DCO COBRA and SOSSEC - CYBER TALK

February 16, 2023

Presenter: Mandiant

Event Title: Mandiant Intelligence –
Current Foreign State Cyber & Cryptocurrency Operations

Panel Presenters:

Mr. Andy DeFazio, Mandiant DoD & IC
Mr. Mike Barnhart, DPRK Operations, Principal Analyst, Strategic Intelligence and Government
Mr. Joseph Dobson, Crypto Operations, Principal Analyst, Strategic Intelligence and Government

MANDIANT

Slick Phish & Cartoon Animals

Insights Into North Korea's Cyber & Cryptocurrency Operations

Michael "Barni" Barnhart

Principal Analyst, Strategic Intelligence & Government

Joseph "Joe" Dobson

Principal Analyst, Strategic Intelligence & Government

Agenda

- Structure of DPRK Cyber Programs
- DPRK Ransomware & Targeting of Healthcare
- DPRK Cyber Espionage Operations
  - Targeting of journalists, policymakers, & dissidents
- DPRK & Cryptocurrency/Web3
  - Heists
  - Phishing
  - Cryptocurrency laundering & masking funds
  - Cryptojacking
  - “IT Worker” Threat

Who Are We?

- Michael Barnhart
- Joseph Dobson

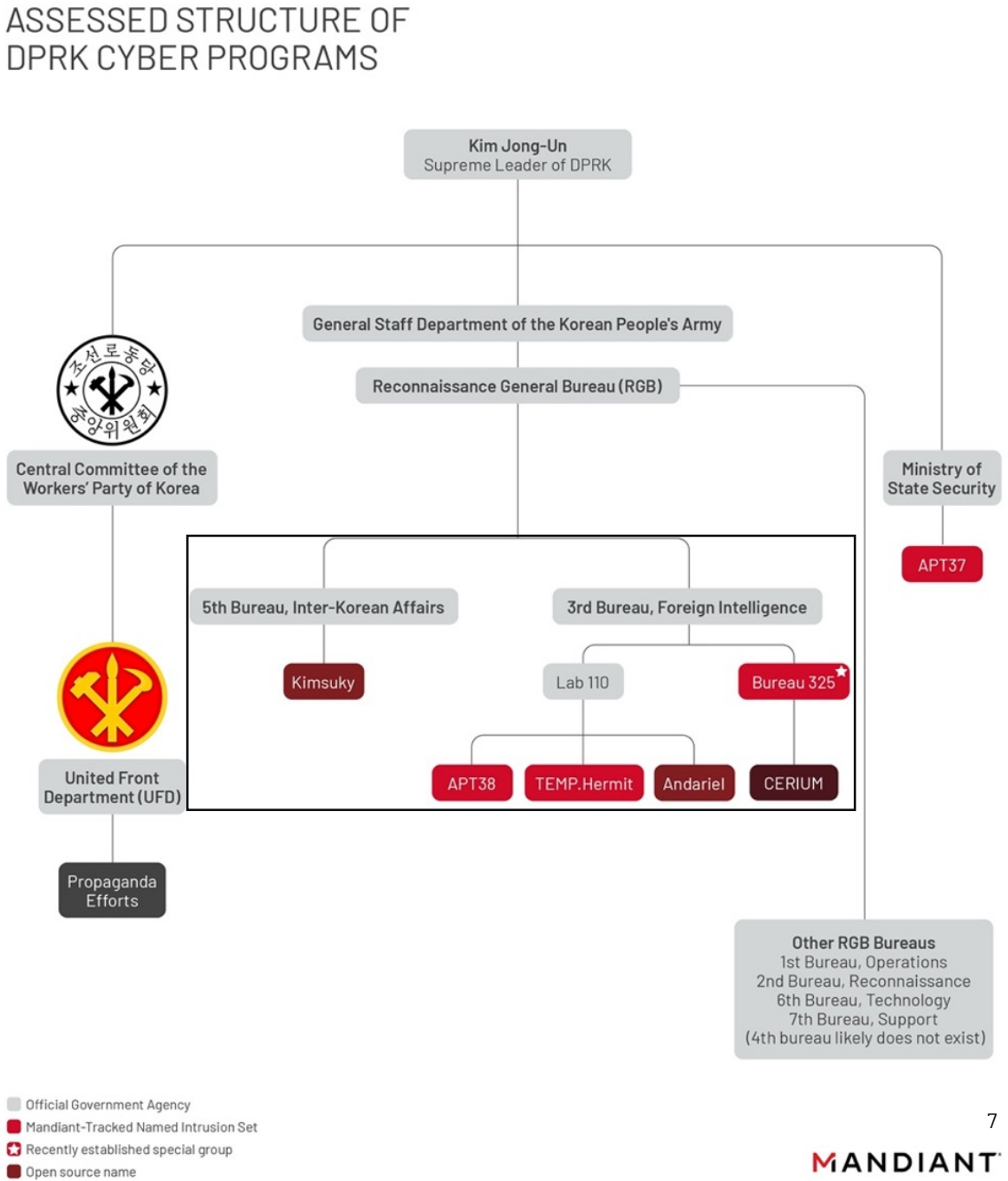
MANDIANT

Example journalist question on human rights: *Is there an effective way to broach this topic with North Korea in a way that satisfies rights advocates, which will be necessary for gaining bipartisan support in the United States for any eventual agreement, but also doesn't cause Pyongyang to shun talks in the first place?*

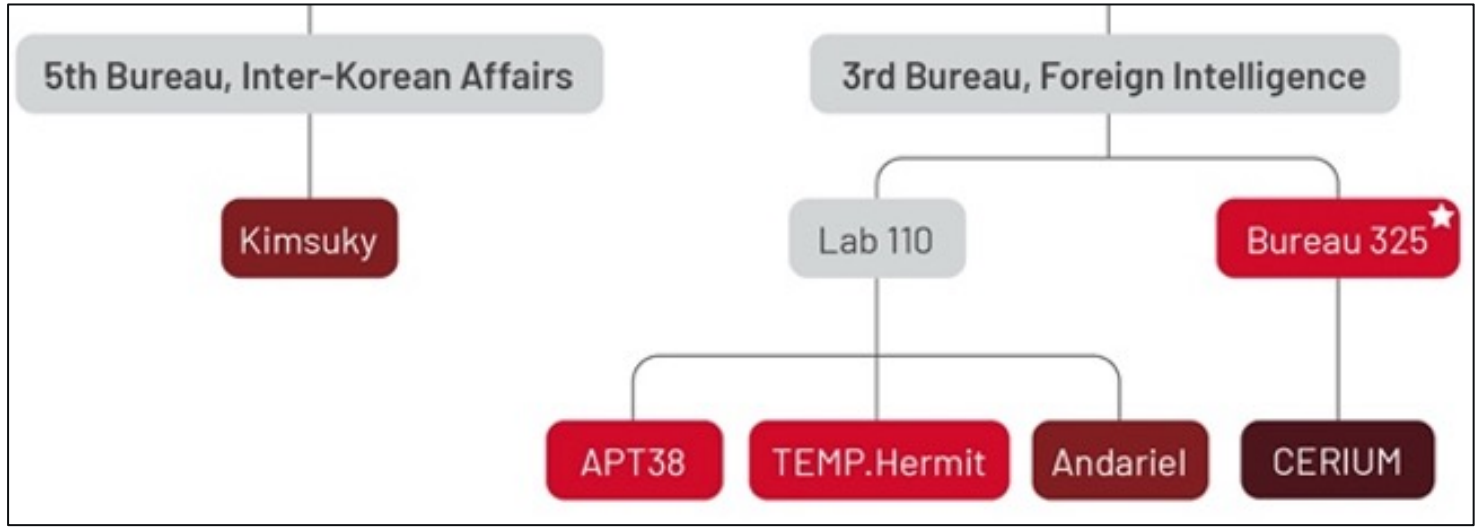
MANDIANT

Example journalist question on using nuclear weapons against low-Earth orbit satellites: *"How might the United States and its allies best deter such an attack or cope with one after it was made?"*

