RAPID7 RESEARCH

OFF THE CHAIN:

Observing Bitcoin Nodes on the Public Internet

By Derek Abdine, Senior Director Rapid7 Labs, Rapid7
Jon Hart, Senior Security Researcher, Rapid7
Bob Rudis, Chief Data Scientist, Rapid7

May 7, 2018

CONTENTS

Introduction ... 3

Bitcoin Network Diversity ... 5

Bad Actors in the Bitcoin Network ... 7

Server Messaging Block ... 9

Ethereum? ... 9

HTTP ... 9

Ports, Ports, Ports ... 9

Who, What, and Why? ... 10

The Future ... 11

Appendix A: Methodology ... 12

Appendix B: Tables ... 13

About Rapid7 ... 20

INTRODUCTION

Over the past several years, blockchain-based technologies, particularly cryptocurrencies like Bitcoin, have seen a massive surge in popularity. As with any technology, when its popularity grows, so does its attractiveness to attackers, the surface area for attacks, and the challenges for defenders. In the hope of understanding the security concerns related to blockchain technologies, we chose to learn about the participants in the Bitcoin peer-to-peer network.

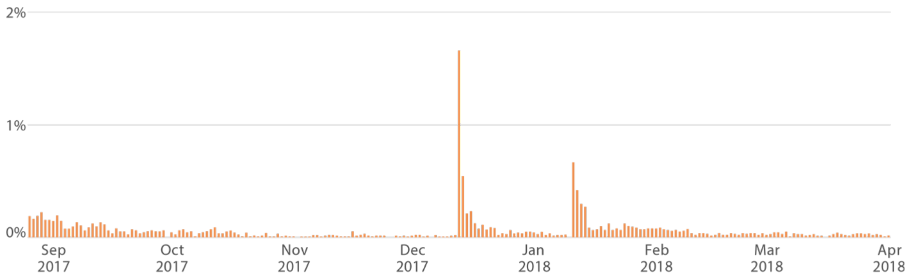
Rapid7's **Project Heisenberg** tracks connections to—and the probing and attempted exploitation of—various services on a large set of globally distributed honeypots. Rapid7's **Project Sonar** is a security research project running since 2013; it uses internet scanning and collection to gain insight into exposure of common services and vulnerabilities, and it provides tools and data to enable and advance security research. **Bitnodes** by Addy Yeow aims to measure the size of the Bitcoin network by finding all reachable bitcoin nodes in the network from within the network.

By combining intelligence from these three sources, we observed curious scanning and probing behavior, as well as the attempted exploitation of high-profile vulnerabilities by some of the very nodes participating in the Bitcoin network.

In the end, we determined that the absolute number of badly behaving nodes is relatively low (in the hundreds), but on a bad day, up to 2% of the total Bitcoin network exhibits suspicious or malicious behavior, as seen in Figure 1.

Figure 1: Daily Percentage of 'Badly Behaving' Bitcoin Nodes

If a Bitcoin node connects to a Heisenberg honeypot, something's not right (with that node)



Source: Rapid7 Project Heisenberg; Bitnodes

While these percentages may seem low, consider that the usual "background noise" of malicious activity we detect across the entire IPv4 internet is sourced from around 0.2% of total internet population of machines. Therefore, on a typical day, the Bitcoin network is approximately three times more "evil" than the rest of the internet. On particularly active days, we see ten times as many malicious nodes in the Bitcoin network as we see on the regular internet, by volume.

What follows is an analysis of what we mean by "the Bitcoin network," how we detect the bad actors on this network, and what we can determine about these malicious nodes and their intentions from a honeypot's perspective.

Fundamentally, Bitcoin is a digital currency that uses cryptography (hence the term “cryptocurrency”) to validate, process, and maintain transactions in a distributed digital ledger known as a blockchain. Let’s unpack that word soup.

BITCOIN/BLOCKCHAIN/CRYPOTCURRENCY PRIMER

News, tech, and social media channels are awash in a cacophony of noise surrounding the buzzwords “Bitcoin,” “blockchain,” and “cryptocurrency”—so much so that it may be difficult to get your bearings. Furthermore, you will likely see the term “cryptocurrency” used interchangeably with “digital currency,” “tokens,” or even “virtual currency.” It’s important to note that not all digital currencies are cryptocurrencies, but the popular ones of the moment—Bitcoin, Ethereum, Monero, Litecoin, et al—have cryptography as a foundation. For this paper we’ll focus on these currencies, and Bitcoin in particular. Instead of being a comprehensive discourse, the goal of this primer is to provide just enough information and context to help readers dive into the rest of the paper.

Fundamentally, Bitcoin is a digital currency that uses cryptography (hence the term “cryptocurrency”) to validate, process, and maintain transactions in a distributed digital ledger known as a blockchain. Let’s unpack that word soup.

