Using blockchain contracts to build botnets

March 10 2022, by David Bradley

Credit: CC0 Public Domain

Blockchain is a decentralized ledger technology that secures the integrity of transactions through digital signatures and will be familiar to anyone who has investigated digital or "crypto" currencies. The technology has many more putative applications than crypto currencies, however, and has been discussed in the context of secure, digital voting and governance systems and corporate contracts. As with any technology, there are ways it might be abused for nefarious purposes, such as the spreading and implementation of malware.

Commonly, networks of interconnected computers, botnets, surreptitiously recruit thousands of computers often through phishing and malware attacks for the benefit of a central entity, the bot commander. The commander might then use the botnet to carry out distributed denial of service attacks (DDoS) on other systems with malicious intent. A botnet might also be used to send spam, host criminal websites, and perform other activities, such as spreading yet more malware and implementing phishing attacks. The key point, however, is that security experts can often identify botnet activity through the internet addresses of the central command machine or simply the activity of the bots within the network.

A new study in the *International Journal of Information and Computer Security*, shows how blockchain technology and smart contracts might be exploited to create a distributed network of computers. Such a network, lacking a central server, could be used to build a botnet, a system for attacking and hacking other online resources for criminal gain or other malicious purposes.

The proof of principle offered by Omar Alibrahim of Kuwait University in Safat, Kuwait and Majid Malaika of omProtect LLC in Washington DC, U.S., should offer fair warning to those running potentially vulnerable computer systems to be on the alert from a new type of attack from bot contracts, "botracts." They point out that commands added into

a blockchain-based smart contract cannot be removed nor modified, making a botract highly resilient to any attempt to disarm it by security experts.

The very nature of blockchain technology, being self-sustaining, distributed, and immutable is what makes it vulnerable to this newly demonstrated exploit. It is the design issues of the underlying technology for deploying smart contracts—implicit end-user trust, lack of code scrutiny, and absence of governance—that are its advantages in legitimate use that might now be exploited for criminal and malicious purposes with unqualified anonymity.

In the short-term, the blockchain community must quickly develop tactical defenses against botracts, now that they have been described, but without resorting to expensive operations. In the long-term, the community needs to undertake a fundamental rethink and redesign of the blockchain with security in mind.

More information: Omar Alibrahim et al, Botract: abusing smart contracts and blockchain for botnet command and control, *International Journal of Information and Computer Security* (2022). DOI: 10.1504/IJICS.2022.121295

Provided by Inderscience