Picture credit: Adobe Stock

PAYING THE PRICE TWICE

David Carvalho *examines the correct way to react to ransomware*

Ransomware attackers extorted $456.8-million from victims in 2022, 40 percent down from the $765.6-million in the previous year. However, before we clink glasses to celebrate victory, there are some significant caveats to consider. There were 19 reported web3 hacks in Q1 2023 – up from 16 in Q1 2022 and 10 in Q1 2021. The recent hack of Euler Finance where $197-million in staked Ether tokens (stETH), was drained from the protocol, is a case in point. How organisations react to these attacks differs vastly and the outcomes will most definitely shape regulation in this beleaguered asset class.

In a January 2023 poll conducted by Naoris Protocol, a decentralised cyber security platform, it would appear that businesses are indeed doubling down on ransomware attackers by **r**efusing to pay the price of clawing back stolen/encrypted data. The poll asked the question: "If you or your company were a victim of a ransomware attack, would you pay the attacker (including trying to negotiate a lower fee)?"

Interestingly, the majority of the just under 600 respondents, (70.8 percent), said that they would not pay the ransom and would report the attack to the relevant authorities. This was surprising, as the findings do not correlate to other statistics on ransomware reporting. According to other reports, just 42 percent of companies who fall prey to a ransomware attack actually report it.

David Carvalho, CEO and co-founder of Naoris Protocol says: "It's much easier to take the moral high ground when the question is theoretical. When confronted with the reality of a ransomware attack that could cost your business millions per day, along with potential brand and reputational damage, businesses may be more reluctant to take a moral stance".

The next largest group in the poll, 16.55 percent, said they wouldn't pay the ransom nor report the attack, but would rely on back-ups to restore data. Other research shows that out of all ransomware victims, 32 percent pay up, but they only get 65 percent of their data back, with only 57 percent of businesses successful in recovering data from backups. So this strategy does not work as an effective measure to retrieve data. To add insult to injury, more than a third of companies who paid a ransom to retrieve their data, were targeted a second time and charged even more than the first attack, with 41 percent failing to recover all of their data.

As well as a rising number of successful reported ransomware attacks in Q1 2023 compared to Q1 2022, attack methods are also evolving. Traditionally, attacks are carried out by encrypting target data and perpetrators charge victims a fee for the decryption key. Now criminals are resorting to"double extortion" tactics, threatening to sell the data if the ransom isn't paid. They also use Denial of Service attacks and harassment via email or phone. While the number of ransomware payouts has dropped, the average ransomware amount is increasing. Unit 42, a cyber risk assessment company reported that the average ransom demanded in 2021 was approximately $2.2-million, a 144 percent increase from the average demand of $900,000 from cases analysed in 2020.

Estimating the number of successful ransomware attacks (attacks that resulted either in data leaks or ransom payments) is challenging, as reporting is opaque and inconsistent. It's estimated that between May 2021 and June 2022, there have been 3,640 successful ransomware attacks globally.

Roughly 73 percent of organisations have suffered at least one ransomware attack in the past 24 months, and 60 percent of companies admitted that cyber criminals had been working inside their company for up to six months before the attack.

Other respondents in the Naoris Protocol poll, (5.32 percent) said they would pay the ransom but not report it, and 7.32 percent said they would pay and report. Again, figures vary widely, according to a survey of 300 US-based IT decision makers, 64 percent had been the victims of a ransomware attack in the last year, and 83 percent of victims paid the ransom.

More than a third of companies who paid a ransom to retrieve their data, were then targeted a second time and charged more than the first attack

There are several top-class organisations doing analytics on cyber-threats, and their reports have brought home the alarming extent and scale of cyber-threats. However, it's important to note that the make-up of sample audiences can vary widely, potentially biasing some results. For example, surveying a group of enterprise CEOs versus a SME cohort presents material variances in the way they approach cyber crime.

