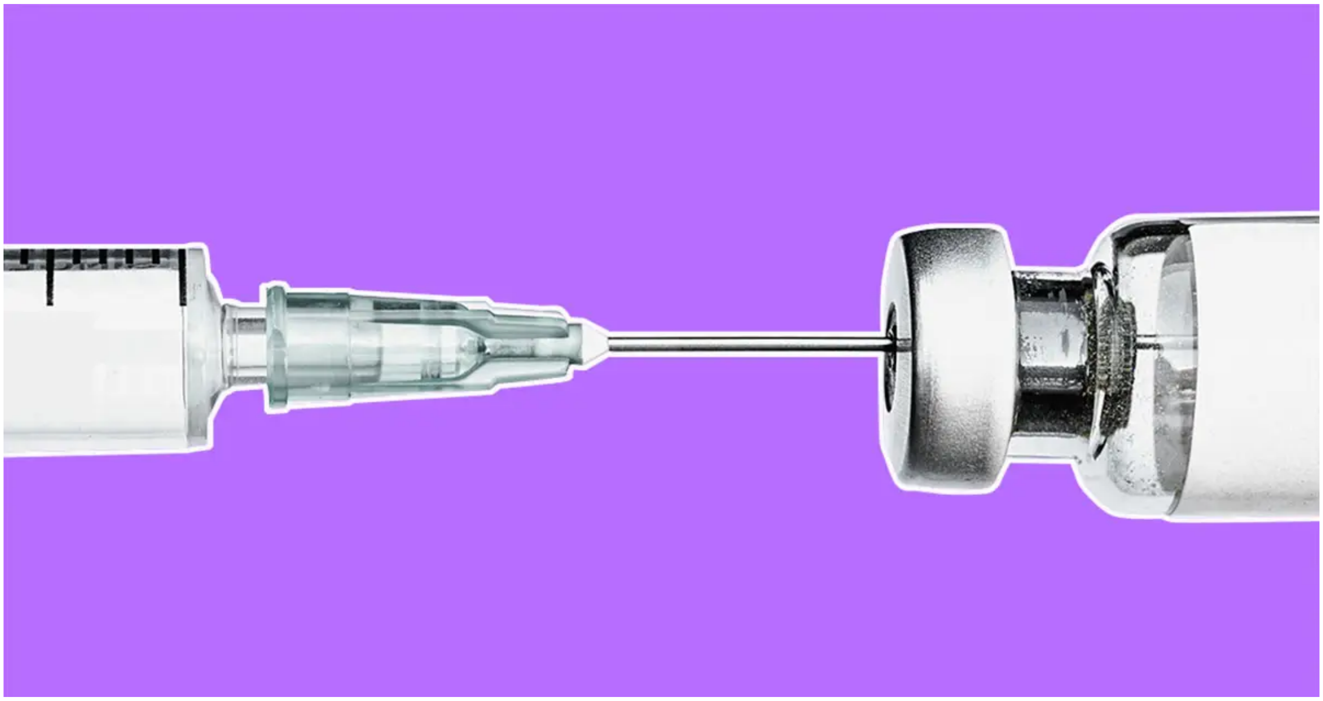
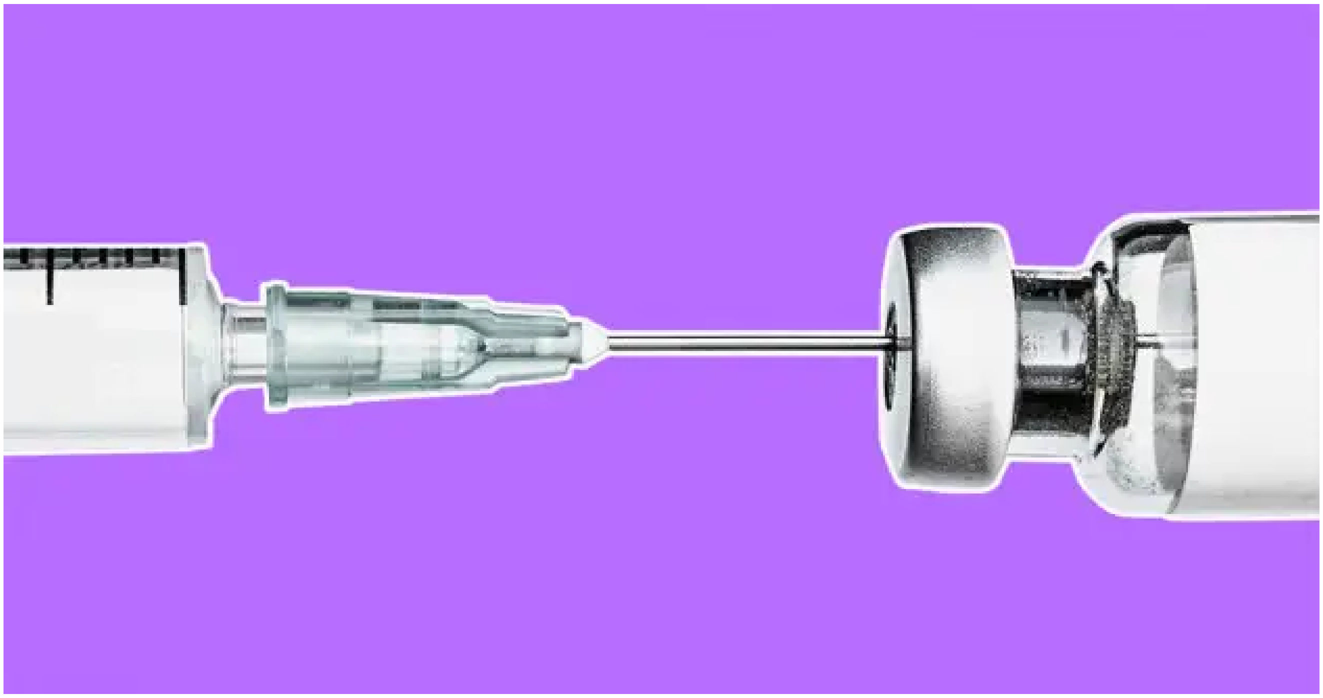
The COVID-19 Vaccine's Global Cold Chain Continues to Be a Target

