Monitor Deloitte.

blockchain INSTITUTE

Prevention of DDoS attacks with Blockchain technology

Distributed Denial of Service (DDoS) attacks are nothing new, but recent attacks are increasing in severity, complexity, and frequency and have therefore become a mainstream concern for businesses and private customers alike

The most recent DDoS attacks have been observed to hijack connected devices such as webcams, baby phones, routers, vacuum robots, etc. to launch their attacks.

The number of devices remotely controllable via apps is growing exponentially and the Internet of Things (IoT) is expected to easily surpass 20 billion connected devices by the end of 2020. One of the associated problems is that many of the connected devices are ill-equipped with security measures to prevent malevolent and improper usage, and thus prove to be the perfect, unsuspecting resources to be recruited into a botnet.

And it is already happening, often on a grand scale with the potential for a devastating business impact. In October 2016, the Mirai botnet, comprising around 100,000 IoT devices, took down numerous popular websites (Twitter, GitHub, Amazon, etc.) in a massive DDoS attack (1.2 TBPS) against the DNS provider Dyn. Similarly, an attempt to create a botnet essentially crashed routers of close to one million subscribers of Deutsche Telekom (one of the victims of the intended attack) when hackers, unsuccessfully, tried to recruit their routers into a botnet, but nonetheless managed to take the routers offline instead, cutting off Internet access for subscribers in the process.

30% of people plan to buy a connected device in the next 12 months.

AZ Digital Ventures Deloitte

The lack of proper security features for connected IoT devices is mainly driven by insufficient prioritization because the potential for disruption has been underestimated in the past, and manufacturing costs and profit potential dictate feature selection. That said, recent events may trigger a re-think to include and promote security features as part of a premium positioning for connected products. At present, infecting IoT devices for creating a botnet couldn't be easier for a competent hacker. And to make matters worse, it is actually possible to illegally rent botnet capacity with currently up to 400,000 connected devices ready to receive instructions. In addition, the way the Internet is structured (in a client/server model) permits a weakness in the infrastructure (DNS servers, Web servers, etc.) to become a bottleneck and a single point of failure.

How Blockchain technology could promote a secure IoT

Today's IoT ecosystem follows a centralized paradigm, which relies on a central server to identify and authenticate individual devices. This allows malicious devices to launch attacks against other equipment by means of a brute force Telnet attack or other attack vectors.

Blockchain technology could enable the creation of IoT networks that are peer-to-peer (P2P) and trustless; a setting which removes the need for devices to trust each other and with no centralized, single point of failure. A Blockchain, being a universally distributed ledger, ensures the security of all transactions through the cryptographic work of certain participants called nodes which validate those transactions, in return for rewards in the form of crypto-currencies such as Bitcoin. This removes the need for a central authority to authenticate a device to interact with another device and also authenticate a user to login to a device.

A DDoS (distributed denial of service) attack occurs when many devices connected to the Internet are recruited (as part of a 'botnet') to 'attack' i.e. simultaneously and repeatedly send traffic to a victim's server with the aim to overload it.

Botnets such as Mirai build their army and launch DDoS attacks in two core steps:

- They scan and compromise IoT devices to grow the botnet, by remotely accessing them using easily guessable login credentials (like admin/admin or 0000, etc.) to then install malware
- hey launch DDoS attacks based on instructions from a Command & Control server on which the botmaster places the instructions for the bots to read and act on

The use of a Blockchain to secure the IoT would mean that all devices and users of those devices would use public key cryptography that would substitue default login credentials. Instead, each user would have his own private key that would be essential for communicating with any device and the private key would be known only to the user, and hence not be easily hackable. Also, only the manufacturer will be able to install firmware on a device by signing the digital content using his private key. The device will not run code coming from an unknown source. The identity/public key pairs will be stored on the Blockchain to enable a device to lookup when any login request/digital content is triggered (as part of a decentralized PKI system based on Blockchain).