Structure of DPRK Cyber Programs

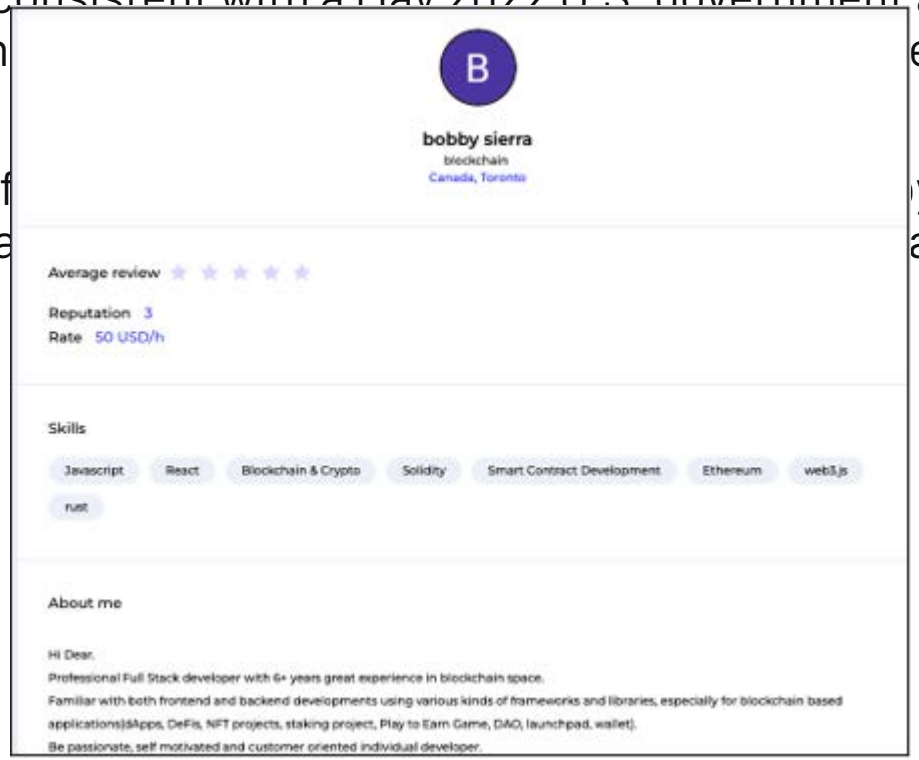


Structure of DPRK Cyber Programs



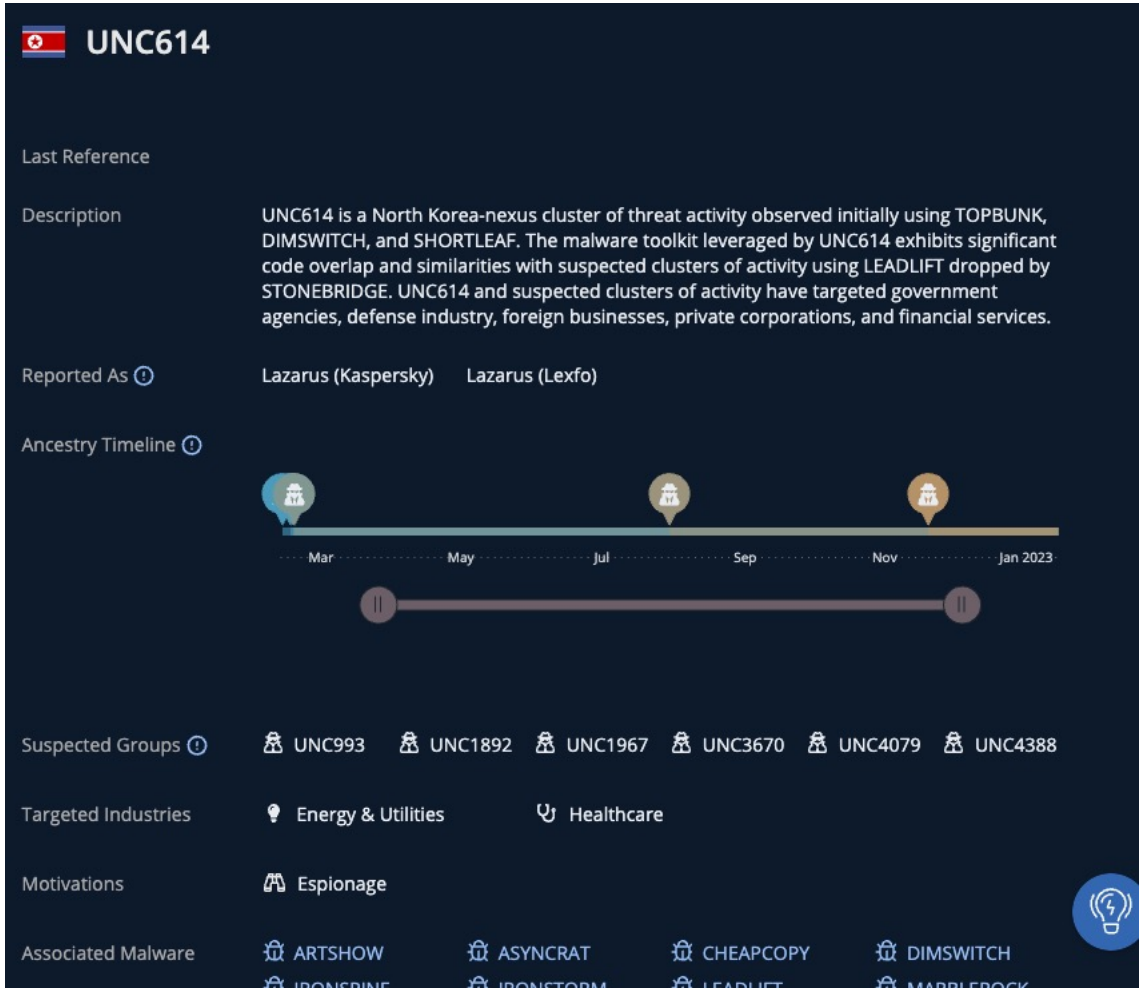
Possible North Korean Attempts to Gain Employment at Blockchain-Based Biopharmaceutical Company

