



# ASERT Threat Intelligence Report 2015-04

## DD4BC DDoS Extortion Threat Activity

For the last year or so, an individual or organization calling itself DD4BC ('DDoS for Bitcoin') has been rapidly increasing both the frequency and the scope of its DDoS extortion attempts, shifting target demographics from Bitcoin exchanges to online casinos and betting shops and, most recently, to prominent financial institutions (banks, trading platforms, payment acquirers) across the United States, Europe, Asia, Australia, and New Zealand. Other verticals receiving extortion threats include ISPs and publishing, with indicators that higher education may have also been targeted. This situational threat brief provides historical context around these attacks and outlines the Tactics, Techniques, and Procedures (TTPs) utilized by the threat actor(s) and will be useful for those individuals and organizations that seek a fuller understanding of the depth, scope, and capabilities presented in order to more quickly defend and deal with an attack by this actor or by other copycat attackers that leverage the same TTPs. An overview of the bitcoin-based financial transactions associated with the threat actor is also included and will hopefully provide interesting information to researchers and law enforcement useful to the process of investigation, attribution and prosecution.

### Executive Summary

News and other security organizations have been discussing the DD4BC (DDoS for BitCoin) attacker or attack group that has been subjecting various targets to extortion based DDoS attacks. Despite a bounty of at least \$26,000 (110 BTC) for information about DD4BC, attacks continue and a higher volume of extortion letters continue being sent as of mid/late May and early June 2015.

Indicators show that DD4BC extortion DDoS attacks started sometime around July of 2014 and continue as of this writing in early June 2015, with extortion demands increasing recently to 100 BTC, depending upon the targeted vertical. Initial targets were in the online gambling arena, though ASERT is aware of more recent attacks that have focused on other organizations, including several financials to include banks, trading platforms and payment acquirers, publishers, and potentially higher education targets which suggests that the attacker(s) are diversifying in their attempt to generate funds.

Initial warning/assessment attacks are smaller, typically 10-15 Gbps, and the full attack launched after the victim refuses to pay the extortion demand have been reported as high as 40-60 Gbps. DD4BC has consistently advertised 400-500 Gbps of DDoS capacity, yet if this capacity is available, it is not being used. It. The more likely scenario is that capabilities are being overstated. Despite this likely scenario, organizations should be

aware that the potential for 400+ Gbps attacks clearly exists within the overall DDoS threat landscape, even if this individual does not wield such capabilities at this time. Despite the overstating of capabilities, organizations that are not prepared are highly likely to experience outages.

The bulk of observed attacks launched by DD4BC are SSDP and NTP reflection/amplification attacks with the occasional SYN-flood and, most recently, Wordpress XML-RPC reflection/amplification attacks.

While the potential for threat actor evolution and increased DDoS capability is present, well-prepared organizations shouldn't have any trouble defending against such attacks via a combination of organic detection/classification/traceback/mitigation techniques as well as cloud-based DDoS mitigation services. Indeed, ASERT originally warned about such attacks well over a year ago [1]. Subsequently, ASERT provided its customers as well as the community at large with insights and a prolific amount of information regarding reflection/amplification attacks [2] [3] [4] [5] [6] as well as information on what can happen when targeted organizations are unprepared [7]. These materials provide in-depth information about how these attacks work, why they work, and precisely how to easily mitigate them using Arbor products and services as well as other network-based mitigation strategies.

## Attack Tactics, Techniques and Procedures (TTPs)

Multiple indicators suggest that the attacker(s) may be using booter/stresser services to perform their attacks. Booter and stresser services are plentiful in the underground, and while many operators of booter/stresser services overstate their capabilities they are still a force to be reckoned with, especially if the network and hosts are unprepared for the various attacks that can be easily and cheaply launched. All of the commodity DDoS attacks from the past are now available in the stresser services, and as new attack techniques are discovered, they eventually make their way into the stressers. Booter code gets stolen, leaked, modified, and re-used, which results in a lot of the same types of attacks being available to a wide population of miscreants. Lists of servers vulnerable to the various types of UDP reflection/amplification attacks are also known to be shared among some of the services, which results in more widespread abuse. At least one booter service advertises an API that allows users and site administrators to find reflection/amplification servers.

Before or during the delivery of the ransom message, the attacker(s) often launch a small attack which they reference in the extortion letter. This first "warning shot" is designed to send a message that the attack is real, but it may also serve as a generic test to assess DDoS defenses. If the site falls over easily, then the attacker(s) may have found a lucrative target. It should be obvious that no one should pay the ransom, for to do so only encourages the criminals to return to a soft target to extort more money and further encourages their continued criminal campaigns.

If the site experiences an outage, or if the target does not pay the ransom, then a larger attack will typically commence and may involve more in-depth attack techniques. In many cases in 2014, the heavier attacks would arrive shortly after the deadline had passed, although recent trends suggest a longer delay may be experienced. In some cases, the attacker(s) do not bother the target again after issuing the initial extortion e-mail, even if the victim does not respond. In other cases, attacks have caused serious outages and in one

instance (Exco.in) another attacker(s) (or a related attacker(s)) took advantage of the confusion caused by the DDoS to deeply penetrate the business and engage in theft of all the bitcoins – a painful financial loss for site operators and all users who had trusted the site with their funds.

## Timeline of Targeted Organizations and Observed Attacks

This is not intended to be an exhaustive list of victims, as some victims have chosen not to make the attacks public, especially if they have paid the ransom. ASERT is aware of attack victims that are not listed.

Additionally, while Arbor's ATLAS initiative has tremendous global visibility, our visibility is not 100% and therefore there may be aspects of an attack that are not included in our analysis data. In other cases, targets were threatened but apparently not attacked for unknown reasons.

- **Bitbook** - Feb 26, 2014 [<https://www.bitcoinsportsbooks.com/scam-warnings/bitbook-biz/>]

There are no public indications that Bitbook was specifically targeted by DD4BC or that the threat actor/group was known as DD4BC at the time of the attacks, however Tactics, Techniques, and Procedures (TTPs) are similar to DD4BC attacks and forum chatter

[<https://bitcointalk.org/index.php?topic=355081.msg8970372#msg8970372>] suggests a possible relationship with DD4BC. Therefore, the attack is noted here with low confidence. The IP address in question, 193.107.87.38, was hit with two small (~340 Mbps) NTP reflection/amplification attacks.

- **GreatBigBit** – July 22, 2014 [<http://coinfire.io/2015/03/12/bitmain-fights-back-against-ddos-group/>]

Greatbigbit.com (at 104.28.7.61) was hit with a variety of UDP flood attacks for approximately eight hours. The maximum observed attack impact was 3.77 Gbps / 371.96 Kpps.

- **Nitrogen Sports** - July 31, 2014, September 23, 2014

[<http://cointelegraph.com/news/112606/nitrogensports-goes-public-to-combat-extortion-blackmail-and-slander>, <https://bitcointalk.org/index.php?topic=355081.1380>]

On 9/23/2014, Nitrogtten Sports claims to have been attacked since July 31, 2014 with publicized attacks on 9/23/2014:

**Figure 1: Nitrogen Sports Commentary about attacks**

*"This particular hacker has been attacking us since July. We actually did pay him for a while to buy ourselves some time to put additional protections in place. When we decided to stop paying him, we managed to mitigate several attacks this week. He has escalated his attacks and his demand for money, and we felt that it was time to take a stand." (<http://www.bitcoingg.com/nitrogen-sports-remains-resilient-amid-attacks-due-to-blackmails-extortions/>)*

One attack was mentioned on September 25, 2014 [<https://bitcointalk.org/index.php?topic=355081.1360>]

**Figure 2:** Additional Record of Attacks on NitrogenSports.eu - September 25, 2014

**NitrogenSports**  
Hero Member  


**Re: NitrogenSports.eu - POKER - SPORTSBOOK - EXCHANGE**  
September 25, 2014, 02:26:29 PM #1371

Activity: 784 Hey guys, we're working through another ddos attack today, and really apologize for the additional downtime. Our tech team is working to fix the issue; we know this is a major inconvenience to you. We're definitely frustrated too and are doing everything we can to give you guys the best service possible.

Nitrogen Sports Forum Rep Thanks for your patience.

 Ignore https://nitogensports.EU - Anonymous Sports Betting! Bet with 0 confirmations! Easy & Fun!

