AN OFFERING FROM BDO'S CYBERSECURITY PRACTICE

CYBER THREAT INSIGHTS

Spring 2020 Report

SPECIAL FOCUS:
FINANCIAL SERVICES INDUSTRY

BDO

In this issue

Preface

With the rapid spread of the novel coronavirus (COVID-19) worldwide during the past few months, more than ever, people are working remotely or exercising "social distancing." As a result of an increase in telecommuting via computers, mobile devices, and virtual interactions, cybercrimes conducted by nation-state cyber-attack groups, organized criminal cyber-attack groups and hacktivists have rapidly increased in both the number and the level of sophistication of socially engineered cyber-attacks. While financial services organizations tend to have more resources to combat cybercrime than other industries, cyber-attack groups have considerable motivation to target these organizations because of the potential for high payouts. Ultimately, all financial services organizations are vulnerable to cyber-attacks, which could result in significant cyber fraud and/or major data breaches.

That's why the *Spring 2020 BDO Cyber Threat Insights Report* focuses on the global financial services industry, with a close examination of recent cyber-attacks against banks, credit cards, automated teller machines (ATMs), financial technology applications, and cryptocurrencies.

One of the key trends we have observed in the past year is the uptick in attacks on ATMs[1] [2] [3] and point-of-sale stations[4] [5], sometimes breaching the bank's clearance systems and sometimes just "flooding" it with credit card numbers and PINs via a brute-force attack. The past year also saw some of the biggest credit card leaks in history, such as the recent databases[6] [7] sold on the "Joker's Stash" market.

Another notable trend is the decrease of cyber-attacks involving the SWIFT financial transactions systems, as well as the increase of cyber-attacks on cryptocurrency transactions. Cyber-attacks that target cryptocurrencies are often attributed to North Korean threat actors, which security researchers say represents a shift in tactics. The financial services industry has exposure to many other types of cyber threats, with organizations targeted by ransomware and attacks aimed at the supply chain.

Our BDO Cybersecurity Advisory Services team currently operate in 35 countries on six continents, with four BDO Global Security Operation Centers running on a 24/7/365 basis. We support a wide range of clients in both the public and private sectors, including an extensive portfolio of financial services firms. Unfortunately, we have seen first-hand a rise of sophisticated cyber threats across the global financial services industry, including socially engineered spear-phishing, impersonation cyber-attacks, business email compromise (BEC), ransomware with advanced encryption, supply chain cyber-attacks, and increasing insider threats. Financial services organizations must understand this wide array of cyber-attacks, as well as the recent trends, in order to implement a threat-based cybersecurity program that protects key vulnerabilities.

Respectfully,

GREGORY A. GARRETT, CISSP, CPCM, PMP
Head of U.S. & International
Cybersecurity Advisory Services

1 vice.com/en_us/article/7x5ddg/malware-that-spits-cash-out-of-atms-has-spread-across-the-world

2 github.com/fboldewin/Libertad-y-gloria---A-Mexican-cyber-heist-story---CyberCrimeCon19-Singapore/blob/master/Libertad%20y%20gloria%20-%20A%20Mexican%20cyber%20heist%20story%20-%20CyberCrimeCon19%20Singapore.pdf

3 securelist.com/my-name-is-dtrack/93338/

4 click.broadcasts.visa.com/xfm/?30761/0/0624013ddc6f39785bf56d504f3b812e/lonew

5 scmagazine.com/home/security-news/malware/new-glitchpos-credit-card-stealer-malware-found-for-sale/

6 zdnet.com/article/details-for-1-3-million-indian-payment-cards-put-up-for-sale-on-jokers-stash/

7 dnet.com/article/455000-turkish-card-details-put-up-for-sale-web-skimmers-suspected/

Cyber Criminals Take Advantage Amid COVID-19 Pandemic

Global businesses have seen a sharp rise in cyber-attacks since the Chinese government disclosed the spread of the novel coronavirus (COVID-19) within China and internationally. Some of the cyber-attacks includes: attacks focused on health-care systems using spear-phishing and ransomware, impersonation attacks combined with business email compromise (BEC) targeting financial systems, supply-chain cyber-attacks focused on re-directed manufacturing operations outside of China, and distributed denial of service (DDoS) cyber-attacks on the energy, hospitality, and travel industries.

With the spread of COVID-19, increased demands for information technology (IT) support services are occurring across nearly all industries, as worldwide employees, students, university faculty, and others are being asked or required to work or study remotely from their homes to reduce the spread of the virus. As a result, nation-state cyber-attack groups and criminal cyber-attack groups are taking maximum advantage to target cyber vulnerabilities in select industries, especially those most impacted by the current crisis.

Realizing that 40% or more of cyber vulnerabilities are directly linked to employee behavior, per Gartner's latest studies, it is vital that organizations focus more on their employees via cybersecurity awareness, education, training, and use of simulations to create a stronger human firewall to protect their vital digital assets. After all, according to IBM Security's latest findings, the average cost of a cyber data breach is now $8.2 million.

TOP FIVE CYBERSECURITY RECOMMENDATIONS

To reduce both the probability of a cyber-attack or a significant data breach and mitigate the negative financial and reputational impacts, we offer the following cybersecurity recommendations which are applicable to all industries:

1. **Create an organizational culture of cybersecurity**
   Ensure the C-Suite consistently promotes and supports all employees practicing effective cybersecurity policies, processes, and procedures via a comprehensive cybersecurity awareness, education, and training program including spear-phishing campaigns and cyber data breach table-top exercises.

2. **Implement advanced cyber diagnostic assessments, on a regular basis, including:**
   - Email Cyber-Attack Assessments
   - Network & Endpoint Cyber-Attack Assessments
   - Vulnerability Scanning Assessments
   - Penetration Testing
   - Spear-Phishing Campaigns

3. **Establish a rapid cyber-attack incident response plan**
   Develop and periodically test an enterprise-wide well-coordinated information system incident response plan to quickly identify, contain, eradicate and recover from cyber-attacks.

4. **Conduct 24/7/365 monitoring, detection, and response (MDR)**
   It is essential to continually monitor, detect, and respond to all cyber incidents including: email system, network, software applications, and all information system endpoints using advanced security information event management (SIEM) software, data visualization tools, automation, and artificial intelligence (AI) capabilities.

5. **Ensure information system resilience**
   Implement and periodically test an enterprise-wide business continuity plan (BCP) and disaster recovery plan (DRP).

Prominent Cyber Threats to the Global Financial Services Industry

1. RANSOMWARE CYBER-ATTACKS INCREASE

Over the past year, ransomware attacks have proved to be an increasing concern in the global cyber threat landscape. Ransomware initially targeted endpoint users, encrypting laptops unexpectedly and demanding a ransom to be paid in bitcoin. Once routine backup procedures became a common practice, cyber-attackers shifted focus to target large enterprises. Threat actors carefully study their target's networks and flaws for months to find the right penetration vector, and then infect the entire company's network. We have also seen a growing use of supply-chain attacks, in which threat actors use an information technology (IT) service provider's network to gain access to their customers' networks.