- In May 2022, Mandiant observed suspected Democratic People's Republic of Korea (DPRK) efforts to gain employment at a cryptocurrency security company and a blockchain-based biopharmaceutical company.
- The accounts appear to be consistent with a May 2022 U.S. government advisory on North Korean IT workers posing as non-North Korean evenue for DPRK programs.
- The organizations targeted f y DPRK operators to target cryptocurrency-related orga anies.



QUINSTATUS Pharma Targeting: DPRK-Nexus UNC614 Suspected Tie

- In Feb 2022, Mandiant identified new samples of QUINSTATUS. At least one of the samples was dropped from a malicious document likely targeting a major pharmaceutical company.
- The malware appears to be signed with a compromised certificate
  - Name: OSPREY VIDEO, INC.
  - Serial Number: 73 2B BD 8D 56 24 BD AC
- Pivoting on recent and older QUINSTATUS samples resulted in identification of new malware families MARBLEROCK and SWEETPEA.
- Malware is all tied to UNC614 and related to a single group publicly reported as Andariel and DarkSeoul.



COVID Kim targeted Healthcare during 2020 - 2022

- In November 2020, Mandiant Threat Intelligence reported that a cyber espionage campaign distributing the CUTELOOP downloader using employment-themed lure material since at least April 2020 had updated its tools marginally and expanded its targeting to include a U.S. pharmaceutical company (20-00022194) . We believe this activity set to be North Korean in origin and noted potential ties to COVID Kim.

- The operation distributing the CUTELOOP dropper has been conducting a job-themed spear-phishing campaign enabled by social media since at least April 2020, although targeting of pharmaceuticals demonstrates a market expansion in targeting.

- Open sources corroborate that the campaign continues to leverage the following tactics, techniques, and procedures (TTPs).
  - Initial communication via direct messaging to establish rapport
  - Redirecting conversations to a separate chat client or messaging service
  - Discussing a new job opportunity as a social engineering lure
  - Using link-shortening services
  - Compromising legitimate domains as potential command and control (C&C)
  - Weaponizing documents mimicking defense contractors or leveraging openly available documents in the same manner

MANDIANT

DPRK & Cryptocurrency/Web3

DPRK & Cryptocurrency/Web3

- Cryptocurrency is a low-cost, high reward target for North Korea
- Offensive operations include:
  - Ransomware
  - **Crypto heists**
  - **Phishing (ERC-20 & NFT)**
  - **Cryptojacking**
  - **Insider threat (IT Workers)**

DPRK & Cryptocurrency: Targeting

- *Everyone* is targeted
  - Most cryptocurrencies are anonymous, but not private
    - Anonymous: Transactions are public
      - Know someone's wallet address? You can see their transactions!
      - Adoption of naming services can reveal identities of owners
    - Private: Only sender/receiver can see information
  - Public blockchains = easy targeting of active wallets
  - Entities with significant funds are more heavily targeted
    - Exchanges
    - Bridges
- Optimism bias – "Why would they target me?"
  - No fish too small

Massive Heists Likely Perpetrated by DPRK

TECH | CRYPTOCURRENCY | NFTS

Axie Infinity's blockchain was reportedly hacked via a fake LinkedIn job offer

It lost over half a billion dollars

North Korean Attackers Behind $100M Harmony Hack: Report

Analysis suggests the hack is the work of the Lazarus Group, the Pyongyang-backed group behind a similar $622 million hack of Axie Infinity.

