U.S. states and in 150 countries, and victim complaints filed with the IC3 and other financial authorities indicate fraudulent transfers have been sent to 115 countries.¹²

Instead of malware or exploiting software vulnerability, BEC scammers rely on social engineering techniques to fool their victims and obtain critical information. These techniques range from sending increasingly personalized and targeted phishing emails, to phone calls in which criminals trick employees into handing over data or credentials. Employees have also been tricked into wiring millions of dollars to bank accounts controlled by the criminals.

As such, the stark reality is that companies' cybersecurity frameworks can no longer be one dimensional.

BEC AND SOCIAL ENGINEERING ATTACKS – A CASE STUDY

In the following BEC case, rather than stealing credentials or compromising email accounts, the culprits set up a spoof email address impersonating a corporate client of a prominent company within the aviation sector. **Note that no identifying details regarding both the company and its client are disclosed.**

Timeline of Events

Armed only with a fake email address, the attackers disguised themselves as the client and contacted the company using a publicly-listed address, requesting a Statement of Account owed. The email, which should have raised red flags as it was sent to a public address, was nevertheless promptly forwarded to the company's accounting department. The accounting department complied and duly provided the attackers with the client's Statement of Account and an invoice, which the attackers, posing as the client, claimed they had not received.

Weaponizing this information, the criminals registered a number of domains impersonating the company. They also created an email address, this time spoofing the original company, which was signed off on using an employee signature the attackers obtained from contact with said accounting department. Using the spoofed domains and email address, the attackers then contacted the real client, requesting funds as per the Statement of Account (which was attached), to be paid to a new bank account. After several correspondences between the attackers and the client, during which the former used details from the invoice and Statement of Account to increase credibility, the client was convinced enough to make the payment.

¹² <https://www.ic3.gov/media/2018/180712.aspx>

Cybersecurity Lessons Learned & Recommendations

- ▶ **Understand BEC actors often seek to obtain information and intelligence on their targets through open-source means and social engineering methods:** Be wary and verify any contact (emails, phone calls, text messages) or requests that require the disclosure of company information, especially matters concerning payments, transactions and information regarding employees.
- ▶ **Verify all requests for a change in payment type and/or location, or the original recipient's financial information:** Make sure all requests are made through legitimate and agreed upon channels.
- ▶ **Establish a standard payment protocol with passcodes when dealing with individual clients:** For example, use verification code phrases before transactions are carried out. While this method may not be foolproof, it constitutes another hurdle an attacker must surmount to be successful.
- ▶ **Raise organization-wide cybersecurity awareness:** Highlight techniques used by BEC actors.
- ▶ **Ensure that when a fraudulent transfer is detected, your organization immediately contacts your financial institution and requests a recall of the funds.** Law enforcement and the FBI may also be able to assist the financial institution in recovering funds.

DISGRUNTLED EMPLOYEE STEALS SENSITIVE DATA FROM NSO

In July 2018, a former NSO employee was indicted for attempting to sell proprietary and sensitive data. The individual worked at NSO for a year and a half, developing automation solutions for the company's products and performing QA, with access to sensitive systems and data. After he was dismissed, in what appeared to be a pre-planned attack, the employee used his credentials to obtain the source code of the firm's product, valued at hundreds of millions of dollars. He then attempted to sell the data on the Darknet for \$50 million in cryptocurrencies.

The NSO Group provides various solutions and services for mobile platforms, notably extracting data for security and defense operations. Its main product is the spy software named "Pegasus," which law enforcement agencies use to take full control of mobile devices. Pegasus enables users to record calls, view photos and text messages, as well as monitor the online activity of devices. This is done through the exploitation of various OS vulnerabilities, including 0-day (previously unknown or reported vulnerabilities). The software, which works both on Android and iOS, is covert and leaves no traces.

It was later discovered that in February 2017, three months after he began working at NSO, the employee conducted online research on how to disable an anti-leak software, McAfee DLP, which was installed on the company's computers. The software prevents the use of any external storage on the systems. Later in April, the employee was told of his dismissal and was summoned for a hearing. As an act of revenge, he then disabled the security software and stole various proprietary tools and source codes. **Note that the company did not detect the disabling of its security software.**

After obtaining the data and attempting to sell it on the Darknet, a potential buyer contacted NSO and alerted the company that its data was leaked. The company then engineered a plan to apprehend the seller, who was later revealed to be the former employee.

Similar Incidents

While this one incident is highly disturbing, there are unfortunately many other cases like it. Below are several other notable, recent examples:

	COMPANY	DESCRIPTION
	Tesla	An employee broke into the company's manufacturing operating system and sent highly sensitive data ¹⁴ to unknown third parties.
	Google – Waymo	A former Google engineer allegedly stole trade secrets from the company's self-driving project and sold them to Uber. ¹⁵
	GlaxoSmithKline Pharmaceuticals	A cancer researcher stole biopharmaceutical trade secrets to sell in China. ¹⁶
	Apple Inc.	A former Apple employee allegedly stole autonomous vehicle trade secrets from the company for a Chinese start-up by the name Xiaopeng Motors, which is also developing autonomous vehicle technology. ¹⁷

Cybersecurity Best Practices:

- ▶ **Ensure Real-Time Monitoring, Detection & Response (MDR):** It is ineffective to install an anti-leak system if it fails to alert in real time, or if an organization cannot detect disablement. Moreover, the effectiveness of such a system is significantly hindered if no one can respond to such alerts in real time.
- ▶ **Implement a policy of "least privilege":** Compartmentalize departments and limit permissions for sensitive systems to only those who require access for their daily work.
- ▶ **Implement an organization-wide policy of promptly disabling permissions of employees:** As soon as they leave—or are being let go from—the company.

