BlueVoyant

BLUEVOYANT REVIEW

Supply Chain Disruptions and Cyber Security in the Logistics Industry

2021

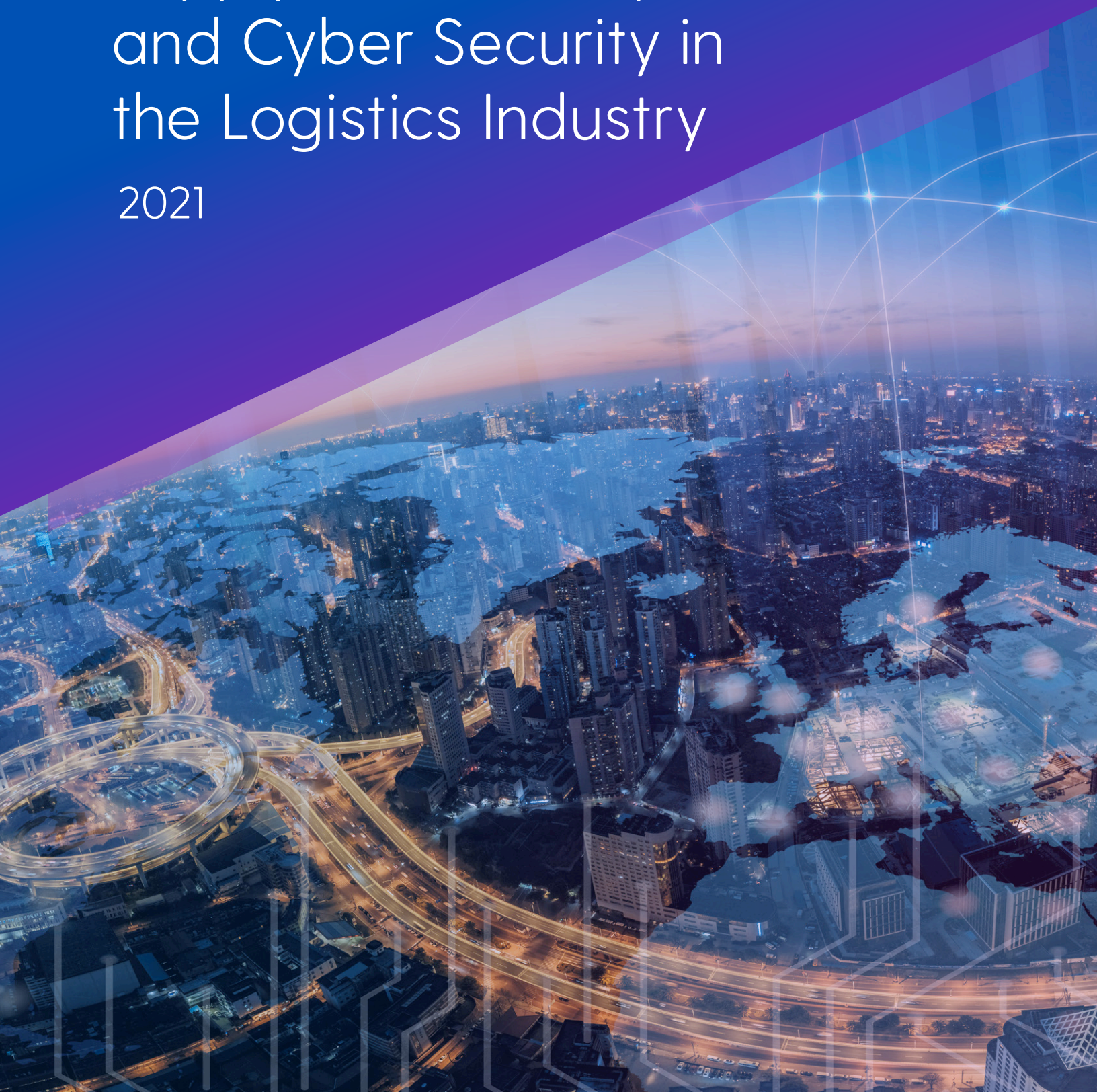


Table of Contents

Introduction

With global health dependent on immediate, safe, and effective vaccine distribution, and with economies operating by the grace of the global shipping sector, **logistics firms are, quite literally, responsible for carrying the world through the current crisis.** With timely operations at a premium, these firms are highly sensitive to disruption and especially vulnerable to ransomware - malware that can bring operations to a standstill and hold companies to hostage until demands are met.

Logistics companies have undergone a tumultuous and transformative year. In the immediate aftermath of COVID-19, air and maritime freight crashed - only to rebound in 2021 as work-from-home economies drove people to ship more necessities and goods directly to their homes. While many major logistics companies are well-known - DHS, FedEx, UPS - the infrastructure supporting this change is a tightly-woven network of many huge, but lesser-known, businesses: logistics software and solutions companies, shipping giants, freight forwarders. Many of these companies are experiencing different rates of rebound[1,2] and capacity[3], just when they are needed most.