securityintelligence.com/posts/covid-19-vaccine-global-cold-chain-security/



Home&nbsp/ Security Services

An Update: The COVID-19 Vaccine’s Global Cold Chain Continues to Be a Target



Security Services April 14, 2021

By Melissa Frydrych co-authored by Claire Zaboeva 5 min read

In December 2020, IBM Security X-Force released a research blog disclosing that the COVID-19 cold chain — an integral part of delivering and storing COVID-19 vaccines at safe temperatures — was targeted by cyber adversaries. After that first report, we recently discovered an additional 50 files tied to spear-phishing emails that targeted 44 companies in 14 countries in Europe, North America, South America, Africa and Asia.

The expanded scope of precision targeting includes key organizations likely underpinning the transport, warehousing, storage and ultimate distribution of vaccines. Spear-phishing attempts were associated with multiple executive activities and other roles, including:

Chief Executive Officers	Global Sales Officers	Purchasing Managers
Company Presidents	System Administrators	Sales Representatives
Directors of Finance	Export Sales Managers	Human Resource Officers
Heads of Marketing & Communication	Heads of Supply & Logistics	Heads of Plant Engineering

The campaign impersonates an executive from Haier Biomedical, a major Chinese biomedical company that is purported to be the world's only complete cold chain provider. The updated findings were made available via our Enterprise Intelligence Management platform TruSTAR in January 2021. In the same timeframe, X-Force reached out to relevant CERTS and global entities in concert with our responsible disclosure policy.

