Cybersecurity and Information Security Newsletter

Issue 4 | October 6, 2020

Did you know that October is **Cybersecurity Awareness Month**? "Cybersecurity Awareness Month – observed every October – was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online."

Learn more here.

Table of Contents

Please feel free to submit cybersecurity and information security news items or request related topics to Daniel Shin (dshin01@wm.edu).

New Measure of Cyber Power Published: The Belfer National Cyber Power Index 2020

The Belfer Center for Science and International Affairs (Belfer Center) at the Harvard Kennedy School released the Belfer National Cyber Power Index 2020 (NCPI), a measurement tool to rank nations based on their cyber power. This ranking criterion measures (1) a nation's intent to pursue multiple national objectives using cyber means, and (2) its essential capabilities to pursue and achieve said objectives. The Index places the United States, China, and the United Kingdom as the top three nations with the most cyber power. Although China has already been recognized as having and exercising significant cyber capabilities (*See* *Cyberspace Solarium Commission*, U.S. Cyberspace Solarium Commission), this is the first time China has been recognized as a major cyber power nation among indices measuring national cyber power.

Background

In the past, several organizations created indices to measure nations' cyber power. For example, the International Telecommunications Union, an agency of the United Nations, released its Global Cybersecurity Index to highlight cyber resilience among member nations. *Global Cybersecurity Index*, International Telecommunications Union. Similarly, the Potomac Institute's Cyber Readiness Index 2.0 "evaluate[d] and measure[d] a country's preparedness levels for certain cybersecurity risks." *Cyber Readiness Index (CRI)*, Potomac Institute for Policy Studies. Although these two indices provide tools to compare nations' cyber abilities, both were published years ago. The Global Cybersecurity Index was last published in 2018 while the Cyber Readiness Index 2.0 was published in 2016. Their applicability to the current global climate is thus limited.

Report Summary

Published this year, the NCPI is the most up-to-date index that uses countries' cyber initiatives and capabilities to measure cyber power. The Belfer Center assessed 30 countries using 27 cyber capability and 32 policy intent indicators to "measure the cyber power of countries against their stated objectives." *National Cyber Power Index 2020* at 9. The top five positions are, respectively, the United States, China, the United Kingdom, Russia, and the Netherlands.

The NCPI also grouped countries based on different levels of national cyber capability and intent. From that perspective, the groupings look as follows:

1. Higher Capability, Higher Intent: U.S., U.K., China, France, and Germany;
2. Higher Capability, Lower Intent: South Korea;
3. Lower Capability, Higher Intent: Russia, Iran, Israel, and Netherlands; and
4. Lower Capability, Lower Intent: Egypt, and Lithuania.

Although the Belfer Center used open source information to develop the necessary indicators, the lack of publicly available data on nations' cyber capabilities and cyber operations may have caused some countries to be under-ranked. The Center itself notes that "countries

deliberately choosing to be opaque will be vastly under-ranked in the Index. [The Center] suspect[s] that Israel falls into this category." *National Cyber Power Index 2020* at 16.

Despite some limitations, the NCPI provides a much-needed updated framework to compare countries based on their cyber capabilities. The added measure of cyber capability and intent provides another valuable indicator to evaluate a country as a cyber actor.

The Index also offers additional insight to encourage cyber policy discussion among stakeholders, including considering how to legally handle cyber warfare under international law. As countries are investing more in cyber warfare, it is even more important to monitor the global cyber landscape because public and private infrastructures, which are becoming ever more interconnected through cyberspace, may become potential targets of state-sponsored crippling cyber-attacks.

Read the full report here.

Ethereum Classic suffers a third 51% attack in August

In August 2020, Ethereum Classic suffered a 51% attack for the third time. In response, the investment firm Ethereum Classic Labs (ETCLabs) accused NiceHash, a cryptocurrency platform that rents out computational power for mining, of having facilitated the 51% attack against the Ethereum Classic network. ETCLabs announced on August 31, 2020, that the firm would consider pursuing unspecified legal action to secure the Ethereum Classic cryptocurrency network. A 51% attack momentarily permits the attacker to monopolize all processing of cryptocurrency transactions, disrupting the network's ability to process new transactions properly. Such an attack threatens the public's confidence in the cryptocurrency and blockchain technology in general.

