Bitcoin's alleged architect troubled by financial woes

SYDNEY/SINGAPORE: Australian Craig Steven Wright is the latest in a line of men alleged to be the mysterious creator of bitcoin, a digital currency that has attracted the interest of banks, speculators, criminals and regulators. Wired magazine, which along with fellow US publication Gizmodo published a story outing Wright based on a stash of leaked documents and emails, called him a genius.

But interviews with those who have done business with Wright, and a closer inspection of documents published by the two technology websites paint a more complex picture. They point to a smart but sometimes abrasive figure facing growing legal and financial problems at least in part caused by his involvement with bitcoin. While it was not immediately possible to support or refute claims that he is Satoshi Nakamoto - the person or group credited with writing the paper, protocols and software that led to bitcoin - some of those who worked with Wright raised questions about the timing of the leak and the likelihood that he was Nakamoto.

"It can't be him, there's no way he could have kept quiet about it this long," said a former senior employee at Hotwire Preemptive Intelligence, who also detailed Wright's difficulties with authorities over his Australian businesses' bitcoin dealings. The former employee, who asked to remain anonymous, citing legal issues, said the collapse of Tokyo-based bitcoin exchange Mt. Gox in early 2014 had a direct effect on Hotwire, which is registered in Australia and is in the hands of administrators attempting to unravel disputes with the Australian Tax Office (ATO). The collapse of Mt. Gox and the disappearance of hundreds of millions of dollars' worth of bitcoin coincided with a decision by the ATO, according to the documents, not to regard Wright's bitcoin as money and that the digital currency therefore was taxable like any other commodity. This punctured Hotwire's hopes it could recover more than A$3 million in tax credits and helped sink the company.

"Their cash flow disappeared right around the time Mt. Gox collapsed," the former employee told Reuters, adding that staff at Hotwire were told that Wright had funds in a bitcoin trust, in which he was a beneficiary along with other unnamed parties.

"When they were trying to find cash flow after they were hit by Mt. Gox, they couldn't sell the bitcoins in the trust to get the cashflow because they couldn't break this wallet as there are other trustees."

Wright has not commented publicly on the Wired and Gizmodo reports, and Reuters' attempts to contact him using various listed email addresses were unsuccessful. Wright's blog was taken down on Wednesday, his Twitter and Google+ accounts were deleted and access to his full LinkedIn profile restricted.

Attempts to reach Wright's lawyer were unsuccessful and another former Hotwire employee said all staff had been instructed not to speak to the media. Wright's whereabouts are unknown. The landlord at his rented Sydney home told a Reuters reporter that Wright had been due to move out with his family before Christmas to move to London, where he recently attended a conference and was, according to his LinkedIn profile, enrolled for a Master's degree at University of London.

Unmasking the mysterious Nakamoto

The ATO was behind raids by Australian police on Wednesday on Wright's home and office in Sydney. It declined to provide any further detail on the raids, citing legal confidentiality. Administrator McGrath Nicol told creditors last month that the ATO slapped a A$1.7 million fine on Hotwire over its tax refund claims. The former Hotwire employee said Wright once paid in bitcoin to buy a banking platform from a Middle Eastern seller. He then sought to claim a goods and services tax return, or import credit, in cash worth millions of dollars which the ATO denied.

Bitcoin experts say that unmasking Satoshi Nakamoto would be significant for the industry. Not only would the proven founder likely hold some sway over the future of the bitcoin protocol, but Nakamoto may also hold enough bitcoin to influence the price of bitcoin.

"What people are looking for essentially is the Bill Gates of bitcoin," said David Glance, a director of innovation at the University of Western Australia and noted bitcoin expert, who doubts that Wright is Nakamato, pointing to pro-capitalist, anti-hacking columns Wright wrote for The Conversation, a local publication, in 2011. After ditching several directorships in July, Wright remains a director of three companies, including Hotwire, which had sought to launch the world's first bitcoin bank. —Reuters

LAS VEGAS: Dag Reckhorn, Faraday Future's global vice president of manufacturing, is congratulated by dignitaries after a news conference on Thursday in Las Vegas, announcing plans for the Chinese-backed electric carmaker's $1 billion manufacturing plant to be built in North Las Vegas. —AP

Amit Yoran's 2016 Predictions

By Amit Yoran, president of RSA

2015 was most notably characterized by security vendors claiming to be able to prevent advanced threat breaches when the reality is, they can't. It was characterized by enterprises recognizing the need to monitor and defend their digital environments differently, but continuing to center their security programs on the same technologies and approaches they have been using - hoping for a different outcome, but not acting differently.

2015 saw threats continuing to evolve faster than most organizations' ability to detect and respond to them. What was considered an "advanced" threat in years past has become a commodity today with sophisticated malware and exploits available for the price of a movie ticket. As troublesome as these observations seem, the most impactful evolution goes almost entirely unreported and misunderstood. The threats that matter most, today's pervasive threat actors execute attack campaigns comprised of multiple compromise methods and multiple backdoors to assure persistence. Incomplete incident scoping has become a critical failure point.

We're starting to see progress in some areas as security investments begin to shift from a maniacal focus on prevention, toward greater balance on monitoring, detection, and response capabilities. It's become clichÈ to say that breaches are inevitable and that faster detection and more accurate incident scoping is the way forward, but too many organizations are trying to do these very different tasks using the technologies and processes they have on hand...not designed nor capable of answering their need. Here are some of the emerging trends that our industry and organizations need to be ready for in 2016:

1. Strategic Data Manipulation and Disruption - Organizations will begin to realize that not only is their data being accessed inappropriately, but that it is being tampered with. Data drives decision making for people and computer systems. When that data is unknowingly manipulated, those decisions will be made based on false data. Consider the potentially devastating consequences of misrepresented data on the mixing of compounds, control systems, and manufacturing processes.
2. Increasing Attacks on Application Service Providers - As organizations become more comfortable with the "as a Service" model, many of their most sensitive applications and data reside in the Cloud. The aggregation of this valuable data from many companies creates an incredibly lucrative target for cybercriminals and cyber espionage. A deeper appreciation of third party risk is needed.
3. Hacktivism and the Attack Surface - Per my earlier comment, as cyber-attack tools and services become increasingly commoditized; the cost of attacking an organization is dropping dramatically, enabling more attacks that do not have financial gain as the primary focus. Sophisticated hacktivist collectives like Anonymous have been joined by relatively unsophisticated cyber vigilantes. Organizations need to realize that financial gain is no longer the only or even the biggest driver of some of their adversaries. Security operations and risk managers should evolve their understanding not only of the threat, but also of what, why, where, and how they are being targeted.
4. ICS (Industrial Control Systems) pushed to the Breaking Point - Intrusions into systems that control operations in the chemical, electrical, water, and transport sectors have increased 17-fold over the last three years. The advent of connected and automated sensors with the IoT aggressively exacerbates these issues. The growth in the use of cyber technology for terrorism, hacktivists and other actors, combined with the weakness of ICS security generally, combined with the potential impact of bringing down a power grid or water treatment plant (hello, California), makes the critical breach of an ICS in 2016 extremely concerning and increasingly likely.
5. Shake-out of the Security Industry - Our industry has been awash in venture capital and as a result, foolish investments have been made in strategies and technologies that are little more than snake oil. As organizations' security programs continue to mature, they are learning that claims of being able to prevent advanced threat breaches are nothing more than fantasy. Expect to see a shake-out in the security industry as organizations maturing understanding of advanced threats increasingly drives their security investment decisions.