ATLAS Intelligence suggests that attacks were directed towards IP address xx.xx.205.2. Attack activity directed towards this IP address include the following highlights (which may be related to other threat actors other than DD4BC; although the proximity of the attack intelligence with the public notification implies a correlation)

#### TCP SYN / SSDP / NTP -> UDP/80

- One eight minute TCP SYN attack @ 118.11 Mbps/377.87 Kpps 9/23/2014 11:37:39 AM
- One 62 minute SSDP reflection/amplification attack @ 7.68 Gbps/3.07 Mpps 9/23/2014 3:03:39 PM
- One 49 minute SSDP reflection/amplification attack @ 8.28 Gbps/3.28 Mpps 9/23/2014 2:01:39 AM
- One 13 minute NTP reflection/amplification attack @ 5.51 Gbps / 1.53 Mpps 9/23/2014 11:36:39 AM

#### DNS Reflection/amplification attacks

- One six minute attack @ 5.75 Gbps / 561.20 Kpps 9/23/2014 11:01:39 AM
- One eight minute attack @ 7.24 Gbps / 721.52 Kpps 9/17/2014 11:16:39 PM

#### SSDP + TCP RST -> UDP/443

- One SSDP reflection/amplification attack @12.70 Gbps / 2.95 Mpps combined with TCP traffic 9/23/2014 1:59:39 PM

Other attacks were directed at UDP/2053, but the volume was substantially lower, peaking at 12.31 Mbps / 3.94 Kpps. These attacks took place between 9/18/2014 and 9/25/2014. UDP/2053 may have been open due to the use of the DNS server option in the Bitcoin Cartographer [https://github.com/mikehearn/httpseed] package, which describes itself as a “Bitcoin peer to peer network crawler and seed server”.

- **Cex.io** – October, 2014 [http://www.coindesk.com/bitcoin-mining-pools-ddos-attacks/]

**Figure 3:** Cex.io mentions BTC-based extortion attack and attack history

*"The attack has been conducted by a hacker who has already DDOSED CEX.IO in October, 2014. Previously, he demanded 2 BTC for stopping the attack. This time, the payment has been raised to 5 to 10 BTC."*

Actual attack dates are not known, although telemetry reveals two attacks in that timeframe towards a destination IP address likely used by cex.io at the time. The first, taking place on 10-6-2014, consists of two hours of UDP flood attacks from UDP/5444 towards UDP/443. A variety of possible services use UDP/5444, although details of which service was used in this possible reflection/amplification attack are not currently available. This flood peaked at 1.24 Gbps/154.93 Kpps. The second attack, from October 13, 2014 appears as a typical NTP amplification/reflection attack at 1.19 Gbps/334.53 Kpps destined towards UDP/888.

- **Bitsquare.io** – October 23, 2014 [<https://github.com/bitsquare/site/issues/30>]

The Bitsquare.io site was mentioned as being unavailable, but forum posts indicate the site admin was extorted for a different, unspecified web property hosted on the same server. In this case, it seems that a 20 Gbps DDoS attack was enough for the hosting provider to take down the server being attacked, therefore protecting other customers but unfortunately completing the attack for the criminal.

**Figure 4:** DD4BC DDoS brings down Bitsquare.io and other sites due to data center decision

btc11 commented on Oct 23, 2014 Collaborator

Hey guys. While I was traveling a really guy emailed from [dd4bc@outlook.com](mailto:dd4bc@outlook.com) to tell me he was going to DDoS the server until I pay him a 2 BTC bounty. The DDoS hit 20GB~ traffic and the data center took the server offline. All data is safe and it's being migrated from Switzerland to France where it will be behind better DDoS protection. Sorry for the lack of communication. It's bad timing that this happened while I was traveling! I'll update you all when it's back online. This will mean an IP change but I don't know what the new IP will be yet.

This is unrelated to the Bitsquare website. The DDoS threat/bounty request was related to the other website on the same server.

Really, really sorry about this!

- **Coinsweeper** - Late October, 2014 [<https://www.bitcoincasino.coingamblingreviews.com/coin-sweeper-back-ddos-attack/>]

**Figure 5:** Coin-Sweeper's explanation of DDoS attack and extortion campaign

*Hi guys! Really sorry - our server is offline right now. A person tried to blackmail us today with threats of a DDoS attack on our server. He started the attack and told us to send him 2 BTC to end the attack.*

*The details of the person are his email address of: dd4bc@outlook.com  
And Bitcointalk Username of: DD4BC  
And he asked us to pay into: 16JEzTkXGeCFPrCoPo9hnSVZWLHMa31fg*

*<https://blockchain.info/address/16JEzTkXGeCFPrCoPo9hnSVZWLHMa31fg>*

*The hosting company contacted us about the attack and our server is offline right now. We are migrating the server to a location with better DDoS protection ASAP.*

- **Mmpool.org** – October 28, 2014 [<https://bitcoin-forums.net/index.php?topic=559011.460>]

**Figure 6:** Message from 'mmpool' describing outage due to DD4BC DDoS Attack

Re: [70 TH] mmpool.org - 1.5% fee split DGM/PPS - tx fees/vardiff/merge mining/tor  
October 28, 2014, 07:57:09 PM

Pool is down because of this:

**Quote**

From: DD4BC TEAM <dd4bc@outlook.com>

Hello

Your mining server is extremely vulnerable to ddos attacks

I want to offer you info how to properly setup your protection, so that you can't be ddosed, at least not with so little power.  
My price is 2 Bitcoin only.

Right now I'm running small (very small) attack which will not crash your server, but you should notice it in logs. Just check it.

If I increase the attack size, I could completely crash, it would drop all connections and damage would be big...  
Don't worry, I will not do it. 😊

I want to offer you info on how I did it and what you have to do to prevent it. If interested pay me 2 BTC to 17aLGgw8AwJdqBtMMG1QtQJgNQQkiyEsp

Thank you.

- **SocialCex.com** – October 29, 2014 [<https://bitcoin-forums.net/index.php?topic=739681.msg9371230#msg9371230>]  
One NTP reflection/amplification attack was observed @ 595.19 Mbps/163Kpps.
- **Blisterpool.com** – November/December, 2014  
[[http://www.reddit.com/r/BitcoinMining/comments/2kndqs/while\\_ddosing\\_my\\_pool\\_check\\_out\\_what\\_this\\_asshole/](http://www.reddit.com/r/BitcoinMining/comments/2kndqs/while_ddosing_my_pool_check_out_what_this_asshole/)]

The blisterpool events observed on November 25, 2014 consisted of SSDP reflection/amplification attacks targeted towards UDP/80. The observed attacks were small, at 80.82 Mbps/32.54 Kpps and 111.76 Mbps/44.86 Kpps. Blisterpool was apparently a smaller operation and the attacker(s) apparently expected an easy target. In addition to the UDP/80 attacks, at least one small spoofed SYN IP address attack was aimed at TCP/9332, related to bitcoin mining operations. Such an attack could easily be performed with scapy, nmap, or other custom scanning tool.

- **Bitalo.com** – November, 2014 [<https://bitcointalk.org/index.php?topic=845595.0>]

176.9.38.40 was hit with a 477.05 Mbps/124.72 Kpps NTP reflection/amplification attack on November 3, 2014. In this case, a ransom of 100 BTC was requested [<http://www.dayherald.com/bitcoin-mining-pools-hit-by-ddos-attacks-utorrent-silently-installs-epicscale/702/>]. A list of attacking IP's was posted [<https://bitcointalk.org/index.php?topic=845595.msg9446165#msg9446165>]. At the time of this writing, all attacking servers appear to have been reconfigured to no longer allow attacks to take place.

- **Mpx.co** - November 15, 2014 [<http://pastebin.com/S4fwBbpQ>]  
Mpx.co was extorted on Nov 15, 2014. The admin did not pay the ransom, and sought creative defenses that apparently proved effective [<http://trilema.com/2014/the-lulz-of-today-ddos-attacks-ransom-notes-tor-anonymity-and-other-faits-darmes-of-the-retarded-generation/>]. The admin of the site apparently coaxed the DD4BC threat actor to join his IRC server. DD4BC joined the IRC channel from an apparent tor node 176.10.116.169. This IP address also corresponds to various perfect-privacy.{info,net,org} domains [<http://www.robtex.com/en/advisory/ip/176/10/116/169/>]. Further discussion of this IP address and associated hosts shall be explored later in the paper.
- **Ruggedinbox.com** – November 17, 2014 [<https://bitcointalk.org/index.php?topic=845595.20>]

The extortion letter is apparently from [dd4bc@unseen.is](mailto:dd4bc@unseen.is). Unseen.is advertises itself as a secure messaging service. This is a bit of a different twist compared to the usual victim profile as of late 2014. Only 1 BTC was requested for ransom, which the ruggedinbox.com forum user stated they would not pay.

