

# IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain

 [securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/](https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/)



[Home](#) &nbsp; [Government](#)

IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain



[Government](#) December 3, 2020

By [Claire Zaboeva](#) co-authored by [Melissa Frydrych](#) 6 min read

At the onset of the COVID-19 pandemic, IBM Security [X-Force](#) created a threat intelligence task force dedicated to tracking down COVID-19 cyber threats against organizations that are keeping the vaccine supply chain moving. As part of these efforts, our team recently uncovered a global phishing campaign targeting organizations associated with a COVID-19 cold chain. The cold chain is a component of the vaccine supply chain that ensures the safe preservation of vaccines in temperature-controlled environments during their storage and transportation.

Our analysis indicates that this calculated operation started in September 2020. The COVID-19 phishing campaign spanned across six countries and targeted organizations likely associated with Gavi, The Vaccine Alliance's [Cold Chain Equipment Optimization Platform \(CCEOP\) program](#), which we explain further in this blog. While firm attribution could not be established for this campaign, the precision targeting of executives and key global organizations hold the potential hallmarks of nation-state tradecraft.

Some details from IBM Security X-Force's analysis of this activity include:

- **The Cover Story** — The adversary impersonated a business executive from Haier Biomedical, a credible and legitimate member company of the COVID-19 vaccine supply chain and qualified supplier for the CCEOP program. The company is purportedly the world's only complete cold chain provider. Disguised as this employee, the adversary sent phishing emails to organizations believed to be providers of material support to meet transportation needs within the COVID-19 cold chain. We assess that the purpose of this COVID-19 phishing campaign may have been to harvest credentials, possibly to gain future unauthorized access to corporate networks and sensitive information relating to the COVID-19 vaccine distribution.
- **The Targets** — The targets included the European Commission's Directorate-General for Taxation and Customs Union, as well as organizations within the energy, manufacturing, website creation and software and internet security solutions sectors. These are global organizations headquartered in Germany, Italy, South Korea, Czech Republic, greater Europe and Taiwan.
- **The How** — Spear-phishing emails were sent to select executives in sales, procurement, information technology and finance positions, likely involved in company efforts to support a vaccine cold chain. We also identified instances where this activity extended organization-wide to include help and support pages of targeted organizations.

IBM Security X-Force has followed responsible disclosure protocols and notified the appropriate entities and authorities about this targeted operation.

## Alert for the COVID-19 Supply Chain

---

IBM Security X-Force urges companies in the COVID-19 supply chain — from research of therapies, healthcare delivery to distribution of a vaccine — to be vigilant and remain on high alert during this time. Governments have already warned that foreign entities are likely to attempt to conduct cyber espionage to steal information about vaccines. Today, in conjunction with this blog, DHS CISA is issuing an alert encouraging organizations associated with the storage and transport of a vaccine to review this research and recommended best practices to remain vigilant.

## **Calculated Spoofing to Compromise the COVID-19 Cold Chain**

---

IBM Security X-Force uncovered targets across multiple industries, governments and global partners that support the CCEOP program. The CCEOP was launched by Gavi, The Vaccine Alliance along with the United Nations Children Fund (UNICEF) and other partners in 2015. Its objective is to ultimately strengthen vaccine supply chains, optimize immunization equity and ensure an agile medical response to outbreaks of infectious diseases. Various classes of medication, and especially vaccines, require storage and transport in temperature-controlled environments to ensure their safe preservation.

The CCEOP initiative is naturally accelerating efforts to facilitate the distribution of a COVID-19 vaccine. A breach within any part of this global alliance could result in the exposure of numerous partner computing environments worldwide.

The spoofed phishing emails appear to originate from a business executive from Haier Biomedical, a Chinese company currently acting as a qualified supplier for the CCEOP program, in coordination with the World Health Organization (WHO), UNICEF and other U.N. agencies. It is highly likely that the adversary strategically chose to impersonate Haier Biomedical because it is purported to be the world's only complete cold chain provider. Likewise, the Haier Biomedical employee who is purported to be sending these emails would likely be associated with Haier Biomedical's cold chain distribution operations based on his role, which is listed in the email signature block.

