CYBER MANAGEMENT ALLIANCE

Cyber-attack timelines:

Educational guides to understanding attacks & enhancing resilience

Company: Travelex

Disclaimer: This document has been created with the sole purpose of encouraging discourse on the subject of cybersecurity and good security practices. Our intention is not to defame any company, person or legal entity. Every piece of information mentioned herein is based on reports and data freely available online. Cyber Management Alliance neither takes credit nor any responsibility for the accuracy of any source or information shared herein.

Contents

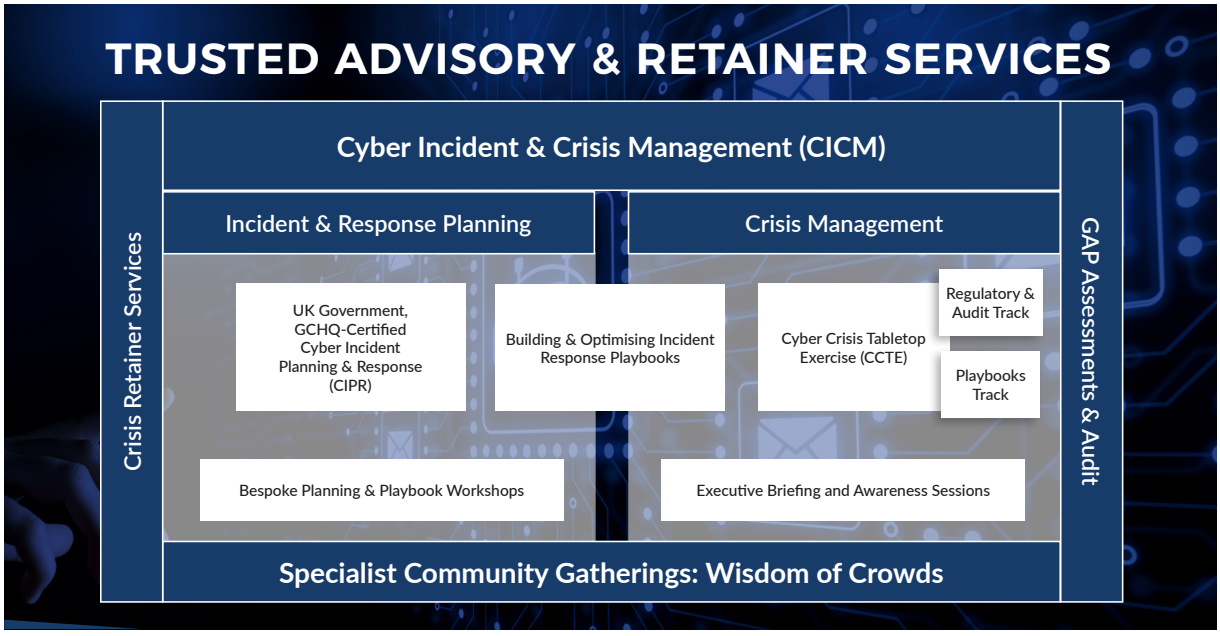
About Cyber Management Alliance Ltd

Founded in 2015 and headquartered in London UK, Cyber Management Alliance Ltd. is a recognised independent world leader in Cyber Incident & Crisis Management consultancy and training. The organisation is renowned globally as the creator of the flagship **Cyber Incident Planning and Response** course certified by the UK Government's National Cyber Security Centre.

Cyber Management Alliance has serviced over 300 enterprise clients in multiple verticals including government, banking, finance, IT, consultancies, healthcare, oil & gas and retail across 38 countries. It has established its leadership by assessing, building and improving its clients' Cyber Incident & Crisis Management capabilities through training, tabletop exercises, health checks and audits.

Cyber Management Alliance helps organisations build and strengthen their Cyber Incident Response capabilities to enable them to rapidly detect and actively respond to business-impacting cyber-attacks.

Today, Cyber Management Alliance has a global and diverse network of over 80,000 cyber executives and practitioners worldwide.



