DARKTRACE

Evolving threats call for evolved thinking™

Energy Sector Threat Trends Report / 2022

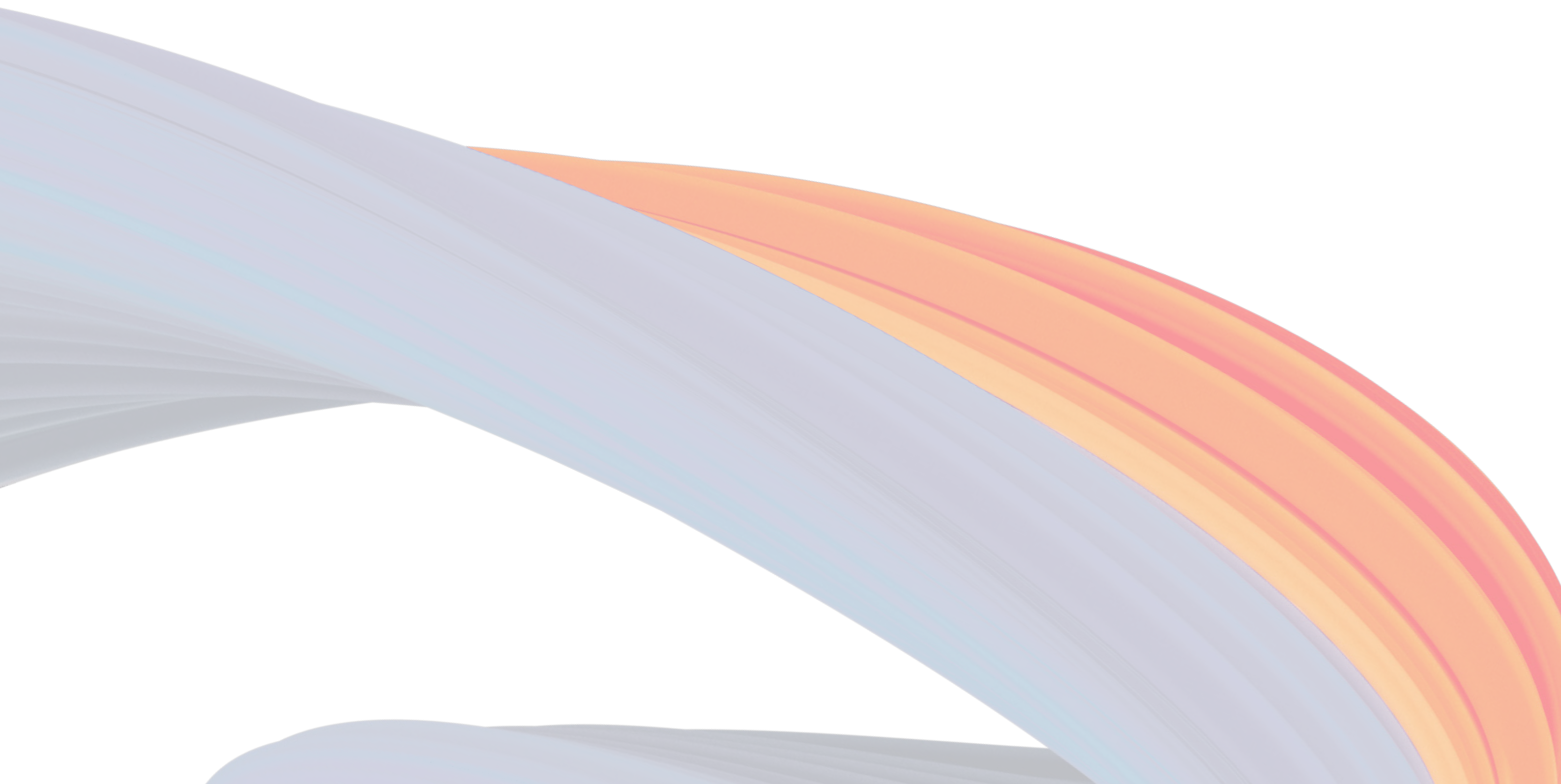
Industry Spotlight

DARKTRACE

CONTENTS

Executive Summary

The global energy sector is facing a time of uncertainty due to a confluence of geopolitical, economic, and environmental factors. Energy prices for consumers are soaring and several energy firms have folded under rising wholesale prices. In tandem, the cyber threat landscape is growing increasingly complex, further complicating the picture for global energy suppliers. While governments and regulatory bodies urge the critical infrastructure sector to double down on cyber defence, Darktrace's exclusive data shows that illegal crypto-mining threats are on the rise in the UK and US energy sectors.