Unlike the United States dollar (USD) or the Chinese yuan (CNY), Bitcoin is not backed by any sovereign entity, bank, or institution. It is not “issued” from a central source like the US Federal Reserve, which controls all USD in circulation. Rather, a network of peer-to-peer (P2P) computing nodes is tasked with performing complex cryptographic math to generate new currency (this is known as “mining”), maintaining a copy of the complete digital ledger (database) of executed transactions (a.k.a the “blockchain”), and validating new transactions. These P2P nodes can be as simple as a home PC or as specialized as a purpose-built device. Nodes are incentivized to participate by being given new coins or being compensated through transaction fees. This paper focuses on the makeup and behaviors of these P2P nodes.

Bitcoins, which can be fractional amounts (e.g. as low as 0.00000001 Bitcoin/BTC), are stored in a digital wallet. Wallets can be on your PC or a removable device, or they can be in a cloud service such as Coinbase; you can even print your wallet to paper. A wallet is identified by a long alphanumeric string, like 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw (which is one of the wallets used as a payment address for the WannaCry attack of 2017).

These wallet IDs are tracked and stored on the network in any transactions involving those IDs. In theory, these wallet IDs provide the appearance of anonymity for each financial transaction. In reality, you can be de-anonymized with relative ease unless you’re very knowledgeable and take great care in how you operate on and off the network. Bitcoin users can be classified by transaction or purchasing patterns, by IP address (this requires a third party to be monitoring nodes as transactions happen, which law enforcement in many global jurisdictions are able to do), or even by how careless one is when converting the digital currency to something more useful in the brick-and-mortar world. There are some in-depth resources, including a paper by Biryukov, Khovratovich & Pustogarov (2014), that readers can dive into for more information on the pseudonymity of Bitcoin.

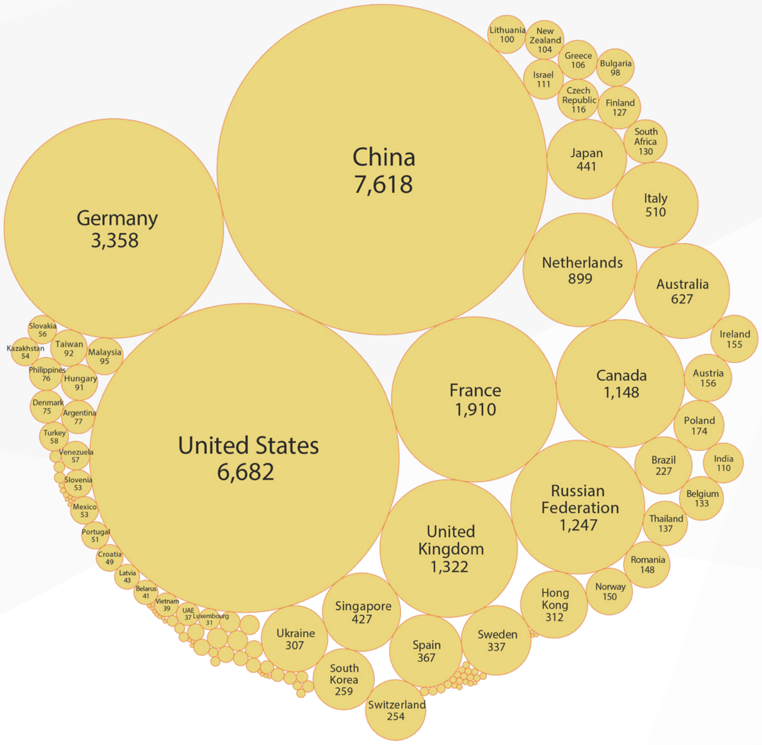
BITCOIN NETWORK DIVERSITY

Bitcoin node operators have the option to participate as "full nodes," which is required for processing and validating transactions on the network. Operators have many security and economic reasons to choose to run a full node, but part of the cost is that the node must be able to accept inbound connections. Therefore, configuring a full node, by default, will spawn a TCP service on port 8333. This service is made available on the public internet either automatically via UPnP configuration, or manually by the node operator. Once exposed, other players in the Bitcoin network can communicate with this full node, and it can perform useful functions for its clients, such as distributing the blockchain, validating the transactions of lightweight wallets, and enforcing the consensus rules backing the Bitcoin network.

Both Project Sonar and Bitnodes have visibility into the Bitcoin network, albeit from different vantage points. We'll briefly discuss what each project is capable of seeing, offer some observations on the respective data, and dive into the usage of these observations in the rest of the research.