Travelex Hack Summary

- **The attacker(s):** Sodinokibi Group (Gold Southfield)
- **Business impact:** Travelex servers were down for approximately 2 weeks, though recovery started within 6 days;
  $2.3 M paid in ransom, allegedly
  Reported quarterly loss of about £25m
- **Ransom paid:** reportedly $2.3 M (approx)
- **Downtime:** Approximately 2 weeks to revive its customer-facing systems in the UK
- **Time to Detect:** None – Ransomware disabled business immediately
- **Time to Disclose to Customers:** Posted a statement disclosing the attack in 2 days
- **Breach Notification to Regulators:** ICO claimed, as per News reports, that they were NOT informed in time
- **Time to Recover:** 2 weeks (only some systems were brought online in 14 days)
- **Period of Persistence:** N/A
- **Vulnerability exploited:** 7 unpatched Pulse VPN Servers with CVE-2019-11510 vulnerability
- **Regulatory Impacts & Fines:** No decision yet

About the Business

- The world's largest currency exchange company, based in the UK and established in 1976, run by B.R Shetty (owns UAE exchange and Finablr).
- The company operated its business across 70 countries with more than 1,200 branches and more than 1,000 ATMs installed at various top airports and high streets across the globe.
- Prior to the cyber-attack and the effects of COVID-19, Travelex was an extremely popular money exchange company as it processed more than 5,000 currency transactions in an hour.
- Travelex had over 7,627 employees working at different locations across the world.

Prior History of Attacks

- In 2018, Travelex accidentally leaked personal information of about 17,000 Tesco customers.
- In the above data leak, all the personal details of Tesco customers were stolen including their Full Name, Date of Birth, email addresses, IP addresses, mobile numbers, delivery addresses, and Partial Payment card numbers, etc.

The Attack

Summary

- On New Year's Eve, 31st December 2019, Travelex was hit by a ransomware attack that disrupted its currency exchange business.
- After confirming the attack, the company immediately put all its servers offline to protect the data of thousands of its customers.
- On 2nd January, 2020, after disclosing the hack incident, Travelex CEO apologised and said that, "We regret having to suspend some of our services in order to contain the virus and protect data. We apologise to all our customers for any inconvenience caused as a result. We are doing all we can to restore our full services as soon as possible."
- The vulnerability named CVE-2019-11510 that the attackers exploited to hack into Travelex's systems was reportedly first discovered by two security researchers OrangeTsai and Meh Chang in March 2019 and Pulse Secure patched up the vulnerability in April 2019. This vulnerability was, allegedly, again found in the Travelex servers and this was pointed out by Troy Mursch, the CEO of Bad Packets, in his Tweet on 13th September, 2019. He mentioned that Travelex remained unable to patch its Pulse Secure VPN which then became the cause of the intrusion.

Attack methodology

- The attack on Travelex was a ransomware cyberattack called 'Sodinokibi ransomware' or REvil and it is based on a ransomware-as-a-service (RaaS) model.
- Sodinokibi was reportedly discovered in April 2019 by CISCO TALOS (an intelligence group) and it belongs to the financially motivated threat group called Gold Southfield.
- According to CISCO TALOS, Sodinokibi gained access to the victim's machines by exploiting Oracle WebLogic Vulnerability.
- Sodinokibi generates and propagates encryption keys by using the Elliptic-curve Diffie-Hellman key exchange algorithm.
- Here, in the case of Travelex, the above-mentioned ransomware group is supposed to have used the same algorithm and gained access to the company's servers.

Continued...

The Attack (cont)

Assets Impacted

- On 31st December, 2019, when the whole world was celebrating New Year's eve, Sodinokibi ransomware entered the servers of Travelex and allegedly stole the personal information of its customers.
- Initially, when the attack occurred on 31st December, 2019, Travelex websites across Europe, Asia and the US were taken offline with a message to visitors that they are down due to "planned maintenance".
- As all the online systems were shut down, no online transaction was possible, and this disrupted the whole business of Travelex.
- On 2nd January, 2020, Travelex websites in Europe, including the UK, Belgian and Holland, Qatar and the United Arab Emirates in the Middle East, and China either did not respond or showed error messages, as per media reports.
- The currency exchange company reportedly took two days to confirm the attack. On 2nd January 2020, the company, allegedly, said that no personal data or information had been compromised as their home investigation team found no data loss.
- On 6th January 2020, an independent investigation by BleepingComputer confirmed that the REvil (also known as Sodinokibi) ransomware had indeed infected Travelex systems as the extension that was attached with the encrypted files was a string of more than five characters ".u3i7y74". This malware typically added different extensions to files locked on other computer systems.
- Around 6th January, 2020, a ransom note from Sodinokibi began doing the rounds in the media. Further, Sodinokibi supposedly confirmed to BleepingComputer that it had encrypted the entire Travelex network and taken more than 5GB of personal data, which included dates of birth, social security numbers, card information and other details of Travelex customers.