Throughout 2019 and into 2020, cyber-attackers increased their focus on government-related entities. Ransomware distributors have heavily targeted local municipalities to shut down critical services for days and sometimes weeks or months. Other public institutions, such as hospitals, as well as national government agencies, have also been attacked on an increasing basis. But the ransomware attack that paralyzed foreign exchange company Travelex at the start of 2020 (described in detail below) has made the financial services industry acutely aware of the potentially devastating consequences.

In May 2019, the city of Baltimore, Maryland, fell victim to an attack using the 'RobbinHood' ransomware. Thousands of computers were crippled, and the city chose not to pay the requested ransom, opting instead to restore from backups. Consequently, the cost of restoring affected systems exceeded $18 million. In October, the South African city of Johannesburg admitted that its systems and servers were hacked and encrypted, which followed a July ransomware attack on its electricity provider. A group dubbed 'Shadow Kill Hackers' claimed responsibility for the October attack and demanded a ransom of four bitcoins (approximately $30,000), which the city refused to pay. That case involved another trend that has become increasingly common – ransomware operators threatening to release sensitive data in cases of non-payment. Victims of groups like Maze and Sodinokibi[8] have also had to contend with such ransomware threats.

Cyber-attackers' choice to focus on public entities rather than private enterprises indicates a shrewd understanding of the political landscape – state organizations are gradually shifting all their services to the internet, including digital payments, but they may not have mature cybersecurity measures in place. Freezing municipal operations via ransomware can cause damage to tens of thousands of citizens with no warning and lead to severe losses for the municipality, which need to provide vital services nonetheless. But financial services organizations remain a lucrative target for threat actors, and the Travelex case proves that large companies are vulnerable to ransomware attacks as well.

8 krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/

2. TARGETED SPEAR-PHISHING CYBER-ATTACKS EXPAND

Almost everyone knows what a typical phishing attack looks like – it features a strange email address with misspelled text and an uncommon top-level domain such as '.xyz' or '.top.' Its content is general, lacks context, and includes references to a purchase invoice, a candidate's CV, or a certain business-related file. For example, in 2019, a new wave of malspam emails distributing the Remcos RAT (a remote access tool with evasive anti-debugging techniques that make it hard to detect) was uncovered. The malware was spread through an encrypted text file, disguised as a resume file. These are still widely observed, and phishing is still the leading cyber-attack vector in corporate networks.

However, many phishing attacks nowadays are far more sophisticated. First, cyber-attackers use a trusted company domain email address by address spoofing or, as seen more recently, by hacking an employee account. Second, the message content is specifically tailored to the targeted person and company, referencing a relevant customer or product and using the same graphics and company details. It seems that cyber-attackers have learned that the key to a successful phishing attack is learning the target organization's language or copying messaging from the target's previous communications to conceal a lack of fluency.

There are two key elements in the increasing sophistication of phishing emails:

1. **Extensive Preparations**
   In the case of enterprise attacks, cybercriminals are investing efforts in reconnaissance work. They investigate the intended victim's network using online resources, research the company, and can even attempt to hack a key employee to target the company's vital resources.
2. **Advanced Concealment Methods**
   Steganography (concealing malicious information within another file), fake malicious fonts, and other advanced techniques are now used to trick recipients into thinking the designated email is not harmful, and its links and attachments are safe. These lead to the creation of well-designed emails identical to those of the organization they pretend to be affiliated with.

   For example, Proofpoint researchers discovered[9] a phishing kit that uses concealment methods and unique encoding to steal information from customers of a well-known bank. First, the users are directed to a landing page disguised as the bank's portal, and login info is requested. Only two fonts were loaded to the font kit, as the fonts directory was missing. In the next stage, the malicious landing page creates a font file personally customized to make the browser process the encrypted text as open text.

Attack infrastructure management has also evolved. Cyber-attackers have developed a technique to ensure operations continue even in case of exposure. By maintaining two attack infrastructures (e.g., servers, domains, malware samples, etc.), if one is exposed, then they can swiftly move to the other infrastructure while re-building the first.

One example is a group known as "Smart Kangaroo" that uses a combination of well-crafted phishing and direct interaction with the target. The group creates a fake website simulating one used by the target and sends them SMS messages linking to the website, enticing them to give away a legitimate verification code from their bank. Then the group either withdraws money from the phished account right away or gains the status of a trusted device on the victim's account, thus not needing any further interaction with them to steal money. Sometimes, the group even calls the target and pretends to be the bank to guide them through the process.

9 proofpoint.com/us/threat-insight/post/phishing-template-uses-fake-fonts-decode-content-and-evade-detection

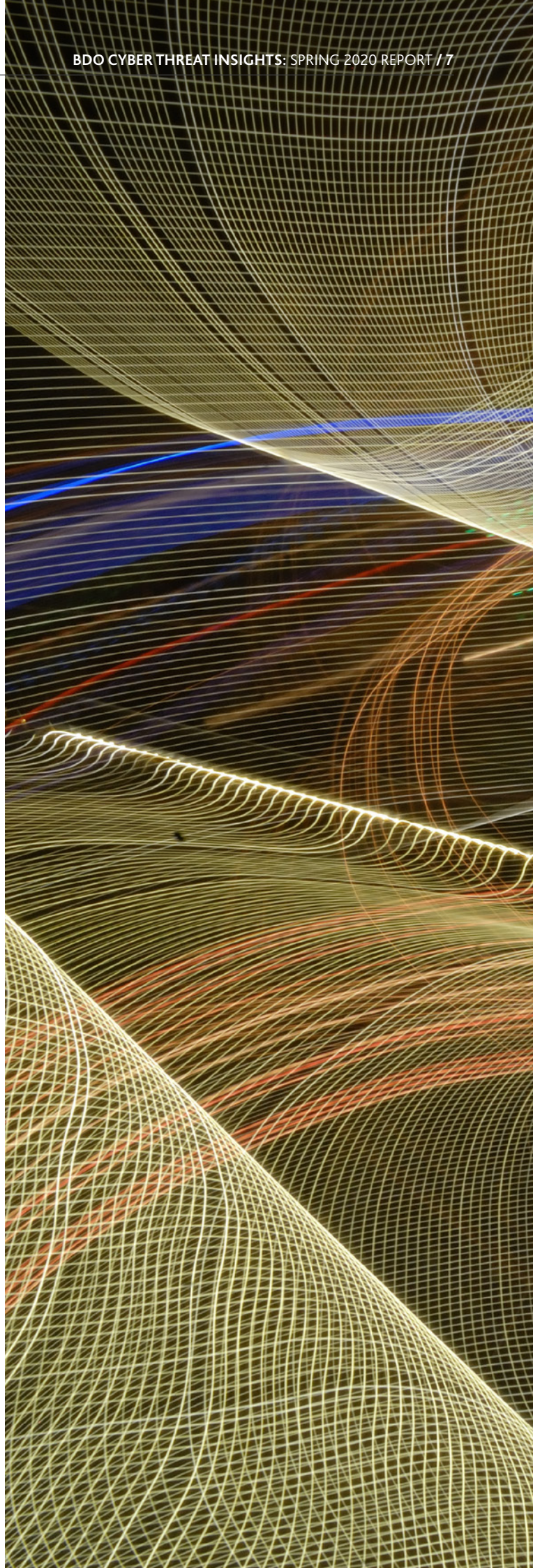
3. IT SERVICE PROVIDER CYBER-ATTACKS ARE ON THE RISE

Companies across all sectors rely on software and hardware suppliers – for IT and project management, cybersecurity monitoring, firmware manufacturing, and more. In a supply chain cyber-attack, a company's IT service provider is often penetrated and leveraged to gain access to its client's network. When it comes to large IT service providers, a single company can open the door to the networks of hundreds of companies – especially a provider that has high-level access to their clients' networks.

