AN OFFERING FROM BDO'S CYBERSECURITY PRACTICE

BDO CYBER THREAT INSIGHTS

2018 1st Quarter Report

BDO

In this issue

Executive Summary

PROMINENT ATTACK VECTORS

Malicious E-mails

These emails contain a malicious attachment, such as a PDF or spreadsheet document. In order to bypass security and email filtration systems, malicious actors have started incorporating social engineering techniques into their attacks. For example, the Russian cybercrime group Carbanak has been known to contact businesses by phone and try to convince the representatives, under various pretenses, to open malicious attachments, thus ensuring their targets are compromised.

Phishing

Spear phishing emails or generic "scattershot" phishing emails are used in a variety of attacks as a means of obtaining sensitive information about their targets' organizational systems.

Exploitation of supply chains

This involves breaching a third-party service provider in order to execute an attack on a company which uses those services or products. Often these attacks are executed in conjunction with the exploitation of vulnerabilities in operating systems (OS) and communication protocols.

HIGH-IMPACT MODES OF ATTACK

Ransomware

Ransomware attacks are becoming increasingly sophisticated and widespread, and can lead to disruption of operation, the shutdown of critical services, and millions of dollars stolen.

Cryptocurrency heists

These heists involve the theft of cryptocoins from cryptocurrency exchange markets, companies, and ICOs (Initial Coin Offerings).

Cryptojacking

Cryptojacking is the malicious mining of cryptocurrency by breaching systems and siphoning computing power.

OVERVIEW OF SIGNIFICANT ATTACKS

1. Ransomware attacks

There is little concrete data regarding the overarching scale of ransomware payment for Q1 2018, however, in our estimation since the beginning of the year it has already surpassed US$1 billion dollars.

One of the most compounding problems in this regard is that ransomware attacks remain grossly under-reported. As many companies and organizations fear loss of clients' and/or investors' trust, victims often opt to pay the ransom as a means to promptly resolve the situation, or otherwise prefer to absorb the financial loss while trying to restore their systems from backups.

Due to the potential loss of life from an attack, a quick resolution is especially pertinent to critical infrastructure and healthcare providers. Accordingly these sectors have become two of the most notable targets for such attacks.

2. Cryptocoin heists and cryptojacking

In the first quarter we have seen an increase in attacks involving the theft of millions in various cryptocoins.

As cryptocurrencies are gaining mainstream momentum, individuals and companies recognizing their potential have amassed considerable amounts of money. This has also attracted the attention of criminal actors, resulting in ever more daring cryptocurrency attacks. For example, in February 2018, a cryptocurrency miner was reportedly detected for the first time on an Industrial Control System (ICS). In addition, there have been numerous attempts to conduct cryptocoin heists this year, some of them successful.

3.ATM jackpotting

In January 2018, a sophisticated attack dubbed "jackpotting", which causes Automated Teller Machines (ATM) machines to dispense all of their cash, hit the US. Jackpotting originated in Russia, spread to other countries in Europe and Asia, and has recently come to the US, targeting machines from various ATM manufacturers such as NCR Corp. and Diebold Nixdorf.

Read more ▶

4. Cybercriminals targeting SWIFT banking systems

Cybercrime targeting financial institutions has significantly increased in recent years, namely on the SWIFT system, used by banks worldwide to send and receive transactional data in a standardized manner. This has become a profitable target of various threat actors.

On January 10, 2018, the year's first attack on the SWIFT system was reported by Mexican state-owned bank "Bancomext". One hundred million dollars were reportedly stolen in this incident, and the bank's payment system was damaged. After analyzing various characteristics of the attack, we assessed that a Russian criminal group might be behind the attack against the Mexican bank, as well as a campaign against financial institutions in Latin American countries.

5. Amplified DDoS attacks

In late February and early March, two massive Distributed Denial of Service (DDoS) attacks of 1.3Tbps and 1.7Tbps, were executed against the code-sharing platform GitHub and an unnamed US based ISP, respectively. These attacks are noteworthy for their attack vector; rather than the more commonplace tactic of using botnets, the attackers exploited vulnerable Memcached servers. Moreover, this method amplified the magnitude of DDoS attacks by a factor of 51,000.

While unprecedented in scale, both attacks were mitigated swiftly with little to no damage. This is a result of implementation of robust DDoS protection measures and the prompt response of cyber protection service providers such as Akamai, as in the case of GitHub.

In these incidents the attacks were successfully mitigated; however it should be noted that other companies and organizations might not leave DDoS attacks unscathed, and could lose a significant amount of money as a result.

6. APT attack hits German government networks

On March 28, 2018, the German government confirmed it had been the target of a large-scale cyber-attack which compromised the computer networks of Germany's Foreign and Defense Ministries. The attack was treated as an ongoing threat against the government's systems, and was reportedly detected in December 2017. There has been no official confirmation of the attacker's identity, however it is believed that the attack was carried out by a Russian threat agent, namely APT28 group (Fancy Bear) or Snake (Turla).