**Figure 7:** Extortion mail to ruggedinbox.com

 **Re: Bitcoin Bounty Hunter: Bitalo DDOS attacker discussion**  
 November 17, 2014, 04:47:29 PM

Hi, same here, target: ruggedinbox.com

Original text:

Hi, we just received this message:

You are going under DDoS attack unless you pay me 1 BTC in next 30 minutes to 1MRFFgSexGzyWgbLEhX1Bi3YXR6FaaebV8

Do not ignore me, as it will just increase the price. Smiley

Once you pay me you are free from me for lifetime of your site.

If you think that I'm bluffing, Google my name. Smiley

Thank you.

(sender: dd4bc@unseen.is)

Our answer:  
 this is a volunteer based project, which provides an anonymous, Tor friendly email service, 100% free and ad free.  
 You may want to direct your energies somewhere else, since you'll not see a penny from us.

- **Betbtc.com** - January, 2015 [<https://bitcointalk.org/index.php?topic=856175.160;imode>]

Few details are available about this particular attack. It appears that the victim had deployed a mitigation strategy, but continued to have at least temporary problems with availability.

**Figure 8:** BetBTC forum posting about DDoS attacks; DD4BC user engages

**BetBTC | The Bitcoin Sports Betting Exchange | Ask your API Betting Credentials**

[≤≤≤ \(33/91\) ≥≥≥](#)

**BetBTC:**  
 Site is online, our apologizes for the downtime.

We already had Cloudflare basic protection but are currently working with our hosting provider and third parties like Cloudflare checking for measures to prevent future attacks like this.  
 We will never negotiate with terrorists.

**tonyq:**  
 Site gone again.  
 :-[

**spiz0r:**  
 Quote from: tonyq on January 07, 2015, 05:42:17 PM

Site gone again.  
 :-[

It's back! :)

**tonyq:**  
 Gone again.  
 ???

**DD4BC:**  
 ;D

Analysis of ATLAS data indicates that this site was hit with a small IP fragment attack @ 230.20 Mbps / 25.11 Kpps. Often, the appearance of IP fragments means that a larger amplification/reflection attack is taking place, but in this case we have no detailed insight into further aspects of this attack.

- **Hivewallet.com** - January 22, 2015 [<https://twitter.com/hivewallet/status/558239628168540161>]

**Figure 9:** Hivewallet Tweet Indicates DD4BC attack campaign

The helpful DD4BC Team is requesting 2 BTC for DDoS "protection" again. Last time they took us partially offline, so please standby, users.

RETWEETS 6 FAVORITES 3

4:27 AM - 22 Jan 2015

- **Bitquick** - February 15, 2015 [<https://www.bitquick.co/bitquick-co-thwarts-ddos-extortion-attempt-from-dd4bc-team.php>]

The victim did not pay. The extortion attempt took place on or around Feb 15, 2015 with the extortion email being sent around 8 AM PST. No evidence of an actual DDoS attack was observed.

- **HashNest/Bitmain/Antpool** - Early March, 2015 [<http://cryptoboard.org/showthread.php?tid=138>].

Antpool and HashNest are owned by Bitmain [<https://bitcointalk.org/index.php?topic=855548.0>] This attack threat continues the tactic of targeting mining pools. The attack is alleged to have taken some of the properties down on an intermittent basis, with HashNest coming back online the weekend following the attack and reports that the AntsPool API was still unresponsive.

**Figure 10:** Bitmain message sent to customers about DDoS attacks

Dear Bitmain Customer,

This morning we received a concerning email from a group of hackers threatening Bitmain and our services with a DDoS attack and demanding a ransom payment to prevent the attack. Bitmain is committed to providing the best service possible to our users, and will not invite future attacks of this sort by giving in to the demands of hackers.

The hackers have demonstrated that they do possess the capability to execute a DDoS and that this is not an entirely empty threat, although we do not know the full extent of their capabilities. During the next few days, BitmainTech.com, AntPool, AntPool.com, and Hashnest.com may experience intermittent outages. Our team is working hard to ensure that the effects of any possible attack will be as minimal as possible.

For those customers mining on AntPool, please make sure that you have configured your backup pools properly in the event that you are unable to access AntPool.

For HashNest users, mining payouts will continue as usual and there is no need to worry about lost revenue.

For sales, if you are unable to access our main website, you may contact us directly at info@bitmantech.com.

Thank you for bearing with us during this time.

All the best,

Bitmain

Service of the website has been spotty for the past couple of days due to these attacks. Only thing to do as a user is sit back and wait.

- **Bw.com** - Early March, 2015 [<https://www.bw.com/news/show-29-proclamation>]

**Figure 11:** Bw.com message about DDoS attacks that matches TTPs of DD4BC

Yesterday around March 10, 2015 at noon 11:00, BW mine pool again by malicious hackers continuous DDOS attacks, resulting in some ore mining pool user can not connect.

No ransom note was disclosed, however the timing and the TTPs match DD4BC.

- **Nicehash.com** – October 31 and November 2, 2014  
[<https://bitcointalk.org/index.php?topic=562238.msg9410834#msg9410834>]

Nicehash reported attacks from October 31 and November 2, 2014 and claimed that network filtering helped with the attacks, but also blocked legitimate traffic consisting of bitcoin miners. This suggests that the attackers were hitting on mining-related ports, as observed elsewhere, and not simple SSDP amplification/reflection floods to UDP UDP/80, as observed during other attack campaigns.

**Figure 12:** Nicehash reports DDoS attack

**nicehash** Sr. Member #2413

 **Re: [ANN] NiceHash.com - sell & buy hash rate cloud mining service / multipool**

November 02, 2014, 08:38:45 AM

Hi,

Activity: 297

NiceHash.com

 Ignore

As you have seen we've been under massive DDoS attacks in the past days. Once again, these are classical extortion DDoS attacks. We are able to mitigate DDoS by network filtering, however, protection and filtering also blocks some good traffic (miners), unfortunately. Attacker is probably attacking by bots. We have gathered some useful data and reported attacker to FIRST (<http://www.first.org/>) and TF-CSIRT (<http://www.terena.org/activities/tf-csirt/>). We are not negotiating with attackers and hopefully they will at least have a restless and disturbed sleep while the security incident groups are trying to identify them. If anybody has any info about these attackers (they are also attacking other pools) we will reward any useful information.

Thank you for understanding and thank you for using our service!

The extortion mail was sent from anonymousemail.us, an anonymous mail provider. The body of the mail message did not use the word “DD4BC”, however the TTPs match DD4BC and the BTC address specified was also used in an extortion letter from a known DD4BC e-mail address to another victim, coin-sweeper.com.

**Figure 13:** Extortion mail sent to Nicehash.com

From: anonymousemail@anonymousemail.us  
 Return-Path: <anonymou@free.hostodon.me>  
 X-Mailer: Anonymous Email - <https://anonymousemail.us>  
 Message-ID: <E1Xkim5-0001Sp-Li@free.hostodon.me>  
 Date: Sun, 02 Nov 2014 01:12:05 +0100

Subject: \*\*\*Spam\*\*\* DDOS 😊

<p>NiceHash is down again.</p>

<p>And you know what to do to stop it.</p>

<p>1 BTC @ 16JEzTkXGeCFPrCoPo9hnSVZWLHMa31fg</p>

<p>I will not ddos it for long, but...i will keep doing it regular until I'm paid.</p>

<p>and you will be losing your customers/miners...</p>

**Figure 14:** The initial extortion e-mail sent to Nicehash

```

Return-Path: <anonymou@free.hostodon.me>
From: anonymousemail@anonymousemail.us
X-Mailer: Anonymous Email - https://anonymousemail.us
Message-ID: <E1XkDCr-0003gy-7K@free.hostodon.me>
Date: Fri, 31 Oct 2014 15:29:37 +0100

Subject: ***Spam*** DDOS!

<p><br />
Your mining server is under DDoS attack.</p>

<p>Pay me 1 BTC and I will stop and you are free for lifetime of your site.</p>

<p><br />
My btc address: 16JEzTkXGeCFPrCoPo9hnSVZWLHMa31fg</p>

<p>DO NOT REPLY! I can't receive your emails. Pay me and I will know it's you.</p>

<p><br />
If you ignore me, and I don't receive your payment within 2 hours, price to stop will increase to 2 BTC and will increase for 1 BTC
for every day of delay/attack.</p>

<p>&nbsp;</p>