¹³ <https://www.bloomberg.com/news/articles/2018-06-18/musk-calls-for-paranoia-after-fire-halts-tesla-assembly-line>

¹⁴ <http://fortune.com/2018/02/05/waymo-v-uber-what-you-need-to-know-about-the-high-stakes-self-driving-tech-trial/>

¹⁵ <http://www.witf.org/news/2018/08/researcher-admits-plot-to-steal-trade-secrets-to-sell-in-china.php>

¹⁶ https://www.washingtonpost.com/news/morning-mix/wp/2018/07/11/ex-apple-engineer-arrested-on-his-way-to-china-charged-with-stealing-companys-autonomous-car-secrets/?utm_term=.ac56b8f2ee69

FAXPLOIT – ATTACK VECTOR LEVERAGES EXPLOIT IN FAX MACHINE PROTOCOL

A report recently published by Checkpoint¹⁷ revealed a new attack method that leverages a vulnerability dubbed “Fexploit.” The report demonstrates how cyber criminals can infiltrate private or corporate networks by exploiting all-in-one printer-fax machines using only a fax number – a detail often found on company business cards. As part of its investigation, Checkpoint’s researchers successfully penetrated an entire IT network using vulnerabilities in the fax protocol using a known fax number. This presents a completely new and simple attack vector from which cyber criminals could launch a campaign against industries that hold protected data. In addition, popular online fax services, such as Fax2Email, use the same protocol, so the same vulnerability may also exist there.

This attack vector may also be leveraged to access networks completely disconnected from the internet, as it is carried out via telephone lines rather than the internet itself. An attacker need only penetrate one access point in the network, a printer-fax device, to enter the entire corporation’s network. From this point, the attacker would be able to hop from one part of the network to the next, infecting other devices in the network through lateral movement.

But the theft of documents is just one option for an attack. Other possibilities include sending a copy of every fax a customer sends to their bank, for example, with sensitive account information included, or changing the content of the fax itself.

Note that while in the past, fax machines were standalone devices, today they are most often integrated within printers and scanners and can be found in nearly every company, organization or home network. Despite the fact that these devices are mostly used for printing purposes, the fax machine is still available and usually connected to phone lines. *This renders it vulnerable to attackers.*

Checkpoint’s research focused on HP’s all-in-one printer fax machines. However, the vulnerability exists within the fax protocol itself – so attackers can leverage the exploit against any fax vendor using this protocol. Many of today’s fax vendors, specifically the manufacturers of the all-in-one devices, have already issued a security patch. Nevertheless, hundreds of vendors remain unaware of this issue, leaving them vulnerable to this type of attack.

LAZARUS GROUP - NORTH KOREAN APT DEPLOYS ITS FIRST MACOS MALWARE

North Korea’s Lazarus Group, the nation-state actor infamous for targeting financial institutions and organizations worldwide, has recently deployed malware targeting MacOS for the first time. Until recently, the group focused solely on Windows platforms. According to reports, over the last few months, Lazarus has successfully compromised several banks and infiltrated several global cryptocurrency exchanges and Fintech companies.¹⁸ The actor’s targeting of non-Windows systems signals an evolution of its Tactics, Techniques and Procedures (TTPs), cause for concern for Mac users.

Dubbed Operation AppleJeus, the infection vector of Lazarus’ recent campaign involved the insertion of malicious code – in the form of an update – for a legitimate-looking crypto trading application. Once downloaded by users, the trojanized application infects their computer with the Lazarus-affiliated tool known as FallChill. The application in question is Celas Trade Pro, an all-in-one style cryptocurrency trading program by Celas Limited. Upon initial inspection, the application appears to show no signs of malicious behavior. However, the presence of a malicious updater has been confirmed.

In the case of MacOS users, a hidden “autoupdater” module is installed in the background to start immediately after installation of the native application and after each system reboot. The module regularly communicates with the C2 server to download and run additional executables. The malware collects information on targeted hosts and encrypts the collected information before uploading it to a webserver using HTTP at the URL [www.celastllc\[.\]com/checkupdate.php](http://www.celastllc[.]com/checkupdate.php), which hosts a legitimate looking website. In both Windows and MacOS, the communication is disguised as an image file upload and download, while carrying encrypted data inside.

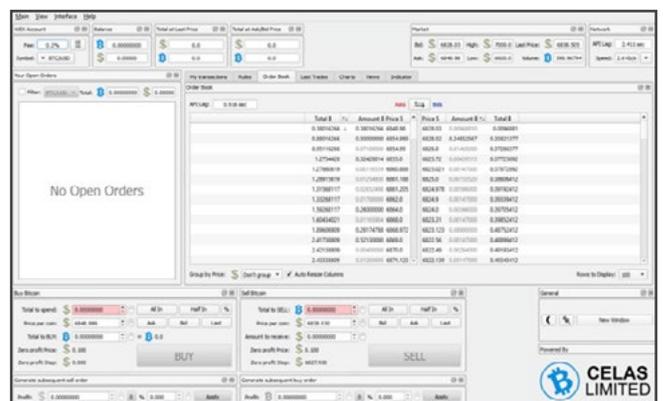


Figure 1: Image of the Celas Trade Pro software

17 <https://blog.checkpoint.com/2018/08/12/fexploit-hp-printer-fax-exploit/>

18 <https://securelist.com/operation-applejeus/87553/>



NEW ANDARIEL RECONNAISSANCE TACTIC LEVERAGES 0-DAY EXPLOIT IN ACTIVEX

Reconnaissance plays a major role for threat actors looking to execute an attack. This means attackers will invest significant time and effort to investigate the systems of their targets. On July 16, 2018, Trend Micro and South Korean security team IssueMakersLab revealed new reconnaissance tactics used by Andariel, a branch of the North Korean threat actor Lazarus Group.^{19 20}