7. Attacks Leveraging Adobe Zero-Day Vulnerability

On January 31, 2018, South Korea's Computer Emergency Response Team (CERT) issued an alert about a newly discovered Adobe Flash Player Zero-Day vulnerability. South Korean security firm HAURI reported that since mid-November 2017, North Korea had been using this vulnerability against various South Korean researchers. In this campaign, attackers used malicious documents or spreadsheets embedded with an SWF file. Upon being opened by the target, a payload would be downloaded from compromised third-party websites hosted in South Korea.

This attack was likely executed by a North Korean threat agent dubbed TEMP.Reaper (Group 123), which primarily targets South Korean entities across various sectors such as government, military, and industrial-defense. During the past year, this actor has expanded its activities to other international targets.

8. Olympic Destroyer

On the eve of the opening ceremony, a series of destructive cyber-attacks led to disruptions in the computer infrastructure of the Pyeongchang Olympic Games, which took place in South Korea between February 9 and February 25, 2018. The attack compromised and temporarily paralyzed various systems (several of which were not reported), such as the stadiums' WiFi networks and broadcasting.

A malware dubbed "Olympic Destroyer" by Talos researchers was likely used in the attack. The attack and infection vectors were most likely via the supply chain - penetrating Atos, the key IT vendor of the Olympics. The identity of the attacker remains unknown. Various security experts have attributed the attack to Russia, North Korea, and/or China.

9. Spectre & Meltdown - vulnerabilities in systems with microchips from major manufacturers

An underlying Central Processing Unit (CPU) architecture design vulnerability has left systems with AMD, Intel and Arm microchips exposed to potential cyber-attacks. We have not seen any indications of this vulnerability being exploited to date. However, it is still possible that, in the future, we could see attacks taking advantage of this. As this is a hardware vulnerability, the solution requires massive organization-wide computer system updates.

In this section, we provide step-by-step recommendations for mitigating potential attacks.

Read more ▶

Recommendations for mitigating vulnerabilities

1. Reallocate additional resources for inter-organizational security systems. With recent developments in hybrid attack vectors, the outer security shell can no longer be prioritized over the internal security framework. Accordingly, organizations and companies must transition to a more holistic security model that can effectively cope with the accelerated evolution of attack methods that we have witnessed over the last couple of years.

2. Segment networks and take core systems offline.

3. Create an emergency backup system that could allow a company to operate up to three months after being hit by a destructive cyber-attack.

4. Minimize the amount of time between when the security patches are released, and when they are installed. Determine how to rapidly implement a policy to install security patches, despite the potential risk of disruption to an organization's normal operations. It is advisable to define a timeframe which is both realistic and agreed upon by the relevant parties within the organization.

5. Raise employees' awareness of new attack vectors - most notably about social engineering techniques and significant campaigns.

6. Perform periodic security testing of cloud-based systems.

7. Implement scanning services on cloud-based applications to alert of any security breaches.

8. Save backups and sensitive information (passwords, etc.) in an encrypted manner.

Read more ▶

Significant Events and Campaigns

2018'S FIRST REPORTED SWIFT ATTACK - MEXICAN BANK BANCOMEXT

On January 9, 2018, the Mexican state-owned bank "Bancomext" reported that it was temporarily suspending its operations in order to conduct computer system diagnostics. The following day, the bank admitted that it had fallen victim to a cyber-attack impacting its international payment platform, presumably its SWIFT system. According to various sources, one hundred million dollars was stolen in the incident. The bank said the attack shared many similarities with various other attacks carried out across Latin America.

At the time this report is being written, it seems that the SWIFT organization is at a loss regarding how to fully resolve this issue. This is not to say that nothing is being done - SWIFT is currently urging its 12,000 members to implement stricter security protocols. As reported by Bloomberg, by December 2017, 90 percent of the firms said they had complied with new basic security procedures, such as improving password strength and adopting two-factor authentication. However, SWIFT's remaining members who have yet to follow suit may still be vulnerable to hackers and scammers.

Based on these recent events, it stands to reason that most of the lagging members are from less developed countries, among them Mexico and India. To illustrate the extent of the problem, according to several reports, there are over 100 financial institutions connected to SWIFT in India alone, including the country's central bank.

As a result, SWIFT has simultaneously rolled out several new services to assist members with detecting breaches. One of these is a real-time alert system that notifies officials about anomalous payment messages. A second service, scheduled to launch later this year, will monitor off-hour and unusually large transactions. A third service will provide a platform for members to share information on attacks and attempted intrusions.

In order to maintain client confidence, SWIFT may have to implement harsher measures if no substantive changes come from the aforementioned steps. This includes going as far as expelling certain members, a move the organization has refrained from doing thus far. SWIFT's final deadline for the implementation of these mandatory measures is the end of 2018.

SWIFT Malware

No additional information about the threat actor or the malware used was provided as of the writing of this report. Nevertheless, on the same day the attack was reported, TrendMicro published a report regarding a new variant of the wiper malware KillDisk, which was previously used against financial organizations in Latin America. This malware was previously seen in other events such as 2016's BlackEnergy campaign that targeted the Ukrainian energy and financial sectors, and the 2017 WannaCry attack. In our assessment, this report exposes a covert part of the attack against Bancomext.