Among the most prominent cyber-attackers are Chinese APT (advanced persistent threat) groups. APT10 is the most notable of these and was responsible for the attack against Norwegian cloud company Visma in February 2019, as well as several other managed service providers (MSPs) in an operation dubbed 'Cloud Hopper.' In 2019, there was a significant rise in this attack vector, and this trend will likely continue in 2020.

Another significant supply chain cyber-attack was 'ShadowHammer,' which exploited pre-installed ASUS Live Update software in order to plant a malicious payload masked as an update. The updates were laced with malicious code through a compromised version of the popular Microsoft Visual Studio development framework, where a malicious linker component added it to the legitimate source code. However, the attack was aimed only at 600 specific computers; the attackers chose the needed MAC addresses and embedded them in advance in the malicious code. The attack was also difficult to detect, as the malicious versions were signed with legitimate ASUS certificates.

Despite the common assumption that supply chain cyber-attacks only target large businesses, the past year saw small- and medium-sized businesses come under increasing cyber-attacks, and they were actually a more common target than larger businesses[10]. Cyber-attacks against MSPs will continue to be a significant cyber threat in 2020, so it's important for all companies to examine the security practices of their IT service providers to understand the access they have and their network security.



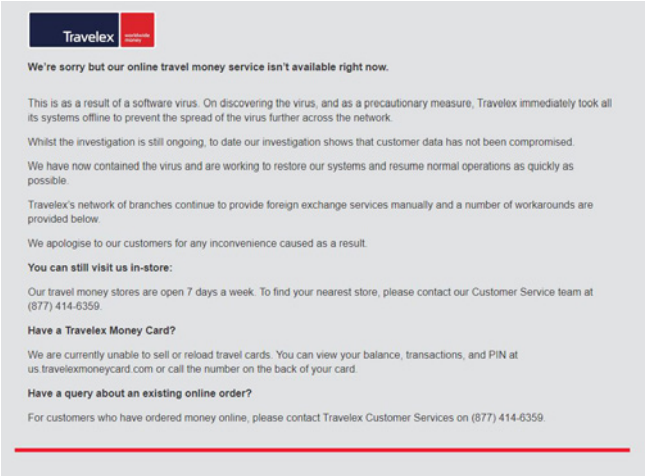
10 datto.com/uk/blog/a-look-at-ransomware-in-2019

Global Financial Services Industry Key Cyber-Attacks

1. TRAVELEX PARALYZED BY CYBER-ATTACK

The leading foreign exchange company Travelex was attacked by ransomware on December 31, 2019. Thousands of corporate computers and servers were targeted and encrypted. The next day, the company's website, cash withdrawal, and transaction services stopped working. Only a generic message of "planned maintenance" appeared on the site.

Ten days later, Travelex published an announcement[11] stating that a virus affected some of its systems, and in order to prevent the spread of the virus, it shut down all systems. But the shutdown lasted much longer than many expected.



11 http://web.archive.org/web/20200108161750/https://www.travelex.com/

Travelex's key clients, mainly banks that use the company's services for foreign currency trading and transmission, were significantly affected by the outage and unable to provide customers with expected services. Samsung's digital wallet was also affected. In addition, the company's prepaid card customers had to come to physical service points in person, and the company's employees had to conduct business using pen and paper[12].

The event attracted considerable attention across the global financial services industry because of the persistent damage inflicted and the company's inability to restore normal business operations. Travelex was assisted by several third-party companies to help mitigate the ransomware. London's Metropolitan Police Service, the National Cyber Security Center, and the Information Commissioner's Office all collaborated in the investigation as well[13].

It was soon reported[14] that the source of the attack was Sodinokibi, a ransomware also known as REvil. Earlier in 2019, it had targeted U.S. dentist offices and municipal systems across Texas. (It is also available for rent from prominent cybercriminal forums in Russian.) The ransomware's operators stated[15] that Travelex must pay the ransom of $3 million dollars (which soon doubled[16]), or the attackers would release roughly five gigabytes of personal information, including dates of birth, social security numbers, credit card information, and more. They also said that they would profit whether the company paid or not, indicating they planned to sell the data.

Travelex refused to pay the ransom and claimed that although some data was encrypted, no customer data was stolen. More than a month later, some services still had not been restored.

12 reuters.com/article/us-britain-travelex/travelex-staff-go-back-to-basics-as-ransomware-cripples-systems-idUSKBN1Z70VS

13 zdnet.com/article/travelex-customers-left-in-cashless-limbo-uk-regulators-now-step-in/

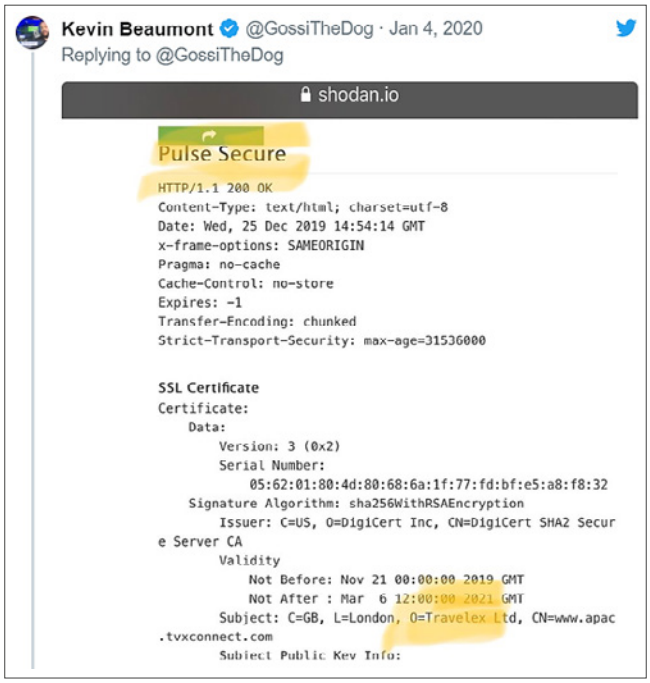
14 computerweekly.com/news/252476283/Cyber-gangsters-demand-payment-from-Travelex-after-Sodinokibi-attack

15 bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-travelex-demands-3-million/

16 bleepingcomputer.com/news/security/sodinokibi-ransomware-says-travelex-will-pay-one-way-or-another/