```

- [Exco.in](#) - February 3, 2015 [<https://twitter.com/ExcoinExchange/status/562744467607019522>]

The attack on Exco.in appears to be more involved than most of the other attacks. During the DDoS attacks, the victims kept their users up-to-date with Twitter. Exco.in staff struggled to maintain operations, and experienced trouble with load balancers. This is not surprising, since load balancers can be overwhelmed in the face of DDoS traffic since they keep state and eventually become resource depleted. Exco.in was also dismayed that the attacker(s) continued to discover IP addresses of servers despite attempts to deploy anti-ddos mitigation, resulting in disabling UDP floods. While the exact method of discovering the real IP behind the proxy network they chose is not known at this time, there are numerous possibilities at play that could allow for this style of attack. Stresser services often advertise a resolver for DDoS protection services that function as a proxy, since such services are known to have limitations in coverage.

While the attack started on February 3rd, the site experienced persistent problems and on February 12th a message about unexpected downtime was posted

[<https://twitter.com/ExcoinExchange/status/565569698210013185>]. The last tweet posted on March 14th discusses a new infrastructure [<https://twitter.com/ExcoinExchange/status/576950784870494208>] but additional messages to forums indicate that the site was compromised by someone named “ambiorx” who stole all the bitcoin. Other forums suggest that ambiorx and dd4bc may be associated or the same person [<http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info>]. Staff behind Excoin put some effort into doxing ambiorx , providing data on reddit

[[http://www.reddit.com/r/Bitcoin/comments/2vzwvb/anyone\\_heard\\_of\\_exchange\\_excolin\\_looks\\_like\\_it/](http://www.reddit.com/r/Bitcoin/comments/2vzwvb/anyone_heard_of_exchange_excolin_looks_like_it/) ]. While a relationship to DD4BC is possible, the attacker(s) “ambiorx” may have simply been opportunistic, although that is unknown. If these allegations are true, it indicates that sites dealing with DDoS are also

vulnerable to other types of compromise while their attention is being directed toward dealing with the DDoS attack. This tactic has been used elsewhere to distract banks from fraud campaigns, and to perform other strategic DDoS in conjunction with other concurrent criminal campaigns.

- **Holytransaction.com** - February 15 and 16, 2015

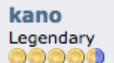

**HolyTransaction**  
 February 15 · 
 
  
 Our servers are under DDos attack. We are working with our host to fix the issue asap. Sorry for any inconvenience.  
[Like](#) · [Comment](#)

Network telemetry reveals traffic hitting an IP address associated with Holytransaction.com at the time of the reported attack. Approximately 22 minutes of UDP floods from UDP/7273 on a small number of hosts in China and Korea to UDP/7273 peaking at 9.58 Mbps/1.06 Kpps. This is not the usual style of attack from DD4BC. There may be other explanations for this traffic, other than a DDoS attack. This port may be associated with “OMA Roaming Location” or possibly a QuickTime Streaming Server [<http://www.adminsub.net/tcp-udp-port-finder/o/278>].

- **Ckpool** - Early March, 2015  
[\[https://bitcointalk.org/index.php?topic=789369.msg10705723#msg10705723\]](https://bitcointalk.org/index.php?topic=789369.msg10705723#msg10705723)

Ckpool appears to use the hostname kano.is and a discussion of the DDoS took place on the popular bitcointalk forum where the user ‘kano’ mentioned a 3 BTC ransom pointing to the user profile for user “D D 4 B C” [<https://bitcointalk.org/index.php?action=profile;u=411920>]. It appears that the DDoS attack impacted the site by creating sporadic availability.

**Figure 15:** DD4BC attack campaign on CKPool (kano.is)


**kano**  
 Legendary  

  
 Activity: 1372  

  
 Linux since 1997 RedHat 4

Re: 2 AVA4.1s Won! [4400 TH] CKPool (kano.is) from the cgminer devs [0.9% PPLNS]  
March 08, 2015, 10:14:25 PM

**Quote from: pekatete on March 08, 2015, 10:10:50 PM**

**Quote from: kano on March 08, 2015, 09:53:59 PM**

Yeah had a problem for about 5 or 10 minutes (40 minutes ago) - but cleared up once I restarted the pool.

I think the problem is still persisting, mine failed over again 6 minutes after your post .... and the site is still not accesible!

Yeah it's a DDOS - seems the server DDOS protection cuts in and everyone is out for 5 or 10 minutes.

This guy says I have to pay him 3BTC ...  
<https://bitcointalk.org/index.php?action=profile;u=411920>

- **Ghash.io** - Early March, 2015 [<http://blog.cex.io/news/official-statement-on-the-last-weeks-ddos-attack-against-ghash-io-mining-pool-14156>]

While the name DD4BC was not specifically mentioned, the TTPs of DD4BC match this target. This attack was attributed to the same person(s) who performed a DDoS upon cex.io in October of 2014. The first ransom demand was 2 BTC, which increased to 5-10 BTC. The website in this case remained operational, however the mining pool itself – the actual target – was down for a six hour period. Ghash.io runs multiple types of mining pools to include Bitcoin, namecoin, IXCoin, DevCoin, and others, including a multipool which allows multiple types of mining. Ghash.io representatives reported attack activity of up to 40 Gbps.

*Figure 16: Notice about DDoS attack on Ghash.io mining pool*

### **Official Statement on the Last Week's DDoS-attack against GHash.IO Mining Pool**

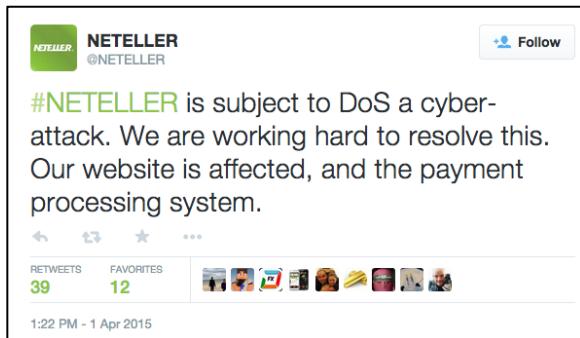
16.03.2015

Last week, GHash.IO has experienced a DDoS-attack against the pool. Although the website itself did work, miners were not able to mine during 6 hours, as a result of the attack taking up to 40 Gbps.

ATLAS telemetry shows early attacks on March 4, 2015 consisting of two hours of NTP amplification/reflection attacks destined towards UDP/3333 on a Ghash.io stratum server. The volume from the March 4th attack peaked at 855.78 Mbps/234.56 Kpps. Some attack activity was observed the next day as well, after the site had changed IP addresses. In that case, a 785 Mbps/207.63 Kpps NTP amplification/reflection attack, again destined towards UDP/3333 was observed to last approximately thirty minutes. These data appear to reflect the earlier attacks, and not the higher volume attacks mentioned on the Bitcoin forum.

- **Neteller** – April 1, 2015. [<http://www.streakgaming.com/forum/neteller-currently-experiencing-going-distributed-denial-service-ddos-attack-t55326.html>]

This attack was mentioned on April 2nd, 2015 and also on the Neteller twitter feed, which indicated that the payment processing system was also unavailable due to the attack, halting operations.

**Figure 17:** Neteller tweet mentions DDoS attack

While it was not mentioned in the tweet, the DD4BC threat actor(s) mentioned and took responsibility for the DDoS upon Neteller in an e-mail to another potential victim on April 10, 2015. In this case, ASERT observed NTP reflection/amplification attacks destined towards UDP/53. Neteller was able to work around the situation within a day or so, based on additional posts.

**Figure 18:** Neteller forum post about DDoS attack mitigation success

This is a screenshot of a forum post from the website casinomeister.com. The post is dated April 02, 2015, at 08:24 PM, by a user named vixen777. The user's profile picture is a baseball card featuring a red cardinal. The post title is "NETELLER is currently experiencing an on-going Distributed Denial of Service (DDoS) attack!". The post content provides information about the attack and how users can access their accounts via a direct link to the member area of the Neteller website.