Background

Ethereum Classic is an alternative cryptocurrency network that was originally based on the Ethereum blockchain. In 2014, Ethereum was developed to become "a next-generation blockchain that had the ambitions to implement a general, fully trustless smart contract platform." *What is Ethereum Classic*, Ethereum Classic.

Proof-of-Work

Ethereum is a Proof-of-Work based cryptocurrency network, where cryptocurrency miners must provide easily verifiable data to prove that they have invested significant computing power before adding a block of new data on the blockchain. In general, a cryptocurrency blockchain is composed of sequential blocks of transaction data containing Proof-of-Work from the network's most powerful miners. If the network encounters multiple blocks purporting to be the next block of data on the blockchain, the network will accept the block containing Proof-of-Work from the most powerful miner. The Proof-of-Work system was implemented by Satoshi Nakamoto, the elusive creator of Bitcoin, to incentivize potentially-greedy attackers to support the blockchain network instead of attempting to undermine it by altering previously accepted blocks of transactions. Nakamoto's system presumed that the benefit of supporting

the blockchain network would always outweigh the cost of undermining the system for any user.

Ethereum Hard Fork?

In 2016, Ethereum's developers initiated a controversial hard fork to reverse the pernicious effects of a hack that had siphoned large amounts of cryptocurrency from the Decentralized Autonomous Organization, a smart contract-driven organization running on the Ethereum network. The hard fork involved invalidating previously accepted cryptocurrency transactions to "undo" the siphoning of stolen cryptocurrencies. After deleting blocks of identified transactions, Ethereum continued to run on the altered blockchain. However, some Ethereum miners continued to process the unaltered blockchain that included the stolen cryptocurrency transactions. With a chain split occurring between the altered and the unaltered blockchain, Ethereum Classic, which uses the unaltered blockchain, was formed, while Ethereum adopted the amended blockchain.

The 51% attack

Competition among cryptocurrency miners makes it nearly impossible for any miner to continuously control what new data gets added to the blockchain. The distributed and decentralized nature of mining networks makes it difficult for any entity to assert total control over processing of cryptocurrency transactions.

When a group of miners possesses computing power exceeding 50% of the cryptocurrency network's computing power, it has monopolistic control over what new data blocks get added to the blockchain. Also referred to as a 51% attack, this monopolistic control can disrupt transaction processing and even reverse completed transactions. Akin to a majority shareholder having significant control over a company, perpetrators of a 51% attack can have temporary control over which transactions get added to the blockchain. *51% Attack*, Investopedia; *What is a 51% Attack?*, Binance Academy.

Between July 30th and August 1st, 2020, an Ethereum Classic miner suddenly inserted 3,693 blocks of past transactions (transactions covering over 15 hours) to the Ethereum Classic blockchain. Usually, the insertion of that many blocks is ignored by the cryptocurrency network, because a single miner conceivably cannot provide competing Proof-of-Work for the past 15 hours that exceeds the computational power of all other miners combined.

According to Ethereum Classic developers, one of the major Ethereum Classic mining pools, a group of miners that pool computational power, went offline to perform maintenance. As a result, the total computational power of all Ethereum Classic miners decreased drastically but temporarily.

While the mining pool was offline, an "offending miner" purchased a vast amount of computational power from NiceHash to produce blocks of transactions on its own with Proof-of-Work, which exceeded the rest of the miners on the Ethereum Classic network. NiceHash is a hash renting service that allows individuals to anonymously purchase hashing power (i.e., computational power) to mine various cryptocurrencies. Individuals pay in Bitcoin, and NiceHash directs its arsenal of mining machines, which belong to other users renting out hashing power, to the individuals' mining accounts.

The offending miner likely purchased enough computational power from NiceHash to exceed the cumulative computational power of other miners on the Ethereum Classic network. The offending miner also likely produced its own blocks of transactions while being disconnected from the Ethereum Classic network. When the offending miner inserted 15 hours' worth of past transactions, its submitted blocks had higher Proof-of-Work than what the rest of the Ethereum Classic miners produced. As a result, Ethereum Classic underwent a blockchain reorganization, where the previously processed blocks by other miners were replaced with the inserted blocks by the offending miner.

Although the Ethereum Classic network suffered a 51% attack, its developers observed that no double-spending attack occurred, suggesting that the offending miner unintentionally initiated a 51% attack. As a result of the attack, various cryptocurrency exchanges either delisted Ethereum Classic as part of the cryptocurrency listings or required longer confirmation times before validating transfers of Ethereum Classic within the exchanges.

