Bibliography details

Name of the Serial/Publication: Veritas

Volume No.: 1

Issue No.: 2

Month & Year of publication: February 2022

Page numbers: Case studies (53-55)

Title of Article: Karnataka bitcoin scam

CONTRIBUTOR (s)

1. Ms. Amulya M

KARNATAKA BITCOIN SCAM

Ms. Amulya M

INTRODUCTION

International hacker Srikrishna Ramesh alias Sriki (26) is the face of the multi-crore bitcoin scam. Sriki, a habitual criminal, claims to have hacked online gaming websites, foreign company portals and the state government's e-procurement portal.

On November 4, 2020, Bengaluru's Central Crime Branch (CCB) police arrested hacker Srikrishna under the Narcotic Drugs and Psychotropic Substances Act for allegedly obtaining drugs using bitcoins via the darknet and peddling it to high-profile clients. On investigation, CCB determined that Sriki was involved in illegal hacking, including that of the Karnataka government's e-procurement portal.

Before going further, we should now understand some terms like Cryptocurrency and how Crypto Mining and exchange take place.

Cryptocurrency: Cryptocurrency is a virtual asset used as a medium of exchange through a network of computers. The currencies are decentralized structures that use blockchain technology and distributed ledgers across numerous computers, also called non-official cryptocurrencies. They are no longer patronized by any government authority and in most cases are without any tangible, physical assets.

How is cryptocurrency earned?

Crypto-mining: Bitcoin mining is the technique of creating new bitcoin by solving computational puzzles. The mining process also confirms transactions on the cryptocurrency's network and makes them trustworthy.
Crypto buying and exchange: Basically, crypto exchanges permit the conversion of one crypto to another and the buying and selling of cryptocurrencies. These platforms set the price of digital assets (both coins and tokens), based on trading activities. Cryptocurrency can be brought from trading platforms like Bitfinex and coinbase. And exchange can be taken by offering to accept cryptocurrency in exchange for service.

Attack Methodology: In his voluntary declaration to the CCB police, Sriki said he had hacked the Bitfinex exchange twice. "Bitfinex became his first largest Bitcoin exchange hack." And the second instance was a simple spear-phishing attack that led to two Israeli hackers operating for the army and getting access to the computers of one of the employees, which gave them access to the AWS cloud account. He exploited a bug in the data centre which gave them KVM (Kernel-based virtual machine) access to the server. They rebooted the server into GRUB (GNU Grand Unified Bootloader) mode, reset the password, logged in, reset the withdrawal server passwords and routed the money via bitcoin to his bit-coin address. And he had made a profit of around 20,008 BTC (bitcoin).

In August 2019, authorities at the e-procurement cell filed charges with the State Police Cyber Crime Branch, professing that an unknown person took Rs 11.5 crore and the officials were able to prevent the theft of another Rs 7.37 crore.
Sriki also admitted he had hacked into the Karnataka government's e-procurement portal in 2019. The accused alleged that he acquired access to the procurement site in June 2019 by exploiting "a remote code execution vulnerability", that gave him access to tender bid details such as transaction details, bid reference, payment amount, IFSCs (Indian

Financial System Code) and bidders account numbers.
Cyber forensic role in Bitcoin Scam Investigation: Four laptops have been recovered from hacker Srikrishna Ramesh. The analysis of hard disks from a laptop has discovered data of a hack carried out at an e-procurement cell of the state government where Rs 11.5 was stolen by a hacker gang.
According to the Cyber forensics report, one hard disk "fragment 01" recovered from a MacBook belonging to Sriki contains hacking data for alleged hacking of the e-proc.gov.in of the e-governance cell of the State Government.
The Cyber forensics team analyzed data held in a cloud server by the hacker and found that Sriki had as much as 76.13 lakh public addresses for Bitcoins and as many as 26 e-wallets. Sources said these could have been acquired by hacking or through data trading on the dark web as part of hacker groups to steal cryptocurrency.

Challenges facing the crypto-landscape in India

Indeed as the government is drafting a bill on cryptocurrency, around five million people are formally using it. But you cannot regulate people holding the cryptocurrency, as the system works on blockchain technology which provides privacy to its users. The government can regulate the trading exchanges or platforms.
In India, Bitcoins are not a legal tender and are not accepted for payment. There are however websites where you can redeem the cryptocurrencies for vouchers from Amazon, Flipkart or other leading brands. It is only an investment that the people are holding.
The government's move to introduce GST (Goods and Services Tax) for crypto trading through the bill would impact the investor and not help curb hacking, experts say.
India is coming up with a new vulnerability disclosure policy. If you are a security researcher or a hacker, you can report the vulnerabilities to the Computer Emergency Response Team.

REFERENCES:

- Frankenfield, J. (2022, January 17). Bitcoin Mining. Investopedia. Retrieved from https:www.investopedia.com/terms/b/bitcoin-mining.asp
- Nandakumar, P. (2021, November 20). The incredible saga of "Sriki", the hacker at centre of Karnataka bitcoin scam. The Week. Retrieved from https://www.theweek.in/news/india/2021/11/19/the-incredible-saga-of-sriki-the-hacker-at-centre-of-karnataka-bitcoin-scam.html