- **Slottyyegas.com and betatcasino.com** - April 5, 2015  
[<http://www.casinomeister.com/forums/showthread.php?t=66669>]

These shared properties claim that a 45 Gbps attack hit them on April 5th, 2015 with 10 BTC ransom note. A representative of the companies made the following statement:

"The threats originated for the Easter Holidays and indeed, come Monday we were hit with 45 Gbps of DDoS bandwidth. This attack was vicious, massive and wide spread and hit our entire range of sub-nets, even our CDN has been compromised (Content Delivery Network) as well as our AWS (Amazon's Cloud Service)."

Despite the wording used here, the infrastructure was not actually compromised (implying a loss of confidentiality and integrity) but was merely saturated with a DDoS attack. ASERT sensors indicate that the attacker(s) used typical SSDP reflection/amplification techniques against this target.

- **Pokerstars.com** - April 10, 2015 [<http://www.hacksurfer.com/posts/betfair-and-pokerstars-hit-with-ddos-attack>]

This site was also mentioned in e-mail from DD4BC to another potential victim on April 10, 2015. Observed traffic consisted of NTP reflection/amplification attacks on 4-10-2015 @ 2.98 Gbps and 1.37 Gbps aimed at UDP/999, along with a TCP SYN flood aimed at TCP/443. As of this writing, there appears to be no accessible service listening on UDP/999. It should be clear that attacker(s) can easily perform some basic reconnaissance with nmap or other port scanner upon their targets, and will aim attacks at ports other than UDP/80 and UDP/443 when some additional benefit seems likely. Insight into operational details of any given target is often easily obtained and can be used to focus attacks that cause more damage.

- **Unnamed online casino** - April 10, 2015

An attack on an unnamed online Casino took place on April 10, 2015. ATLAS statistics show attack activity in the form of SSDP reflection/amplification attacks (source port UDP/1900) to destination port UDP/80 on two occasions, and destination ports UDP/5464 and UDP/123 on another occasion. Again, the attacker(s) may have performed initial reconnaissance upon their target and picked a port involved in some sensitive operation.

SSDP attacks observed:

- 7.68 Gbps/3.18 Mpps aimed towards UDP/80 on April 9, 2015
- 9.78 Gbps/3.18 Mpps aimed at UDP/5464 and 123 on April 10, 2015
- 5.89 Gbps / 1.96 Mpps aimed at UDP/80 on April 14 2015

The attack on April 9 was likely the initial reconnaissance/demonstration flood designed to get the victims attention. It appears that the victims did not pay the extortion demand, as they were attacked two additional times. It is interesting to note that the total volume of attack activity was still less than 10 Gbps, which is far, far below the 400 Gbps speeds advertised by the attack group. It is also possible that due to the limitations of our global ATLAS sensor array that we are only seeing some portion of the attack which accounts for the smaller volume since we are viewing the attack from multiple vantage points.

- **Redbet.com** - April 9, 2015 [<http://www.casinomeister.com/forums/showthread.php?t=66514&page=2>]

Attacks disrupted various services including e-mail, and site users reported two day downtimes. Numerous attacks were observed on April 9 2015 to include the following:

- 20.94 Gbps/6.17 Mpps SSDP reflection/amplification attack towards UDP/80 and 1389
- ICMP flood of 25.93 Mbps / 31.93 Kpps
- 19.34 Gbps/5.41 Mpps of combined SSDP and SNMP reflection/amplification attacks towards ports 1389 and 307
- 30.29 Gbps/9.96 Mpps SSDP amplification attack to UDP/80

- ICMP flood of 32.12 Mbps / 47.17 Kpps
  - 28.12 Gbps/9.90 Mpps SSDP amplification attack to UDP/80
- **Unnamed European Financial target** - May 1, 2015

As the attacker(s) begin to diversify targets past bitcoin pools and online gambling sites, they have set their sights upon other organizations. In this case, a financially-based target that was not related to bitcoin or online gambling was attacked.

  - SSDP and NTP amplification attacks that peaked at 20.33 Gbps / 6.39 Mpps, aimed at UDP/80
  - ICMP flood @ 30.62 Mbps/37.89 Kpps
  - TCP SYN floods aimed at TCP/443 peaking at 53.38 Mbps
- **Expresscoin.com** - Early May, 2015  
[[https://www.reddit.com/r/Bitcoin/comments/34kloj/dd4bc\\_is\\_ddosing\\_expresscoincom\\_for\\_ransom\\_bu\\_t/](https://www.reddit.com/r/Bitcoin/comments/34kloj/dd4bc_is_ddosing_expresscoincom_for_ransom_bu_t/)]

Attacks on expresscoin.com were observed on May 3, 2015 and consisted of 15 minute bursts of UDP traffic floods @ 470.74 Mbps / 541.60 Kpps, destined towards a variety of ports on the target IP. Unlike other targets investigated for this document, obvious signs of reflection/amplification attacks were not observed in this instance.
- **Unnamed Organization** – Early May, 2015

This unnamed victim was sent an extortion letter, which was not paid. DD4BC then launched an SSDP reflection/amplification and NTP reflection/amplification attack for two hours with an attack peak of 34 Gbps that took the organization down. Typical to form, there were more SSDP sources than NTP sources observed. In this case, the attackers leveraged approximately 10,000 sources in their reflection/amplification attack which was aimed at ports 80 and 666.
- **Various organizations in New Zealand and Australia** – May 7, 2015

At first, these attacks were not specifically attributed to DD4BC, but the TTPs matched very closely [<http://www.zdnet.com/article/online-extortion-threat-targets-australian-and-new-zealand-organisations/>], leading to the medium confidence assessment that DD4BC was involved. On May 10, DD4BC was implicated [<http://bitcoinvox.com/article/1674/hacker-group-dd4bc-new-ddos-attacks>] when further information was released. These attacks included a “warning shot” DDoS of an hour or so. Analytics of attack data revealed targets diversifying from the earlier wave of bitcoin mining and online gambling sites.

- **Extortion demand of 100 BTC on unnamed victim** – May, 2015

A private recipient of an extortion letter reported the incident to Arbor ASERT. Recent trends in DD4BC attack suggest higher ransom amounts, yet attack capabilities appear to remain the same as previously demonstrated.

- **Unnamed Financial Institution** - May 7, 2015

This attack continues the usual TTPs of DD4BC – a series of 30 BTC extortion mails sent from “DD4BC Team” using e-mail address dd4bct@gmail.com to a variety of contact addresses at the organization, associated with a warning DDoS consisting of an NTP reflection/amplification attack @ 61.43 Mbps/16.84 Kpps on UDP/80. One difference in this case was that the extortion letters contained the targets IP address instead of their domain name. Based on the extortion letters observed by ASERT, listing IP addresses is less common. Since the initial warning shot attack, no further hostile activity has been observed despite the extortion deadline passing. This is a trend seen elsewhere as well, and could indicate that the attacker is losing some momentum to actually follow through or simply that attacks will take longer to materialize.

- **Attacks on targets in Switzerland** - Early May, 2015 [<http://www.govcert.admin.ch/blog/6/increase-in-ddos-extortion-dd4bc>]

As the DD4BC actor(s) have diversified, victims have seen traffic from 4-30 Gbps, according to govcert.ch. ATLAS data verifies attacks on various targets where attack activity matches the TTPs of DD4BC. One interesting case concerning a known DD4BC attack in Switzerland is a very small NTP reflection/amplification attack upon a financial target on UDP/80 and 443 on May 7th, 2015 that peaked at 97.62 Mbps / 27.09 Kpps.

Analysis of the source IP's (sanitized here) xx.xx.225.57/32, xx.xx.36.33/32 involved in the NTP reflection/amplification attack shows that this infrastructure was also used on a variety of other targets since May 2, 2015 to include a series of broadband IP addresses in the US, Canada, and France. Targets were mostly UDP/80, however a target of UDP/3074 – used in Xbox gaming – was observed. The attack on a gaming port suggests that a botter/stresser service is being used, likely by both DD4BC and other actors due to the diversity of targets.

- **Financials in Iceland** - May 21, 2015

Ransom is listed at 25 BTC. The ransom mail came in from [dd4bcteam@keemail.me](mailto:dd4bcteam@keemail.me) on May 21, 2015. DD4BC sent the target an IP address in the ransom message, and launched two small SNMP

reflection/amplification attack on the target. The first attack was 6.25 Mbps/550 pps and the second was 47.03 Mbps/6.23 Kpps destined towards UDP UDP/80.