Figure 2: Bitcoin Nodes Discovered by Project Sonar

Circle size represents the number of distinct in-country IPv4 addresses discovered



Source: Rapid7 Project Sonar

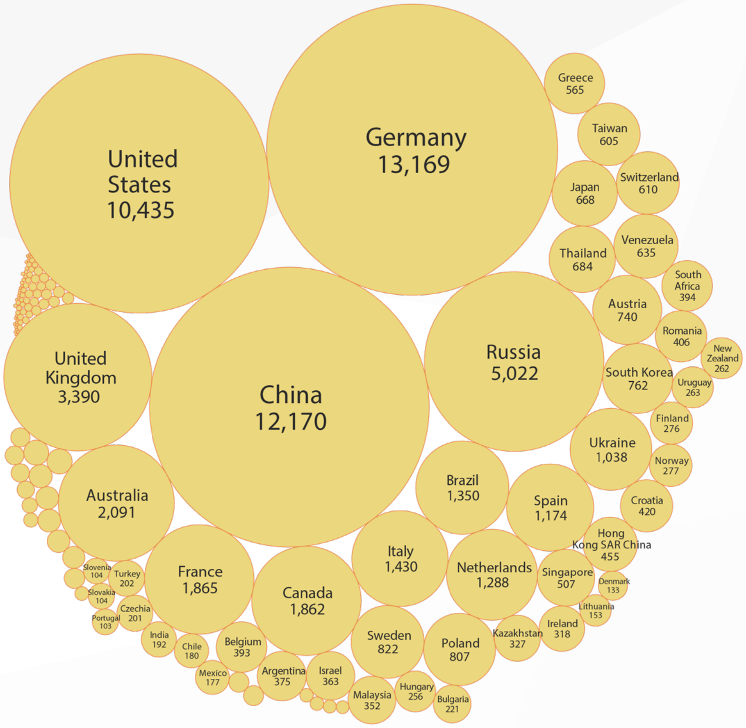
Project Sonar scans the public IPv4 internet on a weekly basis looking for nodes with port 8333/TCP open (Figure 2). Nodes with this port open are then connected to, and the information exchanged during handshaking—including version information and basic capabilities—is stored for later analysis. Project Sonar observed between 10,000 and 12,000 unique IPv4 addresses exposing the Bitcoin service on 8333/TCP during any given week. In the first quarter of 2018, just over 28,000 unique IPv4 addresses were observed.

Bitnodes, in contrast, uses a different method to get insight into the Bitcoin network. Bitnodes uses a set of seed peers to connect to the Bitcoin network and then issues the getaddr command to find that node's list of known, active nodes, repeating this process recursively to discover all nodes in the Bitcoin network at any one time. Like Sonar, Bitnodes records the version information and basic capabilities. Bitnodes takes this assessment further by gaining visibility into Bitcoin peers not operating on the standard 8333/TCP port. Ninety-seven percent of the nodes in Bitnodes operate on 8333/TCP, but there are nearly 600 additional ports in use; these are likely common alternative ports such as 8555, 8334, 8338, 8433, 8833, and more. Additionally, Bitnodes records how long any given peer has been participating in the Bitcoin network.

Rapid7 Labs has been analyzing the Bitnodes data since August of 2017, and in any given day observes between 11,000 and 15,000 unique IPv4 addresses participating in the network (Figure 3). Since the time we started monitoring the Bitcoin network through the Bitnodes API, we've observed approximately 144,000 unique IPv4 addresses, in total. Since the beginning of 2018, we've seen nearly 83,000 unique IPv4 addresses from Bitnodes. Over 23,000 of the nearly 83,000 Bitcoin peers observed in Bitnodes so far this year have also been identified as running the Bitcoin service by Project Sonar.

Figure 3: Bitcoin Nodes Discovered by Bitnodes

Circle size represents the number of distinct in-country IPv4 addresses discovered



Source: Bitnodes

There are many factors that could explain the different numbers observed by Project Sonar and Bitnodes:

- Bitnodes uses a method where the Bitcoin network is almost continuously monitored, whereas Sonar's view is effectively a snapshot over a 2-6 hour period once every week. As a result, a client could be active in the Bitcoin network for all hours of the week, but if it happens to be unreachable during the small window where Sonar audits, for any number of reasons, it will escape Sonar measurement.
- Bitcoin nodes connected on DHCP or similar dynamic environments, like mobile and cloud/VPS providers, are expected to change over time. Therefore, this population of Bitcoin nodes is likely to change addresses on at least a weekly basis.
- Project Sonar maintains a blacklist of addresses that we've been asked to not scan. Of all of the unique Bitcoin nodes from Bitnodes, 167 of them are in networks we were asked not to monitor with Project Sonar.

The remaining sections make note of when Bitnodes data or Project Sonar data is used.

