2019 Podcast Glossary on Emerging Technologies

Anonymous - A non-hierarchical collective of hackers, Anonymous uses hacking (and cracking) techniques to register political protest in campaigns known as "#ops." Best known for their distributed denial of services (DDoS) attacks, past activities have included attacks against the Church of Scientology, Visa, PayPal, and others.

Bitcoin (BTC) – Created in 2009, Bitcoin is a form of digital cryptocurrency that is distributed on a peer-to-peer basis. It has no central bank, and transactions are conducted directly between individuals with permanent, public records stored in a blockchain ledger. Bitcoin is arguably the most well-known cryptocurrency.

BitPay - A payment processing company and software application that allows merchants such as eBay, Amazon, and other online shopping sites to accept bitcoin as payment for goods and services.

Blockchain - A digital file distributed to everyone participating in a cryptocurrency network. The blockchain acts as a kind of general ledger, keeping track of all the transactions that take place in the network. Everyone can look at the blockchain to see what transactions have taken place on the network, and the blockchain is sealed using cryptography so that no one can tamper with it.

Bot - A program that automates a simple action so that it can be done repeatedly at a much higher rate of speed and for a more sustained period than a human operator could. Bots are, in themselves, benign and used for many legitimate purposes, such as online content delivery. However, bots are often used in conjunction with cracking. For instance, bots may be used maliciously to make content calls that comprise denial of service attacks. "Bot" is also a term used to refer to the individual hijacked computers that make up a botnet.

Botnet - A group of computers controlled without their owners' knowledge and used to send spam or to make denial of service attacks. Malware is used to hijack the individual computers, also known as "zombies," and to send them directions.

Cracking - Breaking into a secure computer system, frequently to do damage or for financial gain. However, cracking is also employed to protest government policies or to make social statements.

Cryptocurrency - The broad name for digital currencies that use blockchain technology to work on a peer-to-peer basis. Cryptocurrencies don't require a bank to carry out transactions between individuals. The nature of the blockchain means that individuals can conduct transactions even if they don't trust or know each other. The cryptocurrency network keeps track of all transactions and ensures that no one reneges.

Denial of Service Attack (DoS) - DoS is used against a website or computer network to

make it temporarily unresponsive. This is often achieved by sending so many simultaneous content requests to the site that the server overloads. Content requests are the instructions sent, for instance, from your browser to a website that enables you to view content on that website. Some groups have used DoS attacks as a protest tool while others have used them for financial gain.

Firewall - A system using hardware, software, or both to prevent unauthorized access to a network, computer system, or device.

Hacking - The manipulation of code in the device or software for which the code was written. Some prefer the term "cracking" to describe hacking into a machine or program without permission.

Internet Protocol (IP) address. A distinct numeric fingerprint assigned to each device connected to a network using Internet Protocol. Through an IP address, a computer's activity can be tracked, its location discovered, and its user identified. Crackers can use an IP address to access a computer though one of its many ports, which regulate the flow of information to the computer.

Malware - A software program designed to hijack, damage, or steal information from a device or system. Examples include spyware, adware, viruses, and many more. The software can be delivered in a number of ways, including decoy websites, spam, and infected USB drives.

Peer-to-Peer (P2P) – Networked systems that work like an organized collective by allowing individuals to interact directly with others in the P2P environment. In the case of Bitcoin, the network is built in such a way that each user is broadcasting the transactions of other users.

Phishing - Tricking someone into giving you their personal information, including login information and passwords, credit card numbers, and so on by imitating legitimate companies, organizations, or people online. Phishing is often done through fake emails or links to fraudulent websites.

Spear phishing - A more focused type of phishing that targets smaller groups of victims ranging from a department within a company or organization to a single individual.

Spoofing - Altering the header of an email so that it appears to come from a legitimate or reputable source. A hacker might alter his or her email header, so it appears to come from the victim's bank. Internet Protocol (IP) spoofing is the computer version in which a packet is sent to a computer with the IP altered to imitate a trusted host in the hope that the packet will be accepted and allow the sender access to the target machine.

Spyware - A type of malware that is programmed to hide on a target computer or server and send back information to the master server. Data sought by spyware often include login and password credentials, bank account information, and credit card numbers.

Virus - Self-replicating malware that injects copies of itself into the infected machine. A virus can destroy a hard drive, steal information, log keystrokes, and perform many other malicious activities.