- **Numerous Verticals** – Late May, 2015

Arbor is aware of additional financials, ISPs, and publishing targets that were also sent extortion emails.

## Application Layer Attacks

While the majority of the DD4BC attacks observed have been SSDP and NTP reflection/amplification with a higher percentage being SSDP based, in some cases network defenders have noticed Wordpress based XML-RPC Pingback attacks at layer 7. In one case, the attacker(s) had attempted the usual volumetric attacks after the ransom was not paid, and these attacks were mitigated. Instead of giving up, the attacker apparently began trying layer 7 techniques instead. Note that Arbor customers can use the AIF medium ruleset to mitigate Wordpress Pingback attacks.

Due to the nature of TCP and the XML-RPC techniques used, analysis of Wordpress sites that are being abused to reflect this attack may provide insight into the attacking infrastructure. Unlike the UDP-based reflection/amplification attacks, Booter/stresser systems must make an actual TCP connection to vulnerable Wordpress systems in order to launch the layer 7 pingback attack. This TCP connection and associated logs provide a window of opportunity to gain insight into the infrastructure of the stresser services. ASERT would welcome the opportunity to collaborate with any organizations willing to share such log data.

## Global SSDP Reflectors

One particular DDoS attack attributed to DD4BC came from worldwide sources. While geo-IP mapping is not perfect, it does offer some sense of the geographical distribution of attack sources. When considering that many of the attack sources in this case may be servers abused for reflection attacks, an exact map to attacker(s) infrastructure is imprecise. Considering that many different people often use booter/stresser services at once and some of these services are going to leverage the same vulnerable infrastructure to launch reflection/amplification attacks, such a map may only provide visibility into the minions of one or more booter/stresser services.

While there is limited value in showing maps of all attack data, one DD4BC attack yielded about 330,000 source IP's, with the vast majority of those sites originating SSDP reflection/amplification traffic. Clearly, the number of listening SSDP devices is quite substantial, despite the efforts of groups such as Shadowserver to illuminate the problem for quite some time.

Figure 19: Sources for SSDP amplification DDoS attacks associated with DD4BC – North America

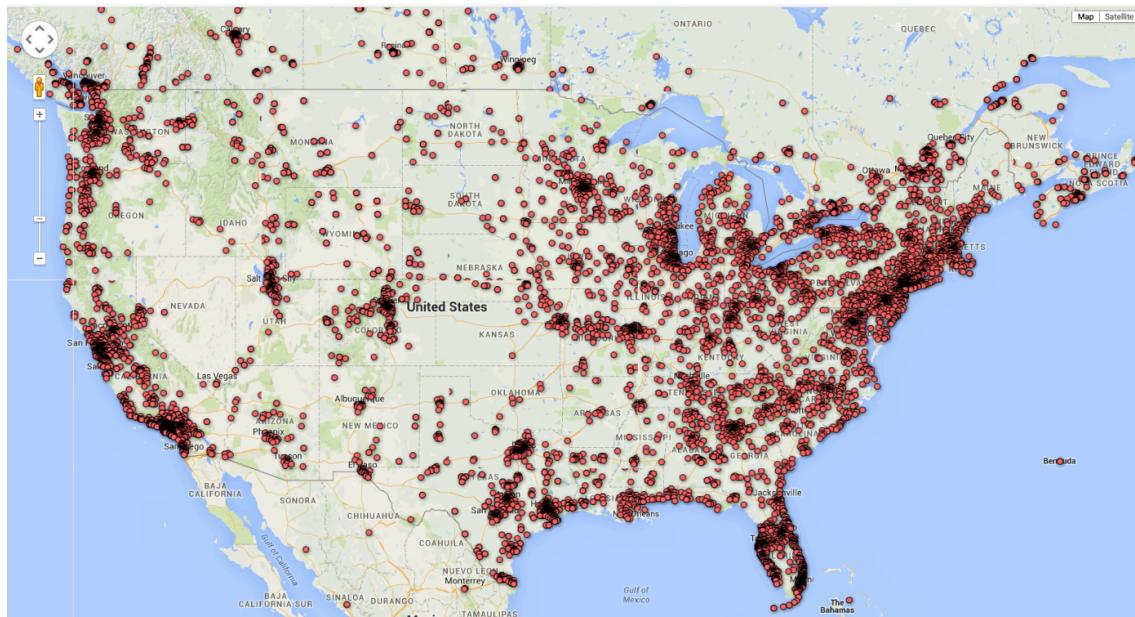
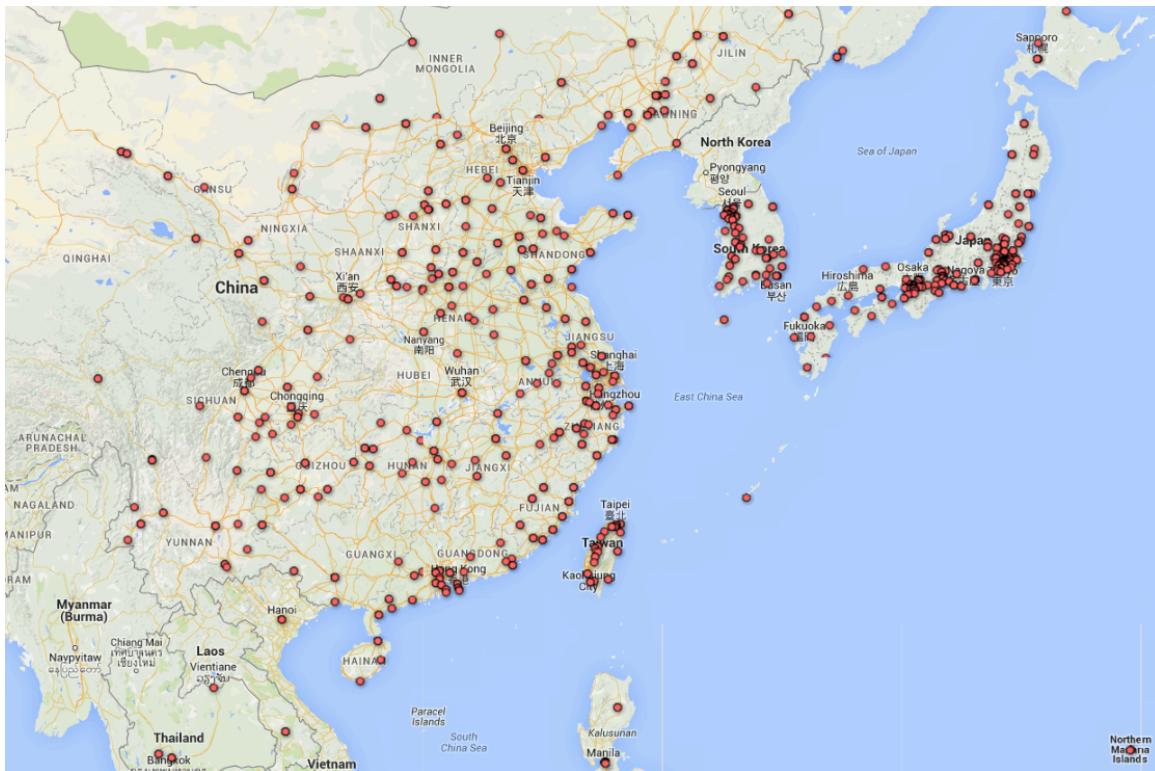


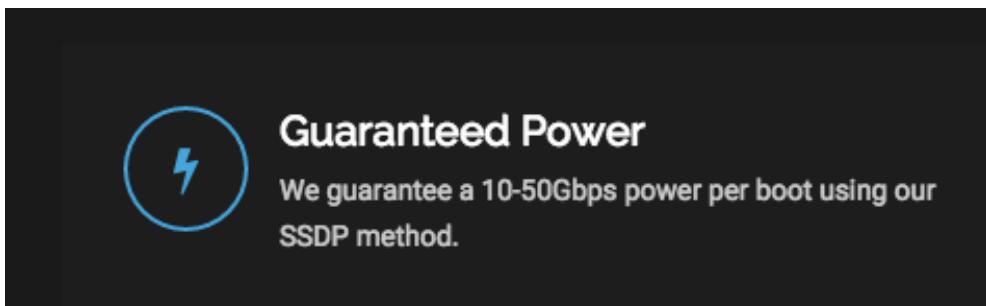
Figure 20: Additional sources for SSDP amplification DDoS attacks associated with DD4BC



**Figure 21:** Additional sources for SSDP amplification DDoS attacks associated with DD4BC

As of this writing, Shadowserver reports that over 13 million IP addresses have responded to their SSDP probe [<https://ssdpscan.shadowserver.org/stats/>]. This represents a huge attack surface, and continues to create availability problems.

Even the forums that cater to minimally skilled cyber-threat actors (aka “script kiddies”) have a great deal of content related to stressers. Reviewing a series of messages from one particular forum where boomer/stresser attack capacity was measured indicates that a great many services offer and boast about their SSDP capabilities. A list of nearly one million IP’s to be used for SSDP reflection/amplification attacks was shared on one underground forum, and other services use server lists that are considered private.

**Figure 22:** Stresser service prominently advertises SSDP capabilities

On these underground forums, various screenshots of dstat output suggest that SSDP is one of the hardest hitting attacks currently deployed, although this depends upon a variety of factors and won't likely be true in every case. Regardless of there being some variability, SSDP poses a substantial threat against an unprepared target.

**Figure 23:** Stresser service discusses SSDP capabilities

**vDos Stresser @vDosStresser - Dec 19**

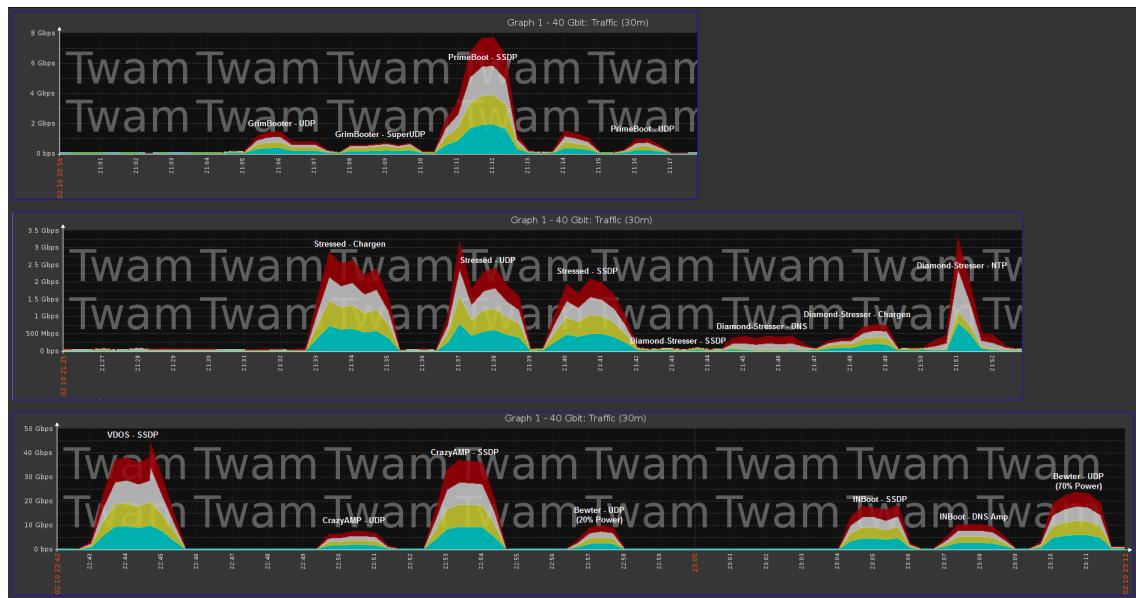
Updated our SSDP amplification lists, hitting extremely hard as always!

The screenshot shows a tweet from the vDos Stresser account. The tweet includes a graph titled "vDos stresser SSDP amplification" with a subtitle "409.33.20.75: 400bit (1h)". The graph plots traffic in Gbps over time, showing several spikes reaching up to 40 Gbps. Below the graph is a table of attack statistics:

	last	min	avg	max
1 (avg)	8.97 Gbps	2.27 Mbps	18.95 Mbps	8.97 Gbps
2 (avg)	9.62 Gbps	2.09 Mbps	20.09 Mbps	9.63 Gbps
3 (avg)	9.53 Gbps	17.14 Mbps	17.14 Mbps	9.53 Gbps
4 (avg)	10.74 Gbps	64.65 Mbps	256.32 Mbps	10.74 Gbps

At the bottom of the tweet, there is a "View photo" link.

**Figure 24:** Dstat of various booters/stressers indicates high capacity SSDP attack capability



## Payment Infrastructure

Other researchers have speculated that the attacker(s) is using a new BTC address for each victim, however in some cases, the same BTC addresses have been used for more than one attack. It is also possible that these addresses are used for other financial transactions that are not related to the extortion campaigns, because various transactions have been observed that far fall below even the apparently negotiated/reduced extortion amounts that have been shared publicly. This suggests other transactions are taking place that might provide for some opportunity for research and/or law enforcement investigation. In other cases, it's possible that a negotiated amount was decided upon in private. Tracking the relevant bitcoin transactions in great detail is beyond the scope of this document, and due to the nature of Bitcoin, such tracking can be quite difficult and of low confidence. Despite these stumbling blocks, some transaction analysis might provide a seed of insight useful to law enforcement or others who seek to uncover the payment infrastructure in place.

Based on the addresses we have been able to collect, the amount of monies obtained by the extortion campaigns appears to be small. We must assume that we do not know about every campaign and every BTC address used by the threat actor and therefore have an incomplete picture. Even if only a few victims pay, it may still be worthwhile to the attacker, considering the limited amount of time required to launch such attacks that appear to be originating from booter/stresser services. If this assumption is true, then the threat actor simply logs into a booter/stresser service to fire off attack traffic, and has to maintain e-mail correspondence and some basic BTC operations. Both of these tasks require minimal costs and minimal time investment.

Bitcoin Addresses used by attacker(s), or alleged to be used by the attacker(s) are in bold red.

**1H2bstU3yCpqJyrNzHSrnperZnTMSwLa5K**. While ASERT does not personally have a copy of an extortion e-mail that contains this BTC address, it was allegedly used by the DD4BC attacker(s), in August 2014 although confidence is limited. [<http://cointelegraph.com/news/112606/nitrogensports-goes-public-to-combat-extortion-blackmail-and-slander>]

**Figure 25:** Low confidence forum chatter suggesting link between DD4BC and 1H2bstU3yCpqJyrNzHSrnperZnTMSwLa5K

The address listed in DD4BC's alleged recent extortion attempts do not have any transactions associated with it at press time. We were given another address **1H2bstU3yCpqJyrNzHSrnperZnTMSwLa5K** which was purportedly used by the hacker back in August. He transfers the funds to what appears to be a mixing service.

On August 11, 2014, at 19:39:18, **1H2bst** received a payment of 1 BTC from 1DMdik1y8s8HsTPiL3FbErqB6FqNw7AUY [<https://blockchain.info/address/1H2bstU3yCpqJyrNzHSrnperZnTMSwLa5K>]. Since early attacks were asking for 1-2 BTC, it is possible that a victim paid the ransom.

On August 11, 2014, at 20:33:49, **1H2bst** transferred 1 BTC to 1BKEhNzWLkezVbXDZA8kD2nJUfQWDTADM8 [<https://blockchain.info/address/1BKEhNzWLkezVbXDZA8kD2nJUfQWDTADM8>]. 1BKEhN then transferred 43.106 BTC to **1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL**, an address of interest.