Meanwhile, Group-IB published its research on the Russian threat actor MoneyTaker, which reviews several of the group's attacks against financial organizations across the world. Group-IB deduced that MoneyTaker is currently developing a malware variant for SWIFT, intended for use against Latin American banks.

Various characteristics of the event (attack vector, malware features, etc.), further reinforce our assessment that a Russian criminal actor was behind the attack against the Mexican bank and additional organizations in Latin America.

Malware Vector Stages

1. **First stage:** the malware is extracted from a different malware that presumably executes several other actions. The extraction path is hardcoded in the malware.
2. **Second stage:** the name of the malware is modified (note that this is somewhat irregular, as this file is usually deleted).
3. **Third stage:** the malware scans any drive that contains a system file.
4. **Fourth stage:** the malware attempts to wipe the relevant hard drives and modify MBR (Master Boot Record) values.
5. **Fifth stage:** after a predetermined period of time (usually 15 minutes), the compromised machine is rebooted.
6. **Final stage:** after vital system files are corrupted or wiped, the machine is unable to reboot and disabled.

Read more ▶

RANSOMWARE ATTACKS

We currently do not have concrete data regarding the overall scale of ransomware payments for Q1 2018. However, in our estimation since the beginning of the year, it has surpassed $1 billion.

One of the most compounding problems in this regard is that ransomware attacks remain grossly under-reported. As many companies and organizations fear the loss of clients' and/or investors' trust, victims often opt to pay the ransom as a means to promptly resolve the situation, or otherwise prefer to absorb the financial loss while trying to restore their systems from backups.

Due to the potential loss of life as a result of an attack, a quick resolution is especially important for healthcare providers. Accordingly, they have become one of the most notable targets for such attacks. Below is a review of several, recent noteworthy ransomware attacks reported.

Hancock Health Hospital Hit with Ransomware Attack Forcing Doctors to Use Pen and Paper, Pays $55K to Recover Data

On January 11, 2018, the computer systems of the Indiana-based Hancock Health Hospital were infected with ransomware, resulting in the shutdown of multiple critical systems. The hospital chose to pay the ransom of 4 Bitcoins, valued at $55,000 at the time of the attack, after assessing that the process of recovering their systems would take too long, spanning multiple days or perhaps even weeks.

The ransomware used in this incident was SamSam, a variant of SAMAS which was first seen in late 2015 when it was used against healthcare organizations and hospitals. In 2018 alone, the ransomware was used against several large companies and organizations in the US, including Adams Memorial Hospital, the municipality of Farmington, New Mexico, cloud-based electronic health records provider Allscripts, and according to Bleeping Computer, an unnamed ICS (Industrial Control System).

As reported by Healthcare-Informatics, Hancock is working together with US law enforcement to gain further insight into the incident. While the identity of the attackers remains unclear, investigators believe that it was executed by a sophisticated Eastern European criminal actor.

In the recent wave of SamSam attacks, the threat agents instructed their victims to transfer the ransom money to the following digital wallet - **1MddNhqRCJe825ywjdbjbAQpstWBpKHmFR** - and then report the transfer via the following address: **jcmi5n4c3mvgtyt5.onion/familiarisingly**.

An examination of the wallet's transactions revealed that it had so far registered 30.4 Bitcoins, and that the latest transaction of 4 Bitcoins appeared to have been carried out on January 19. In many SamSam attacks, the actors propagate the malware by scanning the internet for systems with open Remote Desktop Protocol (RDP) connections, and deploying it after breaching the targeted system via brute force attacks.

However, it appears that in this case, the penetration vector was different – the attackers logged in to the hospital's remote backup server, and then pivoted to other more central servers, where they encrypted critical files.

Read more ▶

SamSam Ransomware Strikes Colorado Department of Transportation

In February 2018, the Colorado Department of Transportation (CDOT) shut down more than 2,000 of its computers which were running on Windows OS and equipped with McAfee security software after the department was hit by a variant of the SamSam ransomware. While the malware locked down the affected computers, it did not successfully steal any data.

The attacking actor demanded payment in Bitcoin. The CDOT refused to comply with the demands, and remained offline while its computers were compromised. The state's Office of Information Technology notified law enforcement and reached out to the FBI for assistance. In addition, McAfee provided a patch to mitigate the attack and prevent further damage to any hijacked files.

Ransomware Attack Targets Two Ontario Children's Aid Societies

Two Canadian aid agencies in Ontario were recently a target of ransomware attacks demanding payment for regaining access to their servers.

The attacker demanded a $60,000 ransom from the Family and Children's Services of Lanark, Leeds, and Grenville after it encrypted most of the agency's servers. The agency claimed that no data was taken out of the system, and that they did not comply with the attacker's demands. Instead, the agency used offline backups of the affected files until cybersecurity officials from the Ministry of Children and Youth Services and a private security firm neutralized the malware. The agency was apparently compromised as it was uploading its data to a centralized database of similar agencies across the Canadian province, although this remains solely a hypothesis.