In May 2017, IssueMakersLab published a review of an Andariel Watering Hole campaign dubbed GoldenAxe,²¹ which targeted the visitors of various South Korean business websites.²² The infection vector in this campaign leveraged a 0-Day vulnerability in the ActiveX browser component. However, on June 21, 2018, Trend Micro discovered that the threat actor **injected a reconnaissance script into four other compromised South Korean websites**, among them a website belonging to a South Korean non-profit organization and three South Korean local government labor union websites.

The reconnaissance ended on June 27, 2018. The script was designed to collect information on visitors via their browsers and was similar to the malware Andariel used during the 2017 GoldenAxe threat campaign.

The threat actor took the original script from PluginDetect,²³ a JavaScript library that detects browser plugins such as ActiveX and Flash - types of plugins that often expose users to attacks. In this case, Andariel used the script to verify its victims during the reconnaissance stage of an attack and then sent the collected information to one of its designated servers.

An analysis of the script the actor used revealed that the script attempted to detect two additional ActiveX objects that were not on the object list of the script used in the 2017 campaign:

- ▶ **DSDOWNCTRL.DSDownCtrlCtrl.1** – an object related to a DRM (Digital Rights Management) software by a South Korean Document Protection vendor.
- ▶ **WSACTIVEBRIDGEAX.WSActiveBridgeAXCtrl.1** – an object related to a South Korean voice conversion software company used by numerous local governments and public institutions.

¹⁹ https://blog.trendmicro.com/trendlabs-security-intelligence/new-andariel-reconnaissance-tactics-hint-at-next-targets/?utm_source=trendlabs-social&utm_medium=smk&utm_campaign=0718_Andariel

²⁰ <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations>

²¹ <http://www.issuemakerslab.com/research3/>

²² <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0189>

²³ <http://www.pinlady.net/PluginDetect/>

SPECIAL FOCUS

The Financial Institutions and Banking Industry

Global financial institutions are lucrative targets for cyberattacks. The sector houses a wealth of sensitive client information and liquid assets that attackers can seize for financial gain. State actors also perpetrate attacks on financial institutions with the intent to manipulate or disrupt markets. In the last three years alone, banks and financial institutions experienced 154 publicly reported data breaches that compromised nearly 150 million records, according to Privacy Rights Clearinghouse.²⁴

Cyberattacks on financial institutions have not slowed in 2018. As businesses get savvier about cybersecurity, attackers are getting smarter and executing attacks with greater proficiency. They are quickly building skills to execute attacks on both traditional financial organizations—banks, mortgage and brokerage firms—and non-traditional financial companies and platforms such as cryptocurrency markets and initial coin offering (ICOs). The second and third quarters of this year saw several notable attacks on crypto exchanges—and those types of attacks are likely to increase.

Even in the traditional banking sphere, the way the world interacts with, invests and moves money is changing—and the cyber threat landscape is transforming in tandem. Gone are the days where brick-and-mortar institutions were the only game in town. The pool of companies with an exclusively online presence is expanding. Those consumers that do maintain brick-and-mortar loyalty still expect easy access to funds on mobile banking and investment apps. While mobile banking applications have strong security, an increasingly connected banking experience can introduce more vulnerabilities.

KEY CYBERSECURITY LESSONS FOR FINANCIAL INSTITUTIONS TO REMEMBER IN 2019

In the subsequent section, we outline the details of five prominent cyberattacks against the sector in 2018. So, what can financial institutions learn from these attacks?



1. **Exercise increased vigilance during bank holidays.** As the U.S. holiday seasons starts, banks and financial institutions are entering a period when their enterprises are typically more vulnerable to cyberattacks. The attacks on Indian Cosmos Cooperative Bank and the National Bank of Blacksburg both occurred while the banks were closed, which permitted the breach to go undetected for a longer period of time.



2. **When the breach is resolved, the financial hits could keep coming.** International regulatory bodies are holding financial institutions accountable for cyber negligence more frequently. The U.K.'s Financial Conduct Authority (FCA) issued their first fine for a cyber failing just this year. In early October, FCA levied a £16.4 million fine on Tesco Bank for a 2016 breach that exploited a cyber weakness the regulatory agency had previously warned the bank about.



3. **Read the fine print of your cyber insurance policy.** In one case detailed below, the National Bank of Blacksburg was left with a larger cyber liability than it anticipated. Proactively discussing what types of breaches are, and aren't, covered with your insurance provider could help you avoid unwelcome surprises down the line.