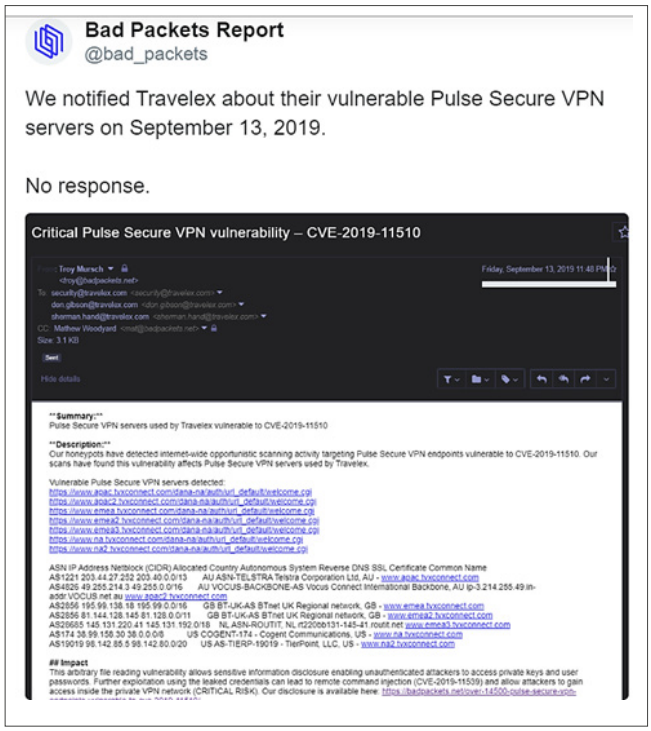
TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) IN THE TRAVELEX ATTACK

One notable aspect of the Travelex ransomware attack is the previous identification of VPN vulnerabilities that were not adequately addressed. On January 4, 2020, security researcher Kevin Beaumont published a post[17] about scans performed against networks using vulnerable versions of Pulse Secure VPN service. The vulnerabilities, found back in April 2019, are critical authentication and RCE vulnerabilities which, when combined, can enable a cyber-attacker to connect to a corporate VPN without a username and password. Even during a special scan on January 4, Travelex still had the vulnerability:



The quoted scan[18]

On September 13, 2019, a direct alert was sent to Travelex via email:

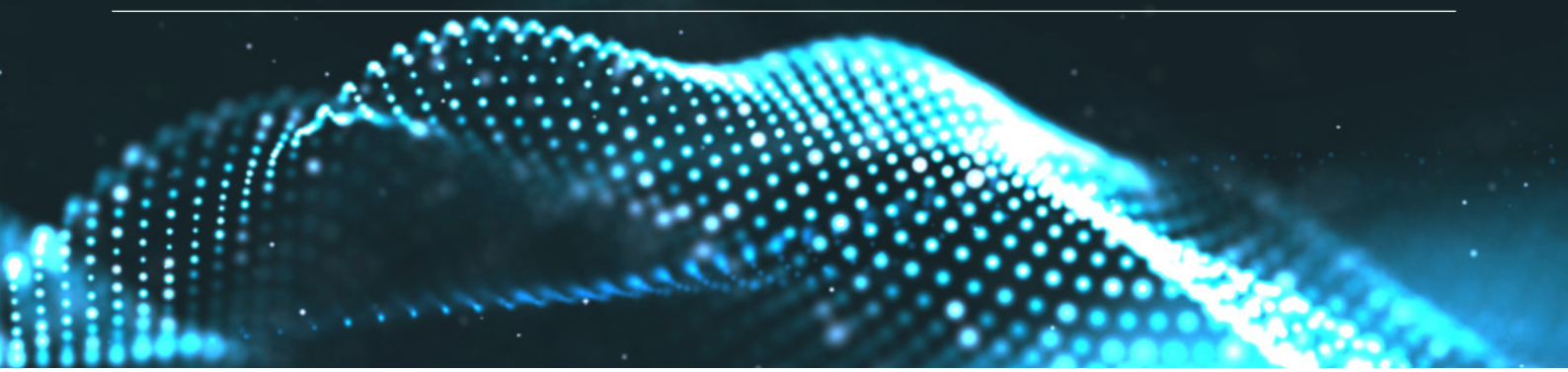


Beaumont wrote that he had discovered two instances of Sodinokibi exploiting the vulnerability. He claimed that in those instances, the cyber-attacker used the vulnerability to access the target network, and after that moved laterally through legitimate tools like PsExec and VNC.

The FBI released an additional special alert in regards to Pulse VPN, following an attack on several organizations and companies in the U.S. The FBI emphasized the fact that a number of cyber-attackers, including several nation-state groups, actively exploit the vulnerability (known as CVE-2019-11510), and it had been used to access a U.S. financial services organization's research network and a municipal government network in August 2019.

17 doublepulsar.com/big-game-ransomware-being-delivered-to-organisations-via-pulse-secure-vpn-bd01b791aad9

18 badpackets.net/



2. INSIDER THREAT ATTACK LEAKS TROVES OF RUSSIAN STATE BANK DATA

Between September and October 2019, large volumes of personally identifiable information (PII) and payment card information (PCI) were compromised for the customers of Sberbank, one of Russia's largest state banks. The PII and PCI data was allegedly put up for sale on Russian underground forums. The stolen data[19] was said to contain details of 60 million credit cards, as well as customer's full names, home addresses, work addresses, phone numbers, and more (The bank has around 18 million active cards, so this probably included both active and inactive cards). After initially denying the leak, Sberbank reported[20] that they had found the culprit after an internal investigation, and they had improved their defense systems against insider threats.[21]

Several days later, a second database[22] was put up for sale, which had roughly a million lines of personal details for customers with debts to Sberbank, and even recordings of their last calls to the bank's call center. Overall, these incidents seem to be the biggest data leak in the history of Russian banking.

3. DTRACK – A NEW MALWARE WITH AN ATM-ATTACKING CAPABILITY

The remote access trojan Dtrack was first reported[23] by Kaspersky in late September 2019. While the capabilities of this backdoor are fairly standard, it has a unique variety of droppers and versions, including one attacking ATMs (found in India). Kaspersky claims that the malware shares some similarities with the 2013 DarkSeoul campaign, so many speculated that this was deployed by a nation-state actor, likely North Korea.

Another related campaign is notable because of the target– a nuclear facility. In October 2019, a tweet[24] was posted in which the user shared a link to VirusTotal showing a malicious file identified as Dtrack. The user claims that the malicious file collects information on the target, and then sends it to a private address via a file-sharing protocol. The username for the file is KKNPP – an abbreviation of Kudankulam, a nuclear site in India, indicating that the attack was specifically tailored. India's Nuclear Power Corporation subsequently confirmed[25] the reports, despite the site management's initial denial of the incident. The corporation said that the infected computer is used for administrative purposes and connected to the internet, but it is isolated from the critical internal network.

In brief, this tool is a troubling instance of a backdoor that can be adapted to different types of targets, be it ATM machines or a nuclear facility.

19 https://www.themoscowtimes.com/2019/10/03/sberbank-hit-by-huge-data-breach-a67570

20 https://www.sberbank.ru/en/press_center/all/article?newsID=ab65754b-74d3-48be-83ac-9c14ef540296&blockID=1539&regionID=77&lang=en&type=NEWS

21 interfax.ru/business/679834

22 kommersant.ru/doc/4134949

23 securelist.com/my-name-is-dtrack/93338/

24 twitter.com/a_tweeter_user/status/1188811977851887616

25 scribd.com/document/432675681/NPC-Admission-on-Malware-Attack#from_embed

4. INVESTIGATION OF AN ATM ATTACK IN MEXICO

In November 2019, security researcher Frank Boldewin of Fiducia & GAD IT, which works with Germany's Cooperative Financial Network, presented his research[26] about cyber-attacks on ATMs in Mexico via a Java (JAR) container-based malware. The malware attacked the JAM NM ATM administration system. The malware was based on access to ATM administration systems, which was used to distribute malicious code to end stations and take complete control over them, including the bill dispensing process.