BAD ACTORS IN THE BITCOIN NETWORK

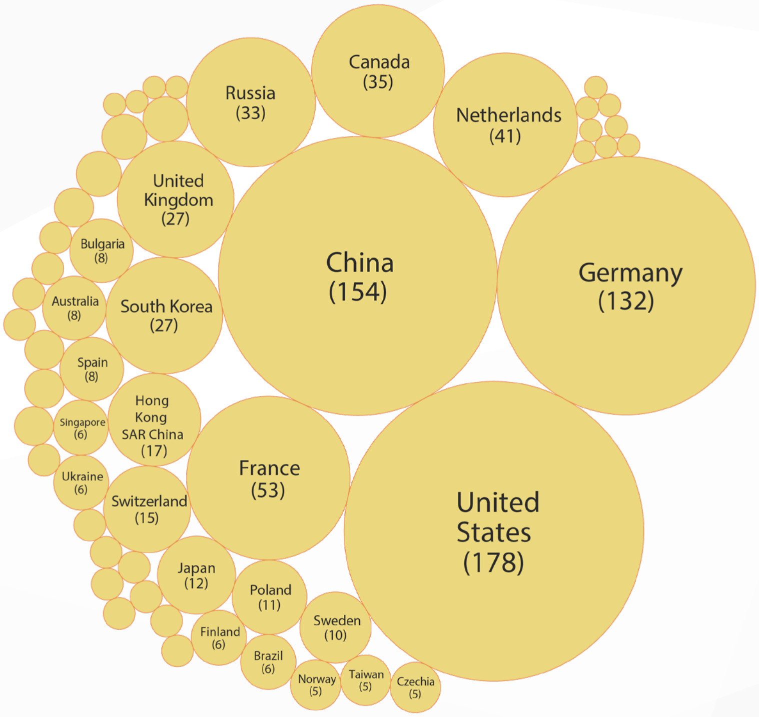
The nodes participating in the Bitcoin network are, at least theoretically, actively involved in producing digital assets that have real-world cash value; this makes them an interesting target in more ways than one, and as such, it is not unreasonable to examine these nodes from a security perspective.

The following analysis is based on combined knowledge from two sources: known Bitcoin peer-to-peer nodes in the Bitnodes network, and activity observed in Rapid7's Heisenberg honeypots between August 2017 and March 2018.

First, less than 1% of the nodes known to be active in the Bitcoin network have ever communicated with our honeypots in some way—a mere 900 or so. Examining the source address of these connections by country, we observed a pattern common in much of our other Internet research: Countries with a larger public IP space tend to show up more prominently than those with smaller allocations, and the same approximate group of countries that make up the top 10 or so are not much different than what you see exploring other internet exposure data like this. For this reason, it comes as no surprise that countries like the United States, China, Germany, France, and Russia all figure prominently in the top offenders category, as seen in Figure 4.

Figure 4: Bad Actors in the Bitcoin Network

Circle size represents the number of originating IPv4 nodes observed from a country connecting to Project Heisenberg



Source: Rapid7 Project Heisenberg

Some stand out more than others.

For example, Russian operators control an estimated 359 bitcoin nodes at any one time, according to Bitnodes data. During the period of observation, we observed 33 of those nodes communicating with our honeypots, or over 9% of the total Russian population. While it's the seventh most-suspect country by distinct source addresses observed, it is the most chatty country by number of connections to our honeypot by a factor of more than 13, as shown in Figure 5. Russian Bitcoin nodes initiated nearly 380 million connection attempts in comparison to the next closest offender, Canada, with only 26 million connection attempts from 35 nodes of their estimated 398 in operation.

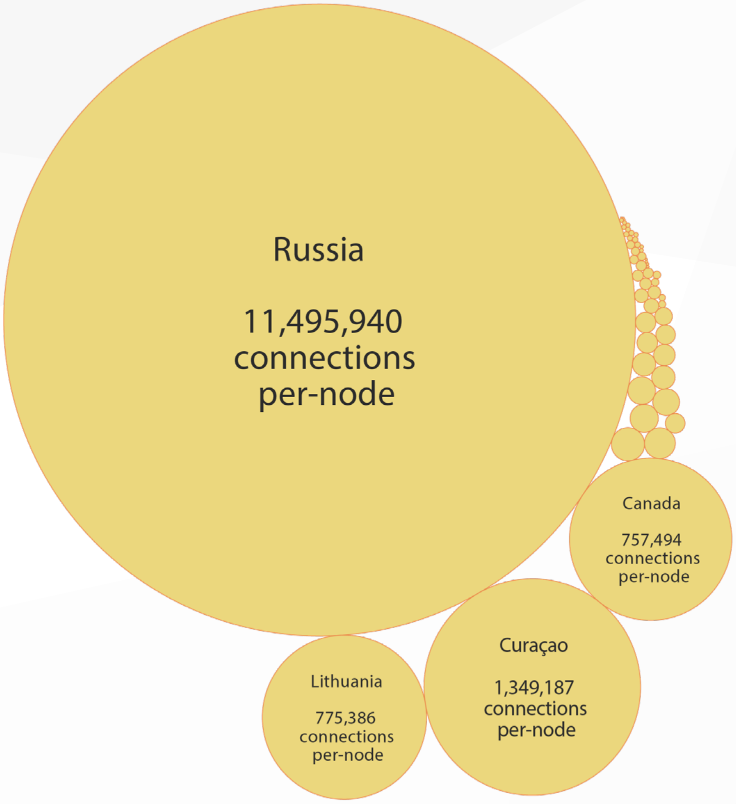
So, what are these approximately 900 suspicious nodes up to? They are known to be participating in the Bitcoin network, and they also happen to be sending unsolicited traffic to our honeypots. This is interesting all by itself, but we can't claim to know the exact purpose of this activity with any certainty. Some of the ports and protocols probed are ones we've seen plenty of times before: SSH, RDP, and VNC, likely in search of default or easily guessed credentials. We also see connection attempts to SMB, almost certainly for the added effect of possible remote code execution with reliable exploit code. Other connection attempts seem unique to the larger blockchain community.