It's unclear from our analysis if the COVID-19 phishing campaign was successful. However, the established role that Haier Biomedical currently plays in vaccine transport, and their likely role in COVID-19 vaccine distribution, increases the probability the intended targets may engage with the inbound emails without questioning the sender's authenticity.

## **Credential Harvesting for Wider Access**

---

The subject of the phishing emails posed as requests for quotations (RFQ) related to the CCEOP program. The emails contain malicious HTML attachments that open locally, prompting recipients to enter their credentials to view the file. This phishing technique helps attackers avoid setting up phishing pages online that can be discovered and taken down by security research teams and law enforcement.

We assess that the purpose of this campaign may have been to harvest credentials to gain future unauthorized access. From there, the adversary could gain insight into internal communications, as well as the process, methods and plans to distribute a COVID-19 vaccine. This includes information regarding infrastructure that governments intend to use to distribute a vaccine to the vendors that will be supplying it. However, beyond critical information pertaining to the COVID-19 vaccine, the adversary's access could extend deeper into victim environments. Moving laterally through networks and remaining there in stealth would allow them to conduct cyber espionage and collect additional confidential information from the victim environments for future operations.

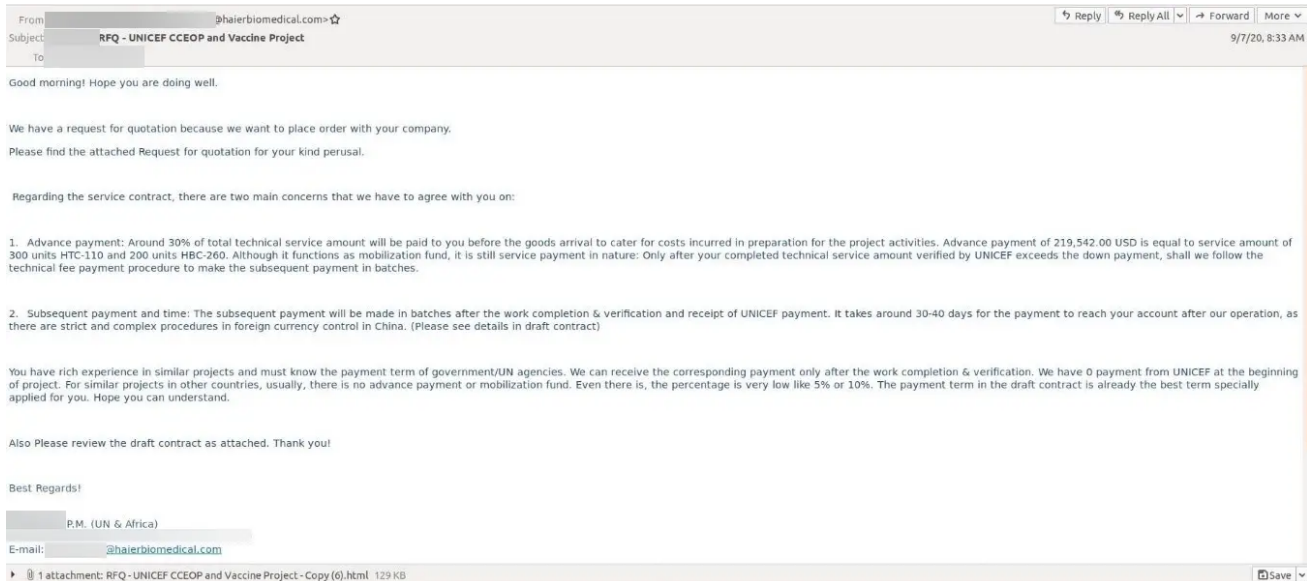


Figure 1: Phishing email sent to executives in organizations related to the COVID-19 vaccine supply chain.

## Global Targeting

Given the specialization and global distribution of organizations targeted in this campaign, it's highly likely that the adversary is intimately aware of critical components and participants of the cold chain.

- **European Commission's Directorate-General for Taxation and Customs Union** — The Directorate-General is responsible for promoting cooperation on customs and tax matters across the EU. It maintains direct ties to multiple national government networks and is associated with trade and regulation. Targeting this entity could serve as a single point of compromise impacting multiple high-value targets across the 27 member states of the European Union and beyond.