²⁴ https://www.privacyrights.org/data-breaches?title=&org_type%5B%5D=260&taxonomy_vocabulary_11_tid%5B%5D=2436&taxonomy_vocabulary_11_tid%5B%5D=2434&taxonomy_vocabulary_11_tid%5B%5D=2257

ONGOING CYBERSECURITY INSURANCE DISPUTE: HACKERS STOLE \$2.4 MILLION IN TWO ATTACKS ON NATIONAL BANK OF BLACKSBURG

One of the most intriguing financial heists in recent years came to a head when The National Bank of Blacksburg in Virginia filed a lawsuit against an insurance firm this summer. The bank discovered it fell victim to phishing attacks twice over the course of eight months—between late May 2016 and January 2017—resulting in \$2.4 million²⁵ in losses. After their insurance firm refused to fully cover the loss²⁶, the bank filed a lawsuit. Let's examine the case specifics:

The Attacks

The threat actors behind these attacks, currently presumed to be Russian, sent spear-phishing emails to the National Bank of Blacksburg in Virginia, infecting a workstation that had access to the debit card transaction system used by the bank, the STAR Network.²⁷ Concurrently, the malware spread and eventually infected another workstation that was authorized to manage National Bank customer accounts and their use of ATMs and bank cards. The malware was leveraged to disable and alter anti-theft and anti-fraud protections, such as four-digit PINs, withdrawal limits, daily debit card usage limits and fraud score protections.

Timeline

FIRST ATTACK: MAY 28, 2016

The first attack took place between Saturday and Memorial Day Monday, when the bank was closed in observance of the federal holiday. In this incident, the threat actors withdrew over \$569,000 from hundreds of ATMs across North America. When the breach was detected, the bank hired cybersecurity forensics firm Foregenix to investigate. Foregenix determined the malicious tools and activity likely originated from Russia. Following this discovery, the National Bank implemented additional security protocols based on recommendations from FirstData, the company that operates the Star Network system. These protocols, which are known as "velocity rules," help the bank monitor and flag anomalous patterns of transactions that are executed within a short period of time.²⁸

SECOND ATTACK: JAN. 7 AND 9, 2017

The attackers presumably maintained access to the bank's systems, which was not detected in the investigation. The second breach was more substantial as the attacker not only regained control of Star Network system, but also compromised a workstation that had access to Navigator, a credit and debit management software used by the bank. This enabled them to disable clients' withdrawal limits for over \$2 million and successfully steal \$1,833,984. In 2017, the bank hired Verizon to investigate the attacks. The investigation uncovered three main insights:

- ▶ The origin of the tools and servers used by the attackers were indeed from Russia
- ▶ There is a high likelihood the same actor executed both attacks
- ▶ The malware used to obtain the initial access to the bank's systems was embedded in a malicious Doc file.²⁹

²⁵ <https://krebsonsecurity.com/2018/07/hackers-breached-virginia-bank-twice-in-eight-months-stole-2-4m/>

²⁶ <https://krebsonsecurity.com/wp-content/uploads/2018/07/1-main.pdf>

²⁷ https://firstdata.com/en_us/products/financial-institutions/debit-processing-atm-and-network/star-network.html

²⁸ <https://chargeback.com/velocity-checks-fraud-prevention/>

²⁹ <https://blog.barkly.com/what-is-macro-malware-2017>

The Lawsuit

To cover the losses, the bank activated its cyber insurance policy with its insurer, Everest National Insurance Company.³⁰ The policy covered two cyberattack scenarios. The first covered "computer and electronic crime" (C&E) with a single loss limit liability of \$8 million. The second covered losses that resulted directly from the use of lost, stolen or altered debit cards or counterfeit cards. This had a single loss limit of liability of \$50,000, and an aggregate limit of \$250,000.

So, what went awry to prompt the lawsuit? The insurance company determined both attacks exclusively fell under the second scenario (credit and debit), rather than the C&E scenario due to two exclusions, and therefore was eligible for only \$50,000 liability in total. The bank is contesting the decision and filed a lawsuit claiming it does not yet know for certain how the hackers extracted the funds in the 2017 heist. In previous heists of this nature (often referred to as "unlimited cashouts"³¹), attackers used multiple "money mules." These are usually street criminals who are given cloned debit cards and stolen or fabricated PINs along with instructions on where and when to withdraw funds. Everest issued a statement³² in response to the bank's claims, stating that the National Bank did not accurately characterize the terms of its coverage nor did it fully explain the basis for Everest's decision.

Insights and Conclusions

There is no foolproof method to fully prevent cyberattacks; accordingly, when organizations insure their assets, it is advised to closely examine various insurance policies and firms together with an expert that specializes in cyberattack claims. Moreover, if possible, we recommend creating a custom tailor-made policy that suits your organization's specific needs.

JAPANESE CRYPTO EXCHANGE ZAIF LOSES \$60 MILLION IN ATTACK

Japan's crypto market was hit by yet another cyberattack, this time resulting in the theft of about \$60 million worth of cryptocurrency. The attack targeted Zaif, a registered cryptocurrency exchange owned by the Osaka-based Tech Bureau Corp. It was successfully carried out just seven months after the massive Coincheck attack that resulted in the theft of \$520 million worth of NEM tokens.³³ The attack occurred despite the fact that Japan's Financial Services Agency (FSA) carried out multiple inspections on cryptocurrency exchanges in the country after the Coincheck attack. Prior to the attack on Zaif, the FSA had already issued two business improvement orders to Tech Bureau, specifically targeting its security and the implementation of anti-money laundering (AML) measures, after it found the company's standards lacking in March.