We discuss several related observations next, with the understanding that any connection to our honeypot is interesting because it is unsolicited; as with any honeypot network, there is simply no reason for an unsolicited connection attempt.

Figure 5: Bad Actors on the Bitcoin Network (Connection Scale)

Circle size represents (total connections to Hesienberg nodes/count of distinct source IPv4s).

This rough average helps normalize the grouped country connections and better reflects the behaviours of individual nodes.



Source: Rapid7 Projects Sonar & Heisenberg

Services with a history of vulnerabilities, misconfiguration, and exploitation show traffic across most of our deployed honeypots, including SMB, SSH, and RDP.

Server Message Block

SMB (445/TCP) has been a popular target for years. Particularly given the publishing of MS17-010 and reliable exploits, it was no surprise to see a fair amount of reconnaissance and attempted exploitation of this service from Bitcoin network nodes. We observed over 3.8 million connection attempts that resulted in almost 3 million attempts to exploit MS17-010. Despite the volume of connections and exploit attempts, this all came from just 17 source hosts using 13 different exploit variants. Half of these attacking hosts were from China, and the next largest population appear to be sourced from Russia.

Ethereum?

UDP port 30303 is most commonly used for the discovery protocol of another blockchain technology, Ethereum. We observed 582 Bitcoin nodes send over 4.5 million probes to 30303/UDP on just five of our honeypots. This implies that the source nodes in question are involved in multiple cryptocurrencies in one way or another, but why such a small subset of our honeypots were probed on 30303/UDP is unknown. China and the United States led the pack with about one hundred distinct sources probing this Ethereum-specific port while also participating in the Bitcoin network.

HTTP

Random probes for HTTP on 80/TCP and other ports is quite normal for any internet-facing node nowadays. Between web crawlers of varying legitimacy and an abundance of targets ripe for exploitation over HTTP, it was surprising to see that this protocol didn’t even break into the top five most-communicated-with ports at under 1.5 million connections. Only 17,000 or so of those TCP sessions turned into HTTP, and almost all of those HTTP sessions were blatant attempts at reconnaissance in one form or other (Nmap probes, open proxy checks, and probes for phpMyAdmin). Fewer than half a dozen Bitcoin nodes participated in HTTP probing with no standouts on a country level.

Ports, Ports, Ports

Services with a history of vulnerabilities, misconfiguration, and exploitation show traffic across most of our deployed honeypots, including SMB, SSH, and RDP. Other ports showed sporadic probing activity across a subset of our honeypot nodes. There were only 34 distinct UDP ports probed across Heisenberg, while TCP, on the other hand, racked up over 8,000 distinct TCP destination ports, thanks largely to port-scanning activity from just one node operating from a cloud provider in the UK that specializes in DDoS protection.

WHO, WHAT, AND WHY?

Relative to the size of the public IPv4 internet, the millions of hosts that communicate with our honeypots on a regular basis represent only a tiny fraction of all internet-connected computers, around 0.2%. However, when we focus just on the portion of the public IPv4 Internet that is participating in the Bitcoin network, things change; over the period measured, about 0.6% of the Bitcoin network is in some suspicious behavior, with "bad days" spiking to about 2% of the population. This is several times more "evil" than the usual background noise on the internet and seems surprisingly large for a network whose raison d'être is so focused on technical security and availability. This begs the question: What are these node operators really up to? There are several possible explanations.

First, these actions could be intended by the legitimate owners of the offending Bitcoin peer-to-peer nodes. It is entirely possible that while a node is participating in the Bitcoin network, chasing the ever-increasing difficulty of mining the next Bitcoin, that its owner is also taking hostile action against the public internet. Bitcoin mining is inherently a competitive endeavor; it may be advantageous for node operators to cause trouble for their fellow miners. Further proof of this is in the documentation from the Bitcoin project itself on how to run a full node. It states that one of the possible problems with running a full node is that the system becomes an attack target: "Bitcoin Core powers the Bitcoin network, so people who want to disrupt the network may attack Bitcoin Core users in ways that will affect other things you do with your computer, such as an attack that limits your available download bandwidth."

What if a legitimate node in the Bitcoin network was compromised through some other means, and now that node is being used as a launching point for attacks against the public internet? A system participating in the Bitcoin network is likely to have access to cryptocurrency, as well as the computational power needed to mine it. Both of those characteristics make it a valuable target.

Similarly, some of these nodes could have previously been regular systems, not participating in the Bitcoin network that was later compromised and is now running a Bitcoin mining client on behalf of the attackers. Thanks to the rise of cryptojacking, where maliciously planted Javascript miners are injected on otherwise normal websites, some systems connected to the public IPv4 internet are both being used to mine cryptocurrency and launch further attacks, all without the consent of the system owner.