- **Energy Sector** — Spear phishing targets included companies involved in manufacturing solar panels. One of the ways that vaccines are kept cold in countries where reliable power is not possible is by using vaccine refrigerators powered by solar panels. A compromise of such technologies could result in intellectual property theft or stealing and selling vaccine shipping containers in black markets across the globe. Targeting also included companies associated with petrochemicals. Among the key components of cold chain is the use of dry ice, which is a byproduct of petroleum production.
- **IT Sector** — Amongst the targets were a South Korean software development firm and a German website development company. The latter supports multiple clients associated with pharmaceutical manufacturers, container transport, biotechnology and manufacturers of electrical components enabling sea, land and air navigation and communications.

## Who is Likely Behind These Attacks?

---

While attribution is currently unknown, the precision targeting and nature of the specific targeted organizations potentially point to nation-state activity. Without a clear path to a cash-out, cyber criminals are unlikely to devote the time and resources required to execute such a calculated operation with so many interlinked and globally distributed targets. Likewise, insight into the transport of a vaccine may present a hot black-market commodity, however, advanced insight into the purchase and movement of a vaccine that can impact life and the global economy is likely a high-value and high-priority nation-state target.

Earlier in 2020, IBM Security X-Force uncovered activity surrounding the targeting of [a global COVID-19 PPE supply chain](#). Similarly, as the global competition races for a vaccine, it is highly likely the cold chain is a compelling target that will be at the top of the lists of national collection requirements worldwide.

## Recommendations to Defenders

---

IBM Security X-Force stands ready to host the COVID-19 supply chain community on our [Enterprise Intelligence Management](#) platform, where they can share threat information and take action on the latest threat intelligence. The following are recommendations for organizations to increase their cyber readiness amidst the developments outlined in this blog:

- **Create and test incident response plans** to strengthen your organization's preparedness and readiness to respond in the event of an attack.

- **Share and ingest threat intelligence.** Threat-sharing initiatives and partnerships are essential to staying alert about the latest threats and attack tactics impacting your industry. IBM Security X-Force has been feeding this threat intelligence into the COVID-19 threat sharing enclave. At the onset of the pandemic, IBM made this enclave freely accessible to any organization in need of more eyes on cyber threats.
- **Assess your third-party ecosystem** and assess potential risks introduced by third-party partners. Confirm you have robust monitoring, access controls and security standards in place that third-party partners need to abide by.
- **Apply a zero-trust approach to your security strategy.** As environments continue to expand, managing privilege access becomes paramount to ensuring that users are only granted access to the data that is essential to their job.
- **Use Multifactor Authentication (MFA) across your organization.** MFA works as a fail-safe if a malicious actor has gained access to your credentials. As a last line of defense, MFA offers a second form of verification requirement in order to access an account.
- **Conduct regular email security educational trainings** so employees remain on alert about phishing tactics and are familiar with [email security best practices](#).
- **Use Endpoint Protection and Response** tools to more readily detect and prevent threats from spreading across the organization.

If your organization requires immediate assistance with incident response, please contact IBM Security X-Force's US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034 Learn more about X-Force's [threat intelligence](#) and [incident response services](#).

