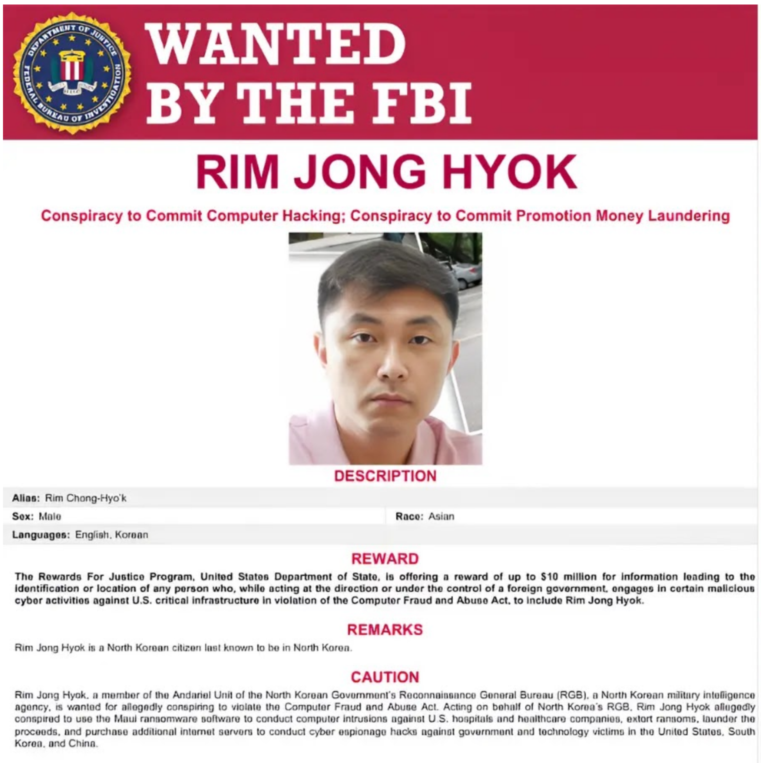
**Powered by GLESEC**

# CYBERSECURITY NEWS CUSTOM REPORT

Generated on 07/26/2024 by

# North Korean Charged in Cyberattacks on US Hospitals, NASA & Military Bases

*07/26/2024 01:50*



WANTED BY THE FBI

RIM JONG HYOK

Conspiracy to Commit Computer Hacking; Conspiracy to Commit Promotion Money Laundering

DESCRIPTION

|  |  |
|---|---|
| **Alias:** Rim Chong-Hyo'k |  |
| **Sex:** Male | **Race:** Asian |
| **Languages:** English, Korean |  |

REWARD

The Rewards For Justice Program, United States Department of State, is offering a reward of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, engages in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act, to include Rim Jong Hyok.

REMARKS

Rim Jong Hyok is a North Korean citizen last known to be in North Korea.

CAUTION

Rim Jong Hyok, a member of the Andariel Unit of the North Korean Government's Reconnaissance General Bureau (RGB), a North Korean military intelligence agency, is wanted for allegedly conspiring to violate the Computer Fraud and Abuse Act. Acting on behalf of North Korea's RGB, Rim Jong Hyok allegedly conspired to use the Maui ransomware software to conduct computer intrusions against U.S. hospitals and healthcare companies, extort ransoms, launder the proceeds, and purchase additional internet servers to conduct cyber espionage hacks against government and technology victims in the United States, South Korea, and China.

A North Korean military intelligence operative has been indicted for orchestrating a series of cyberattacks targeting U.S. hospitals, NASA, and military bases, federal prosecutors announced on Thursday.

Rim Jong Hyok, a member of the Andariel Unit within North Korea's Reconnaissance General Bureau, faces charges of conspiracy to commit computer hacking and money laundering.