The accusation against NiceHash and other hash rental services

ETCLabs accused NiceHash of facilitating the 51% attack and announced a new initiative to "engage law enforcement and global regulators to bring accountability and transparency to hash rental." *Ethereum Classic Labs to Pursue Enforcement and Regulation of Hash Rental Platforms*, Ethereum Classic Labs (Aug. 31, 2020). Most cryptocurrency exchanges implement robust Know-Your-Customer guidelines (KYC) and anti-money laundering programs, including requiring users to produce photo identification and undergo manual identity verification processes before being able to use the exchange services. *See*, *e.g.*, *Identity Verification FAQ*, Coinbase. ETCLabs alleged hash rental platforms like NiceHash operate without adequate regulation, "potentially facilitating money laundering and other illegal activities."

NiceHash responded that the company "closely cooperates with law enforcement to ensure that further investigations and undertakings are conducted swiftly, lawfully and according to our Terms of Service and Privacy Policy." *Official response regarding the latest 51% attack allegations*, NiceHash (Sept. 1, 2020). However, it conceded that its hash rental services could be used to conduct a 51% attack against a cryptocurrency network. ("Technically, it is impossible for NiceHash or any other miner behind a pool to detect if its hash power is/will be abused for a 51% attack.")

Analysis

The U.S. Securities and Exchange Commission (SEC) considers certain crypto-assets to be securities, subjecting them to securities regulations. *Spotlight on Initial Coin Offerings (ICOs)*, U.S. Securities and Exchange Commission. The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) considers entities facilitating cryptocurrency exchanges, including those exchanging cryptocurrencies with fiat currencies, as money services businesses, which require the implementation of anti-money laundering policies. FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*. As such, cryptocurrency exchanges are subject to various regulations by federal agencies.

Cryptocurrency Exchange and Laundering

As ETCLabs correctly pointed out, hash rental services, including NiceHash, are not currently subject to the same types of regulations as cryptocurrency exchanges, because those services do not directly facilitate cryptocurrency exchanges with other types of commodities. Users are merely purchasing computational power, which can be used for cryptocurrency mining purposes. By purchasing hashing power with Bitcoin, users can mine almost any major type of newly created cryptocurrency.

Newly created cryptocurrency coins do not have any transaction history attached, so NiceHash effectively allows users to exchange their Bitcoin with freshly minted cryptocurrencies with no previous transaction history. Cryptocurrency transaction history is an important feature for law enforcement, because it could be used to track illicit transactions. Through NiceHash, criminals have a way to obtain new and transaction-history-free cryptocurrencies with Bitcoin, which itself has all previous transaction history recorded. Because NiceHash allows anonymous users to use its platform, both legitimate users and criminals can obtain fresh cryptocurrencies without any KYC in place. The lack of KYC effectively makes NiceHash and other hashing rental services an attractive platform for cryptocurrency laundering.

FinCEN has broad legal authority to pursue initiatives against money laundering practices and other financial crimes. 31 U.S.C. § 310. Currently, FinCEN has not made any announcements against hashing rental platforms, but the ease of use to potentially launder cryptocurrencies may expand FinCEN's investigative scope to scrutinize and regulate hashing rental platforms like NiceHash.

The 51% attack feasibility revisited

Although the Proof-of-Work requirement greatly incentivizes mining users to process pending transactions and not alter past transactions, it does not eliminate the possibility of data tampering on the blockchain. If a mining user somehow obtains hashing power greater than the rest of the network, then that user can create and submit alternative, past blocks of transactions that would be accepted by the network.

Ethereum Classic had a temporary drop in network hashing power, which made it economically feasible for the rogue miner to purchase enough hashing power to exceed the hashing power of the rest of the mining network. Popular cryptocurrencies, such as Bitcoin and Ethereum, do not have this problem, because the total hashing power of the mining networks is quite immense. NiceHash and other hash rental services, by themselves, simply do not have enough rentable hashing power initiate a 51% attack against popular cryptocurrencies.

The recent 51% attack against the Ethereum Classic network demonstrates the potential fragility of permissionless, decentralized blockchain networks. Implementing Proof-of-Work mechanisms may not be enough to protect against data tampering. Infrastructure using blockchain technology should consider using extra protection, including the implementation of a permissioned blockchain network and the integration of an independent data backup system.

Read the full article here.