Then there is the issue that no one wants to address: what happens to the data that gets stolen? Criminals will still have the files and can sell the information on the Dark Web with impunity. Ultimately, if the company that has been subjected to an attack gets their data back and manages to dodge a reputational bullet by not reporting it, their clients and networks will still pay the price of the breach, worse still, they won't even know their data is in the hands of criminals.

ULTIMATELY THE BEST CURE IS PREVENTION, AND THIS STARTS WITH EDUCATION OF EMPLOYEES

While ethically wrong, it is understandable why companies don't want to reveal they have been a victim of an attack. A report by IBM and Forbes found that 46 percent of organisations that experienced a cyber security breach suffered significant reputational damage. A good example of this is Travelex, a foreign exchange company that collapsed into administration seven months after it suffered a ransomware attack. It disrupted the company for more than a month and it eventually paid the attackers $2.3-million.

It's becoming increasingly clear that companies and institutions will not be able to hide a ransomware breach in the future. Regulators and Governments are suiting up against ransomware amid escalating attacks. It's a race against time, especially in the areas of critical infrastructure and government. Even though it was not a ransomware demand, the recent attack on NATO's Special Operations Headquarters and Strategic Airlift Capability, both working to deliver humanitarian aid to victims of the recent Turkish-Syrian earthquake, is a prime example of the skills of cyber criminals. In a more recent attack, The US Marshals Service (USMS) reported the theft of sensitive law enforcement information, proof positive that even law enforcement is not beyond the scope of hackers.

Currently there is legislation on the table making it illegal for companies to pay ransoms. A 2020 ruling by the US Department of Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) states most cases of paying a ransom are illegal. The EU has followed suit, EU member states can impose fines on paying ransoms under the Security of Network and Information Systems Directive (NIS Directive). Government proposals from leaders in Australia and appeals from Europol are also being tabled.

President Biden recently laid out a new cyber security strategy, urging all industries to start taking their cyber security responsibilities more seriously. Up until now, reporting has been voluntary, with the government encouraging companies to report system intrusions and to regularly "patch" their programmes to shut down newly discovered vulnerabilities. The voluntary stance has not delivered the desired results, so the strategy recommends far broader mandates on private industry, as the vast majority of US digital infrastructure is controlled by this cohort. The US is concerned by attacks from abroad and the increasingly sophisticated technology being used.

WHILE PAYOUTS HAVE DROPPED, THE AVERAGE RANSOMWARE AMOUNT HAS INCREASED

Carvalho says: "Ultimately the best cure is prevention, and this starts with education of employees and individuals on the role they can play in thwarting the attacks of cyber criminals. Emerging technology will also play a massive role in mitigating attacks. In an increasingly networked and decentralised world, every device with an internet connection is a potential point of failure or point of entry for a cyber attack. Traditional cyber security works on the premise that the access points are ring-fenced on their closed infrastructure network. However in an increasingly decentralised and networked business environment, the distribution of devices and cloud servers pose a risk, as they become single points of failure regardless of current cyber security controls, eg: employee's mobile phones, laptops, servers etc. IT architectures are centralised, meaning there is a central point of control or authority. This makes it easy for attackers to target and compromise the entire system or take over processes. This heavily impacts resilience to threats and business continuity, even if threats are detected and risks are identified and known, it's usually too late to stop a major breach".

Decentralised Cyber security Mesh is being recognised as an effective tool against cyber threats, in a decentralised cyber security environment, when a hacker interferes with code in a system or network through a device, there would be an instant alert and the device could potentially be locked out of the network, preventing the full network infrastructure from being compromised – bringing decentralised trust and security enforcement to centralised spaces. Web 2 cyber security is not effective in mitigating web 3 threats, while the technology gap is unresolved, businesses will continue to face cyber threat headwinds. In the meantime, given that 95 percent of all hackers are let in the front door by individuals clicking on phishing links and the like, education would be a very worthwhile investment ●

David Carvalho is CEO and Co-Founder of Naoris Protocol.

Criminals are resorting to"double extortion" tactics, threatening to sell the data if the ransom isn't paid

Picture credit: Adobe Stock