On Sept. 20, 2018, Tech Bureau stated that the exchange first noticed an unusual movement of funds from its platform around 17:00 local time on Sept. 14, 2018. After detecting the suspicious activity, the company suspended all asset deposit and withdrawal services. After further investigation, Tech Bureau discovered that approximately \$60 million in Bitcoin, Bitcoin cash and Monacoin were stolen from the exchange's hot wallet, a wallet that can be accessed online and is not isolated from the internet. About \$19.6 million worth of the stolen currency was owned by the company, while the remaining \$40.1 million belonged to its customers.³⁴

As of yet, Tech Bureau has pledged to compensate users who lost assets and has not provided further details on the exact nature of the attack, as the investigation is ongoing. Meanwhile, Fisco, a Japan-based firm, signed an agreement to invest \$44.5 million in Tech Bureau in exchange for a majority share of ownership. The FSA has asked Tech Bureau to submit a report on the incident and plans to perform an on-site inspection of the company after receiving the document.

³⁰ <https://www.everestre.com/>

³¹ <https://krebsonsecurity.com/2011/08/coordinated-atm-heist-nets-thieves-13m/>

³² <https://krebsonsecurity.com/wp-content/uploads/2018/07/everest-response.pdf>

³³ <https://cointelegraph.com/news/story-of-coincheck-how-to-rebound-after-the-biggest-theft-in-the-history-of-the-world>

³⁴ <https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-theft/amp/>

BANCOR CRYPTOCURRENCY MARKET HACKED, \$23 MILLION STOLEN

On July 9, the cryptocurrency exchange platform Bancor announced it was disabling its operation and services following a breach. The attackers stole Ethereum coins worth \$12 million, as well as \$10 million worth of the company's in-house crypto coin BNT (Bancor Network Token).

Three hours later, at 14:16, the company issued a new statement, officially reporting the breach.

At time of publication, the attack vector is not clear, however it was reported that the attacker emptied several of the company's online crypto coin wallets that contained various popular coins such as Ethereum. Their in-house coin BNT became publicly tradable in June 2017. It is also used by Bancor as a platform to quickly and cheaply exchange various crypto coins.

This exchange is done automatically, and with no third-party intervention, by changing the coins to BNT and then to the requested crypto coin. As Bancor controls the operation of their coin, they were able to freeze its transactions and minimize the loss.

While Bancor was only able to freeze BNT transactions and not those with other crypto currencies, the company claims is working with other crypto exchange markets to try and locate the stolen funds. According to the company, their clients are not affected, and no funds were directly stolen from them, however the value of BNT has dropped significantly due to these events.

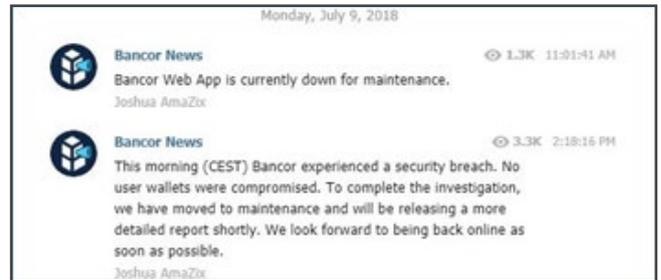


Figure 2: Bancor's announcement on shutting down their service, issued via Telegram on July 9 at 11:01

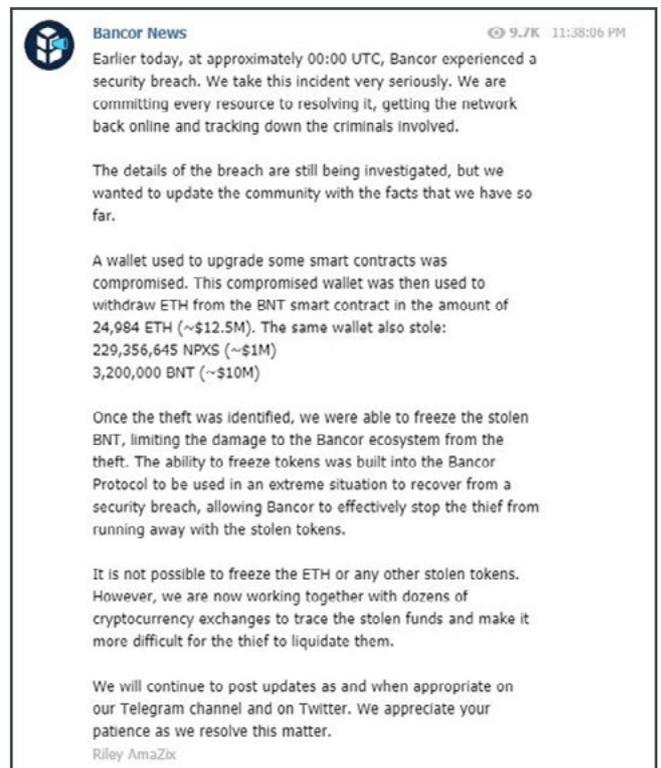


Figure 3: Bancor providing initial details regarding the breach, issued via Telegram on July 9, 23:38

ATTACK ON INDIAN COSMOS COOPERATIVE BANK RESULTS IN \$13.5 MILLION STOLEN

On Aug. 15, 2018, the India-based Cosmos Cooperative Bank³⁵ reported that it fell victim to cyberattacks targeting two core banking systems, the ATM/Debit card system and the SWIFT inter-banking system. The bank lost \$13.5 million as a result of these two attacks, which took place over two days.