Continued...

The Attack (cont)

Business & Environmental Impact

- In the week beginning 1st January, 2020, customers of Travelex started complaining that their money was in limbo. They complained of their holidays being ruined as they were unable to access their own money while travelling abroad.
- The UK's top banks like Barclays, HSBC, Royal Bank of Scotland and Virgin Money, allegedly remained unable to offer money exchange services to their customers as Travelex put all its systems offline.
- Tesco, First Direct, and Sainsbury also became victims of the cyber-attack as they also remained unable to serve their customers with currency exchange services.
- Apart from the banks and other stores, the general customers of Travelex who always preferred online transactions suffered the most as they waited for hours in queues at airports and other stores of Travelex to get money from their Travelex accounts.
- According to The Financial Times, on 9th January 2020, all the staff members at the company headquarters were asked to deposit their laptops for a detailed investigation into the cyber-attack.

Response & Recovery

Company's Response

- Travelex said it first discovered the attack on 31st December, 2019 and took all its sites offline to protect data and prevent the virus from spreading.
- In an official Tweet on 3rd January, 2020, the company Chief Executive, Tony D'Souza apologised that Travelex had to suspend its services. In the initial investigation, the company declared that no personal information of its customers was stolen.
- In communication with the NCSC, Travelex is reported to have said that no personal data of the customers was compromised.
- In the week beginning on 6th January 2020, Travelex began the successful recovery of its internal systems necessary to restore its customer-facing services.
- On 17th January 2020, Travelex announced that the first of its customer-facing systems in the UK were up and running and the phased restoration of its systems globally was firmly underway. "We have a clear strategy for the phased restoration of services, prioritising the UK as this is our single largest market. We have started restoring forex order processing electronically in our UK stores and in some of our UK retail partner locations, and we are also now starting our VAT refund service in UK airports," the company stated.
- But till 27th January, 2020, some of its partners like Tesco, Barclays, HSBC, and Virgin Money were reportedly still offline as the recovery process was still going on.
- On 28th January, 2020, Travelex confirmed that it has resumed its Travelex Wire service.
- On 30th January, 2020, Travelex announced the recovery of its customer facing website in the UK. This service facilitates customers to order travel money for store collection or for home delivery.
- On 14th February, 2020, Travelex reported that it had managed to restore all its systems and business operations in various countries like the UK, Europe, North America, the Middle East, Turkey, Australia, and New Zealand.
- On 24th February, 2020, in addition to the system recovery in the UK, Europe, North America, the Middle East, Turkey, Australia,and New Zealand, Travelex restored its systems in Asia as well.

Continued...

Response & Recovery (cont)

What happened next

- On 17th January, 2020, when the CEO of Travelex announced that the company had recovered its customer-facing systems in the UK, at the same time, the hacker group allegedly told BleepingComputer that "they have received payment from Travelex, but would not specify the amount or provide any proof". And a company person who is familiar with the transaction reportedly said, "Travelex responds back by paying the hackers the equivalent of $2.3 million." Therefore, it may possibly be assumed that Travelex paid $2.3 million in ransom between 6th and 17th of January, 2020.
- Travelex never officially confirmed that it has paid the ransom amount. But on 9th April 2020, Wall Street Journal published a story confirming that Travelex had allegedly paid a ransom amount of $2.3 M (285 Bitcoins) to Sodinokibi group.

Response from Government & Police

- The Met Police were contacted on 2nd January, 2020, two days after the incident took place as they conducted detailed investigations.
- According to The Financial Times, on 8th January, 2020, the National Cyber Security Centre (NCSC) and the Financial Conduct Authority looked into the cyber-attack.
- Travelex allegedly did not notify the ICO within 72 hours regarding the attack and may be liable to give an explanation as to why they kept it hidden from the ICO. Therefore, the ICO may charge a heavy fine to Travelex as it did not upgrade its security measures. But the organisation has not taken any action against the FX company yet.