The vaccine distribution effort has placed an additional burden and emphasis on the sector. At present, vaccines are shipped by air from manufacturers in Europe to European member states, the U.S., and abroad. Again, the vaccine effort draws in many different partners, including not only logistics solutions providers but also specialized businesses, like AmeriCold, that can manage the 'cold chain' required for preserving vaccine doses in low temperatures. BlueVoyant's previous Report on Biotechnology & Pharma disclosed the aggression and volume of attacks targeting businesses involved in vaccine development.

In order to manage these complicated, high-volume networks, logistics companies are increasingly reliant on highly automated systems[4] that ensure 'just-in-time' delivery across roads, ports, airports, and through rail, air, and maritime freight. These systems make logistics as a sector incredibly vulnerable to cyber attacks. Logistics and cyber security have a history: **the global NotPetya ransomware attack in 2017 famously infiltrated the Danish shipping firm Maersk. The attack froze Maersk's worldwide logistics operations in place and eventually cost the firm between US $250-300 million[5].**

Four years on from NotPetya, and with the logistics of the vaccine supply chain in the global spotlight, BlueVoyant reviewed the cyber security readiness of the logistics sector, asking three questions:

1. How is ransomware affecting the supply chain industry?
2. How prepared are major logistics firms to weather ransomware attacks?
3. What can logistics firms do to succeed despite an aggressive threat landscape?

Others are also taking note:

The Biden administration has signed into effect an Executive Order on Supply Chains[6], **with a focus on securing and bolstering the American supply chain against vulnerability to attack.**

This follows on from a new National Maritime Cyber security Plan[7] to govern shipping. This report, drawn from proprietary and open-source datasets, shows that logistics firms still have a lot to learn from NotPetya. We note our findings, as well as our thoughts on what the sector can do to create a safer future, below.

Key Findings

In light of current concerns over global supply chains, BlueVoyant analysts reviewed the cyber security issues facing the logistics industry. BlueVoyant chose to assess the leading twenty logistics companies by market capitalization in order to assess their vulnerability to ransomware and other disruptive attacks. The following is a summary of our findings:

Ransomware attacks are common and on the rise. Consistent with a spike in ransomware attacks across all sectors[8], reported attacks on shipping and logistics firms tripled between 2019 and 2020. Almost all of these attacks occurred through phishing or exploitation of open remote desktop ports.[9]

Malicious actors are interested in logistics companies. Every company's network saw some evidence of threat targeting.

BlueVoyant's datasets revealed that many of the companies surveyed are vulnerable. Despite the risk from ransomware, most were found to have open remote desktop or administration ports and insufficient email security.

Given that these companies, which make up the bulk of the logistics industry, were vulnerable to key avenues of attack from ransomware - and given that ransomware is the number one threat to logistics companies today - **these findings suggest a situation of imminent and extreme risk.**

Threat Landscape

Cyber Attacks on Supply Chain

A recent study found the Covid-19 pandemic to be the decade's single most disruptive event for global manufacturing supply chains[10]. Even without the pandemic, however, evidence from multiple sources indicates that cyber attacks on supply chain companies are experiencing a precipitous increase; furthermore, much of that activity is driven by ransomware[11,12].

A ransomware attack on a supply chain business can be extremely disruptive. *Wired's* coverage of the 2017 NotPetya incident's consequences for shipping conglomerate Maersk (discussed at greater length below) depicts the issue quite compellingly:

> **...customers faced a set of bleak options: They could try to get their precious cargo onto other ships at premium, last-minute rates, often traveling the equivalent of standby. Or, if their cargo was part of a tight supply chain, like components for a factory, Maersk's outage could mean shelling out for exorbitant air freight delivery or risk stalling manufacturing processes, where a single day of downtime costs hundreds of thousands of dollars. Many of the containers, known as reefers, were electrified and full of perishable goods that required refrigeration. They'd have to be plugged in somewhere or their contents would rot.**[13]

Supply chain disruptions are increasingly common: a recent McKinsey study estimated businesses will, on average, suffer disruptions lasting at least one month every 3.7 years even without an increase in the frequency of malicious cyber activity.[14] A 2020 3D Hubs report revealed that 72% of companies studied have suffered supply chain disruptions due to cyber attacks over the past decade.[15] While a June 2020 survey cited in that report found that only 9% of respondents ranked cyber attacks the top supply chain disruption of the last 10 years, the report also notes that other researchers recorded 290 cyber attacks against supply chain companies in 2019 alone.[16] Other factors could, moreover, increase the frequency of cyber attacks that disrupt supply chains.

Attacks on shipping in particular have been on the rise.