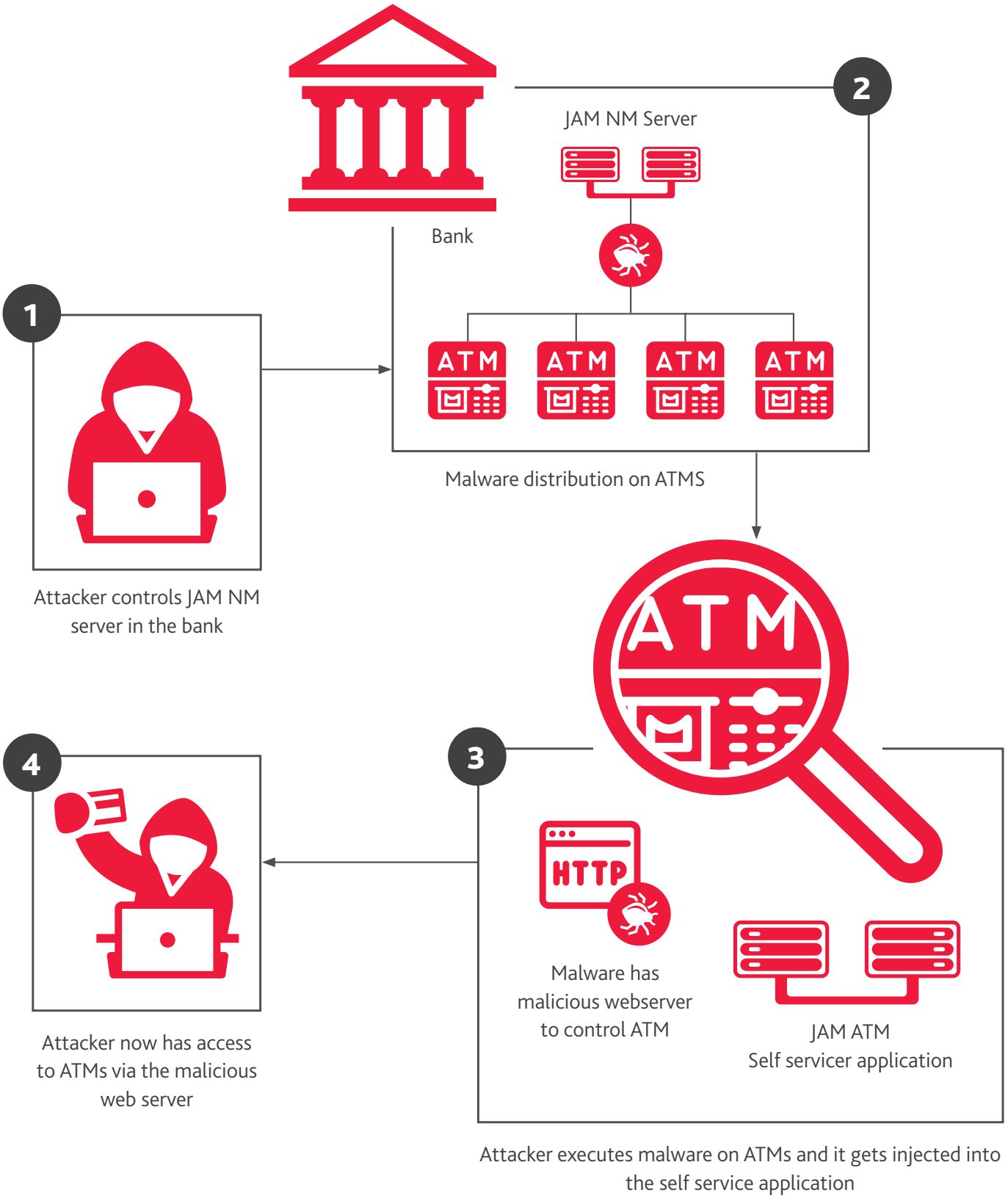
The attacks were attributed to a local criminal group named Bandidos Revolution Team, based on local police investigations following threats on the infected bank. During the investigation, theft incidents from the ATMs were linked to luxury purchases and activity by suspicious actors. Several of the group's members were arrested, including the leader.

The initial infection likely occurred with a malicious file that masquerades as an update to the JAM NM system, which is a Java-based system used to monitor and control ATM machines. The file attached a malicious agent to a legitimate administration process.

The moment that the malicious code reaches the ATM and is injected into the self-service application, it opens an HTTP server and listens to the operator's instructions. The tool is able to dispense money from the machine, carry out JavaScript commands, activate methods in the app, and download and execute additional JAR files, and even execute shell commands.

26 github.com/fboldewin/Libertad-y-gloria---A-Mexican-cyber-heist-story---CyberCrimeCon19-Singapore/blob/master/Libertad%20y%20gloria%20-%20A%20Mexican%20cyber%20heist%20story%20-%20CyberCrimeCon19%20Singapore.pdf

A CHART THAT OUTLINES THE TOOL'S INFECTION CHAIN



Source: Frank Boldewin, Fiducia & GAD IT

5. NEW CYBER TOOLS OF THE FIN7/CARBANAK BANKING CYBER GROUP

In October 2019, FireEye published a review of two new tools[27] used by the FIN7 financial cybercrime group. The first tool, called BOOSTWRITE, is a dropper that downloads a number of malicious files, including a known spyware called CARBANAK and a new tool called RDFSNIFFER. The new tool performs basic backdoor operations (file download and upload, command execution, etc.), as well as phishing and man-in-the-middle (MitM) traffic exfiltration attacks of traffic generated by the NCR Aloha Command Center traffic tool – an NCR remote management tool used by clearing points, also referred to as point of sale or PoS.

FIN7 has been a prominent APT group active since 2015[28], also sometimes known by the name Carbanak, although these appear to be two distinct groups using the same malware[29]. This criminal cyber-attack group is driven by financial gain and primarily attacks the financial sector, as well as retail and hospitality. It mainly targets U.S. entities but has committed attacks in many different countries. The FIN7 group is also known to use money mules that collect stolen funds and transfer them over the SWIFT network to the actors' accounts. Overall, FIN7 has hit over 100 financial institutions in more than 40 countries and has led to cumulative losses of well over $1 billion for the global financial services industry.

The new tools are embedded as DLL files, and below is an analysis of each of the tools:

BOOSTWRITE

The BOOSTWRITE loader takes advantage of the way Microsoft DirectX Typography services look for the required DLLs to function, forcing these services to load its malicious code instead of the legitimate directory called "Dwrite.dll". Once loaded into memory, the tool creates a file with a name beginning with ~rdf and a random number group under the current user's TEMP folder. This file is used to record messages that indicate the progress of the tool activity. Then the malicious directory scans itself for detection and decryption of an IP address and a port to deploy two more malicious files as part of the infection process. Once these are deployed and tested, they are activated and loaded into memory, and then the loader transfers control to the original and legitimate directory.

While most of the BOOSTWRITE samples are unsigned, one example – signed with a MANGO ENTERPRISE LIMITED license – was detected by FireEye and uploaded to the Virus Total portal.

RDFSNIFFER

As part of the infection process, two more malicious files are deployed. The RDFSNIFFER tool is deployed in addition to the CARBANAK malware via the BOOSTWRITE loader. This is a DLL library, which is loaded with the same process as the legitimate Aloha Command Center Client software. Once loaded, the DLL uses several Win32 API functions, which allow it to intercept the original software's communications and ensure that the sessions do not timeout. In addition, the malicious module is capable of performing basic backdoor operations, as described above.

27 fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html

28 attack.mitre.org/groups/G0046/

29 attack.mitre.org/software/S0030/

Notable Global Events – Q4 2019

1. CRITICAL VULNERABILITIES IN THE EU AUTHENTICATION SYSTEM EIDAS

In October 2019, European authorities released a patch[30] to fix two major vulnerabilities in the eIDAS (Electronic Identification, Authentication, and Trust Services) authentication system. This system is used by authorities to verify transactions between different entities in EU countries. A report by SEC Consult had cited a technical advisory issued[31] for the eIDAS-Node software, which found issues in the authentication protocol of eIDAS-Node and how it handles authentication certificates.

The first vulnerability was related to how the program verifies the certificate it receives to approve a transaction: It didn't verify whether the entity's certificate has been correctly signed by the issuer. Thus, a potential attacker could produce a manipulated SAML response (a standard for changing verification data) with a forged certificate, thus successfully posing as a legitimate entity in the EU.

The second vulnerability is in the trust check of the signer's certificate. Although eIDAS has a function to verify whether the signer's certificate is trusted, it continues processing the SAML response without checking the result. In other words, the program checks the trustworthiness of the entity which issues the certificate for the transaction but ignores the results. Thus, an attacker can produce a forged certificate for itself and not care about validations, because they are skipped or ignored anyway.

These vulnerabilities are severe because a potential attacker can pose as any individual or organization in Europe, which opens many possibilities for fraud and theft.

30 zdnet.com/google-amp/article/major-vulnerability-patched-in-the-eus-eidas-authentication-system

31 sec-consult.com/en/blog/advisories/15587/

2. CHINESE ESPIONAGE GROUP TARGETS COMPANIES THROUGH VPN 2FA BYPASS

Fox-IT published a research paper[32] in December 2019 about a widespread espionage campaign by the Chinese group APT20. The group, which is mainly known for attacking Eastern Asia through tactics such as "watering holes" (infection, impersonation, or redirection to a site which is highly probable that the target will visit), succeeded in installing a wide espionage infrastructure against organizations in different sectors – both public and private. One of the most dangerous characteristics of this campaign is the capability to steal credentials, including tokens, not only for lateral movement on the attacked network but also to ensure remote access to the network through VPN connection at later stages even without backdoors. Furthermore, the group exploits vulnerable servers and existing webshells on target systems and uses proxy and credentials-harvesting capabilities for lateral movement.

For initial access, the group compromises vulnerable servers, often JBoss-type, or uses the access provided by webshells, which often have already been implanted by other actors. Upon gaining access, the group performs initial reconnaissance on the network to find high-privilege users, such as admins, and map the network before lateral movement. Among the tools used at this stage are a user-mapping tool, a keylogger, a directories-listing tool, and several proxy capabilities.

In some cases, the group appears to have stolen an RSA SecurID token, which is a soft component used to create credentials for two-factor authentication (2FA). This authentication method is considered more secure because it makes it more difficult for an attacker to gain access, even if he or she has some credentials. In this specific case, the VPN uses a mechanism that generates one of the factors based on the token. However, the system check is not implemented in a robust way, so the attacker can bypass this check though a simple patch. In other words, one of this campaign's most important characteristics is exploiting VPN connections for later re-access to the target by using the stolen token to bypass 2FA.

32 fox-it.com/en/news/whitepapers/operation-wocao-shining-a-light-on-one-of-chinas-hidden-hacking-groups/

3. A NEW IRANIAN WIPER DETECTED - ATTACKS IN THE MIDDLE EAST

In December 2019, IBM's Incident Response and Intelligence Services (IRIS) team published a report[33] about a destructive new Iranian malware named ZeroCleare. It targeted the energy sector in the Middle East, and the malware likely belongs to one or two Iranian groups (The researchers assess that it could be a joint effort). The tool attempts to propagate in the targeted network as quickly as possible, and then it destroys the infected computers by rewriting and destroying several vital components.

ZEROCLEARE'S INFECTION FLOW

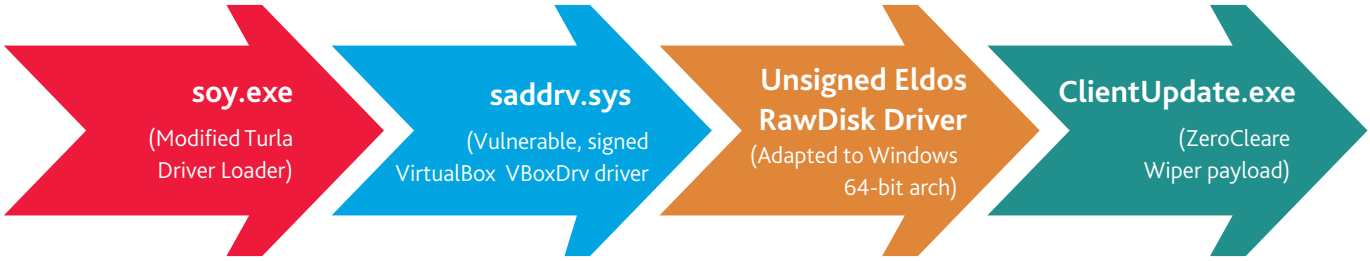


Figure 1: ZeroCleare's Top Level Infection Flow

Source: IBM X-Frorce

ZeroCleare is a post-exploitation tool (a tool used after the targeted network has already been penetrated). The tool has two versions, for 32-bit and 64-bit processors, but only the 64-bit version works at this stage. The other version collapses, and the activation fails. The general method of action is as follows: infect a domain controller; then propagate from there to other computers in the network; exploit a vulnerable driver that is signed by Microsoft to activate another, unsigned but legitimate driver; and then install the main tool ZeroCleare.

In order to install the tool, the attackers use an application named Turla Driver Loader (TDL), which is a tool that bypasses Windows defense systems (the defense systems necessitate using Microsoft-signed drivers only). TDL loads a signed and vulnerable driver, a VirtualBox driver, that enables it to execute kernel-level shellcode. By exploiting this vulnerability, the attackers load a legitimate but unsigned driver, EldoS RawDisk, which enables it to work directly with disks and the logical partitions between them. Once the driver is installed, the main tool, under the name ClientUpdate.exe, is installed on the computer and executed. This way, the tool bypasses Windows defense mechanisms (Driver Signing Enforcement policy or DSE)

The tool creates a buffer of random bytes, and then it uses the function DeviceloContol in order to re-write the existing information on the infected computer with random information. In this way, the loading mechanism and logical partitions between the disks are destroyed, rendering the infected system useless.