Email Significance

Exploring the available emails, X-Force uncovered multiple features which likely signal the actor's exceptional knowledge of the cold chain. While our previous reporting featured direct targeting of supranational organizations, the energy and IT sectors across six nations, we believe this expansion to be consistent with the established attack pattern, and the campaign remains a deliberate and calculated threat.

- The uncovered emails were sent between Sept. 7-9, several months in advance of the approval of any COVID-19 vaccine variant, which indicates the attacker was prepositioning in emerging global infrastructure.
- Both the email subject and contents discuss requests for quotes regarding the Cold Chain Equipment Optimization Platform (CCEOP) program and contain references to specific products (a specific solar-powered vaccine refrigerator and ice-lined refrigerator) from Haier Biomedical's product line to store and transport vaccines at the same temperatures of the COVID-19 vaccine.

- The related HTML files mention organizations involved in the manufacturing of solar panels, as well as petrochemical production (dry ice as a primary byproduct), which directly aligns with the aforementioned products.
- The English language in the email aligns with the educational background of the sender spoofed in the signature block.

Overlapping Infrastructure

Directly following our December publication, X-Force uncovered an additional spear-phishing email, remarkably similar to the original samples we found. The email was addressed to a German pharmaceutical and bioscience solutions company involved in vaccine production, among other specialties, who appears to be a client of one of the original targets we uncovered. This context to the initial targeted email prompted further investigation.

The connections between the previous and the new files we found feature overlapping command-and-control (C2) infrastructure, and appear to display the same blurred PDF with a login screen prepopulated with the user's email address as the ID. Once a user ID and password are keyed in, the credentials are sent to a C2 server. X-Force assesses that this activity is aimed at obtaining user credentials for future or secondary attacks.

Most Targeted Industries

The potential targets, categorized into most targeted industries, may present various avenues into the overall COVID-19 supply chain. They include:

Transportation — X-Force research suggests at least eight unique organizations within the automotive, aviation, maritime and transport services sectors across Italy, Korea, Japan, Colombia and the United States may have been targeted.

Health care — Our findings indicate likely targets include organizations associated with biomedical research, medical manufacturing, pharmaceuticals and hygiene services and headquartered in the Czech Republic, Germany and U.S. The corporations specialize in a variety of disciplines including immunology, manufacturing of medical accessories, construction of surgical materials, the creation of pharmaceutical ingredients and online pharmacies distributing COVID-19 rapid tests.

Information Technology & Electronics — A total of six organizations across Bulgaria, France, Poland, Ukraine and the U.S. associated with web-hosting services, software development, IT operations and outsourcing and online platform providers were subject to activity. Collection against these organizations could provide actors with insight into key technical requirements concerning the cold chain and vaccine storage.

In addition to the sectors detailed above, notable clusters of uncovered email addresses were found to be associated with government organizations, as well as refrigeration and metal manufacturing technology. X-Force uncovered likely instances of activity directed against government ministries and departments in Europe, specifically supporting import/export of special goods, transport and public health and safety. All addressees are specific individuals of these organizations, including the precision targeting of (at the time of the campaign) a major central European country's department head of prevention.

As reported in the X-Force Threat Intelligence Index 2021, industries that governments worldwide have heavily relied on for COVID-19 response efforts were at the epicenter of targeting during 2020, with attacks on manufacturing, energy and health care doubling from the previous year. This serves as yet another reminder that organizations and industries on the forefront of critical infrastructure and critical supply chains, such as the COVID-19 cold chain, are targets of high interest to adversaries.

What Are Attackers Likely Looking For?

With more than 350 logistics partners around the world, UNICEF and the COVID-19 vaccine cold chain will rely on seamless, multimodal transport systems to ensure that vaccines are transported in a timely and safe manner around the world. Attackers could be looking to infiltrate this extended supply chain to gain privileged insight into some of the following aspects:

- Privileged insight into national Advance Market Commitment (AMC) negotiations surrounding the national procurement of vaccines.
- Key timetables for distribution, information regarding expedited passage of COVID-19 vaccines through various nations and territories.
- Export controls and international property rights, government measures taken to facilitate the time-sensitive cargo including pre-arrival processing.
- Collection or duplication of electronic submission of documents for pre-arrival processing.
- Transit and World Trade Organization (WTO) trade facilitation agreements, clearance for transport crews and security of the cargo, border crossing regulations and physical inspections.
- Key technical requirements surrounding warehousing and energy/electrical component requirements for maintaining temperature-controlled environments during vaccine storage.