"At present, a series of cyber attacks have plagued the shipping industry. Israeli cyber security company Naval Dome reports that since February this year, **the number of attacks on the shipping industry has soared by 400%**. Over the past three years, cyber attacks against operational technology (OT) systems in the maritime industry have **increased by 900%**, and by the end of this year, the number of reported incidents will reach a record number. Among them, there were **50 major OT attacks reported in 2017, increased to 120 in 2018, more than 310 in 2019, and more than 500 in 2020."**[17]

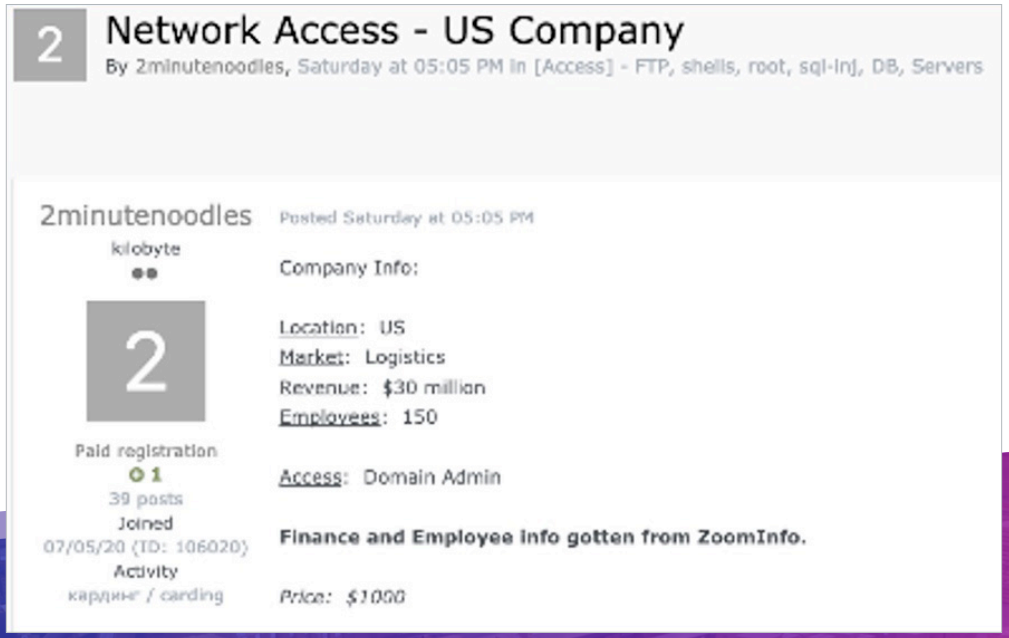
Shipping and logistics is vulnerable as a sector because it is targeted both by nation-state groups as well as cybercriminals. Geopolitical tensions can be disruptive and spark attacks or interference in shipping businesses, such as incidents resulting from issues like Brexit and ongoing US-China trade disputes.[18] The boundary between cyber activity and geopolitical contestation is quite porous and private businesses are often softer targets for such activity than state institutions. NotPetya's rapid spread is a particularly powerful example of this, as the available evidence indicates that threat actors initially deployed NotPetya to target Ukrainian businesses as part of ongoing Russian operations, after which the infection spread more widely than was foreseeable.[19] Although Maersk and other businesses in the logistics sector, including Deutsche Bahn, may have been collateral damage in the particular case of NotPetya, similar activity could presumably have an even more severe impact on supply chains if nation-state actors set out to disable logistics companies specifically. Indeed, some such incidents may already have occurred: Deutsche Bahn also suffered an infection with the WannaCry strain of ransomware, which analysts attribute to the North Korea-linked Lazarus Group, in May 2017.[20] More recently, analysts have attributed a days-long service interruption at Iran's Shahid Raja'i port in May 2020 to an Israeli cyber attack[21] and attacks on shipping businesses in the South China Sea to Chinese hacking groups.[22]

Dark Web

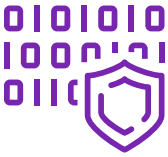
Cybercriminals also attack supply chain and logistics firms for more opportunistic reasons. As an example, BlueVoyant analysts were able to uncover cybercriminals looking for access to shipping and logistics companies - as well as exploits and access to logistics companies for sale.

An Exploit[.]in forum member solicits access to US trucking companies. While Exploit is typically regarded as a top-tier cybercriminal forum, the credibility of this actor may be in question, since their offering price is well below market level. However, this image shows that logistics have been in the cross hairs for a few years now.

In August 2020 a threat actor offered access to a US logistics company, on Exploit[.]in. This posting is demonstrative of the quantity and quality of information threat actors provide when selling accesses. The price, $1000 USD, reflects the lower end of market prices for domain administrator privileges.