Current Market & Business Issues for Travelex

- On 2nd March, 2020, Travelex reported that it expected a quarterly loss of £25 million due to the Ransomware attack and Coronavirus.
- On 12th March, 2020, Finablr, the owner of Travelex started teetering on the brink of collapse as its share price tumbled down by nearly 80%. It went from £45 to £4.50 on 12th March, 2020. Finablr declared that it was appointing a financial advisor to advise the company in the matter of insolvency.
- In a statement on 18th March, 2020, Travelex mentioned that it is capable of operating independently as a stand-alone entity with the support of its key financial stakeholders.
- On 24th March, 2020, as per media reports, Travelex took a decision to suspend all UK bureaus and began offering home delivery services to its customers seeking money exchange services.
- According to a report on 22nd April, 2020, Travelex put itself on sale due to its parent company Finablr's insolvency issue and thanks to the twin shocks of an unexpected ransomware attack and the impact of COVID-19.
- On 5th June 2020, a report said that a number of bidders, including the private equity firm Marlin Equity & an investment vehicle controlled by the billionaire banker Joseph Safra, made offers for Travelex.
- On 12th June 2020, Travelex bondholders allegedly pressed the company's syndicate of banks, which includes Barclays and Goldman Sachs, to negotiate a potential deal and to enter into talks about restructuring after an emergency auction of the business stalled.
- On 6th August 2020, as PwC carried out the complex restructuring deal for Travelex, the joint administrator at PwC, Toby Banfield said, "Unfortunately, as the majority of the UK retail business is no longer able to continue trading, it has regrettably resulted in 1,309 UK employees being made redundant today."

Twitter Handles

1. @cm_alliance
2. @amisecured
3. @GossyTheDog
4. @_mike_chambers_
5. @TravelexUK
6. @bad_packets
7. @joetidy
8. @HalifaxBank
9. @Martin_Malt
10. @LloydsBanl
11. @barryschofield
12. @tony95519737
13. @HSBC_UK
14. @MalwareTechBlog
15. @hacks4pancakes
16. @MalwareJake

for Travelex

1. #Travelex
2. #cybersecurity
3. #moneyhack
4. #Ransomware
5. #TVXHackday
6. #Hackday
7. #databreach
8. #cyberattacks
9. #CyberSecurity
10. #cyberthreat
11. #Ransom
12. #REvil
13. #Sodinokibi
14. #ThreatThursday

References

About the Business

- https://en.wikipedia.org/wiki/Travelex
- https://www.bloomberg.com/profile/company/2917958Z:LN
- https://www.decisionmarketing.co.uk/news/17000-tesco-customers-hit-by-travelex-data-breach
- https://www.mirror.co.uk/money/17000-tesco-bank-travel-money-12179818
- https://www.thesun.co.uk/money/5799780/thousands-of-tesco-bank-travel-money-customers-data-leaked-by-travelex/
- https://threatpost.com/travelex-knocked-offline-malware-attack/151522/

What was the incident?

- https://twitter.com/TravelexUK/status/1212840156480315401/photo/1
- https://www.bbc.co.uk/news/business-50977582
- https://threatpost.com/travelex-knocked-offline-malware-attack/151522/

What Attack Methods were Used?

- https://www.acronis.com/en-gb/articles/sodinokibi-ransomware/
- https://www.secureworks.com/research/revil-sodinokibi-ransomware
- https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
- https://portswigger.net/daily-swig/what-is-sodinokibi-the-ransomware-behind-the-travelex-attack

Continued...

References (cont)

What Assets were Impacted?

- https://www.computerweekly.com/news/252476283/Cyber-gangsters-demand-payment-from-Travelex-after-Sodinokibi-attack
- https://www.mirror.co.uk/money/breaking-travelex-being-held-ransom-21231768
- https://news.sky.com/story/travelex-takes-sites-offline-due-to-software-virus-attack-11899921
- https://www.techradar.com/uk/news/travelex-website-was-hit-by-sodinokibi-ransomware
- https://threatpost.com/sodinokibi-ransomware-travelex-fiasco/151600/
- https://www.telegraph.co.uk/business/ready-and-enabled/security/how-could-travelex-have-retained-customer-trust-after-cyber-attack/
- https://www.theguardian.com/technology/2020/jan/02/travelex-forced-to-take-down-website-after-cyber-attack

Who was Impacted?

- https://news.sky.com/story/high-street-banks-hit-by-travelex-ransomware-attack-11904240
- https://www.independent.co.uk/news/business/news/travelex-cyber-hack-data-breach-foreign-exchange-money-a9275736.html
- https://www.theguardian.com/technology/2020/jan/07/travelex-being-held-ransom-hackers-said-demanding-3m
- https://www.bbc.co.uk/news/business-51026383
- https://www.zdnet.com/article/travelex-customers-left-in-cashless-limbo-uk-regulators-now-step-in/
- https://www.eveningexpress.co.uk/news/business/barclays-lloyds-rbs-and-hsbc-all-hit-by-travelex-cyber-attack/

Continued...