Initial Attack on ATM/Debit Systems (Saturday, Aug. 11)

The first attack took place on Aug. 11 throughout the course of 7 hours between 15:00 and 22:00. Note that Aug. 11 was a Saturday, when the bank was closed for business. Below are the known details:

- ▶ The attackers breached the bank's systems prior to perpetrating the attack via an unknown vector at an unknown date. After which they leveraged their access to obtain control of the bank's debit systems with an unreported type of malware. This system manages PIN code changes, ATM cash withdrawals restrictions and other sensitive transactions. While it is currently unknown what debit systems the bank uses, the vast majority of banks in India are based on National Payment Corporation of India's (NPCI) National Financial Switch system (NFS).
- ▶ The attackers created a proxy switch server that enabled them to respond to ATM cash withdraw requests from around the world. This enabled them to execute unlimited withdrawals via cloned debit cards, created prior to the execution of the attack. The cards issued were VISA and RuPay, which belong to NPCI.
- ▶ Over the course of several hours, the money mules conducted 14,849 cash withdrawals from ATM machines in at least 28 countries around the world. In total 800 cards were used; 400 in India and another 400 in other countries. At time of publication, the names and locations of the banks where the attackers withdrew the money were not disclosed to avoid jeopardizing the investigation.

Second Attack on SWIFT Inter-Banking System (Monday, Aug. 13)

The following outlines the known details:

- ▶ The attackers breached the bank's SWIFT systems via an unknown vector at an unknown date.
- ▶ The second attack was executed on Aug. 13, two days following the first attack, seemingly shortly after the bank detected the ATM/Debit system breach.
- ▶ The attackers transferred about \$2 million to a bank account of a company by the name ALM Trading Limited, at Hang Seng Bank in Hong Kong.³⁶
- ▶ Additionally, the attackers also transferred about \$350,000 to a bank account in India.

Investigation of the Attacks

Once the bank detected the breach, it immediately reported the attack and shut its VISA and RuPay Debit card payment system. The bank hired a cybersecurity company to conduct a forensic investigation of the event, which is still ongoing.

According to the bank, the perpetrators are highly sophisticated and likely obfuscated their tracks by various means. A full investigative report is expected to be published in October.

While the identity of the attackers is unknown, various assessments are attributing the attack to the North Korean nation-state threat group Lazarus, which has executed numerous attacks on financial institutions around the world in recent years.

Unresolved Questions of the Cosmo Attack

Several questions remain unanswered in the Cosmos cyberattack. It is still unknown how and when the attackers' breached the bank and established their foothold on its operational network. The attackers likely did not have access to the bank's operational network, and only a full control of several of the bank's core systems, which they leveraged for attacks on the ATM/Debit and SWIFT systems.

Regarding the initial attack on Cosmos' ATM and debit systems, it is unclear at what point the proxy switch server established by the attacker intercepted the cash withdraw requests; prior or after they reached the bank systems. As of writing this report, it seems that the attacker only intercepted the withdraw requests of VISA and RuPay Debit.

35 <https://timesofindia.indiatimes.com/business/india-business/hackers-siphon-over-rs-94-crore-off-a-co-operative-bank-in-pune/articleshow/65411078.cms?from=mdr>

36 <https://www.dailypioneer.com/todays-newspaper/cosmos-cooperative-bank-loses-rs-94-cr-in-cyber-heist.html>

There are currently no indications that they had access to the bank's debit card payment system. If the requests between the bank and the payment companies were "signed", encrypted and examined by the payment companies, it is likely the attack would have failed.

What prompted the attackers to strike twice, and target two different systems? The second cyberattack was smaller in scale and executed two days after the initial attack, before the bank realized its systems had been compromised. It is possible that the attackers understood the attack would soon be detected, and thus decided to execute a smaller and quicker attack on the bank's SWIFT system.

System Failures that Prompted the Cyberattack

- ▶ **The bank's anti-fraud systems failed.** The anti-fraud systems are the last line of defense, and at times, the only means to prevent cyberattacks. In an ideal chain of process, the fraudulent ATM withdrawals would have triggered the following actions:
 - Cosmos bank should have flagged and alerted the irregular activity.
 - Each of the banks in the aforementioned 28 countries should have also flagged and alerted in real time about repeated withdraws over a short period executed with the same cards.
 - This irregular activity should have also been flagged and alerted by VISA and RuPay Debit. It is possible that this did occur, however Cosmos Bank did not respond to the alerts.
- ▶ **The anti-fraud systems failed to alert in real time about the fraudulent SWIFT transactions.** Some of the contributing factors include:
 - **The transactions were executed when the bank was closed.** Similar to many previous attacks on banks, executing the attack outside the hours and days of operation, increases chances the attack will be detected after it is too late. In this incident, the attack was only detected on Monday after the employees returned from their weekend vacation.
 - **Cosmos bank did not have a real time 24x7 alert system in place.** A continuous monitoring and alert system likely would have thwarted the attack if it was working in conjunction with anti-fraud systems.

What We Know About the Attackers

The attack included a coordinated and simultaneous cashing out of ATMs in at least 28 countries around the world by numerous money mules. Such a complex operation requires the involvement of many individuals for it to succeed as it did. In our assessment, this type of attack is more in line with Russian cybercrime groups than North Korean APTs.