It could be that some of this unusual traffic is not malicious at all and is simply the result of misconfigurations. Our hundreds of honeypots change IPs from time to time, and it is possible that the IPs we land on were previously used by machines and networks more closely related to Bitcoin mining. This scenario could be exacerbated by dangling stale DNS records, cached DNS records being used by the attacking nodes, or some other expired IP address information.

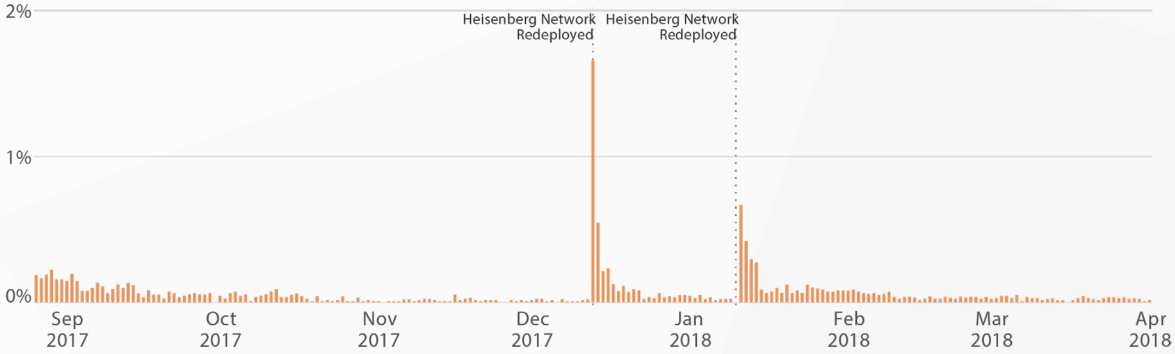
This seems even more likely if you overlay the knowledge of when our honeypots changed IP addresses with the connection graph from the introduction to this paper—a clear pattern emerges. Figure 6 shows where increases in activity from Bitcoin nodes seem to correlate with the days where our honeypots changed IPs.

One possible area of future research would be a longitudinal study classifying the node types as "benign" (regular miners), "malicious" (those nodes also performing sketchy/malicious actions against general internet nodes), and "researcher" (individuals and organizations like Rapid7 who regularly stand up/tear down infrastructure to study services—like Bitcoin mining—on the internet).

Figure 6: Daily Percentage of 'Badly Behaving' Bitcoin Nodes

If a Bitcoin node connects to a Heisenberg honeypot, something's not right.

Some days (that seems to coincide with our honeypot network redeployments, which then gain new IPv4 addresses) nearly 2% of the Bitcoin network has nodes that behave "badly."



Source: Rapid7 Project Heisenberg; Bitnodes

If you are actively participating as a Bitcoin miner, one takeaway is to recognize that there are a small number of participants in the Bitcoin network actively taking hostile action against otherwise innocent nodes on the public internet.

THE FUTURE

In this paper, we've presented background information on three projects with unique viewpoints into the Bitcoin network, shared observations of the Bitcoin network derived from these projects, and offered some possible explanations for these observations.

The nodes explored on 8333/TCP by Sonar and Bitnodes are likely what are considered full Bitcoin nodes, serving as the backbone of the cryptocurrency by validating the hundreds of thousands of transactions that take place each day. If you are actively participating as a Bitcoin miner, one takeaway is to recognize that there are a small number of participants in the Bitcoin network actively taking hostile action against otherwise innocent nodes on the public internet. If you are not on your guard already, you should be now.

These hostile nodes reached outside of the Bitcoin network and started actively probing and attacking, looking for a way to siphon value from the target systems. What if these same nodes are also actively attacking the very network they participate in or the clients they support? All an attacker has to do is connect to this open, public network and they'll be able to discover tens of thousands of systems that likely have wallets containing Bitcoin, other cryptocurrencies, or available compute power and network bandwidth for the taking. It's almost like a prioritized list of targets.

It is likely that merely suspicious activity rather than overtly malicious intent is behind some of what we observed in our honeypots, and that much of this is just life on the public internet. Anything with a publicly routable IP address is bound to get all sorts of suspicious and malicious traffic on a regular basis, and our honeypots are no different in this regard.

Some of the behavior we saw can only be taken as malicious, such as the 17 hosts, mostly from China IPv4-space, which were actively slinging exploits for MS17-010. That they were also participating in the Bitcoin network makes it all the more interesting.

There is a future for blockchain technologies and cryptocurrencies like Bitcoin. What exactly this future will entail, particularly from a security perspective, remains to be seen.

Are you interested in security topics related to blockchain technologies? Have questions, comments, or feedback on this research? We'd love to hear from you either in our blog comments or by emailing us at research@rapid7.com.

APPENDIX A: METHODOLOGY

In January, 2018, Rapid7 Labs configured custom, weekly Project Sonar scans on TCP port 8333 to identify Bitcoin nodes on the internet and collect basic node information. The Labs team also worked with Bitnodes to retrieve historical Bitcoin node activity. The IPv4 addresses collected from these two data sources were used to extract all communication data from those nodes to Rapid7 Labs Project Heisenberg honeypot database.

