Picture credit: David Mcbee

CHAIN REACTION

Ralph Chammah *reveals how proactive threat detection is the key to overcoming blockchain security challenges*

Since the idea was first introduced during the 2008 global financial crisis, blockchain technology and cryptocurrency has skyrocketed. Storing information in several databases (blocks) that are linked together chronologically through cryptographic hashes to form a distributed network (chain) has provided an alternate yet effective way to store data. The global blockchain market is now expected to hit $67.5-billion by 2026. Blockchain has also been critical within the realm of banking, financial services and insurance (BFSI), furthering the commercialisation of blockchain technology through decentralised finance (DeFi) services for investors. There are over 6,000 cryptocurrencies being traded freely within the global cryptocurrency market, reaching $990-billion in capital.

Yet with this great rise in capital comes a wave of cyber criminals trying to penetrate blockchain and gain access to the data and wealth within. Despite the increasing onslaught of blockchain attacks and the astronomical valuations of its related businesses, the lack of clear global regulations, standards and guidelines has put all players at risk. With blockchain technology still being in the beginning of its lifecycle, several design and development vulnerabilities in its architecture place blockchain at a much higher risk of exploitation by cyber actors wishing to wreak havoc. These security challenges further extend to companies exclusively storing and transacting cryptocurrencies through digital wallets – in one bold move from a cyber actor, their entire business could be put at risk.

There are over 6,000 cryptocurrencies being traded freely within the global cryptocurrency market, reaching $990-billion in capital

Several well-known vulnerabilities within blockchain architecture have existed since its early days. Blockchain mining attacks, time jacking, crypto jacking, forking attacks, eclipse attacks and smart contract vulnerabilities such as re-entrancy attacks, overflow attacks and balance attacks are just a few that persist. These attacks are possible due to the following main exposure points seen in its architecture:

EXPLOITING USERS

Cyber criminals are first and foremost able to attack organisations through their weakest points of entry – the user. They will often steal credentials to gain access to user accounts and then aim to escalate privileges in order to steal data from within. Targets may include employees, customers, shareholders and even other stakeholders who have direct access to the enterprise environment. Without the correct training to spot and avoid these kinds of attacks, users will be more likely to become a victim of a phishing attack and other forms of impersonation attacks.

DIRECT ATTACKS

Legacy systems prove easy targets for cyber criminals to exploit, allowing them to quickly gain access to mission critical blockchain facilities storing or processing digital asset transaction traffic in an inter-connect eco-system. This opens the door for further exploitation – essentially in leaving systems unmaintained, the back door is left open to attack.

RANSOMWARE ATTACKS

Companies within the blockchain and crypto industry are still required to abide by data privacy and protection regulations. Yet it is no secret there is still a lack of concrete regulations and guidelines within the sector. Ransomware attacks can hamper the availability of data, resulting in long-drawn downtimes and disruption in business operations. These attacks have only become more frequent with the onset of remote working and an overall lack of cyber awareness has paved the way for more favourable conditions for attacks. Blockchain organisations with only reactive cyber maturity levels are soft, easy targets for cyber actors especially since cryptocurrencies can then also be used as an agent for further ransom extortions.

VULNERABILITY

Like wallets used to store cash, cryptocurrency is deposited in digital wallets, which can be accessed through cryptographic keys. There are two sets of keys, first the public key – which can be used to deposit digital assets in an address just like a bank account number – and secondly, a private key, which can be used to withdraw money from the wallet like a pin number. Private key security is critical to safeguarding the digital assets stored within crypto wallets. Basic attacks on crypto wallets aim to locate files where private keys are stored. However, since 2018, attackers are able to re-construct private keys by decoding electromagnetic signals emitted by devices in an attempt known as side-channelling attack. Additionally, several attacks on crypto wallets leverage human error, pre-existing vulnerabilities and connection interception, which eliminates the need for private keys to hijack a wallet.

DEFI PROTOCOLS

Although the number of DeFi protocol hacks decreased in 2022 compared with previous years, an average of $32.6-million was stolen in each attack. The heaviest DeFi hijack of that year alone was worth $569-million. With nearly $240-billion locked in, DeFi protocols are a certain target for adversaries.

DESIGN FLAWS

Under the DeFi umbrella, smart contracts are largely used in interoperability protocols which link multiple blockchains together. Design flaws can allow adversaries to call privileged smart contracts controlling the flow of digital information between linked blockchains. The assets can then be directed into a cybercriminal-controlled address to be traded freely over an exchange. Organisations leveraging the smart contract technology need a secure system development life cycle through DevSecOps considerations.