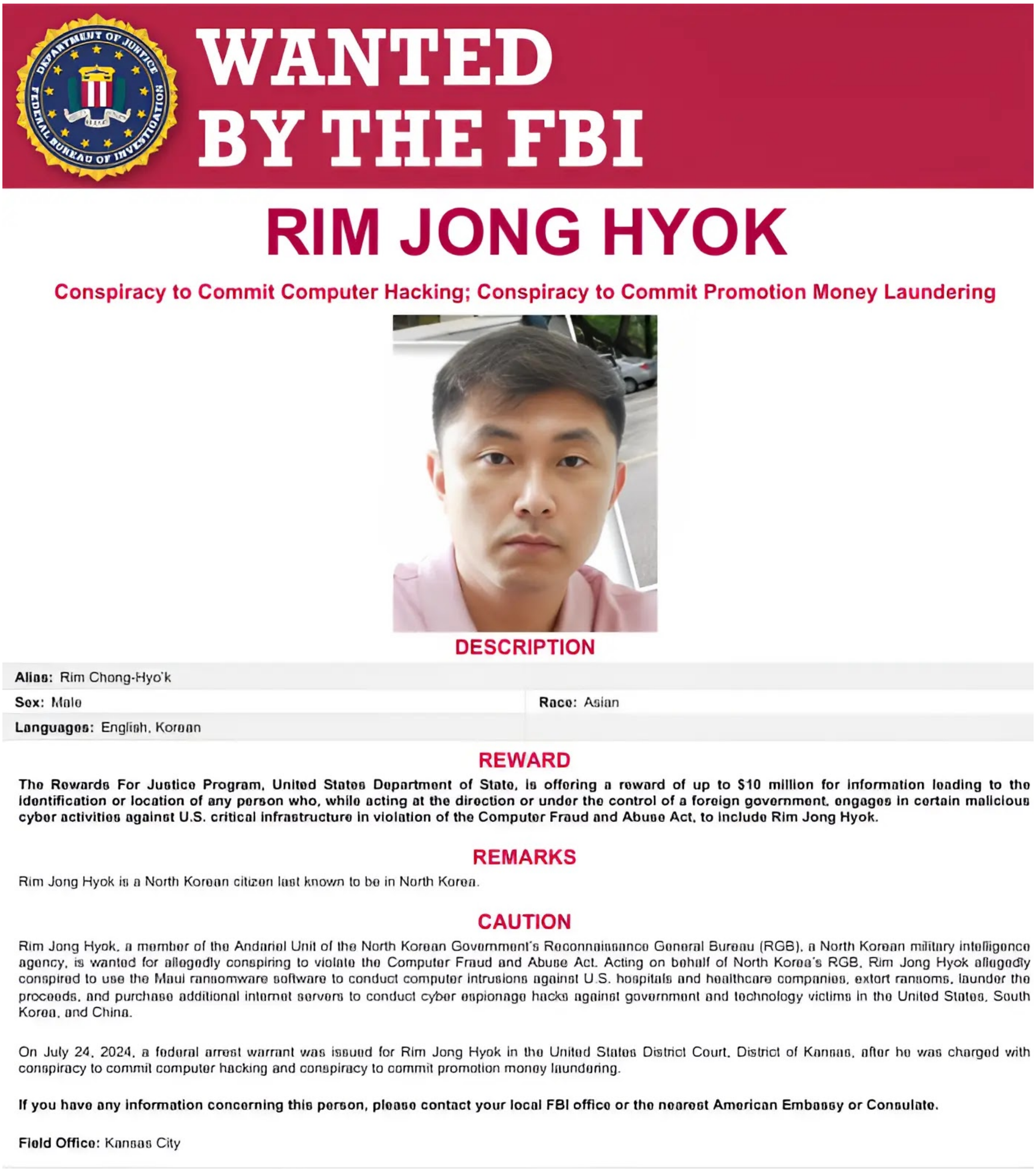
The indictment, issued by a grand jury in Kansas City, Kansas, alleges that Rim and his co-conspirators deployed ransomware attacks against U.S. healthcare providers, disrupting patient care and extorting ransom payments. The hackers then laundered the proceeds through Chinese facilitators to fund further cyberattacks on defense, technology, and government entities worldwide.

According to court documents, the Andariel group targeted at least 17 entities across 11 U.S. states, including NASA and two U.S. Air Force bases. In one instance, the hackers gained access to NASA's computer system for over three months, extracting more than 17 gigabytes of unclassified data. The group also infiltrated defense contractors in Michigan and California, stealing sensitive information related to military aircraft, satellites, and other defense technologies.

The attacks on healthcare providers were particularly disruptive, with at least one Kansas hospital paying approximately $100,000 in Bitcoin to regain access to encrypted files and servers. The FBI later recovered this ransom payment along with funds from a Colorado healthcare provider affected by the same Maui ransomware variant.

Deputy Attorney General Lisa Monaco stated, "This latest action, in collaboration with our partners in the U.S. and overseas, makes clear that we will continue to deploy all the tools at our disposal to disrupt ransomware attacks, hold those responsible to account, and place victims first."