The second agency, the Children's Aid Society of Oxford County, paid its attackers a $5,000 ransom after malware infected its local servers, blocking access to sensitive data. No additional information was reported on the incident, however the agency confirmed that no data was stolen.

Canadian Engineering Firm Pays $1,300 After Ransomware Encrypts Servers

In January 2018, Canadian engineering firm DGH Engineering paid $1,300 in Bitcoin after a ransomware attack encrypted its servers along with its data backup system, which contained sensitive commercial information and employee payroll details. The infection vector consisted of an email containing a malicious link sent to an employee at the firm.

The attack resulted in a four-day shutdown of the company's servers. Officials at the firm, fearing for their assets, ultimately gave in to the attackers after negotiating the ransom demand down from $20,000. The ransomware variant that affected the organization is unknown.

Ransomware Attack On a Local US Newspaper Compromises California Voter Records

In late January 2018, two databases of the California daily newspaper The Sacramento Bee, stored on a third-party server, were targeted by anonymous attackers demanding payment in Bitcoin. The databases contained records of 19.5 million California voters and contact information of 53,000 current and former Bee subscribers. The newspaper had obtained the voter registration database from the California Secretary of State for reporting purposes.

The paper refused to pay the demanded ransom, and has since deleted the compromised databases. The newspaper discovered the breach when a developer noticed that a database did not upload correctly.

The developer then found the attacker's ransom note. The Bee's databases were compromised one month prior to the attack, when its firewall did not come back online after routine maintenance was performed on the server, leaving it exposed for about two weeks. The newspaper said it took immediate steps to bolster its security.

SOURCES AND FURTHER READINGS REFERENCES

FBI: Victims aren't reporting ransomware attacks

SamSam ransomware hits US hospital, management pays $55K ransom

SamSam ransomware attacks hit healthcare firms

Hospital pays $55K ransomware demand despite having backups

The cyber-attack – from the POV of the CEO

SamSam virus demands bitcoin from CDOT, state shuts down 2,000 computers

Ransomware attacks hit two Ontario children's aid societies

Engineering firm pays $1.3K after ransomware affects servers, backups

Ransomware attack on Sacramento Bee database exposes voter records of 19.5M Californians

Read more ▶

FIRST JACKPOTTING ATM ATTACKS IN THE US

In January, a sophisticated attack dubbed "jackpotting", which causes ATM machines to dispense all of their cash, hit the US. Jackpotting originated in Russia several years ago, has spread to additional countries in Europe and Asia, and recently the US, targeting machines from various ATM manufacturers such as NCR Corp. and Diebold Nixdorf.

The Malware

In the latest attacks, the attackers use Ploutus.D. This is a variant of Ploutus, which was first detected back in 2013, when it was used in Mexico. The malware was developed with.net, and can run either as a Windows Service or as a separate program.

Ploutus interacts with the Kalignite multivendor ATM platform, developed by the ATM software vendor KAL.

Samples from the recent attack indicate that Ploutus targets Opteva 500 and 700 series ATM machines, manufactured by Diebold Nixdorf. However, with minor changes to the code, it could easily be modified to be compatible with ATM machines from other vendors, as about 40 manufacturers use the Kalignite multivendor platform.

Attack Vector

To deploy the malware, attackers require physical access to the ATM's internal computer. Often in these type of attacks, the attackers approach stand-alone machines (for example, machines located in pharmacies, large retailer shops, drive-thru banks, etc.), and either pick the machine locks, use a stolen master key, or destroy parts of the machine to gain access to its internal computer. Moreover, attackers may impersonate ATM maintenance professionals in order to lower suspicion of their actions.

After gaining access, the attackers connect a laptop and upload a mirror image of the ATM's OS which contains the malware.

Once completed the compromised machine will appear out of service to any potential customer.

At this point, the attackers can remotely control the machine and issue a command to dispense cash, which is picked up by money mules. Once the command is issued, the machine will empty all of its cash within several minutes unless the attacker presses cancel on the keypad.

According to a 2017 analysis of Ploutus.D by FireEye, this malware is one of the most advanced ATM malwares identified in recent years. The Secret Service has stated in an alert that Windows XP based ATM machines are notably vulnerable, and recommended promptly updating them to Windows 7 or later versions of the OS.

New Lazarus Attack Detected Against Mexico

On January 8, 2018, the Mexican government reported that it detected activity of a malware called FallChill. This malware is attributed to the North Korean threat agent Lazarus (HiddenCobra). It was identified by the Mexican Attorney General's Office, through the Criminal Investigation Agency (AIC), in collaboration with the FBI.

It should be noted that while the attacked organization was not named, it was described as a private telecommunications company located in Mexico City. FallChill was first detected in 2016, and was used against aerospace, communications, and financial organizations.

FallChill is a RAT (Remote Administration Tool), which enables the attackers to issue multiple commands from a command and control server to compromised systems via dual proxies. FallChill typically propagates either via a file dropped by other HIDDEN COBRA malware, or via hacked websites that covertly infect visiting users. Data gathered from the infected machine, such as OS info, IP and MAC address, is encoded with RC4 encryption and sent to the command and control server.