## Indicators of Compromise (IOCs)

---

### Malicious HTML Files: RFQ – UNICEF CCEOP and Vaccine Project – Copy (#).html

---

SHA256 Hashes

d32b4793e4d99bb2f9d4961a52aee44bbdba223699075ed40f6a6081e9f1e6b4

ace86e8f5d031968d0c9319081a69fa66ce798e25ec6bbd23720ee570651aa04

7f53eca4a3e083ad28c8d02862bc84c00c3c73a9d8b7082b7995f150713d4c51

e3de643f3acebf1696a2b275f4ab1d0bacb5a8ba466ee8edbaaffaaa44cd2f10

a8c42db5ccddbde5b17ce3545189329a33acfd4a8b9aff0c7e4294709b60af6

07dbe854a34e61349adcc97dd3e2eb5a9158e02568bae3e2aae3859aeeb5b8a9

7898d4596b6125129698866dbfa1a71d069aee3fd84ecb43343c3bf377a7abe2

---

---

7fc47e4fdce42b032b8ad0438cb5c76ed42a36d8c6a3e16d42dd0b69f49f33bd

---

83f8934fadccbaaa8119cd542382fbb9b97dfd196ef787b746ccaaf11f1d444e

---

6126052b0b200e04ce83a3fa470efee6ba82882674ebcc46c326b0a6c7fbfab4

---

75768be2e98b8010256f519a19a2a47d8983686389b2eeab300aca063b229be5

---

b98984a7bf669518b074ef1c8fc4240e4ad6f4a2ccc80a7940a0b56150809e37

---

33c44f32de3153d7705371c4a0c8d695a4e4eb22b4c4f2f3bda519631efb09af

---

a90056d8d0853f54dec3c8738fbcea6185f87aae6102cff2c0e1def49ccde977

---

68f4e8b58367ae1d0f8c392b43f459b1d942faf979953233a104cd74944b88f4

---

0ec6a1a0b353c672307220fe69ca4c3be6e516505e1f16b5bb8f3b55adaa0c0e

---

61e7f48f41414d3c945b7317023ca27e5d3f011b0a2e16354641748cc0f9df8e

---

0ac984f340a2903228b17e28c3a0f4507f5fc780bfe6505f196d2b92feccfab8

---

9143c2499a1cb2fb4e86ba6f9552f752358d8c8b635376aa619305431a3eec50

---

49468e2cbaab71a1035f45ef1d4a7cd791e2d5c2bbbfc9d29249d64f40be9aa4

---

8dc052382d626a2b1fb9181bdc276858386098e1919276c682a0a2b397dab80b

---

61bae857955c5cabf20119a918a0ebd83cbe9a34ebc6ee628144d225ab0867df

---

93643badb18f8dccba1eae3d0a44e8a91d4646cb4d1d4b61e234bf7edc58969c

---

c22ec0725f45221e477c9966a32b8faadd3e320c278043e57252903be89664cc

---

d5cd18bd27b7525d5e240d5dca555844ec721f8f4be224b91c047b827b7e5529

---

3e6b7d3055b50c2fd65231d1f757e3f0a6a1dbd803601d2e4223ace4d2bc1198

---

d32b4793e4d99bb2f9d4961a52aee44bbdba223699075ed40f6a6081e9f1e6b4

---

28511c50efe2fc02f7a437864e48f8c2983637507c2f8d8773e32ed9a420c895

## C2 URLs

---

hxxps://e-mailer.cf/next[.]php

hxxps://e-mailer.ga/next[.]php

hxxps://nwa-oma2.ml/next[.]php

hxxps://routermanager.ga/next[.]php

hxxps://routermanager.gq/next[.]php  
hxxps://routermanager.ml/next[.]php  
hxxps://routermanagers.cf/next[.]php  
hxxps://routermanagers.ga/next[.]php  
hxxps://routermanagers.gq/next[.]php  
hxxps://routermanagers.ml/next[.]php  
hxxps://serverrouter.cf/next[.]php  
hxxps://serverrouter.ga/next[.]php  
hxxps://serversrouter.cf/next[.]php  
hxxps://serversrouter.gq/next[.]php  
hxxps://nwa-oma.ml/next[.]php

### **Sender Email Addresses**

---

[[email protected](#)][.]com

DNS SOA Addresses

rahim[[@](#)]protonmail[.]com

kilode[[@](#)]cock.li.