Rapid7 Labs researchers combed through packet captures and connection records to identify known malicious activity/exploits plus generally odd/curious communications, using the aggregated findings as the corpus for the report.

IPv4 address geocoding was performed with commercial databases from MaxMind.

Dangerous User Behavior

Account Visits Suspicious Link
Password Set To Never Expire
Network Access For Threat

Threat Probing

Asset Connects To Network Honeypot
Watched Impersonation

Threat Movement

Account Authenticated To Critical Asset
Lateral Movement Domain Credentials
Lateral Movement Local Credentials
Suspicious Authentication

Remote Entry

Wireless Multiple Country Authentications
Multiple Country Authentications
Ingress From Non Expiring Account
Ingress From ServiceAccount
Service Account Authenticated From New Source
Account Authenticated To Critical Asset From New Source
New Local User Primary Asset
Ingress From Disabled Account

Failed Access Attempt

Authentication Attempt From Disabled Account
Brute Force Against Domain Account
Brute Force Against Local Account
Brute Force From Unknown Source

Malicious Behavior On Asset Level

Remote File Execution
VirusAlert
Log Deletion Local Account
Harvested Credentials
Log Deletion
Virus Alert
Network Access For Threat

Suspicious Behavior On Asset Level

Malicious Hash On Asset

Malicious Behavior Network Level

Advanced Malware Alert
Protocol Poison
Administrator Impersonation

Account Adjustment

Account Privilege Escalated
Account Enabled
Account Password Reset
Account Locked
DomainAdmin Added

APPENDIX B: TABLES

Table 1: Summary of Unique Bitcoin IPv4 Addresses Discovered by Project Sonar (by Country)

COUNTRY	NODE COUNT
Aland Islands	1
Algeria	2
Andorra	1
Anonymous Proxy	12
Argentina	77
Armenia	2
Australia	627
Austria	156
Bahrain	2
Bangladesh	1
Barbados	1
Belarus	41
Belgium	133
Belize	3
Bermuda	2
Bolivia (Plurinational State of)	1
Bosnia and Herzegovina	6
Brazil	227
Bulgaria	98
Cambodia	1
Canada	1148
Chile	29
China	7,618
Colombia	8
Costa Rica	9
Croatia	49
Curacao	8
Cyprus	8
Czech Republic	116
Denmark	75
Dominic Republic	3
Ecuador	3
Egypt	2
El Salvador	1
Estonia	29
Ethiopia	1
European Union	1
Faroe Islands	2
Finland	127
France	1,910
Georiga	15
Germany	3,358
Ghana	1
Greece	106
Guadeloupe	12
Guernsey	1
Honduras	1
Hong Kong	312
Hungary	91
Iceland	19
India	110
Indonesia	14
Iran (Islamic Republic of)	18
Ireland	155
Isle of Man	2
Israel	111
Italy	510
Jamaica	1
Japan	441
Jersey	1
Jordan	1
Kazakhstan	54
Kenya	3

COUNTRY	NODE COUNT
Kuwait	1
Kyrgyzstan	4
Lao People's Democratic Republic	1
Latvia	43
Lithuania	100
Luxembourg	31
Macao	6
Malaysia	95
Malta	5
Mauritius	1
Mexico	53
Monaco	2
Mongolia	3
Montenegro	3
Morocco	9
Myanmar	1
Namibia	1
Nepal	1
Netherlands	899
New Zealand	104
Nigeria	3
Norway	150
Pakistan	3
Panama	9
Paraguay	3
Peru	5
Poland	174
Philippines	76
Portugal	51
Puerto Rico	3
Qatar	5
Republic of Korea	259
Republic of Moldova	26
Reunion	11
Romania	148
Russian Federation	1,247
Saint Lucia	1
San Marino	7
Saudi Arabia	6
Serbia	18
Seychelles	21
Singapore	427
Slovakia	56
Slovenia	53
South Africa	130
Spain	367
Sri Lanka	1
Sweden	337
Switzerland	254
Taiwan, Province of China	92
Thailand	137
The former Yugoslav Republic of Macedonia	5
Turkey	58
Ukraine	307
United Arab Emirates	37
United Kingdom of Great Britain and Northern Ireland	1,322
United States of America	6,682
Uruguay	28
Uzbekistan	5
Venezuela, Bolivarian Republic of	57
Viet Nam	39
Virgin Islands, U.S.	1
Unidentified	20

Table 2: Summary of Unique Bitcoin IPv4 Addresses Discovered by Bitnodes (by Country)