SOURCES AND FURTHER READINGS REFERENCES

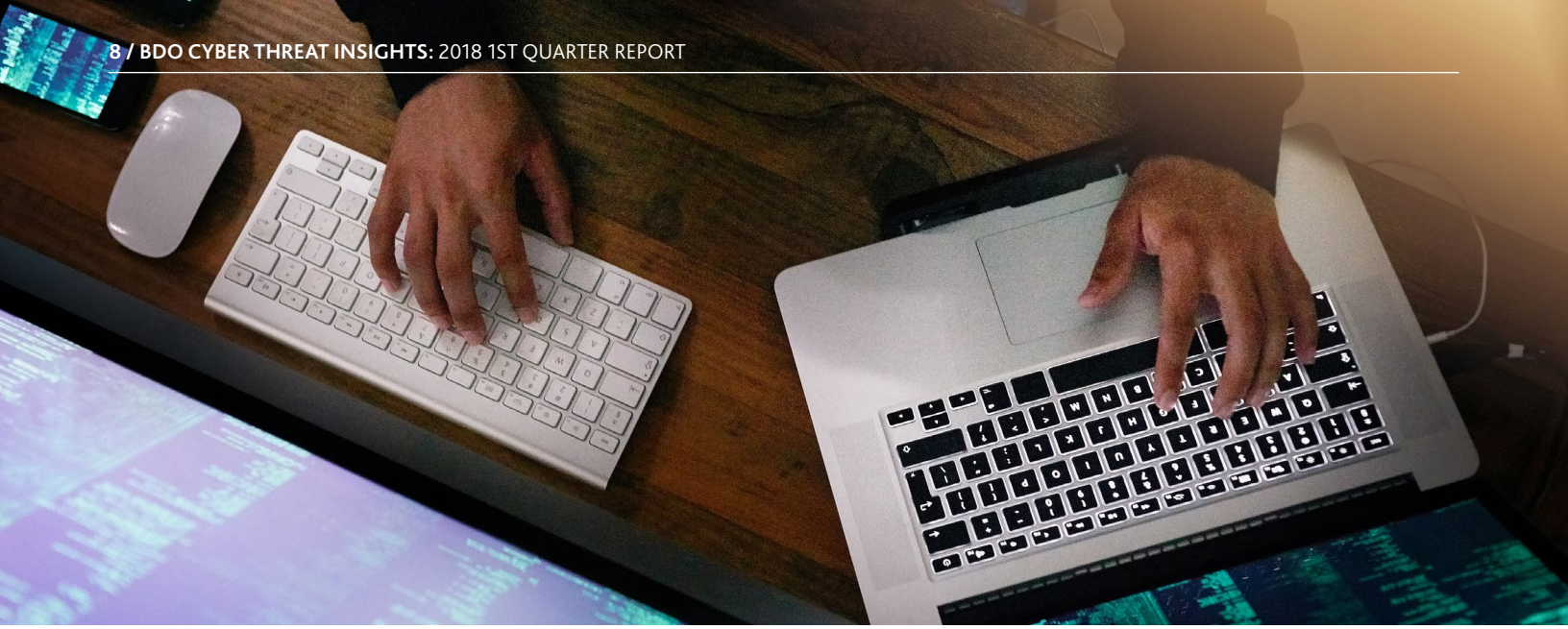
[First 'Jackpotting' Attacks Hit U.S. ATMs]

[Secret Service warning: Jackpotting ATM attacks reach the US]

[KAL ATM Software]

[PGR, en colaboración con FBI, identifica y erradica software malicioso]

Read more ▶



WALMART VENDOR DATABASE LEAK

In February 2018, Kromtech Security researchers discovered a database containing the details of 1.3 million individuals in the US and Canada which became publicly accessible following a cloud configuration error on Amazon's S3 bucket. At first it appeared to be a database belonging to Walmart jewelry, since the storage bucket was named 'walmartsql'. However upon further inspection, it was revealed that the database belonged to MBM Company Inc., a Chicago based jewelry company, which operates under the name Limogés Jewelry and is also a Walmart vendor.

The database backup was named **MBMWEB_backup_2018_01_13_003008_2864410.bak**, which indicates it had been available since January 13, 2018. The database included email addresses, encrypted credit card details, payment information, order details, and even passwords stored in plain text. The records were dated from 2000 to 2018. There is currently no evidence that malicious entities accessed the database.

- It should be noted that the cloud's data security is not solely the responsibility of Amazon, but also that of the customer. There have been numerous cases in which a configuration error on the part of the customer has resulted in security breaches.
- According to a report by Threat Stack, nearly three quarters of organizations commit Amazon Web Services (AWS) configuration errors.
- Another recent research report, done by French cybersecurity company HTTPCS, has found that 5.8% of all Amazon S3 buckets are publicly readable, and 2% are publicly writable, allowing anyone to modify, corrupt, or hold the data for ransom.
- In addition, firms using AWS must be aware of information stored with third-party companies, whose security may constitute a weak link in the supply chain.