### **Additional Related URLs**

---

hxxps://mailerdaemon[.]cf

hxxps://mailerdaemon[.]ga

hxxps://mailerdaemon[.]gq

hxxps://mailerdaemon[.]ml

hxxps://mailerdaemon[.]tk

hxxps://routermanager[.]tk

hxxps://routermanagers[.]tk

hxxps://serverrouter[.]tk

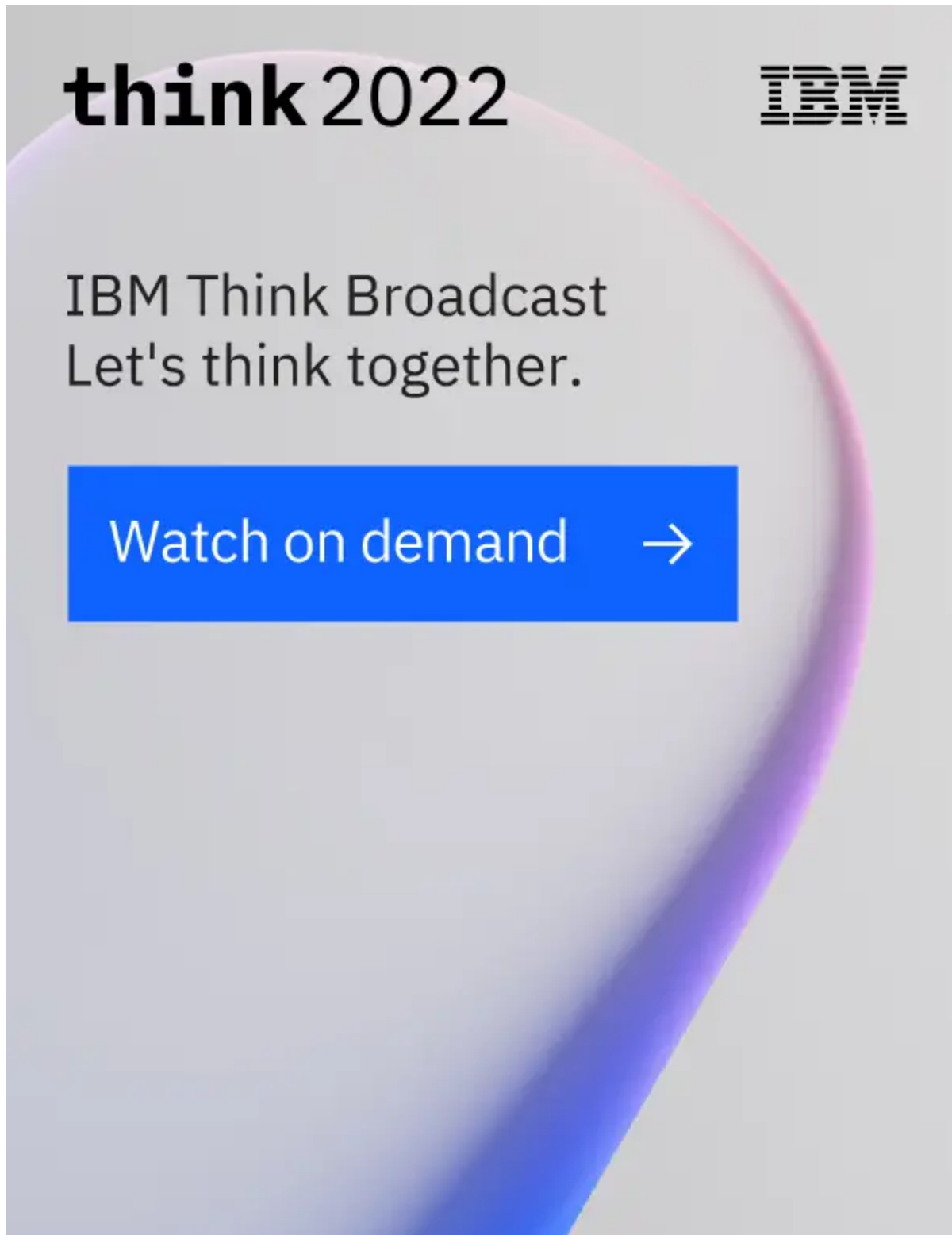


Register for the webinar: “New Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain”

Claire Zaboeva

Senior Strategic Cyber Threat Analyst, IBM

Claire is a Senior Strategic Cyber Threat Analyst on the Threat Hunt & Discovery Team within IBM X-Force. Claire has over 10 years of analytic experience...

The graphic features a light gray background with a large, curved, multi-colored shape on the right side that transitions from pink at the top to purple at the bottom. The text is positioned on the left side of this shape.

**think 2022** **IBM**

IBM Think Broadcast  
Let's think together.

Watch on demand →