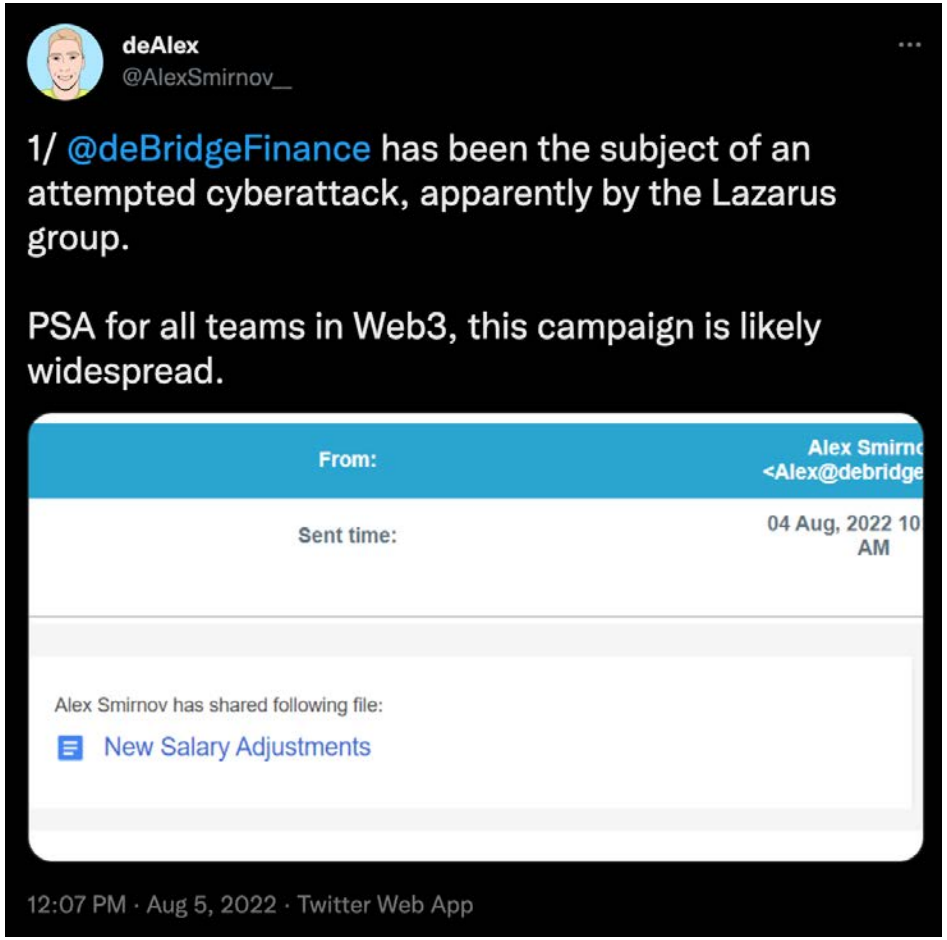
Harmony

Harmony is an open and fast blockchain. Our mainnet runs Ethereum applications with 2-second transaction finality and 100 times lower fees.

©2022 Mandiant

The DPRK Phishing Threat

- Phishing has been extremely fruitful for North Korea
  - Effective in cyber operations & cryptocurrency operations
  - Employment-related phishing is a favorite
    - Open source: DPRK phishing attack enabled a $540 million crypto heist
  - Alex Smirnov of deBridge Finance detailed a suspected North Korean phishing attack



DPRK Token (ERC-20) & NFT Phishing

- Non-Fungible Token
  - Fancy way of saying "something unique"
  - Fungible: A *photograph* of the Mona Lisa painting
  - Non-fungible: The *actual* Mona Lisa painting
- NFT Functions:
  - Art
  - Domain Names
  - Land in virtual worlds
  - Music
  - Access (to concerts & conferences)

Cryptocurrency Laundering & Masking Funds

- Cryptocurrencies generally use public ledgers
  - Funds can often be tracked from one wallet to the next
- Significant use of cross-chain bridges
- "Mixers" are used
  - They "mix" together funds from many wallets, output to many wallets
    - Difficult to trace transactions
  - Tornado Cash

"Cross-chain bridges" connect blockchains

For example, a "bridge" can be used to move funds between Bitcoin and Ethereum.

