Researchers find Bitcoin's Lightning network susceptible to cyberattacks

May 12 2020, by Diana Hernandez-Alende

Credit: CC0 Public Domain

Bitcoin, the decentralized digital currency without a central bank, saw a

decline in price due to COVID-19. After announcements of travel restrictions, the price plummeted from $8,000 to $3,800 in one day, according to a report by CryptoCompare.

Despite the crash, people haven't lost interest in Bitcoin. Forbes reported that Americans are using their stimulus checks to buy Bitcoin and other cryptocurrencies.

In 2017, Bitcoin launched Bitcoin Lightning, an overlay network that allows for a faster, efficient and more affordable way to send Bitcoin globally. This was in response to network clogging.

The benefit of a speedier transaction, like sending Bitcoin in seconds, also comes with a disadvantage. Researchers at FIU have discovered that Lightning enables attackers to perform cyberattacks such as controlling botnets.

Botnets are a set of devices that infect computer machines with malicious software. The researchers published a paper on the subject and built a proof of concept called LNBot.

"The goal of the research is to show that Lightning can be used to control a botnet," said Ahmet Kurt, a Ph.D. student in electrical and computer engineering and co-author of the paper. "We offer potential countermeasures to stop botnets like the LNBot."

Such attacks with this botnet include denial of service (DoS) attacks, information and identity theft and spam messages.

How would these attacks take place on Bitcoin Technology?

According to Kurt and the research team—consisting of doctoral students Enes Erdin and Mumin Cebe, and College of Engineering &

Computing professors Kemal Akkaya and Selcuk Uluagac—botmasters would corrupt computers with infectious programs, to control the computers using command and control (C&C) servers, without giving away the botmaster's identity. Botmasters are hackers who control botnets.

Botmasters create a command infrastructure to control bots and have a communication channel between themselves and the bots. The system is a one-way conversation, where servers wouldn't be able to respond to botmasters.

After two years of the introduction of Lightning, the network grew exponentially with 12,400 nodes. Nodes refer to a device, like a computer, that contains a copy of the transaction history of the blockchain.

In general, Bitcoin offers some anonymity. However, the activity of botnets can be traced by any observer, leaving the history of the malicious activity on the blockchain.

The aim of creating Lightning was to decrease the load on the Bitcoin network, providing affordable fees for transactions and reducing the validation times of transactions. With Lightning, Bitcoin transactions are "off-chain" and are not recorded on the blockchain, making it a decentralized system. Users' identities also remain fully anonymous.

Kurt's research focuses on how Lightning is the ideal place for botmasters to take advantage of the existing techniques and perform malicious cyber activities.

"Since transactions aren't recorded on the blockchain, a botmaster can communicate with the C&C servers, and would never be discovered because there is no way to trace it back to the original botmaster," said

Kurt.

Kurt and the team's LNBot is in Bitcoin's Testnet, which is the network Bitcoin developers currently use for testing. There, the researchers show that by encoding payments through Lightning, a botmaster can send commands to the C&C servers. Then, the servers would relay the messages to the bots they control, launching an attack.

The researchers worry there are few steps to prevent these attacks. A major setback is Lightning does not have a central model to authorize or reject messages on what can or can't be passed.

Possible countermeasures that may help detect potential activity and limit the damage to a user, according to Kurt, include taking down Lightning to prevent future attacks and compromising and turning off a C&C server.

A C&C server can be detected, resulting in the revelation of its IP address. Law enforcement could use this IP address to find the physical computer. However, this wouldn't reveal the identity of the botmaster.

Provided by Florida International University