What is Crypto-mining?

Crypto-mining is the process of creating new units of crypto-currency or 'coins' by solving mathematical puzzles generated by each respective currency's algorithm. It refers to the process whereby a global network of computers running, for example, the Bitcoin code, work to ensure that transactions are legitimate. High-powered computers compete to be the first to validate a series of transactions called a block and add the block to the blockchain. Where once this could be achieved on regular CPUs, the process was too slow and now the crypto-currency is generated using large mining pools[1] spread across the world. Mining pools include incredibly expensive and powerful computers whose sole function is to run algorithms to solve the mathematical puzzle that allows their owner to win a Bitcoin block.

Despite a challenging year in terms of price for crypto-currency, more miners than ever are joining the network, which is driving up the difficulty of mining new coins. If we take Bitcoin as an example, on average, the difficulty adjustment of mining Bitcoin occurs roughly every two weeks, or 2,016 blocks, to ensure that the current schedule of all Bitcoin being mined and in circulation by the year 2140, remains. In the original Bitcoin whitepaper, author Satoshi Nakamoto explained that if blocks are generated too fast, the difficulty increases. In October 2022, Bitcoin mining difficulty (the complexity that miners must overcome to solve valid blocks) hit a new all-time high. As the difficulty increases, so does the power needed to mine.

Crypto-jacking vs Crypto-mining

The tools necessary for crypto-mining are increasingly accessible, but the energy required has never been more expensive. There are many individuals and organisations mining crypto-currencies legally, but the processing power needed, and the huge associated energy cost, incentivises bad actors to 'steal' energy and processing power from other devices and networks. By secretly using devices belonging to other individuals or organisations to mine crypto-currencies without their knowledge or consent, bad actors can get crypto-currencies without shouldering the huge energy cost. This is called crypto-jacking.

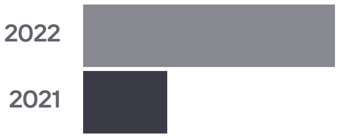
From facilitating drugs trafficking, terrorism, and online child exploitation, to even reportedly funding North Korea's WMD programme, crypto-currencies offer bad actors anonymous, untraceable ways in which to transfer and launder money. Policymakers, supervisors, and law enforcement agencies are gradually responding; and the private sector is developing solutions to help.

The Data

Darktrace data indicates UK and US energy sectors under strain from an increasing proportion of crypto-jacking threats.

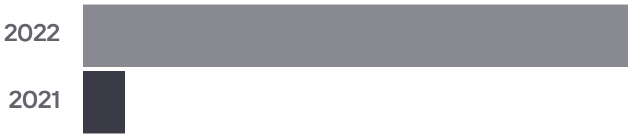
US energy sector

'High Priority Crypto-Currency Mining', accounted for **3x more** of all cyber incidents in the sector in 2022 compared to 2021.[2]



UK energy sector

'High Priority Crypto-Currency Mining', accounted for **13x more** of all cyber incidents in 2022 compared to 2021.[3]



[1] A crypto-currency mining pool is a group of miners that work together to optimise their chances of mining a block and share rewards among each other in proportion to the computing power contributed by them in successfully mining a block. This mode of working naturally further incentivises seeking ways to harness more processing power.

[2] High Priority Crypto-Currency Mining, which belongs to the Impact MITRE attack tactics category accounted for 5.84% of all incidents in the US energy sector in 2022, compared with 1.87% in 2021.

[3] In the UK energy sector, 'High Priority Crypto-Currency Mining', which belongs to the Impact MITRE attack tactics category, accounted for 12.41% of all cyber incidents in 2022, compared with 0.95% in 2021.

MITRE Category: Impact

Under the industry standard MITRE ATT&CK categories, crypto-jacking fits into the 'Impact' category, meaning the adversary is trying to manipulate, interrupt, or destroy your systems and data.

> " Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach. "

Threat Stories

EMEA

In mid-March 2022, Darktrace DETECT/Network™ identified likely crypto-mining activity within the network of an energy support company operating in Denmark. 5 similar internal servers were seen connecting to IPs associated with suspicious coin miner activities. Each of these devices also used a TCP channel associated with Stratum- a protocol that enables crypto-mining pooling using network resources. It was clear that someone was trying to mass pool crypto-mining capabilities.

By alerting the security team to this cluster of activity, Darktrace allowed the security team to review this behaviour. The servers were subsequently taken offline by the security team, meaning any potential crypto-jackers could not continue their work.

US

In September 2022 Darktrace observed a failed crypto-mining incident within the environment of a local US energy provider. A desktop inside the business repeatedly made unsuccessful DNS connections to a rare 'nanopool' address. Nanopool is a mining pool that provides services to share processing power and mine a range of popular crypto-currencies including Monero and Ethereum.

This unusual behaviour quickly triggered Darktrace DETECT/Network to alert. Although unconfirmed, popular Open Source intelligence had also associated this endpoint with a large malicious botnet (known as 'Sysrv-hello') suggesting the potential for a larger crypto-jacking infection. Although these connections were unsuccessful, an internal user reported this alert for further investigation. In doing so the customer was able to verify the threat and prevent it from escalating into any malicious activities.

Expert Analysis

The three-fold increase in the total proportion of crypto-mining attacks attempted against Darktrace customers in the US energy sector, and the thirteen-fold increase in the UK, is alarming but not surprising. Energy suppliers typically have vast OT infrastructure with access to huge supplies of energy, making it a prime target for energy-hungry crypto-jacking. It is important to note that crypto-jacking is also a serious insider threat, with employees occasionally using their workplace's corporate digital infrastructure to mine, sometimes without realising it is illegal to do so.

Crypto-mining has historically been thought of as a relatively acceptable form of compromise compared with other more overtly destructive cyber-attacks like ransomware. But the damage of a crypto-jacking infection can be slow, insidious, and long-lasting. Aside from slowing down systems and damaging productivity, running rogue software within your digital estate can easily turn into ransomware, data exfiltration or act as an initial entry point for a human-driven attack at the snap of a finger.

Throughout 2022 we saw a variety of western governments warning critical infrastructure sectors to improve their cyber security. Threat actors pay attention to prevailing perceptions, and will have seen this as an indication of structural weakness that they can exploit. The energy sector involves large monolithic organisations where there is a wealth of physical internet-connected equipment but a corresponding scarcity of cyber security personnel. To threat actors this implies a greater chance of remaining 'on premises', maintaining access, and evading discovery.

The indicators of crypto-jacking can be exceptionally subtle, making them particularly difficult for security teams to spot. More sensitive tools like AI are increasingly being leveraged to give defenders the visibility they need to spot the low-profile activity of crypto-mining software, wherever it has landed.

Looking Forward

Crypto-currencies are extremely volatile in value, and 2022 has been no exception. The collapse of TerraUSD and LUNA earlier this year, and the more recent implosion of crypto-trading platform FTX, made headlines around the world and led to higher levels of crypto-scepticism. If crypto-currencies lose so much value as to be uneconomical for hackers to spend their time and effort mining, even by illegal means, we may see a move away from crypto-jacking attacks. However, despite the dramatic failures of certain coins, crypto-currencies are still a long way from being valueless. Demand remains high, despite or even because of the recent fall in the price of many coins, with active users on decentralized apps and smart contract developers both increasing in 2022. The world of crypto is certainly accustomed to enduring turbulence. Given the usefulness of crypto-currencies to criminals as an untraceable way to transfer and launder their illegal gains, it's fair to say crypto-jacking won't be going anywhere yet.

Environmental concerns have led some crypto-currencies to move away from the traditional model of mining which requires so much processing power and energy. Uptake of these new methods has been slow, and growing pains have been reported around greener methods which utilise hard discs leading to shortages. If these coins were to become the norm, it may disincentivise persistent crypto-jacking attacks. However, until then, the reality remains that crypto-jacking offers criminals run-rate, steady and untraceable sources of income, and it is a threat that remains largely underestimated by security teams.

List of Contributors

David Masson, Director of Enterprise Security

Max Heinemeyer, Chief Product Officer

Mike Beck, Chief Information Security Officer