Cryptojacking

- Some cryptocurrency can be generated by “mining”
  - Processing power + luck is needed
- Cryptojacking is the hijacking of processing power for cryptomining
- DPRK actors mine on compromised devices
  - XMRig is a preferred miner
    - Used to mine Monero (XMR)
    - XMRig is common among threat actors

The “IT Workers” Threat: Background

- The US Government issued an advisory on North Korean “Information Technology Workers”
- Revenue generation is the focus of North Korean IT workers
  - Goal: Generate funds for WMD program
- Primarily located in China & Russia
  - Smaller presence in Africa & Southeast Asia
- Significant focus on virtual currency (cryptocurrency)
- “Some DPRK IT workers have designed virtual currency exchanges or created analytic tools and applications for virtual currency traders”

By The Numbers:*

- **”Thousands” of IT workers**
- **10x earned income vs typical factory employment**
- **DPRK government withholds up to 90% of wages**

*These details come from the US advisory on North Korean “IT Workers”

The “IT Workers” Threat: Why Should Anyone Care?

- North Korean “IT Workers” pose a risk similar to that of an “insider threat”
- Sensitive, proprietary information might be exfiltrated
- Vulnerabilities may be introduced
- Can be used to enable North Korean cyber intrusions
- Violates US & UN Sanctions
- The threat actors aren’t always obvious
  - “…proxy accounts belong to third-party individuals, some of whom sell their identification and account information to the DPRK IT workers.” –*Guidance on the Democratic People’s Republic of Korea Information Technology Workers*”
- The risk is difficult to overstate

The “IT Workers” Threat: Mandiant’s Findings

- Mandiant’s findings corroborate the US advisory
- North Korean “IT Workers” are active on freelancing/gig websites
  - Skillsets focused on cryptocurrency & full stack development
    - Actively deploying smart contracts on multiple cryptocurrency platforms
  - Often claim to live in USA, Canada, Eastern Europe (including Ukraine)
  - Maintain profiles & portfolios on freelancing websites
    - Actively pursue work by approaching gig providers

Mandiant-Tracked “IT Workers” are:

- **Active on social media**
  - Career/business social networking
  - Programming forums
  - Chat/messaging applications
- **Getting jobs/gigs**
  - Reviews (of unknown authenticity) are mixed
  - Negative reviews detail bait-and-switch tactics
    - Weak language skills & false claims

The “IT Workers” Threat: Mandiant’s Findings

- Mandiant-tracked suspected North Korean “IT Workers” have:
  - Pursued employment at crypto project DAOs
  - Hounded potential employers for jobs
  - Responded to project proposals
  - Created NFT projects & minted NFTs
  - Collaborated with non-DPRK personnel on ERC proposals
  - Membership in various social media groups
- ***North Korea is a leader in state-sponsored web3 threat activity***

What is a DAO?

A DAO is a decentralized autonomous organization. Typically crypto-centric, DAOs are not centrally run, but can function like club or company.

DAOs often “pay” members by issuing tokens – making them an attractive employer for DPRK “IT Workers”

Outlook

- DPRK Cyber Operations
- DPRK Crypto/Web3 Operations

MANDIANT®

Questions?

SOSSEC Membership is Required for Award on PEO EIS, DCO Cyberspace Operations Broad Responsive Agreement (COBRA) Other Transaction Agreement (OTA)

Benefits of Joining the SOSSEC Consortium

- ✓ Opportunity to perform work under seven (9) OTAs for the Air Force, Army and National Geospatial-Intelligence Agency
- ✓ Opportunity to build members' business base by applying their technologies/expertise to meeting urgent DoD requirements
- ✓ Simple, streamlined process to compete for DoD work
- ✓ Average 60 days from requirements definition to award
- ✓ Flexible treatment of intellectual property
- ✓ OTA access to any DoD user with approval of OTA customer
- ✓ Transition from Prototype to Production without further competition

Go to **www.sossecinc.com** and click on the **JOIN** Tab to access the membership application. The process is simple and rapid. There is no joining fee, and the membership fee is $500 per year. Membership is open to Industry (traditional, nontraditional, small business), not for profit and academic institutions that share the values of the SOSSEC Consortium.

For questions about SOSSEC COBRA OTA, contact Gene Del Coco at edelcoco@sossecinc.com or Ed Aguirre at eaguirre@sossecinc.com.