At this stage we have not ruled out the possibility that the two attacks were executed by two different actors. It is possible that the bank systems were compromised by two attack groups, one that specializes in ATM systems, and the other in SWIFT systems. Alternatively, it is also possible that the first group breached the bank's systems and sold their access to another group, who later executed the attack on the SWIFT system.

One thing is clear: The attackers were highly proficient and had an intimate knowledge and understanding of the inner workings of banks' wire-transfer and withdrawal process. Cybercriminal groups are constantly improving their methods and skills—we've seen that evidence with worsening attacks waged by Carbanak and nation-state actors such as North Korean APTs. Accordingly, we expect the group that carried out the Cosmos attack will begin targeting additional core banking systems in the future.

RUSSIAN THREAT GROUP "MONEYTAKER" STEALS \$1 MILLION FROM RUSSIAN BANK VIA AWS CBR SYSTEM

On July 3, 2018, Russian cybercriminal group MoneyTaker stole about \$1 million from Russia's PIR bank. The actor gained access to the Russian Central Bank's Automated Workstation Client (AWS CBR) system, which is equivalent to the inter-banking communications and transactions system SWIFT. The group then transferred the stolen money to 17 different accounts at major Russian banks and cashed out without leaving traces.³⁷

MoneyTaker primarily targets interbank payment systems such as SWIFT or AWS CBR.³⁸ According to the investigation executed by Group-IB, MoneyTaker has conducted 21 known attacks against banks so far. Sixteen were executed against banks in the U.S., while five attacks were aimed at banks in Russia. The average damage per incident amounted to \$500,000 in the U.S. and \$1.2M in Russia. The group also stole documents about interbank payment systems that could inform subsequent attacks, and executed an attack against a banking software company in the UK.³⁹

MoneyTaker is highly sophisticated, often using self-developed hacking methods and tools, including file-less malwares. The cybercriminal group also uses tools that are widely used such as Metasploit, NirCmd, psexec, Mimikatz, and Powershell Empire, which makes it more difficult to establish attribution. The group is known for their covert operation, obfuscating their activity by using 'one-time' infrastructure and meticulously deleting evidence following their attacks.⁴⁰ Nevertheless, cyber researchers have identified this modus operandi since late 2017.⁴¹

How MoneyTaker Perpetrated the Attack

The attack on PIR bank began in late May 2018, after the group managed to obtain access to the bank's systems via a compromised router. As mentioned in Group-IB's report, this technique is a characteristic of MoneyTaker, and was previously used at least three times against banks with regional branch networks.⁴²

On July 3, after establishing a persistent foothold for over two months, the group hacked the bank's main network, accessing the AWS CBR system. Once in, they transferred funds to mule accounts prepared in advance across 17 major banks around the world, which were cashed out immediately via ATMs.

The attack was detected the following night, on July 4, when the bank's IT staff identified unauthorized transactions with large sums. They promptly contacted the regulator and requested to block the AWS CBR digital signature keys, however it was too late to stop the financial transfers. MoneyTaker successfully withdrew \$920,000.

Beyond stealing funds, the group deleted OS logs on many of the bank's computers to hinder its ability to respond to the incident and conduct an investigation. This tactic is one MoneyTaker has used in prior attacks. The cybercriminal group also left behind PowerShell scripts, which could have enabled them to re-establish access to the bank's network and execute new attacks if they hadn't been discovered by Group-IB and removed by the bank's sysadmins.⁴³

Insights and Conclusions

According to Group-IB, MoneyTaker is one of the most sophisticated and prominent threat actors that banks face around the world. In the group's most successful attacks, MoneyTaker used routers as an entry-point. To mitigate the risk of an attack via routers, it is recommended to:⁴⁴

- ▶ Routinely review your systems and insure they are up to date with the latest firmware.
- ▶ Routinely check for changes in router configuration.
- ▶ Test systems for brute-force vulnerabilities.

37 <https://www.group-ib.com/media/new-attack-MoneyTaker/>

38 <https://thehackernews.com/2017/12/bank-hackers.html>

39 <https://arstechnica.com/information-technology/2018/07/prolific-hacking-group-steals-almost-1-million-from-russian-bank/>

40 <https://www.group-ib.com/media/new-attack-MoneyTaker/>

41 <https://securityaffairs.co/wordpress/74586/cyber-crime/moneytaker-cyber-heist.html>

42 <https://www.securityweek.com/MoneyTaker-hackers-stole-1-million-russian-bank>

43 <https://arstechnica.com/information-technology/2018/07/prolific-hacking-group-steals-almost-1-million-from-russian-bank/>

44 <https://www.group-ib.com/media/new-attack-MoneyTaker/>

ADOPT A THREAT-BASED CYBERSECURITY MODEL IN 2019

It's time for the financial industry to reassess its cybersecurity posture. Many companies concentrate cybersecurity investments on what they consider to be their most valuable informational assets. The problem with this approach, though, is that what they themselves deem most valuable often differs from the hacker's prime target.

To approach cybersecurity with the hacker's end goal in mind, take a different approach: threat-based cybersecurity. Instead of, or in addition to, focusing on protecting critical data assets or following the basic script of a cyber program, threat-based cybersecurity concentrates investments in the most likely risks and attack vectors based on the organization's unique threat profile.