References (cont)

What Actions did the Company Take?

- https://news.sky.com/story/police-investigating-ransomware-attack-on-currency-exchange-travelex-11903064
- https://www.telegraph.co.uk/technology/2020/01/13/travelex-begins-bring-site-back-online-6m-ransomware-attack/
- https://www.computerweekly.com/news/252476624/Travelex-begins-to-restore-foreign-exchange-services-two-weeks-after-Sodinokibi-attack
- https://www.zdnet.com/article/two-weeks-after-ransomware-attack-travelex-says-some-systems-are-now-back-online/
- https://www.theguardian.com/business/2020/jan/13/travelex-services-begin-again-after-ransomware-cyber-attack
- https://portswigger.net/daily-swig/travelex-ransomware-attack-pulse-secure-vpn-flaw-implicated-in-security-incident
- https://www.pymnts.com/news/security-and-risk/2020/travelex-back-online-after-cyberattack/
- https://twitter.com/bad_packets/status/1213536922825420800
- https://www.reuters.com/article/us-britain-travelex/travelex-says-uk-money-transfer-and-wire-services-back-online-after-hack-idUSKBN1ZR1S5
- https://www.bbc.com/news/business-51364102
- https://www.scmagazineuk.com/thousands-businesses-risk-via-pulse-secure-vpn-flaw-updated-response/article/1670064 *(Regarding Pulse secure VPN)*
- https://doublepulsar.com/big-game-ransomware-being-delivered-to-organisations-via-pulse-secure-vpn-bd01b791aad9 *(Regarding Pulse secure VPN)*

Continued...

References (cont)

What did the Government Do?

- https://www.computing.co.uk/news/3084926/travelex-gdpr-ransomware-ico
- https://www.hayesconnor.co.uk/why-has-travelex-not-told-the-ico-about-its-data-breach/
- https://www.scottishlegal.com/article/ian-birdsey-travelex-cyber-attack-underlines-need-for-business-to-mitigate-risk
- https://uk.finance.yahoo.com/news/travelex-virus-update-website-attack-virus-when-up-running-normal-data-refunds-115958162.html
- https://www.pymnts.com/news/security-and-risk/2020/uk-police-investigate-travelex-ransomware-attack-ransom-demand/
- https://www.computing.co.uk/news/3084903/travelex-ransomware-attack
- https://www.manchestereveningnews.co.uk/news/uk-news/travelex-cyber-attack-hackers-ransom-17526292

What is the Current Situation of Travelex?

- https://www.itproportal.com/news/travelex-paid-dollar23-million-in-ransom-to-restore-its-systems/
- https://www.bankinfosecurity.com/travelex-paid-23-million-to-ransomware-attackers-report-a-14094
- https://www.pymnts.com/news/security-and-risk/2020/travelex-reportedly-paid-ransom-to-hackers/
- https://financefeeds.com/travelex-reports-services-recovery/
- https://adcg.org/travelex-restores-service-after-six-week-outage/

Continued...

References (cont)

Current Market and Business Issues Travelex is Facing After the Hack Incident

- https://uk.investing.com/news/stock-market-news/travelex-expects-25-million-hit-due-to-ransomware-attack-2062939
- https://www.proactiveinvestors.co.uk/companies/news/914053/finablrs-travelex-takes-25mln-quarterly-hit-from-ransomware-attack-coronavirus-914053.html
- https://www.cbronline.com/news/travelex-owner-finablr
- https://www.reuters.com/article/us-travelex-fin-m-a/forex-firm-travelex-looks-to-sell-itself-amid-troubles-at-parent-company-idUSKCN2242KW
- https://www.nasdaq.com/articles/forex-firm-travelex-looks-to-sell-itself-amid-troubles-at-parent-company-2020-04-22
- https://tools.eurolandir.com/tools/Pressreleases/GetPressRelease/?ID=3711908&lang=en-GB&companycode=ae-fin&v=
- https://financefeeds.com/travelex-says-capable-operating-separately/
- https://www.telegraph.co.uk/business/2020/04/22/travelex-puts-salein-latest-blow-parent-finablr/
- https://www.securitynewspaper.com/2020/03/18/ransomware-attack-has-led-travelex-to-bankruptcy/
- https://www.travelex.co.uk/customer-update

CYBER MANAGEMENT ALLIANCE

info@cm-alliance.com https://cm-alliance.com +44 203 189 1422 @cm_alliance