In addition to the main tool and drivers, the group uses several BAT files and PowerShell commands, mainly for smaller actions like checking the processor's architecture or executing a file. One script, ClientUpdate.ps1, is of particular interest because it attempts to distribute the main tool as quickly as possible to as many computers with a network of agents (located on central computers) and clients (located on regular end-stations). After the script finishes several preliminary actions, it allocates the clients that need to be infected to the agents. Through this, the tool attempts to shorten the infection time and the attack time when the command comes.

33 ibm.com/downloads/cas/OAJ4VZNJ

Protecting the Financial Services Industry Through Threat-Based Cybersecurity

Digital tools have helped make the global economy more interconnected than ever before, but they have also exposed financial services organizations to a wide range of vulnerabilities. Travelex learned this the hard way when in their 2019 cyber-attack by the Sodinokibi ransomware. Far from a seamless web of services, the ransomware attack turned Travelex into a protracted pileup of frustrations. The fallout from this incident should encourage all organizations to carefully review their cybersecurity practices and ensure there are processes for preventing the spread of malware, ensuring valid authentication protocols, blocking network intrusion, restricting lateral movement on the network and enabling rapid response.

However, ransomware is hardly the only cyber threat, and financial services organizations remain an attractive target because they process substantial amounts of money and hold troves of valuable customer data—including names, addresses, phone numbers, dates of birth, social security numbers, employment information, payment card information and more—that can be used to perpetrate lucrative acts of fraud. And with the expansion of digital technologies in financial services, from chatbots and IoT devices to digital banking and digital payments, there are increasing access points to protect from potential intrusion.

There are also many different threat actors to guard against, including cybercriminals, hacking groups, nation-state groups and even internal staff. In some cases, such as the Sberbank data leak in Russia, a rogue employee may steal customer data and give it to cybercriminals. The much more common concern is a spear-phishing attack, where an employee could be duped into providing crucial information or unwittingly giving up login credentials. It's important to have mechanisms in place that limit the potential damage from insider threats and to train employees about the warning signs of a possible phishing attempt.

In the face of expanding cyber threats and increasingly sophisticated cyber-attackers, financial services organizations should protect themselves with a threat-based strategy for cybersecurity, which acknowledges the common attack vectors and safeguards those areas that are most likely to be targeted by threat actors.

THREAT-BASED CYBERSECURITY

Financial services organizations can take several concrete steps to detect and respond to risks more effectively, including:

Bolster their access controls – technical policies and procedures to ensure only authorized employees have access to sensitive data —and be more stringent about who they grant access.

Implement stronger audit controls – to track and identify internal and external access to and exploration of information systems that contain account details and personally identifiable information (PII).

Strengthen intrusion detection systems (IDS) – to more accurately monitor traffic moving throughout their email, network, and information system endpoints to identify suspicious activity and address threats in real-time.

Make top-down personnel education a priority for everyone – from the Board of Directors to the C-Suite, managers, and employees, ensure all individuals with access to an organization's networks, medical devices and data understand their roles and responsibilities in defending against cyber threats.

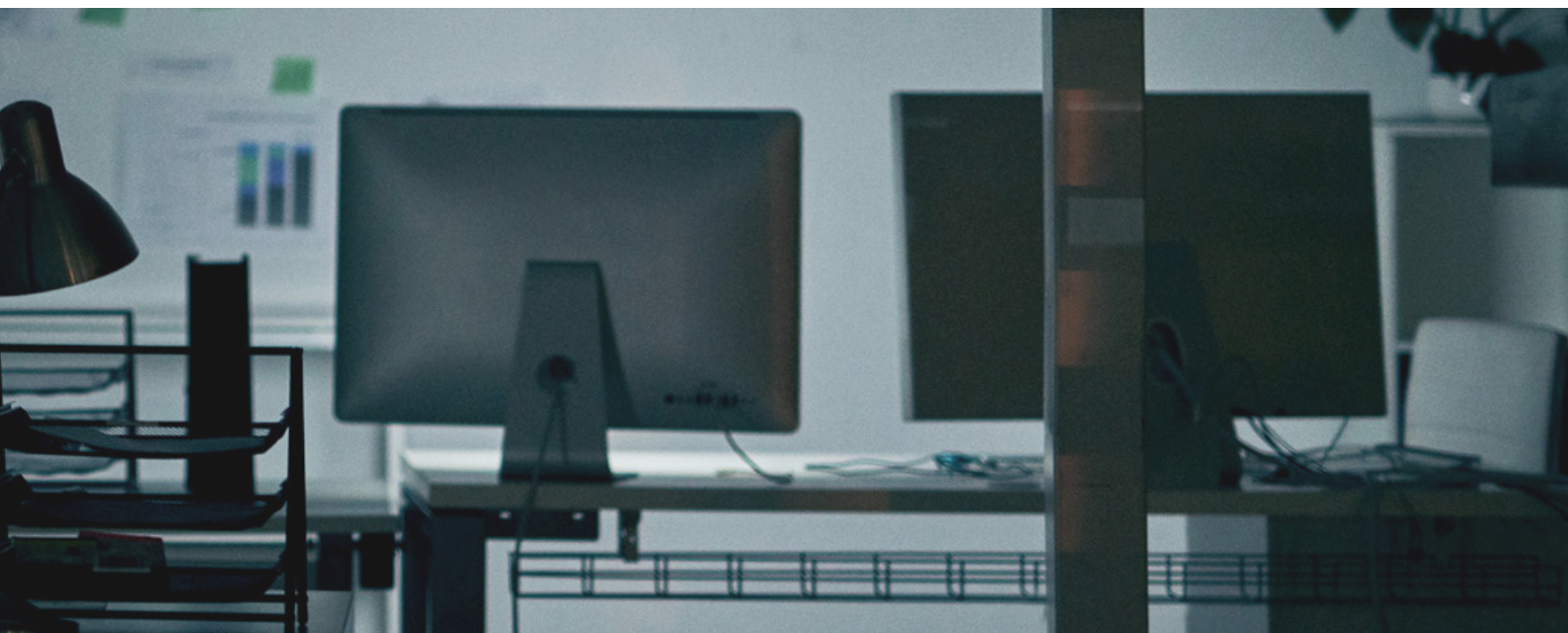
Create an internal and external crisis communication plan – to align with existing enterprise risk management frameworks.

Implement cyber insurance claims preparedness and adequate coverage – to identify and quantify incurred event response costs for inclusion in an insurance claim.

Create an incident response plan – to include the participation of organization leadership and key personnel from all technology, business, administration and clinical functions.

Develop and test a Business Continuity Plan (BCP) – in order to have real information resilience, it is vital to have an effective information back-up capability that can quickly replace any data loss.

With increased adoption of technologies (e.g., cloud computing, data analytics, fintech applications, AI-powered chatbots, IoT devices, digital payments and more) across the financial services industry, threat-based cybersecurity can form an integral part of digital transformation efforts that will help carry the business forward through the next decade.



BDO Cyber Threat Intelligence (CTI) Services

THREAT INTELLIGENCE – "PROACTIVE DETECTION OF A BREACH"

Situational awareness is "the perception of environmental elements and events with respect to time or space, the comprehension of their meaning and the projection of their future status," while intelligence is "the ability to acquire and applied knowledge and skills."

BDO Cyber Threat Intelligence (CTI) is a combination of both: the objective of acquiring knowledge and skills to support better organizational ability and anticipate cyber events that could impact the future status of the business environment.