Also, since a Blockchain would mean that the IoT devices are part of a P2P network, the attacker's Command & Control server will not be able to gain access to publish the DDoS attack instructions. Hence, a rogue device will not be able to be controlled by the botmaster for the conduct of DDoS attacks.

Blockchain technology can hence support the creation of a secure P2P network, where IoT devices would interconnect in a reliable way while avoiding threats and rogue instructions from malicious sources. Current promising developments in regards to blockchain scaling show that the network could in future be able to support billions of devices.

In addition, a Blockchain could also be used to prevent DDoS attacks in several other ways as well:

- To address the type of DDoS attack on the DNS servers at Dyn, a Blockchain could be the basis for a decentralized DNS naming system. Today, DNS basically remains a centralized (on servers) one-to-one mapping of IP addresses to domain names. Access to it is controlled in such a way that

the people who own the domain are allowed to update the domain record. The same access control could be implemented on a Blockchain, allowing only legitimate parties owning the respective private key to update it. Since the (name, value) pairs would be stored on the Blockchain, they would be copied ubiquitously across all the nodes. Thus there would be no single point of failure (i.e. no DNS servers) and hence no possibility of a DDoS attack. These concepts are not just a construct of ideas: there are companies such as Blockstack, Namecoin, Nebulis, and many others that are currently working towards building such a decentralized DNS system.

- A further, more idealistic use of Blockchain technology is enshrined in the idea of reengineering the entire structure of the Internet as we know it, from a centralized client/server model to a decentralized model that does not rely on specific servers. No servers would mean no DDoS attacks. But how would this work? It would work by making use of the collective processing power and storage of the millions of connected devices in a peer-to-peer network secured by a Blockchain. Here, the data and applications would reside on a P2P network. Each data file would be broken into smaller pieces and stored in multiple nodes on the Blockchain. To retrieve a data file, one would not need an IP address. Rather, other parameters would be used to locate and retrieve data from the various nodes seamlessly. This setup would eliminate the need for centralized servers, hence eliminating

The Internet of Things (IoT) is expected to easily surpass 20 billion connected devices by the end of 2020.

Consequently, Blockchain technology is not only expected to affect banking and finance industry processes significantly, but also has the potential to provide the (technological) basis and features to make many aspects of everyday 'technological life' more secure and easier.

Potential risk – Blockchain Miners as targets for DDoS attacks

But a Blockchain itself could also be a target of a DDoS attack. An example would be a Sybil attack. Here the attacker tries to take control of the miner network with the creation of many mostly pseudo-anonymous clients. Such an attack is carried out by means of various denial-of- service attacks, such as the massive sending of data to make miners' work more difficult, so that miners are no longer able to process Blockchain transactions appropriately. But there are already a number of patents currently filed to prevent these direct DDoS risks for Blockchain.

Ongoing proliferation of connected devices will be one of the use cases that will help to accelerate the mass marketability of Blockchain technology

Nevertheless, mass-marketability for Blockchain-based solutions still seem some way off, since usability and user experience of many Blockchain use cases and applications are still in their infancy and need further refinement to facilitate widespread acceptance.

But we expect that to change quickly, and the market is likely to gain further traction with increasing end-user acceptance, which in turn would attract yet more developers to create new and easy-to-use Blockchain-based applications and solutions.

Contact us

Milan Sallaba
Partner
Technology Sector
Head Germany
Monitor Deloitte
Tel: +49 89 29036 7770
msallaba@deloitte.de

Mirko René Gramatke
Director
Tech Enabled Business Innovation
Strategy Lead
Monitor Deloitte
Tel: +49 89 29036 7811
mgramatke@deloitte.de

Thanks to further contributing authors:

Sawan Kumar
Senior Consultant
Deloitte Consulting

Jens Herrmann Paulsen
Senior Consultant
Deloitte Consulting

Monitor
Deloitte.

Issued 3/2017