The U.S. State Department is offering a reward of up to $10 million for information leading to the identification or location of Rim, who is believed to be in North Korea. The indictment highlights the growing threat of state-sponsored cyberattacks and their potential impact on critical infrastructure and national security.



# WANTED BY THE FBI

## RIM JONG HYOK

**Conspiracy to Commit Computer Hacking; Conspiracy to Commit Promotion Money Laundering**

### DESCRIPTION

| | |
|---|---|
| **Alias:** Rim Chong-Hyo'k | |
| **Sex:** Male | **Race:** Asian |
| **Languages:** English, Korean | |

### REWARD

**The Rewards For Justice Program, United States Department of State, is offering a reward of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, engages in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act, to include Rim Jong Hyok.**

### REMARKS

Rim Jong Hyok is a North Korean citizen last known to be in North Korea.

### CAUTION

Rim Jong Hyok, a member of the Andariel Unit of the North Korean Government's Reconnaissance General Bureau (RGB), a North Korean military intelligence agency, is wanted for allegedly conspiring to violate the Computer Fraud and Abuse Act. Acting on behalf of North Korea's RGB, Rim Jong Hyok allegedly conspired to use the Maui ransomware software to conduct computer intrusions against U.S. hospitals and healthcare companies, extort ransoms, launder the proceeds, and purchase additional internet servers to conduct cyber espionage hacks against government and technology victims in the United States, South Korea, and China.

On July 24, 2024, a federal arrest warrant was issued for Rim Jong Hyok in the United States District Court, District of Kansas, after he was charged with conspiracy to commit computer hacking and conspiracy to commit promotion money laundering.

**If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.**

**Field Office:** Kansas City

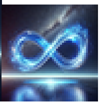
In response to the attacks, U.S. authorities have seized approximately $600,000 in virtual currency proceeds and are working to return the funds to victim organizations. Additionally, private sector partners like Microsoft and Mandiant are implementing measures to block Andariel actors from accessing victims’ networks and publishing research on the group’s tactics.

As the search for Rim continues, cybersecurity experts emphasize the need for organizations to remain vigilant and prioritize network security to protect against similar attacks in the future.

## Cyber Threats in Canada: Keychain Attacks

*07/26/2024 02:41*

Member-only story



Aardvark Infinity

·

Follow

Published in·3 min read·Just now

--

Share

Keychain Shadows: Cyber Threats in Canada #BlackGreyRed

This image illustrates the intricate and pervasive nature of keychain attacks as cyber threats in Canada. The biomechanical elements, glitch aesthetics, and a haunting color palette blend seamlessly, creating a surreal and enigmatic atmosphere. Each detail is rendered with lifelike precision, evoking a sense of hidden dimensions and unseen truths within the digital landscape.

**Date:** July 25, 2024

Keychain attacks pose a significant threat to cyber security, targeting credential storage systems to steal sensitive information. This essay examines the technique of keychain attacks (T1634.001), their impact on Canadian entities, and the strategies to mitigate these threats effectively.

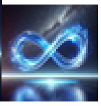
Keychain attacks involve exploiting vulnerabilities in credential storage mechanisms such as Apple’s Keychain, which securely stores passwords, private keys, and other sensitive data. Attackers often use privilege escalation or root access to retrieve this data.

1. **Privilege Escalation**: Attackers gain elevated privileges or root access on the device, bypassing security measures to access the keychain database.

## Cyber Threats in Canada: Malware Development and Acquisition

*07/26/2024 02:44*

Member-only story



Aardvark Infinity

·

Follow

Published in·3 min read·Just now

--

Share

**#4144: Malware Maelstrom**

In this piece, Baphomet rises from a digital landscape symbolizing malware development and acquisition in Canada. The chaotic glitches and digital distortions signify the pervasive cyber threats, while the background’s malware code, digital skulls, and encrypted data capture the essence of cybersecurity challenges. This composition blends the enigmatic allure of the occult with the stark reality of modern cyber threats.

**Date:** July 25, 2024

Malware development and acquisition are critical aspects of modern cyber threats, with adversaries either creating their own malicious software or obtaining it through various means. This essay explores the tactics of developing (T1587.001) and obtaining (T1588.001) malware, their impact on Canadian entities, and strategies for mitigating these threats.

Adversaries often develop custom malware tailored to their specific needs and objectives. This can include the creation of payloads, droppers, backdoors, and other post-compromise tools.

1. **Custom Development**: Threat actors such as the Sandworm Team have developed sophisticated malware like NotPetya...