SOURCES AND FURTHER READINGS REFERENCES

[MSSQL database containing the personal information of approximately 1.3 million people found in another public Amazon S3 Bucket]

[Verizon data found on open AWS S3 server]

[National Credit Federation unsecured AWS S3 bucket leaks credit, personal data]

[Impact Study – Amazon S3 AWS buckets configuration]

[Open AWS S3 bucket exposes sensitive Experian and census info on 123 million U.S. households]

[Open AWS S3 bucket exposes private info on thousands of FedEx customers]

[Open AWS S3 bucket managed by Walmart jewelry partner exposes info on 1.3M customers]

Read more ▶

OLYMPIC DESTROYER – DESTRUCTIVE MALWARE ATTACK IN SOUTH KOREA TARGETING THE 2018 WINTER OLYMPICS

The Pyeongchang Winter Olympics took place in South Korea between February 9 and February 25, 2018. Prior to the opening ceremony, there had been numerous concerns regarding potential cyber-attacks amid tensions between South Korea and its neighbor to the north.

In addition, there were concerns regarding a possible retaliatory attack by Russian entities after the Russian delegation was suspended due to doping allegations.

At the eve of the opening ceremony, a series of destructive cyber-attacks led to disruptions in the computer infrastructure of the Pyeongchang games that compromised and temporarily paralyzed various systems (several of those were not reported), such as the stadiums' WiFi networks and broadcasting stations.

Furthermore, shortly before the ceremony began, the official Winter Olympics website went down for several hours, disrupting ticket sales, downloads, and online visitor services.

On February 11, 2018, Olympic officials announced that these malfunctions were a result of a cyber-attack, but no further information concerning the attack vector or identity of the actor(s) was revealed. Nevertheless, Cisco Systems' Talos research team identified malware it called the Olympic Destroyer, which was likely used in the attack.

Several characteristics of the malware were previously seen in the NotPetya and Bad Rabbit attacks, which were most likely conducted by Russian threat agents.

Attack Vector and Malware Workflow

According to Talos, the identified malware appears to operate in a solely destructive manner and does not communicate with a command and control server. The attack and infection vectors were most likely carried out via the supply chain - penetrating Atos, the key IT vendor of the Olympics which was previously attacked several months ago.

Below is the Olympic Destroyer's workflow:

After initial infection, two malware variants are dropped onto the victim host, which steal usernames and password credentials from the victim's infected browsers and computer systems. Talos researchers have identified 44 account credentials within the binary code of Olympic Destroyer.

The malware uses a legitimate Microsoft tool called PsExec, as well as the Windows Management Instrumentation (WMI) interface, to perform lateral movement within the network. This is carried out while using stolen credentials and infecting other systems.

The malware deletes shadow copy files and backup system logs in order to prevent future information recovery.

The attacker covers its tracks by deleting the System & Security Windows event log, including the recovery console of the infected host.

The malware maps shared network folders and deletes every file it can access and finally shuts down the compromised system, leaving the victim unable to reboot.

SOURCES AND FURTHER READINGS REFERENCES

Atos, IT provider for Winter Olympics, hacked months before Opening Ceremony cyber-attack

Read more ▶

CYBER ATTACK HITS GERMAN GOVERNMENT, COMPROMISING SECURE AND SEGMENTED NETWORK

On March 28, 2018, the German government confirmed it had been the target of a largescale cyber-attack that compromised computer networks of Germany's Foreign and Defense Ministries. The attack was treated as an ongoing threat against the government's systems, a German lawmaker said, despite earlier claims the breach had been an isolated event. There have been several reports claiming the attack was detected in December 2017, and had been ongoing for up to one year.

The attackers reportedly searched for data on specific topics, and rather than steal vast quantities of data, they apparently chose their targets carefully. According to Johannes Dimroth, a spokesman for the German Interior Ministry, German officials had averted any immediate dangers after learning of the cyber-attack. Further, Dimroth stated that the affected network was classified for government use only, but did not contain any highly sensitive information.

Germany's Interior Ministry later claimed that the attack had largely failed, despite the fact that the attackers had been able to infiltrate two federal institutions, they reportedly did not gain access to the federal government's more secure data network.

Currently, there has been no confirmation of the attacker's identity, though German officials blamed Russian actors for the event, namely the APT28 group (Fancy Bear) and more recently Snake (Turla). At the time this report is being written, it is unclear how much and what type of data was compromised; however on March 3, 2018, German politician Armin Schuster told reporters that the attack had caused "considerable damage," and that that the government was attempting to limit the damages.

A report by the Süddeutsche Zeitung newspaper and broadcasters NDR and WDR claimed a small amount of data had been copied, including some related to Russia.

Russian threat agent APT28 was previously accused of targeting the German parliament in 2015, as well as other European governmental institutions, and the US presidential election campaign. The Kremlin officially dismissed allegations it was involved in those incidents, and in the recent attack in Germany.

DUTCH BANKS AND TAX OFFICE HIT BY A SERIES OF DDOS ATTACKS

Between January 27 and January 29, 2018, several Dutch banks and the Netherlands' tax office were hit by a series of DDoS attacks. The attacks ranged in duration from several minutes to several hours, denying users access to the banks' websites and apps.

However, it should be noted that no money was stolen and no sensitive data was compromised.