On November 11, 2019, “streetskip”, a notorious and prolific seller of hacked corporate accesses, offered access to a US logistics company. This post is also illustrative of the quantity and quality of information provided by threat actors.[23]



STREETSKIP
a prolific seller of hacked corporate accesses

Translated from Russian, this post reads:

продам доступ в логистическую компанию через ГАРАНАТ

страна сша
домен админ.
2980пк
4траста
"доступ в саму компанию"
Revenue: [redacted]
чем занимаются:

Входящая логистика

- *Управление складом*
- *Распределение запасных частей*
- *Распределение готовой продукции*
- *Оптимизация запасов*
- *Консалтинг и поддержка технологии цепочки поставок*
- *Возможности моделирования цепочки поставок / инвентаря*
- *Консалтинговые услуги по цепочке поставок*

hxxps://prnt[.]sc[redacted]

I will sell access to a logistics company through a guarantor

Country: USA
domain admin.
2980pc [personal computers]
4trusts [trusted accounts]
"access to the company itself"
Revenue: [redacted]
what do they do:

Inbound logistics

- *Warehouse management*
- *Distribution of spare parts*
- *Distribution of finished products*
- *Stock optimization*
- *Consulting and support of supply chain technology*
- *Supply chain / inventory modeling capabilities*
- *Supply chain consulting services*

hxxps://prnt[.]sc[redacted]

These are not, strictly speaking, ransomware attacks - access to corporate networks and data in lieu of a monetary demand upfront - though they could be used as an entry points for a ransomware attack. Cybercriminals using this data could also commit a potentially wide range of fraud, attacks, and data breach/theft using the access for sale.

Ransomware

It is undisputed that the largest cyber security threat facing supply chain and logistics companies is neither nation-state attacks nor data breaches for sale on the dark web; it is ransomware.

BlueVoyant analyzed ransomware events targeting logistics-related companies to identify those ransomware families/threat actors, and their respective initial attack vectors, to inform our vulnerability analysis of top logistics companies. The analysis of open-source reporting of ransomware attacks identified a sharp spike in attacks from 2019 to 2020 - which is consistent with other ransomware reporting across other sectors.

The graph shows that ransomware attacks on supply chain companies took place at an average of once every two months until 2020, when the rate of attack tripled to two per month.

These attacks took on different shapes, but shared certain common characteristics. Some ransomware attacks occur without public attribution: disruptions from a February 2019 attack against warehousing and logistics company Container World with an unidentified strain of ransomware continued for weeks following the initial incident.[24]

Threat actors have mounted two ransomware attacks against logistics and shipping technology company Pitney Bowes in the last 3 years. In October 2019, an infection with the Ryuk strain of ransomware caused an outage that prevented clients from using a number of its services.[25] In May 2020, data from Pitney Bowes appeared on the Maze ransomware operation's data leak site; Pitney Bowes claimed to have disrupted that attack before encryption could take place, although the leak indicates threat actors had already stolen some data prior to detection.[26]

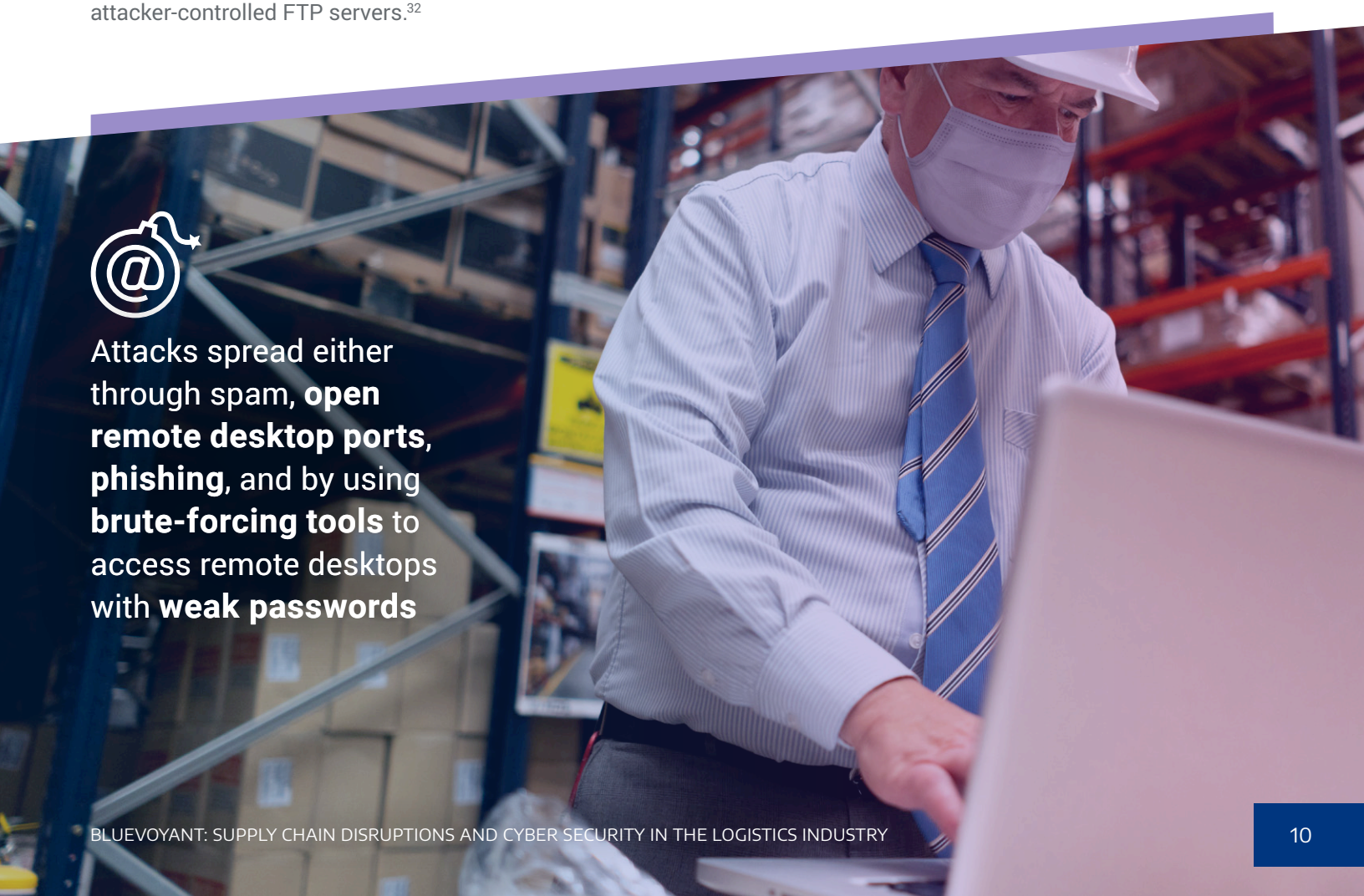
Ryuk targets enterprise environments; researchers attribute it to the WIZARD SPIDER threat actor group and have observed it spreading both in independent spam campaigns and through the TrickBot malware. TrickBot itself spreads mainly through spam, though it can also spread laterally using EternalBlue after an initial infection.[27]

Research indicates that a number of different groups distribute Maze and spread it both through spam and exploit kits.[28] Analysts have observed threat actors distributing these exploit kits through a site impersonating a cryptocurrency app, and at least one phishing campaign distributed it while impersonating American and European government agencies.[29] Other groups spreading Maze have used compromised email accounts from within target organizations or by impersonating delivery and phone services.[30] Upon infecting one victim system, Maze spreads laterally using a variety of tools, including Cobalt Strike Beacon, RDP, Metasploit, and EternalBlue.[31] After spreading across a network, Maze exfiltrates victim data to attacker-controlled FTP servers.[32]

In early February 2020, shipping company Toll Group announced that it had stopped its deliveries because of an infection with the Netwalker strain of ransomware.[33] Delays resulting from this infection persisted for at least 18 days after its initial announcement.[34] The available artifacts led analysts to suggest that **Netwalker spreads both through phishing and by using brute-forcing tools to access remote desktops with weak passwords**.[35]

Toll Group fell victim to a second ransomware infection in May 2020, as the operators of the Nefilim strain of ransomware published data exfiltrated prior to the encryption of Toll Group's systems. Like other current strains of enterprise ransomware, it most likely spreads through exposed remote desktops.[36]

Because the strains of ransomware involved in the **attacks discussed above have spread either through spam or open remote desktop ports,** analysts attended particularly closely to these points of entry when scrutinizing BlueVoyant datasets.



Attacks spread either through spam, **open remote desktop ports**, **phishing**, and by using **brute-forcing tools** to access remote desktops with **weak passwords**

Threat Intelligence Findings

BlueVoyant uses proprietary and third-party data to assess cyber security risk: to identify vulnerabilities, to find and to surveil threat activity, and to monitor for potential compromises. By applying the analysis of ransomware above, and by identifying specific threat vectors that ransomware groups persistently use - i.e., phishing campaigns and exploiting exposed remote desk top ports - BlueVoyant looked for persistent areas of risk. BlueVoyant also analyzed observed threat traffic, looking for indications of threat targeting and then breaking down any observed threats into useful categories.

By selecting the twenty leading logistics companies by market capitalization, the analysis should cover issues that addresses the industry as a whole: the logistics industry is quite concentrated.

Findings: Threat Targeting

BlueVoyant observed threat targeting for every one of the twenty observed companies. These threats were broken down into different categories:

16 OF 20

***Companies** that had evidence of brute force attacks*

14 OF 20

***Companies** that had targeted attacks using proxy networks*

20 OF 20

***Companies** that had traffic coming from known botnets*

All companies with an online presence have some measure of malicious traffic. Much of that traffic – e.g., programmatic botnet traffic – is not especially targeted or sophisticated. Typically, evidence of brute force attacks and the use of proxy servers suggests more intentional targeting. Here, the large percentage of such traffic suggests that threat actors recognize supply chain companies as a high-value targets.

"Threat actors recognize **supply chain companies** as a high-value targets."

Findings: Potential Compromise

BlueVoyant also looked for evidence of the target companies' infrastructure attempting to communicate with known malicious domains and IP addresses. Traffic from a company to a malicious IP or domain is sometimes simply evidence of security software conducting routine reconnaissance of suspicious domains and IPs. However, it can also be suggestive of compromise: a network or device is reaching out to a malicious command & control (C&C) server.

