Awareness of Illicit Cryptomining-Related Activities May Improve Detection

Cybercriminals and terrorists are drawn to cryptomining as a method of generating revenue because of its profitability and potential for reduced detection. Cryptomining, also known as cryptocurrency mining, is a legal activity and process in which miners receive newly mined units of cryptocurrency as a reward for verifying transactions. Illicit cryptomining-related activities involve cyber intrusion through cryptojacking (through running malware on an unwitting host machine) or actively participating in theft of electricity. Public safety and private sector awareness of observable indicators that are potentially indicative of illicit cryptomining-related activities may assist in the identification and prevention of such activities.

SCOPE: This product raises awareness of illicit crypto-mining-related activities provides best practices to protect against such activity. This product supplements the First Responder's Toolbox "Identifying Indicators of Illicit Cryptocurrency Use May Enhance Investigations."

INDICATORS OF ILLICIT CRYPTOMINING-RELATED ACTIVITIES: Public safety may encounter illicit activities during calls to service or investigations (drug-related operations or emergency medical calls). Educating the private sector (hotels, landlords, schools, and utility services) on how to detect potential suspicious activities and behaviors may improve reporting. Some indicators may include:

- Calls or reports of blown out or smoking power transformers, damaged grid equipment, electrical-related fires or injuries, or unusual power readings (stolen or massive spikes in electricity).
- Calls or reports of suspicious persons manipulating the use of electricity in building facilities, college campuses, or hotels.
- Calls or reports of changes to computing, networking, and power delivery device performance, to include devices shutting down because of the lack of available processing power, abnormal computer processing activity, overheating device batteries, reduction in device or router productivity, or sustained connections to unusual domains.
- Unusual heat signatures emanating during legal justification (properly obtained warrant) for thermal imaging.

NOTE: Many of the activities described herein may involve constitutionally protected activities and may be insignificant on their own. Evaluate instances without a reasonable alternative explanation while considering the totality of the circumstances, additional indicators, or observed behaviors indicative of illicit activities or terrorism before reporting as suspicious activity.

CRYPTOJACKING MALWARE: Malicious actors are increasingly targeting standard electronic devices (cable boxes, digital video recorders, personal computers, and smart televisions), as well as other Internet of Thing devices.

Awareness of Illicit Cryptomining-Related Activities May Improve Detection *(continued)*

- Unauthorized use of structures (abandoned building, storage unit, or vacant residence) with multiple stacks of computer equipment or video game stations, files on a computer consistent with cryptojacking, or lack of request for service or permit from utility company for high power to support cryptomining.
- Evidence of safety hazards or tampering of equipment, to include: dismantled meters; altered (jumper cables or metals), damaged, exposed, or unsafe wiring connections; lack of proper insulation surrounding connections or wires; or multiple holes in walls, particularly underground areas (basements), where electric meters may be located.

PRIVATE SECTOR PARTNERSHIPS: Illicit actors may target critical infrastructure or other private sector companies using technology, such as cloud services, to access computer processing power. This may cause degradation to network performance and systems, financial loss, physical damage, or normal operation disruption. Joint training with private sector partners on indicators of illicit cryptomining-related activities may increase chances to identify and report such activities. Furthermore, developing partnerships with private sector partners may improve regular information sharing on technical indicators for broader awareness of latest tactics, techniques, and procedures.

Cryptocurrencies—such as Bitcoin, Ethereum, Litecoin, Monero, and Ripple—are digital currencies used as a medium of exchange. Cryptocurrencies operate independently of central banks, using encryption techniques and blockchain technology to secure and verify transactions.

Cryptojacking is the process whereby illicit actors hijack the processing power of victims' devices and systems by exploiting vulnerabilities (operating systems, software, and webpages) to illegally install cryptomining malware on devices and systems. Once malware is installed, illicit actors earn cryptocurrency.

Cryptocurrency miners are often individuals or groups of people contributing processing power to solve complex mathematical puzzles to earn the right to validate a batch of transactions and add that batch to a blockchain; the first person to solve the puzzle earns a set amount of cryptocurrency as a reward, although not all blockchains operate in this manner.

Awareness of Illicit Cryptomining-Related Activities May Improve Detection *(continued)*

RESOURCES

DHS

- **Cyber Crimes Center** https://www.ice.gov/investigations/cybercrime-investigations
- **Cybersecurity and Infrastructure Security Agency** bolsters the nation's capacity to defend against cyber-attacks by providing federal civilian departments and agencies cybersecurity tools, incident response services and assessment capabilities to safeguard the .gov networks that support essential operations. https://www.cisa.gov/
- The **Homeland Security Investigations (HSI) Cornerstone** outreach initiative seeks to detect and close vulnerabilities in US financial, trade, and transportation sectors. HSI special agents are available to provide training and share red-flag indicators, criminal typologies, and methods with business industries that manage the very systems that terrorists and criminal organizations seek to exploit. For more information, contact cornerstone@ice.dhs.gov or visit https://www.ice.gov/outreach-programs/cornerstone.

FBI CYBER CRIME https://www.fbi.gov/investigate/cyber

The **FEDERAL TRADE COMMISSION** works to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. https://www.consumer.ftc.gov/

The **US DEPARTMENT OF TREASURY** maintains a strong economy by promoting conditions that enable economic growth, economic and job opportunities, and stability at home and abroad; strengthen national security by combating threats and protecting the integrity of the financial system; and manage the federal government's finances and resources effectively. https://home.treasury.gov/

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

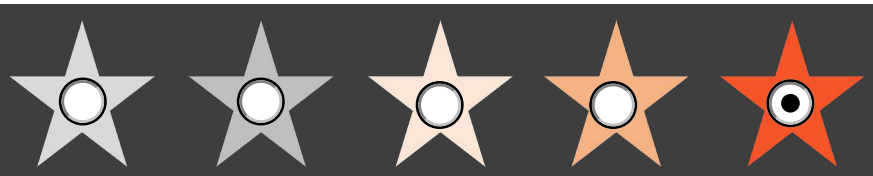
PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: Awareness of Illicit Cryptomining-Related Activities May Improve Detection

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT