McAfee Labs

Blockchain Transactions Create Risks for Financial Services

By Raj Samani on Dec 16, 2015

Like 6 Share 37 G+1 1 Tweet Email

This post was written by Raj Samani and Christiaan Beek of Intel Security, and Shane D. Shook, PhD.

Trust is the most valuable commodity in the digital age. Failure to trust the systems or organizations in which we place our digital assets leads us to look at alternate providers, or to withdraw entirely from a suspect service. Within the financial services industry, the notion of trust is of paramount importance to institutions and account holders alike. Investors must be confident that the money they have in their accounts is available for use whenever they need it, and that the routes and terminals involved in buying Christmas presents, for example, are protected with many layers of security.

But what happens with this concept of trust if, for example, one in every 25 withdrawals made from an ATM is authorized by a bank operated by a known criminal organization? Or if one of every six credit card purchases was transacted by a terminal suspected to be controlled by known criminal organizations? It is likely the implied level of trust customers have in the financial system would be shaken; moreover, they would certainly seek a more trustworthy provider for financial transactions.

Looking at trust among cryptocurrencies, Intel Security has undertaken an analysis of Bitcoin to determine the likely risk to transactions made with this increasingly popular method of payment. In particular, we focused on the risks to the security of the network that serves the “blockchain,” the public database of all Bitcoin transactions. Although our research did not identify any specific risks associated with the security of the funds exchanged, we did identify risks that may affect the reliability of the blockchain itself. Our focus was predominantly on Bitcoin relay nodes, and the integrity of those nodes.

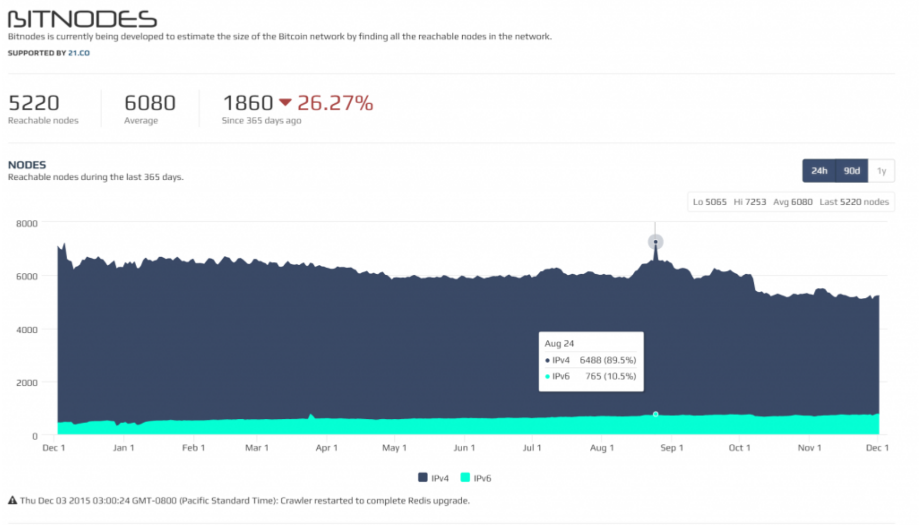
Whenever these transaction relay nodes do not offer a sufficient level of integrity (for example, being a part of botnet operations), they could be used to manipulate Bitcoin transactions through route control, denial of service, or by modifying transaction protocols. Moreover, a botnet-controlled relay node can be monitored to reveal the identity of one party in a transaction. If enough relay nodes are connected by a botnet operator, it may even be possible to deanonymize the other parties. Further, as the blockchain and related products have evolved, vulnerabilities in software clients have cropped up. Attempts to exploit the Bitcoin peer-to-peer network are known in research as well as in the wild; thus the knowledge of botnet- or malware-associated peers is a concern.

Background

The blockchain is a public ledger that facilitates payment through cryptocurrencies (such as Bitcoin) for goods or services of more than 10,000 vendors and many thousands of individuals, including legitimate (food, airfare, books, cars) and illegitimate (malware, extortion/ransom, drugs). The blockchain is also being explored for commercial purposes with new offerings created for “secure exchange” services such as currencies, contracts, and equities trading or clearing.

The blockchain includes literal details concerning every transaction between addresses that have successfully negotiated a transfer, such as Bitcoin payments from one wallet to another, including time, sender and receiver wallet addresses, amounts, and relay IP addresses (both v4 and v6) of "bitnodes" that facilitate the transactions' communications.

At any time there are around 9,000 active bitnodes, some that operate as "full nodes" (peers) and others that serve as relays or a type of proxy, also known as a "lightweight node."



BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

SUPPORTED BY 21.CO

5220 Reachable nodes | 6080 Average | 1860 ▼ 26.27% Since 365 days ago

NODES

Reachable nodes during the last 365 days.

24h 90d 1y

Lo 5065 Hi 7253 Avg 6080 Last 5220 nodes

Aug 24
● IPv4 6488 (89.5%)
● IPv6 765 (10.5%)

⚠ Thu Dec 03 2015 03:00:24 GMT-0800 (Pacific Standard Time): Crawler restarted to complete Redis upgrade.

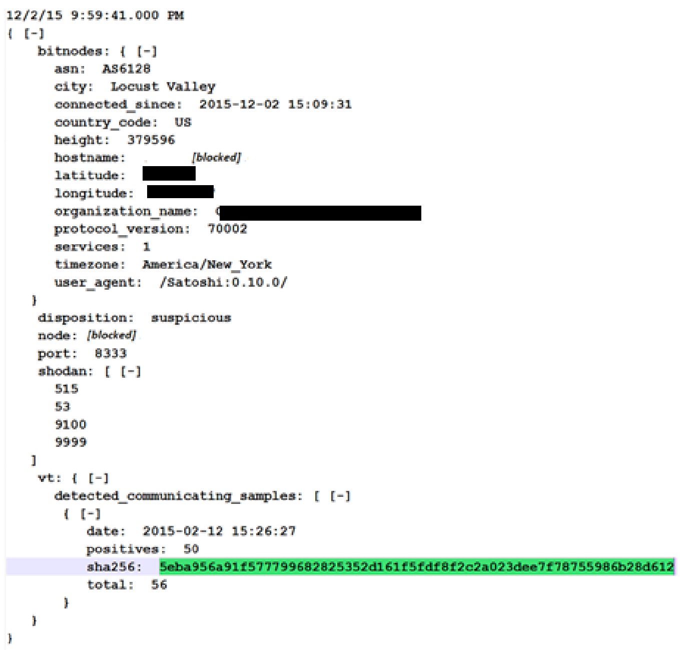
Source: https://bitnodes.21.co/

Related Risks

Approximately 2% of the bitnodes were coincidentally included for use by malware samples, and another 1% of bitnodes were included on Internet blacklists related to botnet control servers or other compromised hosts, according to data collected from Blockchain.info and Bitnodes.io (which peer with approximately 70% of active nodes) as well as open-source intelligence (OSINT) about botnets and malicious network addresses of nearly 145,000 unique IP addresses that relayed blockchain transactions for Bitcoin between February–December 2015. Those figures are historical summaries that when viewed in real time reflect more significant risks to the security of blockchain transactions.

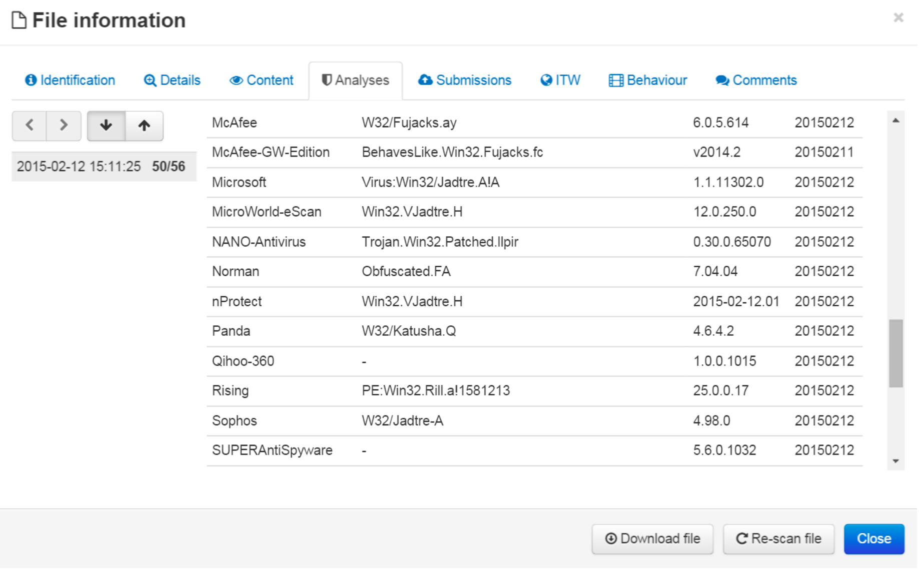
For the same period, a real-time review of active bitnodes (available peers) demonstrated that at any given time 4% of bitnodes addresses were included for use by malware samples (available for review on Virustotal.com), and an additional 13% of bitnodes appeared on public Internet blacklists. Thus in effect one in six Bitcoin transactions were relayed by nodes under the control of malicious operators. The difference between the historical and real-time statistics is simple: Bitnodes that correspond with malware or botnets act as blockchain relays more often than others.

For example, let's look at the following details of a bitnode active on December 2:



```
12/2/15 9:59:41.000 PM
{ [-]
   bitnodes: { [-]
     asn:  AS6128
     city:  Locust Valley
     connected_since:  2015-12-02 15:09:31
     country_code:  US
     height:  379596
     hostname:        [blocked]
     latitude:  [redacted]
     longitude:  [redacted]
     organization_name:  [redacted]
     protocol_version:  70002
     services:  1
     timezone:  America/New_York
     user_agent:  /Satoshi:0.10.0/
   }
   disposition:  suspicious
   node:  [blocked]
   port:  8333
   shodan:  [ [-]
     515
     53
     9100
     9999
   ]
   vt:  { [-]
     detected_communicating_samples:  [ [-]
      { [-]
         date:  2015-02-12 15:26:27
         positives:  50
         sha256:  5eba956a91f5777996828253 52d161f5fdf8f2c2a023dee7f78755986b28d612
         total:  56
      }
   }
}
```

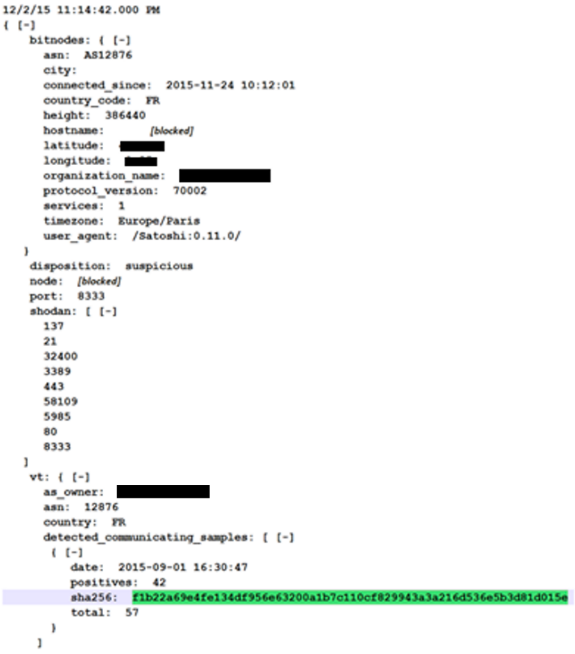
The malware sample that used the preceding bitnode (IP address) was a Fujacks Trojan, a well-documented botnet backdoor that allows a botmaster to remotely control the infected computer, collect information, and install other malware or tools that suit the botmaster's (or subscribers') interests.



2015-02-12 15:11:25 **50/56**

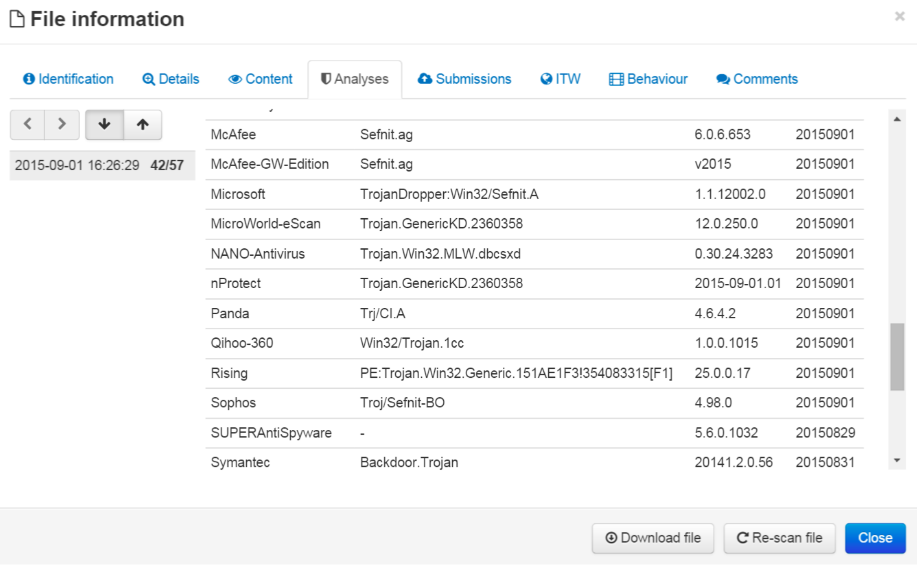
McAfee	W32/Fujacks.ay	6.0.5.614	20150212
McAfee-GW-Edition	BehavesLike.Win32.Fujacks.fc	v2014.2	20150211
Microsoft	Virus:Win32/Jadtre.A!A	1.1.11302.0	20150212
MicroWorld-eScan	Win32.VJadtre.H	12.0.250.0	20150212
NANO-Antivirus	Trojan.Win32.Patched.llpir	0.30.0.65070	20150212
Norman	Obfuscated.FA	7.04.04	20150212
nProtect	Win32.VJadtre.H	2015-02-12.01	20150212
Panda	W32/Katusha.Q	4.6.4.2	20150212
Qihoo-360	-	1.0.0.1015	20150212
Rising	PE:Win32.Rill.a!1581213	25.0.0.17	20150212
Sophos	W32/Jadtre-A	4.98.0	20150212
SUPERAntiSpyware	-	5.6.0.1032	20150212

This bitnode has been active since November 24:



```
12/2/15 11:14:42.000 PM
{ [-]
   bitnodes: { [-]
     asn:  AS12876
     city:
     connected_since:  2015-11-24 10:12:01
     country_code:  FR
     height:  386440
     hostname:        [blocked]
     latitude:  [redacted]
     longitude:  [redacted]
     organization_name:  [redacted]
     protocol_version:  70002
     services:  1
     timezone:  Europe/Paris
     user_agent:  /Satoshi:0.11.0/
   }
   disposition:  suspicious
   node:  [blocked]
   port:  8333
   shodan: [ [-]
     137
     21
     32400
     3389
     443
     58109
     5985
     80
     8333
   ]
   vt: { [-]
     as_owner:  [redacted]
     asn:  12876
     country:  FR
     detected_communicating_samples: [ [-]
      { [-]
         date:  2015-09-01 16:30:47
         positives:  42
         sha256:  f1b22a69e4fe134df956e63200a1b7c110cf829943a3a216d536e5b3d81d015e
         total:  57
      }
    ]
```

The associated malware is the Sefnit Trojan, a botnet backdoor that not only allows the botmaster to remotely control the host, but upon installation also injects a TOR client to mask botnet communications. Compromised computers could suffer the installation of any malicious tools. For example, past infections of Sefnit include ad-click fraud. There is also documented coincidental history of the use of Sefnit by malicious botmasters to mine bitcoins using infected computers. As with many botnets, take down efforts are sometimes temporary, and the subsequent utility of the botnet changes and on occasion expands.



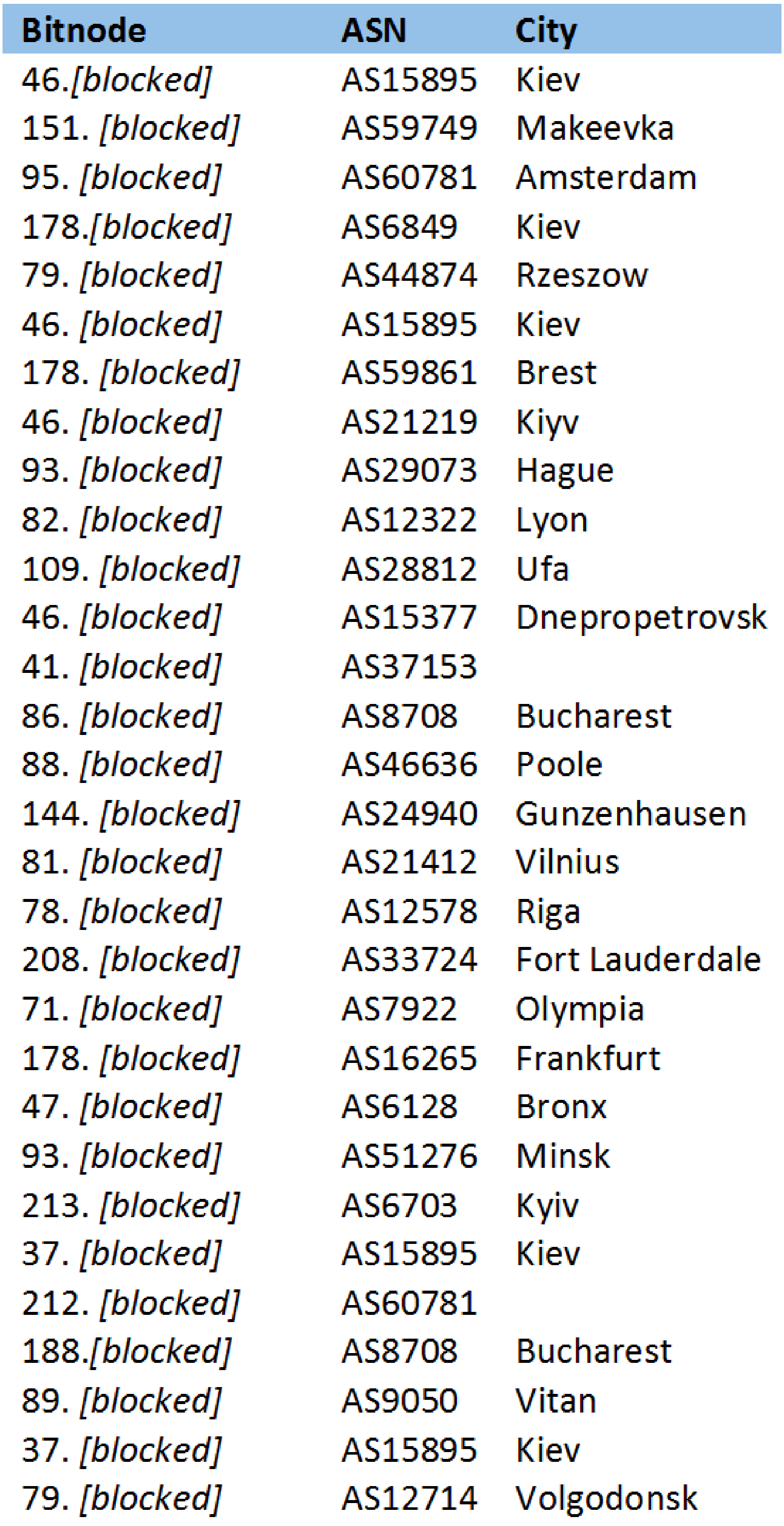
2015-09-01 16:26:29 42/57

McAfee	Sefnit.ag	6.0.6.653	20150901
McAfee-GW-Edition	Sefnit.ag	v2015	20150901
Microsoft	TrojanDropper:Win32/Sefnit.A	1.1.12002.0	20150901
MicroWorld-eScan	Trojan.GenericKD.2360358	12.0.250.0	20150901
NANO-Antivirus	Trojan.Win32.MLW.dbcsxd	0.30.24.3283	20150901
nProtect	Trojan.GenericKD.2360358	2015-09-01.01	20150901
Panda	Trj/CI.A	4.6.4.2	20150901
Qihoo-360	Win32/Trojan.1cc	1.0.0.1015	20150901
Rising	PE:Trojan.Win32.Generic.151AE1F3!354083315[F1]	25.0.0.17	20150901
Sophos	Troj/Sefnit-BO	4.98.0	20150901
SUPERAntiSpyware	-	5.6.0.1032	20150829
Symantec	Backdoor.Trojan	20141.2.0.56	20150831

Our analysis of the varied malware samples that relate to bitnode addresses which have relayed blockchain transactions during the past 18 months demonstrates that most of the botnets are related to Zeus. Zeus source code has been readily available (in several publicly released iterations and sold in specific versions) since at least 2011. It is a popular “starter kit” for botnet creation, and anyone with relatively modest technical capabilities can build and operate a botnet. More important though, botnets offer subscriber services that can facilitate more exotic crimes than simply compromising access to a computer.

The preceding Sefnit malware sample used that bitnode (IP) address as a TOR relay address, so that not only Bitcoin transactions would relay through that bitnode, but other TOR users could also use that host. Unfortunately not only legitimate TOR users, however: Computers infected with that Sefnit malware would be inducted into a botnet that used that TOR relay (coincidentally the bitnode address).

OSINT and Intel Security threat intelligence, respectively, confirmed that 3% of the unique bitnode addresses observed between February and December 2015 were included in malware samples for botnet communications, as control or routing. Of those addresses, the following 30 bitnodes accounted for 25% of associated malware submissions.



Bitnode	ASN	City
46.*[blocked]*	AS15895	Kiev
151. *[blocked]*	AS59749	Makeevka
95. *[blocked]*	AS60781	Amsterdam
178.*[blocked]*	AS6849	Kiev
79. *[blocked]*	AS44874	Rzeszow
46. *[blocked]*	AS15895	Kiev
178. *[blocked]*	AS59861	Brest
46. *[blocked]*	AS21219	Kiyv
93. *[blocked]*	AS29073	Hague
82. *[blocked]*	AS12322	Lyon
109. *[blocked]*	AS28812	Ufa
46. *[blocked]*	AS15377	Dnepropetrovsk
41. *[blocked]*	AS37153	
86. *[blocked]*	AS8708	Bucharest
88. *[blocked]*	AS46636	Poole
144. *[blocked]*	AS24940	Gunzenhausen
81. *[blocked]*	AS21412	Vilnius
78. *[blocked]*	AS12578	Riga
208. *[blocked]*	AS33724	Fort Lauderdale
71. *[blocked]*	AS7922	Olympia
178. *[blocked]*	AS16265	Frankfurt
47. *[blocked]*	AS6128	Bronx
93. *[blocked]*	AS51276	Minsk
213. *[blocked]*	AS6703	Kyiv
37. *[blocked]*	AS15895	Kiev
212. *[blocked]*	AS60781	
188.*[blocked]*	AS8708	Bucharest
89. *[blocked]*	AS9050	Vitan
37. *[blocked]*	AS15895	Kiev
79. *[blocked]*	AS12714	Volgodonsk

Our analysis of submitted malware samples that used those bitnode addresses indicated that 83% of related samples were from the following malware families:

Malware in Top 30 Bitnode Addresses (Feb–Dec 2015) With Number of Submissions

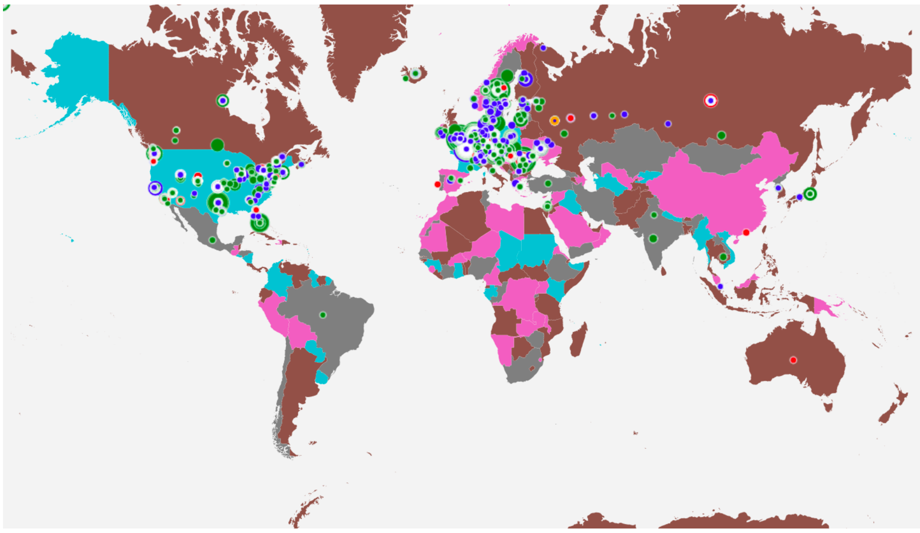
Allaple	4,611	Carberp	52	Dacic	11
Kelihos	860	Renos	42	Senta	8
Bladabindi	378	Dugenpal	41	Sisron	6
Pykspa	106	Bagsu	35	Vitro	5
Bulta	71	Glupteba	32	Teerac	5
Fynloski	71	Swrort	28	Peaac	4
Zbot	65	Waledac	25	Bumat	3
Dynamer	61	Skeeyah	25	Reveton	1
Sality	57	Omaneat	24	Simda	1
Virut	53	Runpoor	18		

Where are they?

This begs the question: Which came first? Was the bitnode (host) set up by a botmaster for nefarious purposes, or was a host compromised and misused for botnet control purposes? As far as blockchain uses go, does it matter? The result is that the particular host is under the botnet control.

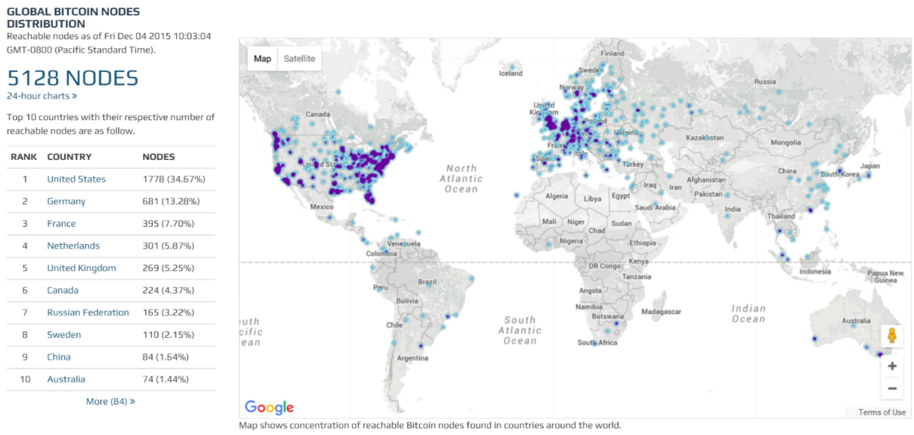
Many people mistakenly assume that blockchain transactions are always protected by the use of TOR; however, our analysis of the IP addresses regarding TOR nodes indicates that less than 0.25% of known bitnodes are also TOR nodes. TOR is commonly recommended for use with blockchain software clients, so the coincidence of bitnodes that also serve as TOR nodes is an additional risk to be considered by vendors or subscribers to blockchain technology.

The following map shows the geographic outlay of TOR nodes on December 2.



Source: http://cdetr.io/tor-node-map/

Bitnodes are deployed globally according to concentrations of users who support the technology. Consequently, the nodes that coincidentally are used for other purposes (such as TOR or malware control) are equally global in their geolocations. There is general overlap in geographic regions between TOR and bitnodes, although the overlap in addresses is very limited.



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Fri Dec 04 2015 10:03:04 GMT-0800 (Pacific Standard Time).

5128 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	1778 (34.67%)
2	Germany	681 (13.28%)
3	France	395 (7.70%)
4	Netherlands	301 (5.87%)
5	United Kingdom	269 (5.25%)
6	Canada	224 (4.37%)
7	Russian Federation	165 (3.22%)
8	Sweden	110 (2.15%)
9	China	84 (1.64%)
10	Australia	74 (1.44%)

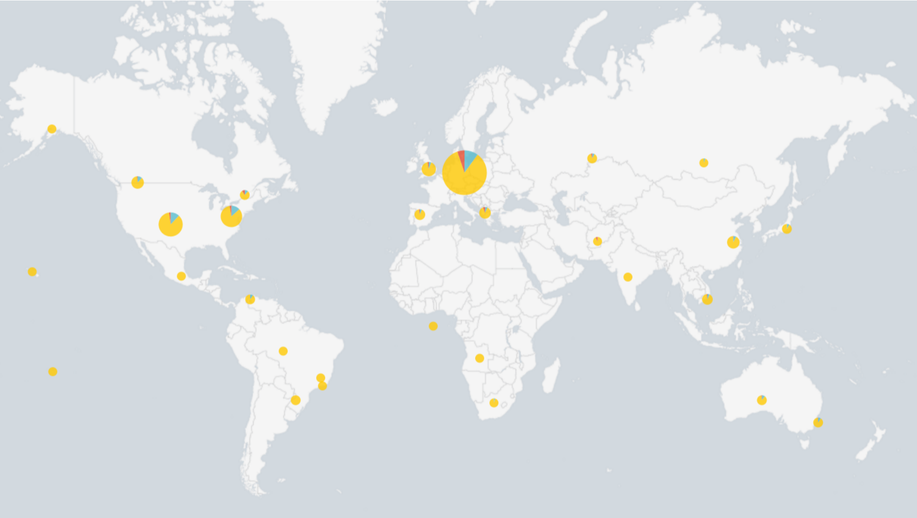
More (84) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

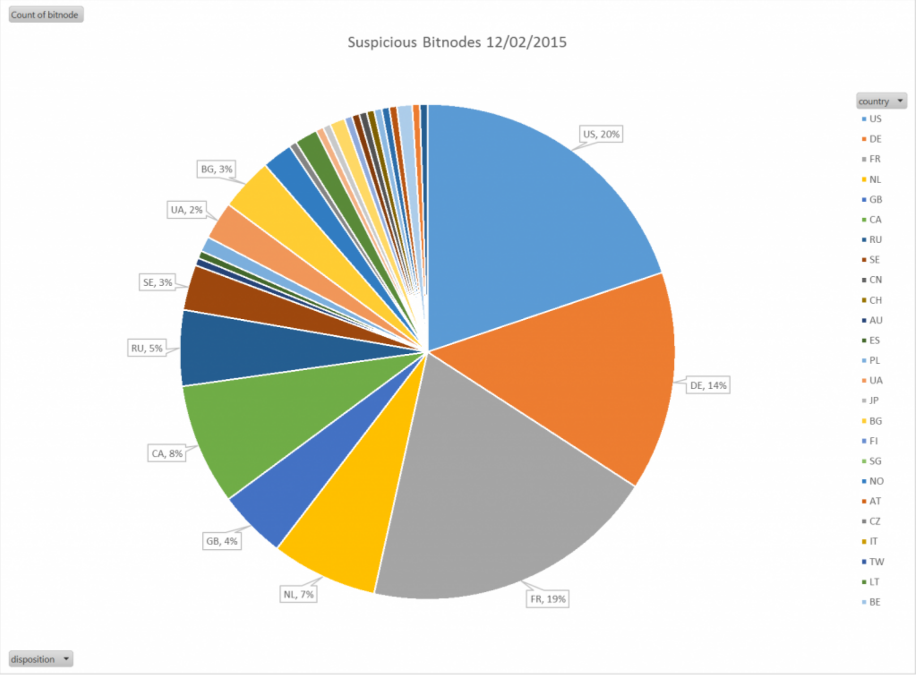
Source: https://bitnodes.21.co/

Applying OSINT to the blockchain

By using OSINT and proprietary information we can create dispositions of bitnodes by their risk categories. The following map indicates the regional concentrations (on December 2) by bitnodes as (red) Suspicious, (blue) Interesting, and (yellow) Normal. “Suspicious” indicates a bitnode that appears on blacklists and has high detection rates in samples that use the bitnode address. “Interesting” is a bitnode address that is a known TOR exit node or appears in any malware samples. “Normal” encompasses all others.



Only a relatively small percentage (17%) comprise Suspicious or Interesting nodes. The following chart indicates the breakout of Suspicious nodes by country code.

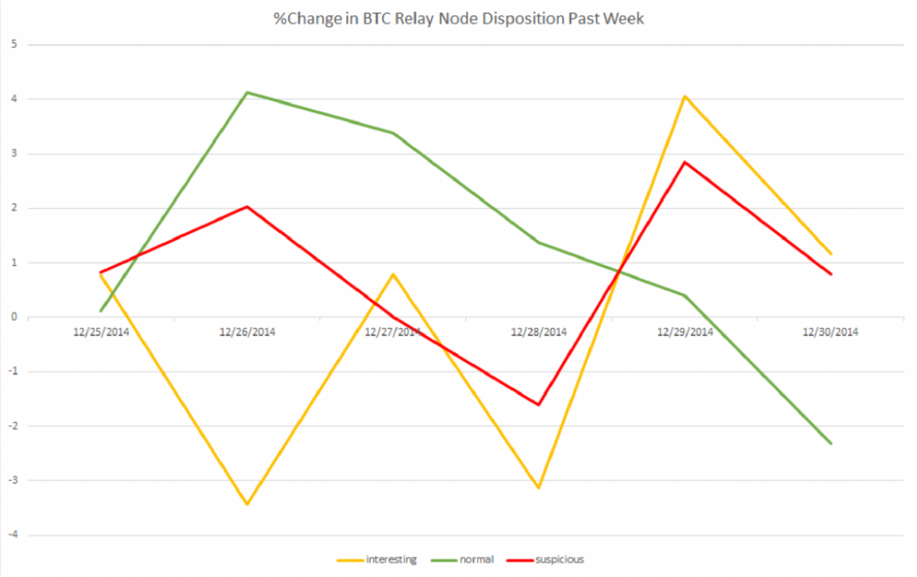


Other host providers include cloud services and public or free Internet hosts. Such services are sought out and used extensively by botmasters as they often allow limited free use, or full subscription use for a defined period (commonly one to three months before they are abandoned or terminated). Indeed, between February and December, 20% of all unique bitnodes we analyzed existed for no more than one day, 72% for less than one month, 99% for less than three months, and less than 1% existed for more than three months.

More on TOR

The coincidence of the TOR network and bitnodes may be more than OSINT demonstrates. For example, In December 2014 the "LizardSquad" hacked the TOR network, taking control of 30% to 40% of active nodes. One effect of the attacks was an increase in new bitnodes.

The following graph illustrates a 4% increase in Normal nodes and a 1% increase in Suspicious nodes, with a 4% decrease in Interesting nodes that occurred on December 26, 2014, when the TOR attacks began.



This data could be interpreted to mean that the additional nodes were botnet nodes previously masked by TOR. The new interesting and suspicious nodes were the product of antimalware submissions and blacklist updates that were reported by researchers. By December 30, 2014, the TOR network had recovered, and the number of visible bitnodes decreased as they were again masked; in the interim, however, the aggregate had increased to an estimated 23% of all bitnodes related to botnets.

In effect, the December 2014 attacks by LizardSquad (and subsequent research performed by security organizations around the world) revealed previously unknown nodes on the Bitcoin network, some associated with malware or botnets. This demonstrates the extent (about 6%) of TOR nodes that provided anonymity to blockchain transactions—at least in that period.

What this means for financial risk

Bitcoin has an estimated market cap of $5.4 billion. On December 2, 2015, a total of $634 million (depending on the exchange venue) in transactions value was routed through the global bitnodes. Although only the noted 17% of bitnodes are indicated to be “known associates” of malware or botnets, those nodes accounted for 31% of the volume of (unconfirmed) transactions relayed that day. In other words, almost $200 million of Bitcoin transactions were relayed through suspect nodes.

What does this mean? There is no risk of these funds being stolen because the blockchain has mechanisms to protect the transaction with distributed (and autonomous) processing and validation. There are, however, availability concerns that go beyond simple outages, for example, the possibility of “value” impediments because the route is manipulated in the peer map of related clients. (The exchange value of Bitcoin is related in part to the volume available for trading and the availability of peers to process the transactions.) Outages may be brief, but they have immediate consequences as peer discovery from “good” to “bad” nodes depends fundamentally on the availability of good nodes.

Beyond interruptions, there is the risk of malicious entities gaining insights into transactions. Botmasters can simply monitor the peers that they control to understand the origin and valuable details of the transactions in their exchange form. Although they will not see into traded contracts, or be able to steal from cryptocurrency exchanges, they can monitor who is trading with whom and how often—and potentially control when/if and where their traffic is able to route.

The health of any network is crucial to the integrity of the service it supports. Financial products and services related to the blockchain may be affected by botnet- or malware-associated nodes that relay transactions, currently or in the future, as the sophistication of attacks and exploits continues.

A final note

Much more specific details of risks are available when the blockchain (ledger) and bitnodes are tied to threat intelligence. On December 2 two ransomware payment addresses for Virlock were used in 14 transactions. Five of the 14 transactions were relayed by bitnodes associated with malware or botnets. Although blacklisting Bitcoin addresses can be a difficult proposition (as many addresses have been stolen from legitimate users’ wallets over time and misused in much the same way that stolen credit card numbers are used sporadically by cybercriminals), some insights of specific addresses are useful to understanding the risk of transactions made with otherwise “anonymous” counterparties.

We might conclude from this research that Bitcoin is a payment platform that cannot be trusted, but that is not the case. Yet we depend on a trustworthy payment platform, and understanding the associated risks allow us to build appropriate controls to mitigate those risks to tolerable levels. Bitcoin, much like any other payment platform (electronic as well as physical) has risks associated with it that appear to be specific to a decentralized virtual currency. Our intention is to highlight some of these risks such that measures can be introduced to mitigate those risks to a level acceptable to all of us operating within this digital society.

Tags: cybercrime, E-Commerce, internet security, cybersecurity

Like 6 Share 37 G+1 1 Tweet Email

No Comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

reCAPTCHA

Type the text

Privacy & Terms

Post Comment

Intel Security on Twitter

lSecurity We've been named as leaders in the @Gartner_inc MQ for Intrusion Prevention Systems. Find out why: https://t.co/FFNC217yMC
2 hours ago·Reply·Retweet·Favorite

Security Find out why s love anonymous apps, and how to coach them through the social landmines. https://t.co/vevWMxWN3d
3 hours ago·Reply·Retweet·Favorite

Follow @IntelSecurity

Also Find Us On

About | Subscribe | Contact & Media Requests | Privacy Policy | Legal | FAQ