While clear attribution remains presently unavailable, the rise of ‘vaccine nationalism’ and increased global competition surrounding access to vaccines suggests the higher likelihood of a nation-state operation.

A Reminder to Stay Vigilant

The COVID-19 pandemic has created an unprecedented race between rival nations on an unequal economic plane. It is almost inevitable to see this type of adversarial activity in a threat landscape that is already extremely active on the nation-state attack front.

Any disruption to the requisite conditions, including freight, storage and logistics, could result in impotent or unsafe vaccines, leading to devastating effects on global health security. A better understanding of espionage efforts that could result in actions against the supply chain raises the importance of staying vigilant and aware of the related risks and ramifications. For recommendations on how to increase their cyber readiness, defenders can read our original research blog.

For more in-depth analysis surrounding this campaign, please access TRUSTAR.

Indicators of Compromise

HTML Files

File Name	SHA256
Draft Contract-091020-12.html	18d368e5ee1bbb9b7311e353cfd5475d772e8df6c4aa1c79b41800f07059b761
Draft Contract-091020-14.html	9714f0d45dcf6a67c96a3fcfcf4661cf234b08808edda19a92b30ddda8833367
Draft Contract-091020-7.html	7390f07d8d0f3762d0d58c72cbfba4e2ee02a324ebbf3edb372e91172ffa8ea3
Draft Contract-091020-6.html	e64e2e432f7d27843e53cd209f521e1c73ad25e521d96ebba2d51a33636e3645
Draft Contract-091020-14.html	05d542f51875185bfeba8a696465ed519eff8d8fc60af884396597098c7b6234

File Name	SHA256
Draft Contract-091020-11.html	edf49cada51c2654c75141306b35dd048bb3aa42ec881c5780be5b2c1dcadb11
Draft Contract-091020-7.html	1329ee2f527325fca0b84df95c848e881a8acc5d4bde13127f1208e20b57f6e6
Draft Contract-091020-6.html	131cb0f858b9f1ba2f5532d45fd5bf910ed4f14bbfcb1c9ec89e71e01455a4a5
Draft Contract-091020-4.html	43cc23e20f4a844bf012fe126a7f99f9ccb294cd26f45e7519f8c2838a1f05a9
pdf request for Quotation (1).html	3c22d882ae4ecbab92e6f0ff383f32aa73253a602e052ab46846f24fbded1a2e
pdf request for Quotation (1).html	07fef0ba6f59544efdae43f15520c51a1d0e86b226b28bc40704c2419d1a7caa
pdf request for Quotation (10).html	66f670d2740379de9233cb7797712e92cf27c822ee716a5d989bd7cc4809ef37
pdf request for Quotation (12).html	1dc6f66f7974ad716ff13b18f5fa8c1045ca298a35bd9b2f96ce5402011733d9
pdf request for Quotation (12).html	9874e8c69ba3deae8de3178a49a35dc6cf1c7568726c26f6e5ca34a0200491b2

File Name	SHA256
pdf request for Quotation (14).html	e8b85f246aa88a18552ef4b1407e1a302474c51753d71918b1c53b8e995b32ae
pdf request for Quotation (14).html	23024e98f96aef1ba314aeaed2bc9c07a1b100add71a1a6181bfb386d1dfa415
pdf request for Quotation (2).html	bbefe5aa411760f38ab393a574b249735033923684e4f824c5340365defd6b6c
pdf request for Quotation (2).html	7f86dbf27179b540cbda1a67916333b2318f405ee90580f37bde14c8e1b49098
pdf request for Quotation (2).html	b08ba117e431a03898df528c7dc8f989b3060972c198520d83c757160a0d310c
pdf request for Quotation (2).html	f258ba3e915bc2a54695434994116b7e1750db020b46b53ba91b5414a6422885
pdf request for Quotation (2).html	89204d0dc59cd647186ba5e8ce8b5521e8581e3bf8810c5163a23d5e1c544a93
pdf request for Quotation (3).html	6d312f0c7c51448a4324f5511bc09f13ce3a649b9f083023da223a3ddef242e3