BlueVoyant Findings Indicate

10 OF 20

***Companies** observed generating traffic to blocklisted/denylisted assets*

7 OF THOSE 10

***Reached out** to assets blocklisted as suspicious infrastructure*

1 OF THOSE 10

***Generated traffic** to assets associated with ransomware*

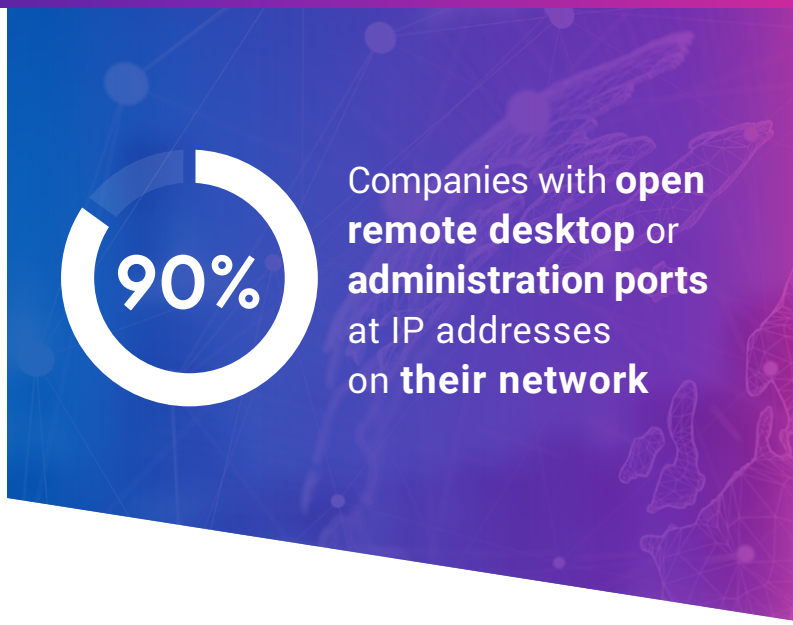
IT Hygiene and Email Security

This analysis was the most important. For the purposes of this report, the threat targeting analysis can only confirm that threat targeting occurred - not that it was successful. Similarly, compromise evidence is concerning, but not conclusive. However, vulnerability analysis is not only conclusive, but also highly informative. Are logistics companies hardened against attack? Are they aware of and prepared against typical threat tactics by ransomware groups? **More specifically, are they focused on email and port security?**

BlueVoyant's analysis of IP space data associated with the logistics companies it studied identified exposures and other vulnerability issues in company infrastructure, including operating systems, server software, patch cadence and authentication methods.

This analysis suggests that most companies are vulnerable. BlueVoyant analysts found that 90% of the leading companies studied had open remote desktop or administration ports at IP addresses on their network. Many of the ransomware strains that have infected logistics companies in the recent past access victim systems through desktop ports, which suggests that the same threat actors could infect the companies BlueVoyant studied, should their operators so choose.

Similarly, the majority of the companies studied appeared to have some issues with their email security. Analysts looked for basic DNS-based email security protocols that protect against phishing and spoofing attacks. There are three methods BlueVoyant investigates in order to assess email security: Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication Report and Conformance (DMARC). SPF is an email validation protocol designed to detect and block email spoofing by allowing receiving mail exchangers to verify that incoming mail comes from an authorized sender.



DKIM is an email authentication method designed to detect and prevent email spoofing by using digital signatures. DMARC is built on the other two protocols and works to filter out spoofed emails that might otherwise evade SPF or DKIM protection.

Findings indicate that domains belonging to 14 of 20 companies lacked an SPF record and at least one domain belonging to most companies lacked DMARC and DKIM records.

14 OF 20

***Companies** have domains that lack an SPF record*

Finally, BlueVoyant's device data found 16 of 20 companies to have devices running unsupported software on their networks and half of the companies studied appeared to be running software with high-severity vulnerabilities on their servers.

16 OF 20

***Companies** with devices running unsupported software on their networks*

Such vulnerabilities could present opportunities for malicious actors of all stripes to exploit outdated software, especially bearing in mind that IT management issues appear to have had a hand in NotPetya's infection of Maersk's systems.

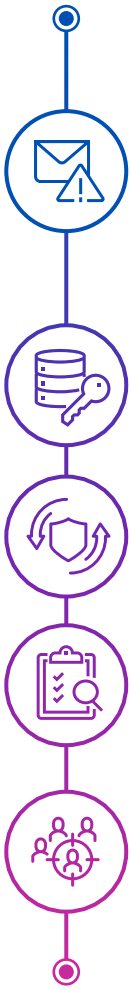
Conclusion

Across all sectors, ransomware **attacks are on the rise** – and both BlueVoyant analysis and external sources indicate that **shipping and logistics are facing a steeply rising threat.**

NotPetya was an especially damaging case, and subsequent coverage of Maersk's experience has implied that it was spectacular enough to serve as a wake-up call for the logistics industry. More than three years later, the sector remains vulnerable to malicious cyber activity, and especially and specifically vulnerable to ransomware attacks.