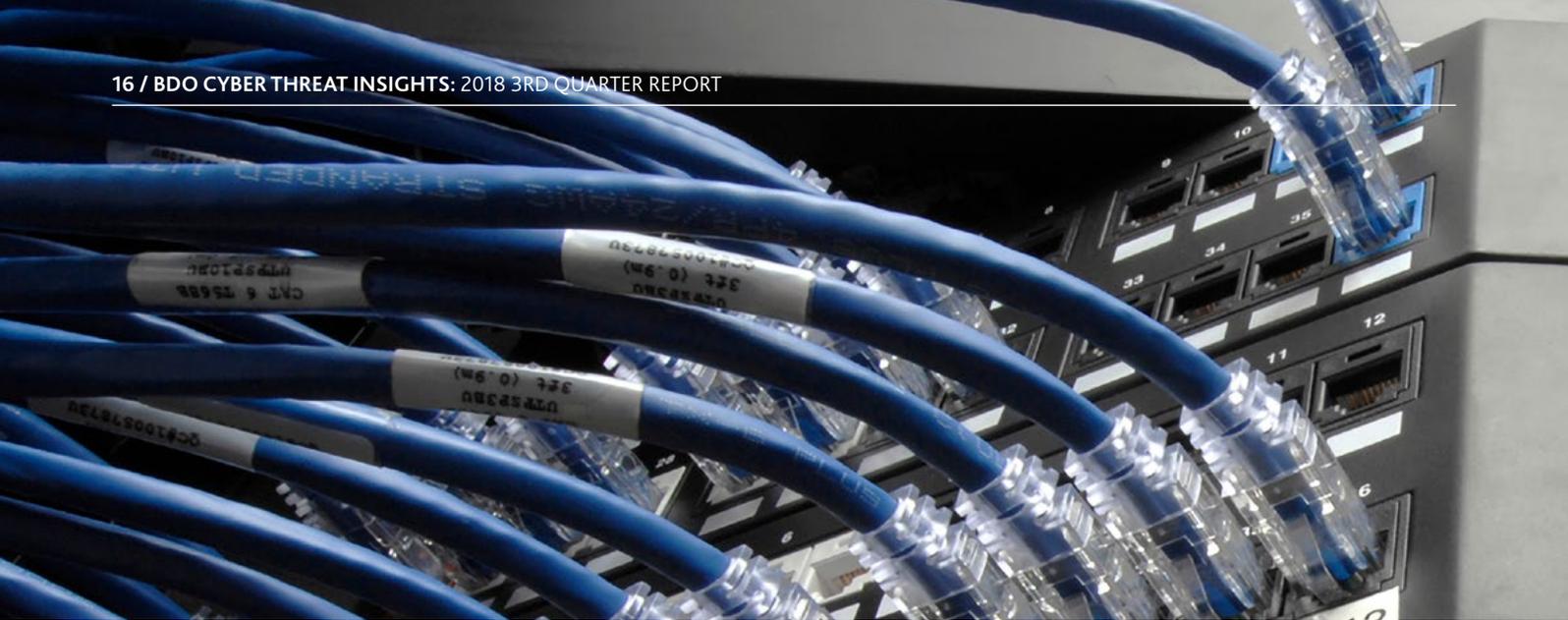
Banks also need to recognize that cybersecurity is an all-hands-on-deck undertaking. The CIO could be leading the charge, but the full C-suite and board has an integral role in protecting the institution's security.

The CFO, in particular, has a critical role to play. As steward of the bank's finances, CFOs should be directly engaged in protecting those assets and investing in the means necessary to secure the institution.

Today, when companies conduct a cost-benefit analysis on whether to adopt stronger user-privacy controls or other enhanced security, they often opt to do nothing — as long as the potential fines or remediation costs are in a tolerable range.

The cybersecurity conversation needs to shift away from achieving just a "minimum baseline" to instead striving for "as much as is reasonably possible." While regulations are still actively being shaped, companies and their leadership teams need to let ethics guide them to protect their data assets and customers.





BDO Cybersecurity Services





Cybersecurity Leadership Team



GREGORY GARRETT

Head of U.S. & International Cybersecurity
Tel: +1 703-770-1019
ggarrett@bdo.com
Resident Country: USA



LEON FOUCHE

Partner and National Cybersecurity Lead
Tel: +61 7 3237 5688
leon.fouche@bdo.com.au
Resident Country: Australia



GRAHAM CROOCK

Director, IT Audit, Risk & Cyber Laboratory
Tel: +27826067570 or +27824654539
gcroock@bdo.co.za
Resident Country: South Africa



SANDRA KONINGS

Partner, Cybersecurity Practice Leader
Tel: +31 (0) 6 5150 8151
sandra.konings@bdo.nl
Resident Country: Netherlands



JASON GOTTSCHALK

Partner, Cybersecurity Practice Leader
Tel: +44 (0)79 7659 7979
jason.gottschalk@bdo.co.uk
Resident Country: UK



ANDREAS VOGT, PH.D.

Partner, Head of Section BDO Security & Emergency Services
Tel: +47 48171714
andreas.vogt@bdo.no
Resident Country: Norway



STEPHAN HALDER

Senior Manager, Forensic, Risk and Compliance
Tel: +49 40 30293 169
stephan.halder@bdo.de
Resident Country: Germany



OPHIR ZILBIGER, CISSP, CRISC

Partner, Head of Cybersecurity Centre
Tel: +972-52-6755544
OphirZ@bdo.co.il
Resident Country: Israel

People who know Cybersecurity, know BDO.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 73,800 people working out of 1,500 offices across 162 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2018 BDO USA, LLP. All rights reserved.