According to reports it appears that some of the attacks used Zbot, a Windows based Trojan. Dutch security researcher Rickey Gevers reported that the attacks were up to 40Gbps.

According to ESET, most of the traffic originated from Russia. However, the researchers pointed out that this does not necessarily indicate that the attackers were in Russia. Nevertheless, these attacks did take place several days after the Dutch media published a report claiming that Dutch Secret Service (AIVD) were monitoring and investigating the Russian threat agent APT29 (Cozy Bear) – a nation-state group attributed to the Russian government. This group has been linked to numerus cyber-attacks, including the attack on the Democratic Party during the 2016 US election.

SOURCES AND FURTHER READINGS REFERENCES

Germany admits hackers infiltrated federal ministries, Russian group suspected

Cyber-attack on German government largely failed: interior Ministry

Dutch banks and tax office hit by DDoS attacks

Russian servers linked to DDoS attack on Netherlands financial network

Russian hackers suspected in cyber-attack on German Parliament

D.N.C. Says Russian hackers penetrated its files, including dossier on Donald Trump

Kremlin dismisses allegation Russia behind German cyber attack

Read more ▶

INDIAN BANK FRAUDS CARRIED OUT BY EXPLOITING THE SWIFT SYSTEM

In 2018 two events involving the exploitation of the SWIFT banking system were reported in India. The larger case involved the theft of $1.77 billion. Both cases are the latest events in a long series of attacks targeting SWIFT systems in various global banks during the last two years.

As opposed to most attacks on SWIFT, which are executed by breaching the system, the latest fraud at India's state-run Punjab National Bank was carried out by bank officials who issued unauthorized Letters of Undertaking (LOU) and Letters of Credit (LC). The officials took advantage of deficient company regulations and security measures.

First Event - $1.77 Billion Letter of Credit Fraud at Punjab National Bank

According to the Punjab National Bank (PNB), the scam spanned six years, between 2011 and 2017, during which several of the bank's officials as well as its deputy manager issued more than 100 unauthorized Letters of Credit [LCs] to various firms linked to Indian billionaire Nirav Modi and his uncle Mehul Choksi. The letters were used to obtain credits to the sum of $1.77 billion, belonging mostly to Indian lenders abroad.

The detection of the scam led to the implementation of additional controls at PNB. The bank will now only allow senior PNB officials to initiate SWIFT messages and clerks will no longer be authorized to do so. In addition, SWIFT transactions must be authorized by three officials, as opposed to only two. Adding to these measures, PNB announced it is establishing an additional control unit called the "Treasury Division Mumbai," which will supervise all SWIFT requests received and sent by the bank, especially from its own branches. This includes the issuance of LCs and LOUs.

Fraudulent issuance of LCs was first detected in January 2017, after hackers breached the internal networks of three different state-owned Indian banks (two in Mumbai and one in Calcutta). The hackers issued fake LCs to be used in fraudulent international transactions. After the scam was exposed, India's central bank, the Reserve Bank of India, instructed the country's financial institutions to implement additional measures for verifying documents transferred via the SWIFT system and checking them against the originals, which are stored in the core systems of the banks.

Nevertheless, it appears that some Indian banks failed to implement these new measures.

In late February, reports announced that PNB suffered a massive data breach affecting about 10,000 clients. The breach was exposed by the cybersecurity firm CloudSek. At the time this report is being written, the leak is still underway and no information regarding the attack vector has been released. PNB dismissed the reports, and claimed that the breach did not take place.

Second Event - Hackers Breach SWIFT System at City Union Bank

On February 18, 2018, Indian City Union Bank reported that it was the victim of a large-scale cyber-attack. According to the bank's statement, attackers hacked its SWIFT system and transferred $1.8 million in three remittances to accounts in New York and Frankfurt that were linked to entities in Dubai, Turkey, and China. The bank said it had successfully blocked one of the transactions, amounting to $500,000. The modus operandi of the attackers appears to be similar to a large number of previous attacks targeting SWIFT.