COUNTRY	NODE COUNT
Aland Islands	2
Albania	1
Algeria	82
Andorra	11
Angola	2
Anonymous Proxy	4
Argentina	375
Armenia	4
Aruba	4
Asia Pacific	40
Australia	2,091
Austria	740
Azerbaijan	5
Bahrain	16
Bangladesh	1
Barbados	1
Belarus	96
Belgium	393
Belize	4
Bermuda	3
Bolivia (Plurinational State of)	1
Bonaire, Sint Eustatius and Saba	5
Bosnia and Herzegovina	51
Brazil	1,350
Bulgaria	221
Cambodia	4
Canada	1,862
Chile	180
China	12,170
Colombia	25
Costa Rica	10
Croatia	420
Cyprus	13
Czech Republic	201
Denmark	133
Dominican Republic	11
Ecuador	20
Egypt	5
El Salvador	2
Estonia	56
Ethiopia	1
European Union	33
Faroe Islands	1
Finland	276
France	1,865
French Guiana	1
Georgia	11
Germany	13,169
Ghana	5
Greece	565
Guadeloupe	80
Guam	1
Guernsey	2
Honduras	4
Hong Kong	455
Hungary	256
Iceland	28
India	192
Indonesia	31
Iran (Islamic Republic of)	26
Iraq	6
Ireland	318
Isle of Man	3
Israel	363
Italy	1,430
Jamaica	1
Japan	668

COUNTRY	NODE COUNT
Jersey	1
Jordan	2
Kazakhstan	327
Kenya	6
Kuwait	5
Kyrgyzstan	12
Lao People's Democratic Republic	1
Latvia	97
Lebanon	4
Lithuania	153
Luxembourg	46
Macao	16
Malaysia	352
Malta	28
Martinique	1
Mauritius	1
Mexico	177
Monaco	2
Mongolia	4
Montenegro	4
Morocco	80
Myanmar	1
Namibia	1
Netherlands	1,288
Netherlands Antilles	9
New Caledonia	1
New Zealand	262
Nigeria	10
Norway	277
Oman	17
Pakistan	14
Panama	18
Paraguay	2
Peru	7
Philippines	54

COUNTRY	NODE COUNT
Poland	807
Portugal	103
Puerto Rico	7
Qatar	5
Republic of Korea	762
Republic of Moldova	36
Reunion	62
Romania	406
Russian Federation	5,022
Saint Lucia	1
Saudi Arabia	61
Senegal	9
Serbia	29
Seychelles	11
Singapore	507
Slovakia	104
Slovenia	104
South Africa	394
Spain	1,174
Sri Lanka	1
Sweden	822
Switzerland	610
Syrian Arab Republic	1
Taiwan, Province of China	605
Tajikistan	1
Thailand	684
The former Yugoslav Republic of Macedonia	78
Trinidad and Tobago	1
Tunisia	19
Turkey	202
Ukraine	1,038
United Arab Emirates	75
United Kingdom of Great Britain and Northern Ireland	3,390
United States of America	10,435

COUNTRY	NODE COUNT
Uruguay	263
Uzbekistan	3
Venezuela, Bolivarian Republic of	635
Viet Nam	64
Virgin Islands, British	1
Virgin Islands, U.S.	1
Zimbabwe	1
Unidentified	1,583

Table 3: Summary of Bitcoin Node Data as Seen by Project Heisenberg (by Country)

COUNTRY	TOTAL DISTINCT IPV4S	TOTAL CONNECTIONS
Argentina	2	433
Armenia	1	785
Australia	8	24,142
Austria	3	5,012
Belarus	1	95
Belgium	3	3,368
Belize	2	17,581
Brazil	6	2,130
Bulgaria	8	27,447
Canada	35	26,512,308
Chile	2	398
China	154	4,190,948
Curacao	1	1,349,187
Cyprus	1	15
Czech Republic	5	2,170
Denmark	2	86
Estonia	3	9,089
Finland	6	12,720
France	53	628,177
Germany	132	4,159,581
Hong Kong	17	371,959
Hungary	4	43,111
India	1	620
Israel	2	2,838
Italy	4	2,200
Japan	12	75,208
Lithuania	2	1,550,772
Luxembourg	1	1,915
Malaysia	2	912
Netherlands	41	541,123
New Zealand	2	40,643
Norway	5	23,376
Poland	11	21,108

COUNTRY	TOTAL DISTINCT IPV4S	**TOTAL CONNECTIONS**
Portugal	3	4,842
Republic of Korea	27	295,310
Republic of Moldova	1	12
Romania	2	1,788
Russian Federation	33	379,366,026
Saudi Arabia	1	204
Serbia	1	1
Singapore	6	93,323
Slovakia	2	980
Slovenia	2	1,290
South Africa	2	921
Spain	8	6,353
Sweden	10	38,532
Switzerland	15	182,129
Taiwan, Province of China	5	3,969
Thailand	4	7,708
The former Yugoslav Republic of Macedonia	1	138
Ukraine	6	32,315
United Arab Emirates	1	2
United Kingdom of Great Britain and Northern Ireland	27	417,386
United States of America	178	4,041,820
Venezuela, Bolivarian Republic of	1	937
Viet Nam	2	188

ABOUT RAPID7

Rapid7 powers the practice of SecOps by delivering shared visibility, analytics, and automation that unites security, IT, and DevOps teams. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response, and log management for organizations around the globe.To learn more about Rapid7 or get involved in our threat research, visit **www.rapid7.com**.

QUESTIONS?

Email us at research@rapid7.com