The BDO CTI Reports are based on research performed by the BDO Cybersecurity Centers. Our Cyber Threat Intelligence Centers in the U.S. and Israel work as an integrated team to transform reactive organizational situational awareness into proactive situational awareness to Cyber Threats. This enables an organization to better understand the likelihood and characteristics of a breach and enables an additional layer of proactivity in the detection of unidentified breaches that might be happening.

HOW DOES IT WORK?

Cybersecurity Research

Our Cyber Research teams reverse-engineer cyberattack techniques, malicious code and lateral movement to identify actual targets and methods used by different perpetrators with different malicious agendas.

Online Fictitious Identities

Our Cyber Intelligence team maintains online fictitious identities to enable their activity within threat communities, to infiltrate an online forum or create a connection with suspected threat actors or hackers, and establish online 'chatter' platforms, to establish 'trusted' conversation environments.

Monitoring Cybercrime Forums

Our Cyber Intelligence team monitors various cybercrime forums to identify premeditated attacks on organizational networks or personnel by monitoring any type of hostile chatter regarding these 'targets.'

Monitoring Data Leakage Platforms

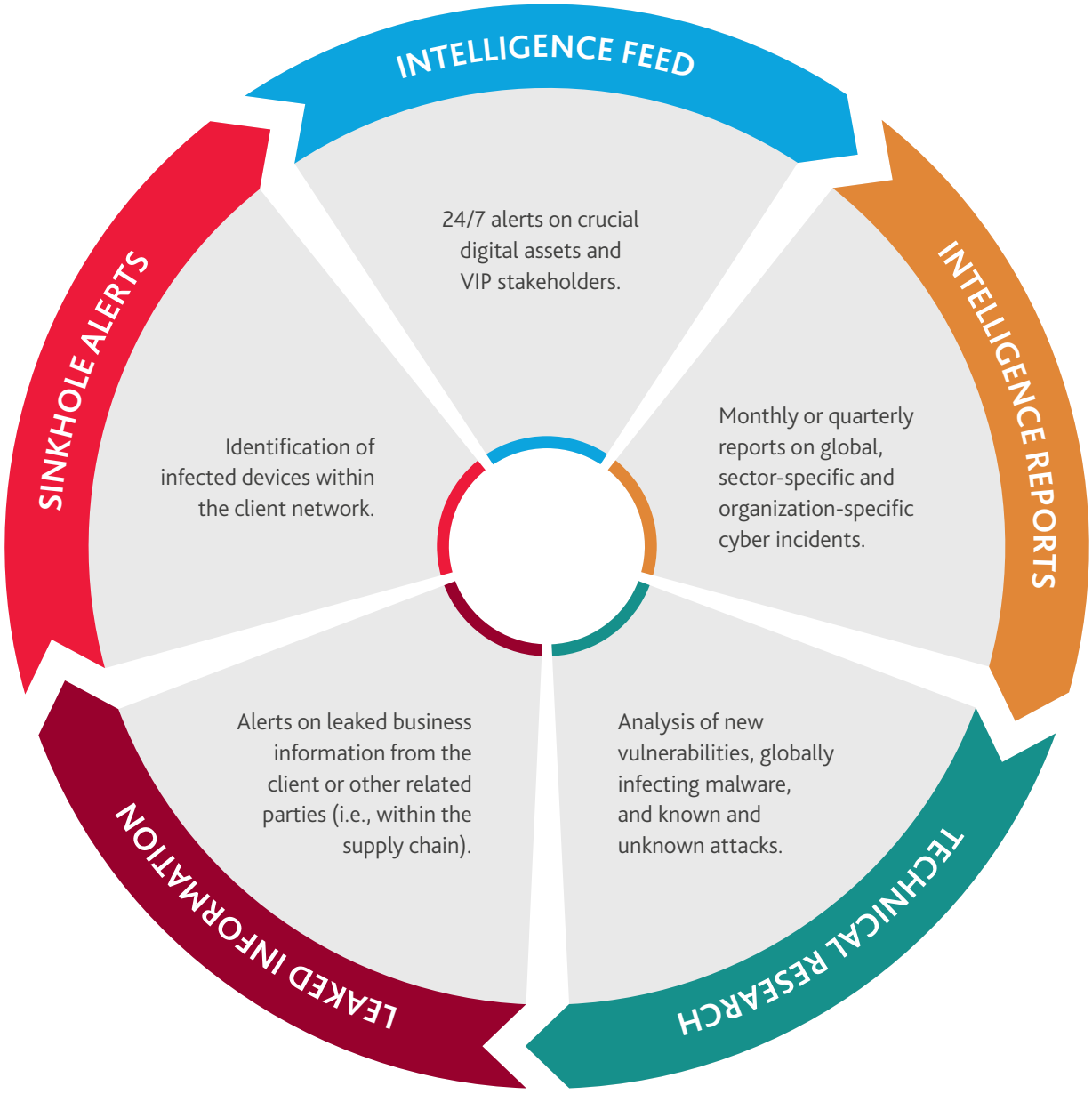
Our team can trawl hacker-oriented data leakage platforms to identify specific data leakage that might lead to a potential attack against an organization.

CONTACTS:

TOMMY BABEL
Head of Cyber Resilience & Threat Intelligence Services
BDO Cyber Security Center, Israel
tommyb@bdo.co.il

NOAM HENDRUKER
Director, Head of Global Consulting Group
BDO Cyber Security Center, Israel
tommyb@bdo.co.il

BDO CTI DELIVERABLES



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

- 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
- Cybersecurity education, training, & simulations
- Security Incident & Event Management (SIEM)
- Email & Network Attack Detection & Monitoring Services

Cybersecurity Leadership Team

GREGORY GARRETT
Head of U.S. &
International Cybersecurity
703-770-1019
ggarrett@bdo.com

VIVEK GUPTA
National Leader, Cybersecurity
416-369-7867
vgupta@bdo.ca

SAUMIL GIRISH SHAH
Partner, Business Advisory Services
Risk & Technology, Cybersecurity
+91-80-6815-0000
saumilgshah@bdo.in

MICHIEL JONKER
Partner
+27-10-590-7240
mjonker@bdo.co.za

SCOTT HENDON
BDO Head of Global Private Equity
214-665-0750
shendon@bdo.com

GLENN POMERANTZ
BDO Head of Global Forensics
212-885-8379
gpomerantz@bdo.com

OPHIR ZILBIGER
Partner
Head of Cybersecurity, BDO Israel
+972-52-6755544
OphirZ@bdo.co.il

LEON FOUCHE
Partner
Head of Cybersecurity, BDO Australia
+617-3237-5688
leon.fouche@bdo.com.au

SANDRA KONINGS
Partner
Head of Cybersecurity, BDO Netherlands
+31-30-284 9960
Sandra.Konings@bdo.nl

ANDREAS VOGT
Partner
Head of Cybersecurity, BDO Norway
+47-481-71 714

JASON GOTTSCHALK
Partner
Head of Cybersecurity, BDO United Kingdom
020-3219-4536
Jason.Gottschalk@bdo.co.uk

STEPHAN HALDER
Director
Cybersecurity, BDO Germany
+49-40-30293-169
stephan.halder@bdo.de

People who know Cybersecurity, know BDO.