File Name	SHA256
pdf request for Quotation (3).html	9b5fd4adafaaae5c94268e9a8f5728daaf82bf6013cf87750d0f9ce52266b983
pdf request for Quotation (5).html	7e740bdeec6866101b98173f84baf01daa78dea57a9f83f17b20e41d9a3bc13e
pdf request for Quotation (5).html	4fe1c28bca69b843e3dc70093bc4ca50a68cc9c52f9874f15314fcb2e78890ad
pdf request for Quotation (5).html	809af05c41576c3cbdc5a84dfb2d4d73f75befd36a2b7bb4412130a7839a92b9
pdf request for Quotation (8).html	e9b0b0b1589f8711d87df700183c618f5c9ce00b2206cbfd9b5ec60ae65036c0
pdf request for Quotation (8).html	499e7f2026f0d9f8e6fae03e14f45392233e89920e31bd6eb81129364242832e
pdf request for Quotation (8).html	24e54f51da72eb5e5e4f13c913068f40f4118b7c8616a6b6e3ac5d6a4128c194
pdf request for Quotation (8).html	df9ca5897fcaad95d0ecdc4a033c775d473355e66c0936efc382caba1b24ba22

File Name	SHA256
pdf request for Quotation (8).html	6f5ba1ffd5df43e6b64fc6d26bd238a200d6f20bb1f8a9c77d615c5a279deec8
pdf request for Quotation (9).html	d6915a015c056e54d2bfe7567a6bf760cdbb2bca0e3dfa1f4261136c7a0fb40d
pdf request for Quotation (9).html	5158767e275b32061be40fa1ade7e552a121c5f5fb11f531731728fd757726bd

Domains

e-mailer.cf	routermanager.tk	nwaoma.cf
e-mailer.ga	routermanagers.tk	nwaoma.ga
nwa-oma2.ml	serverrouter.tk	nwaoma.gq
routermanager.ga	nwa-oma.cf	nwaoma.ml
routermanager.gq	nwa-oma.ga	nwaoma.tk
routermanager.ml	nwa-oma.gq	nwaoma1.cf
routermanagers.cf	nwa-oma.tk	nwaoma1.ga
routermanagers.ga	nwa-oma1.ga	nwaoma1.gq
routermanagers.gq	nwa-oma1.gq	nwaoma1.ml
routermanagers.ml	nwa-oma1.ml	nwaoma1.tk
serverrouter.cf	nwa-oma1.tk	nwaoma2.cf
serverrouter.ga	nwa-oma2.cf	nwaoma2.ga
serversrouter.cf	nwa-oma2.ga	nwaoma2.gq
serversrouter.gq	nwa-oma2.gq	nwaoma2.ml

nwa-oma.ml	nwa-oma2.tk	nwaoma2.tk
mailerdeamon.cf	nwa-oma3.cf	nwaoma3.cf
mailerdeamon.ga	nwa-oma3.ga	nwaoma3.ga
mailerdeamon.gq	nwa-oma3.gq	nwaoma3.gq
mailerdeamon.ml	nwa-oma3.ml	serversrouter.ga
mailerdeamon.tk	nwa-oma3.tk	serversrouter.ml
		serversrouter.tk

Melissa Frydrych
Threat Hunt Researcher, IBM

Melissa is an analyst on the Threat Hunt & Discovery Team within IBM X-Force. She has over 9 years of experience, investigating and analyzing cyber threa...