Unfortunately, these wide-spread vulnerabilities are still unaddressed in a time of increased scrutiny and reliance on supply chains — as countries wait for efficient and safe vaccine distribution programs, and as entire work-from-home economies rely on global shipping more than ever.

This also comes at a time of surging ransomware campaigns. Across all sectors, ransomware attacks are on the rise - and both BlueVoyant analysis and external sources indicate that shipping and logistics are facing a steeply rising threat. Given the sensitivity of distribution networks to disruption, the global reliance on supply chain firms and the lingering warning of the NotPetya attack, many members of the supply chain sector should be readier than they are.



There are a number of steps the supply chain sector should take to improve their operational preparedness.

1. Secure email services and mailservers against phishing and spoofing. Supply chain companies can use email services to help implement basic security protocols. They can also deprecate unused mailservers and enforce simple, standardized email security training and awareness programs so that employees all recognize the dangers and the signs of phishing attempts.

2. Secure port and network configurations. Ransomware attackers are not exactly hiding their attack vectors - time and again, when phishing attacks fail, they exploit unsecured remote desktop and remote administration ports. Securing these ports is a simple and important step to removing one major avenue of threat.

3. Update and patch software. These are simple steps that help mitigate risk of exposure to new (or old) CVEs, which threat actors can use to exploit networks.

4. Be aware of regulations. New OFAC regulations, announced in 2020, stipulate that ransomware payments made to "specially designated nationals" - often specific foreign ransomware gangs - can incur penalties. In some cases, these restrictions even apply to entering negotiation.

5. Consider advanced threat detection products or managed security services. Ransomware gangs are well-known and cyber security researchers obsessively document and share relevant indicators of compromise (IOCs) and knowledge about their tactics, techniques, and procedures (TTPs). Utilizing advanced security services will help to protect against a multi-faceted and evolving body of threats.

SOURCES

1 https://www.freightos.com/freight-resources/coronavirus-updates

2 https://unctad.org/news/covid-19-cuts-global-maritime-trade-transforms-industry

3 https://www.accenture.com/us-en/insights/travel/coronavirus-air-cargo-capacity

4 https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/automation-in-logistics-big-opportunity-bigger-uncertainty#

5 https://investor.maersk.com/news-releases/news-release-details/annual-report-2017

6 https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/24/remarks-by-president-biden-at-signing-of-an-executive-order-on-supply-chains

7 https://www.hsdl.org/?abstract&did=848704

8 https://www.zdnet.com/article/ransomware-huge-rise-in-attacks-this-year-as-cyber-criminals-hunt-bigger-pay-days

9 https://www.acronis.com/en-us/articles/ransomware-logistics

10 https://www.3dhubs.com/get/supply-chain-resilience-report/

11 https://www.intelligencefusion.co.uk/insights/resources/intelligence-reports/the-rising-risk-of-cyber-attacks-on-logistics-and-transport/

12 https://www.reutersevents.com/supplychain/supply-chain/shipping-industry-hit-multiple-cyber-attacks 13 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

14 https://www.mckinsey.com/business-functions/operations/our-insights/risk-resilience-and-rebalancing-in-global-value-chains?cid=other-soc-twi-mip-mck-oth-–&sid=3559905540&linkId=96607824

15 3D Hubs, "Supply Chain Resilience Report: Industry Trends and Supply Chain Strategy for Manufacturing," 2020. p. 2

16 Ibid. p. 12

17 https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years

18 Ibid. p. 15

19 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

20 https://www.forbes.com/sites/oliverwyman/2017/06/28/time-for-transportation-logistics-to-up-its-cybersecurity-as-hackers-put-it-on-target-list/#3df6e4bb6fb9; https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html;

21 https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

22 https://thediplomat.com/2019/08/the-cyber-dimension-of-the-south-china-sea-clashes

23 hxxps://exploitinqx4sjro[.]onion/topic/164146

24 https://globalnews.ca/news/5045899/container-world-hack

25 https://www.bleepingcomputer.com/news/security/global-shipping-firm-pitney-bowes-affected-by-ransomware-attack

26 https://www.bleepingcomputer.com/news/security/maze-ransomware-fails-to-encrypt-pitney-bowes-steals-files

27 https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/; https://blog.malwarebytes.com/detections/trojan-trickbot

28 https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html

29 https://www.bleepingcomputer.com/news/security/maze-ransomware-says-computer-type-determines-ransom-amount/; https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us

30 https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html

31 https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html

32 https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html

33 https://www.bleepingcomputer.com/news/security/new-ransomware-strain-halts-toll-group-deliveries

34 https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12309205

35 https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor

36 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nefilim-ransomware-threatens-to-expose-stolen-data