Most organisations rely on perimeter security measures to protect their networks from cyberattacks, but these measures are no longer sufficient. Past attacks faced by digital asset firms have often been reported only after an illicit transaction was successfully executed on or across blockchain(s). Detection of cyberattacks later in their lifecycle can lead to adverse financial, reputational and/or regulatory impact – something organisations, especially in the blockchain space, can rarely afford or survive. To keep ahead of the attackers, more proactive threat hunting is essential. Detecting and stopping attacks before they do damage can be achieved by checking for early signs of abnormal behaviour.

THE LACK OF CLEAR GLOBAL REGULATIONS AND STANDARDS HAS PUT ALL PLAYERS AT RISK

In cyber threat hunting, an organisation's environment is proactively searched for unknown vulnerabilities and undetected attacks. By collecting and analysing data from various on-chain and off-chain activities, threat hunters develop and test hypotheses about potential threats based on cyber threat intelligence, known attack techniques and other information. This grants an enhanced visibility of overall security posture, while also simplifying both threat detection and incident response activities.

Having software with integrated native out-of-the-box compliance alerting and advanced analytics to identify and flag compliance breaches is also key. In an uncertain regulatory environment, this software will enable blockchain and crypto firms to monitor for compliance and cybersecurity under the same joint effort. Identification of cyber risks affecting blockchain specific infrastructure is key to the development of proactive cyber maturity efforts.

The use of this type of more proactive threat hunting can enhance the security posture and overall

vigilance, cultivate a culture of proactive risk management and mitigation, and provide an enhanced picture of attack surfaces and adversary tactics across blockchain operations.

With the intertwining of blockchain and cybersecurity in an ever-evolving threats landscape, it is imperative that you continuously enhance your business to match the current landscape. Yet navigating a challenging environment and adopting the best practices can be overwhelming for business and function leaders. Without proper guidance, this implementation can be difficult or even impossible. Here are five simple cybersecurity steps organisations need to follow in order to begin taking effective action.

IN ONE BOLD MOVE FROM A CYBER ACTOR, AN ENTIRE BUSINESS CAN BE PUT AT RISK

Re-assess your existing threat hunting procedures. Before looking into how to upgrade, it is a good idea to first evaluate the current maturity of your organisation in regard to its existing threat hunting procedures. What is your current security posture or SOC efficiency? Organisations should additionally assess their readiness against threats by leveraging the combination of using a cybersecurity maturity model and collect insights from various frameworks and threat databases.

Decide on a threat hunting path. After understanding their threat-hunting needs and goals, organisations can start researching and finding the right software to perform threat hunting. Security tools that natively incorporate SIEM, UEBA and AI analytics can help threat hunters pivot and get a comprehensive overview of the potential threat. If the security team finds a threat, then they resolve it and follow the organisation's procedures to maintain the security posture. A key part of that process is deciding whether to cultivate threat hunters within the organisation, outsource threat hunting to a third party or develop a hybrid arrangement using both in-house and out-of-house expertise – also known as SOCaaS.

Address the skills shortage. Security upgrades are never ending, as cyberthreats will never relent. Criminals will continue to become more sophisticated, requiring dedicated resources to keep up with demand. As a result of a skills shortage, recruiting cybersecurity professionals has been difficult. In response to ever-evolving threats and a lack of in-house cybersecurity skills, cybersecurity-as-a-service (CyberaaS) has grown as a way to deploy proactive defences without expanding IT resources. In the event of an attack, organisations can prepare to mitigate the damage by outsourcing or augmenting IT teams to include managed cybersecurity services.

Introduce AI. In today's era of intelligence, real-time analytics and predictive analytics depends on the quality and quantity of the data. It is imperative that the underlying data is complete and easily accessible and information and insight derived should be accurate, clear, timely and actionable. Predictive AI-based threat hunting platforms are potential solutions to this problem because they integrate threat-hunting tools with dashboards for exploring threat signals and vulnerable assets. Through utilising these tools, any organisation can establish a centralised cybersecurity command centre that identifies, prioritises and prevents cyber-attacks across the blockchain.

Prepare and practice an incident response plan. This is good practice for any cybersecurity division, not just for blockchain operators. As threat hunting operations grow, security managers must develop an incident response plan that can accommodate any changes in protocols as it relates to detection, reporting, triage and analysis, containment and post-incident clean-up including regulatory disclosure.

It's impossible to stop all cyberattacks, so when a breach occurs it is vital the cyber-security team is alerted as soon as possible. False-positive alerting generates tremendous noise for security teams globally. By utilising machine leaning, engines are able to observe historic true and false positives for similar events using enforced learning to decide whether an alert should be triggered. In order to minimise attacker impact and further secure an environment, organisations must prioritise proactive, hypothesis-driven discovery in the form of threat hunting in light of ransomware incidents and advanced persistent threats that continue to expose the stress points of traditional detection capabilities ●

Ralph Chammah is CEO at OwlGaze.

After understanding their threat-hunting needs and goals, organisations can start researching and finding the right software to perform threat hunting

Picture credit: Ivan Babydov