SOURCES AND FURTHER READINGS REFERENCES

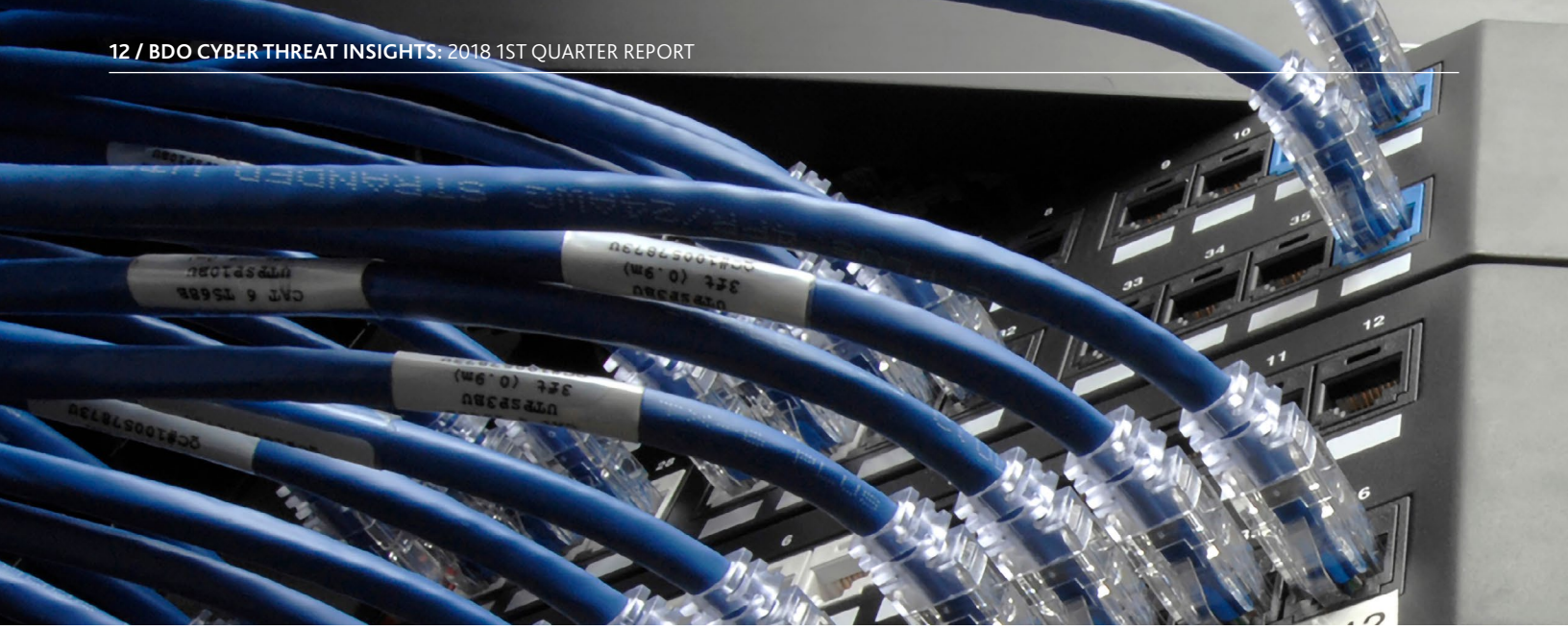
[PNB adopts strict SWIFT controls after mega fraud case]

A Letter of Credit is a document issued by an individual or entity as a guarantee that money for the supplied goods would be paid to the vendor according to the specified conditions. LCs are occasionally issued as a letter to the buyer signed by the bank or as a document sent via SWIFT to the supply vendor's bank. In addition, a beneficiary may redeem an LC to receive a payment for a transaction. LCs are primarily used in international trade, especially in transactions of significant value between two entities based in different countries. It should be noted that the LC provides a one-time guarantee; as soon as it is sent, its conditions are binding.

Please note that reports concerning the event also revealed that a similar attack on the SWIFT systems of three banks in India occurred in June 2016. In one of these cases, the malicious entity carried out a transferred $150 million to a US bank. However, the transaction was blocked by the bank.

For more information please see: "220117 – 2. Hackers Breached Indian Banks' SWIFT system and Issued Fake Letters of Credit (LC)".

Read more ▶



BDO Cybersecurity Services

PAYMENT CARD INDUSTRY (PCI)

- PCI assessment and remediation
- Third-party assessments

INFORMATION GOVERNANCE AND DATA PRIVACY

- Data mapping
- Data privacy assessments
- Data privacy strategy and implementation
- Privacy officer consulting
- Information governance assessments

CYBER INSURANCE

- Cyber insurance claim preparation
- Coverage adequacy evaluation

CYBER RISK ASSESSMENTS

- Level 1- 3 risk assessments against multiple frameworks
- Cyber risk remediation

INCIDENT RESPONSE

- Data breach investigations
- Network/host active threat monitoring
- Threat hunting - exec, enterprise, nation state, insider
- Threat intelligence - deep/dark web, social media analysis
- Training & testing - 1st responder, table top, RED team, simulations
- IR data analytics

CYBERSECURITY STRATEGY, POLICY AND PROGRAM DESIGN

- CIO & CISO advisory services
- Cyber strategy consulting
- Regulatory compliance
- Government relations consulting

CYBER THREAT INTELLIGENCE

- Dark web recon
- Dark web analysis
- Social media

MANAGED SECURITY SERVICES

- Network Operations Center (NOC)
- Security Operations Center (SOC)
- Penetration testing
- Vulnerability assessments
- Cloud migration & security
- Virtual desk-top services
- Cybersecurity education, training, & simulations
- Security Incident & Event Management (SIEM)

Read more ▶

Cybersecurity Leadership Team

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

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

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

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

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

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

ANDREAS VOGT, PH.D.
Director / Head of Section BDO Security & Emergency Services
Tel: +47 48171714
andreas.vogt@bdo.no
Resident Country: Norway

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

Read more ▶

People who know Cybersecurity, know BDO.

MARKUS BRINKMANN

Partner, Forensic, Risk & Compliance
Tel. +49 40 30293 355
markus.brinkmann@bdo.de
Resident Country: Germany

STEPHAN HALDER

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

www.bdo.de