37 https://www.researchandmarkets.com/reports/5119392/freight-and-logistics-market-growth-trends?utm_source=CI&utm_medium=PressRelease&utm_code=573mr4&utm_campaign=1448044+-+Global+Freight+and+Logistics+Market+Report+2020%3a+Top+5+Companies+Command+More+than+50%25+Market+Share+-+Forecast+to+2025&utm_exec=chdo54prd

About BlueVoyant

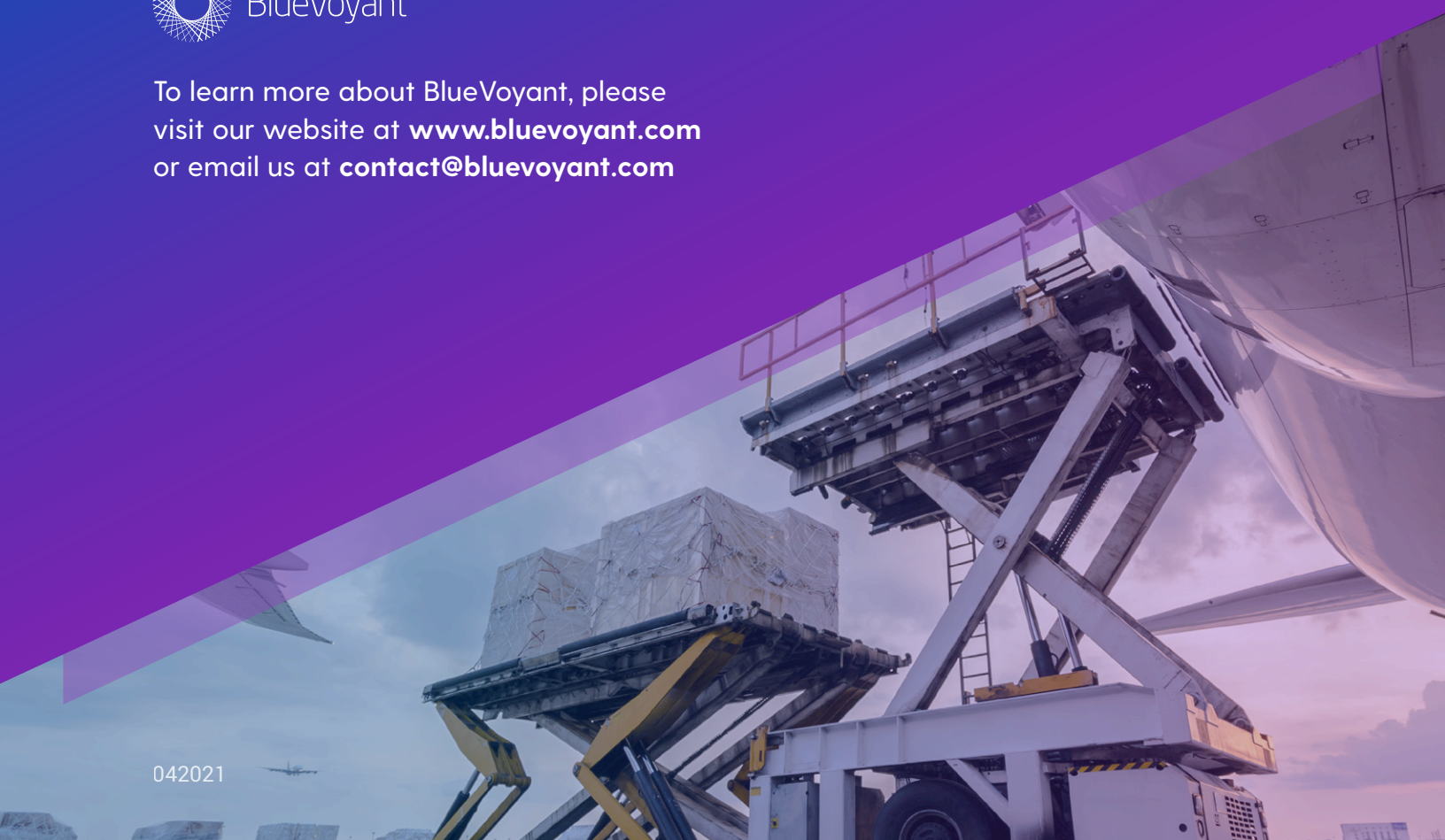
BlueVoyant is an expert-driven cyber security services company whose mission is to proactively defend organizations of all sizes against today's constant, sophisticated attackers, and advanced threats.

Led by CEO, Jim Rosenthal, BlueVoyant's highly skilled team includes former government cyber officials with extensive frontline experience in responding to advanced cyber threats on behalf of the National Security Agency, Federal Bureau of Investigation, Unit 8200 and GCHQ, together with private sector experts. BlueVoyant services utilize large real-time datasets with industry leading analytics and technologies.

Founded in 2017 by Fortune 500 executives, including Executive Chairman, Tom Glocer, and former Government cyber officials, BlueVoyant is headquartered in New York City and has offices in Maryland, Tel Aviv, San Francisco, Manila, Toronto, London, Latin America and Budapest.

BlueVoyant®

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**



042021