**1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL** has been discussed at length and associated with numerous malicious activities [<https://www.blocktrail.com/BTC/address/1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL/links>] and has been called a BTC-E hot wallet by some, and a possible private mixer account by others and was discussed on reddit

[[http://www.reddit.com/r/Bitcoin/comments/2mlmk9/thief\\_bot\\_watching\\_the\\_default\\_brainwallet/](http://www.reddit.com/r/Bitcoin/comments/2mlmk9/thief_bot_watching_the_default_brainwallet/)] and other sites [<https://bitcointalk.org/index.php?topic=791367.msg9144759#msg9144759>]. This address has also been mentioned to be used by a mixer service [<https://muut.com/i/localbitcoins/general-discussion:my-account-was-just-hijacked>]. Due to the nature of mixing services, tracing the transactions further can become very difficult or impossible. Further investigation reveals that this address is part of a wallet called “BTC-e.com-output” [<https://www.walletexplorer.com/wallet/BTC-e.com-output/addresses>] and has the highest number of transactions out of all the addresses in that wallet (3274 addresses at the time of this writing). BTC-E describes itself as “a deposit collector for real money and virtual currency bitcoins (BTC)” and also states “BTC-e.com serves as a platform for individuals interested in buying and selling Bitcoins using an assortment of world currencies”. We do not accuse BTC-E.com themselves of any criminal activity, but merely note that this address has been reportedly used in criminal activity on numerous occasions. Most of the addresses in the wallet appear to have very little or no activity, except for the top three:

**Figure 26:** BTC-e.com-output wallet enumeration reveals 1FsVcd address involved in highest number of transactions

Wallet  <b>BTC-e.com-output</b> <a href="#">(show transactions)</a>			
address	balance	incoming txs	last used in block
<a href="#">1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL</a>	0.	15763	356662
<a href="#">1HXq2DHd4hJMiV7FgkM6mD88AsW9UP6U9d</a>	0.	745	357142
<a href="#">1Pj2Qdzrk9rzNSz2Teh3ChuBitXzLtKkz8</a>	0.	130	329902
<a href="#">141bowN8drrEhwyL3KkN4UKC92ky3zDyH8</a>	0.	11	341400
<a href="#">1KKTKrk7ogv36Aig2pFqSB9r2e1KZpopb</a>	0.	11	325073
<a href="#">1J9NdhS8qpGwEZ2nAXqfTsB9EgDf2R5PnQ</a>	0.	9	329498

We will outline some of the prominent mentions of this address that demonstrate involvement in criminal or malicious activity. We cannot claim that every transaction going through 1FsVcd is malicious; however there have been enough reports to warrant interest.

- A reddit post on /r/Bitcoin discusses alleged bot activity that performs a series of transactions which end up in the 1FsVcde address.

**Figure 27:** Tracing of activity associated with BTC address 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL

Thief BOT watching the default brainwallet address and steals anything that come in! Then goes to a monster address. Looks phishy. (self.Bitcoin)  
submitted 6 months ago by [jonstern](#)

This address  
<https://blockchain.info/address/1HZwkjkeaoZfTSaJxDw6aKkxp45agDiEzN>  
Has a bot that instantly grabs any Bitcoin that comes through and transfers it to this address called "Cold Storage."  
<https://blockchain.info/address/36f9dsGq4sw1xy44ZAuMQ1AAiAyHZxBagF>  
Then pieces go here:  
<https://blockchain.info/address/36f9dsGq4sw1xy44ZAuMQ1AAiAyHZxBagF>  
Then they go HERE. A MONSTER of an address:  
<https://blockchain.info/address/1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL>  
I'm suspecting a major thief is at work if you follow the chains of TX. Crazy!  
How does one setup a monitoring script to watch addresses and automatically perform TX? Is this a brute force botnet? WTF?

[[http://www.reddit.com/r/Bitcoin/comments/2mlmk9/thief\\_bot\\_watching\\_the\\_default\\_brainwallet/](http://www.reddit.com/r/Bitcoin/comments/2mlmk9/thief_bot_watching_the_default_brainwallet/)]

- 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL** has been involved in a scam around the August 2014 timeline. A site called TimeToBit.com apparently collected bitcoin payments and then disappeared. According to someone tracking that situation, the money was moved into this BTC address [<https://bitcointalk.org/index.php?topic=744692.40>].
  - TimeToBit.com received a variety of press, which seemed to help its popularity. Some twitter users were vocal about providing support, such as @Knightbot13, who has listed their name as “Bean Fighter” and “Arkham Knight”.

**Figure 28:** User Advertising Timetobit.com, an alleged scam site that moved funds to 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL

Are you looking in #Bitcoin cloud mining?  
@timetobit is your best choice visit  
timetobit.com choose your plan.  
#btc #cloud #mining

RETWEET 1

4:42 PM - 30 Jun 2014

- Additionally, In December of 2014, Sophos Naked Security reported on a viral ransomware demanding 0.619 BTC payment to address 198tX7NmLg6o8qcTT2Uv9cSBVzN3oEozpv [<https://nakedsecurity.sophos.com/2014/12/05/notes-from-sophoslabs-ransomware-with-a-difference-this-one-is-a-true-virus/>]. Further investigations of this address revealed that BTC were moved from 198tX to 1N43vMz9qB1xcBFFzCGnENSmBrE3sXifrn, which then moved coins to **1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL** in the amount of 22.38450048 BTC (worth USD \$8444.78)

[<https://blockchain.info/tx/3d10e5be1ae8758b711386b2ef60d664431d5c518a6f83447df8ecc60c001dd4>].

Further investigation by “cazalla” [<http://qntra.net/2014/12/virransom-the-latest-ransomware/>] reveals that **1FsVc** was involved in at least two other incidents:

- A scam site called dice.ninja. Apparently, someone allegedly behind a scam involving the theft of BTC was “doxed” – had private information released publicly that identifies a person. After the doxing, some refunds from the scam were apparently originated from the 1FsVc address (although this is a low confidence finding, based on a forum post) [<https://bitcointalk.org/index.php?topic=745422.1000>]

**Figure 29:** Dice.ninja scam mentions BTC address 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL

The screenshot shows a forum post titled "Re: dice.ninja - Now with Plinko!" by user "imp0ster" on October 15, 2014, at 05:07:18 AM. The post has ID #1014. A quote from another user, "lolled", is shown: "Another development seen in chat. 17U1LyjKzm2tr8LjpYkFGtvburfyG1rd9q is the return address on the first deposit to the Ninja Address. Someone said, AK claimed its his PD wallet address. Can we get a verification on that?" Below this, "imp0ster" responds: "No I said that the first deposit to the 1Ninja coldwallet was by 184bpd4aMttcUBMV7QXfcPxT9V2nnMdQdQ, which is a return address for a deposit into AK's PD address in [this transaction](#)". The user then adds: "Anyway, I am 'Imposter' on moneypot/jd/prc(don't use those sites though, have only played with bits for fun on moneypot). Anyway, when the dice.ninja heist happened livechat went wild, as I was bored I started investigating. I have had personal contact with dooglus and eric to confirm some stuff such as access times and IP addresses, however these are my own accusations. I am not financially involved in any of this, I barely ever had 2 coins to my name 😊". Finally, "imp0ster" says: "I'll put everything I know in this post, some stuff might not be highly relevant, this is everything I found, I need you guys to verify everything and do additional blockchain analysis, there might also be parts where I screwed up." A note at the bottom states: "First things first, after the doxxing of Jeremy Hise refunds were being issued with 1QAitJvHj5GqzLW6pmheGXTctEwCWR9sNi as a sending address. The funds originate from 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL(a BTC-E hotwallet). Signed messages in refund transactions confirmed the owner of the 1QAitJvHj5GqzLW6pmheGXTctEwCWR9sNi address to being DMF and T04D, the messages were signed with the 1NinjabSP8jQAVaA8y9u5fsjNpB5S22xPv key."

- 100 BTC stolen from a primedice account [<https://bitcointalk.org/index.php?topic=791367.0>]

**Figure 30:** Scam accusation connects to BTC address 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL

The screenshot shows a forum post by user "otrkid70" on September 21, 2014, at 09:22:16 PM. The quote is: "some of that \$ withdrawn ended up tied with this other scam accusation read here <https://bitcointalk.org/index.php?topic=744692.0> attached to this address 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL".

- Address used to hijack payments, in conjunction with DDoS attack activity [<http://ltcgear.com/farm-payments/the-news/>]

**Figure 31:** Apparently coordinated attacks on BTC infrastructure involving 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL

As about identifying class A attackers, as I already informed certain parties from community, a direct connection to database was established starting from IP 178.21.117.208 belonging to directvps.nl and address 1AeFq5RbXiY1vsRqZjcF7fVodCxXwmDcMX (along with many others) was planted in database for payments. 1AeFq5RbXiY1vsRqZjcF7fVodCxXwmDcMX aggregates large amount of coins and sends funds to address 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL (owner can be determined with 100% certainty) For those needing a tip, here's an article <http://qntra.net/2014/12/virransom-the-latest-ransomware/>

- Underground actors known as “**royalsales**” and “**royalhost**” have allegedly used 1FsVc address in their criminal operations, according to underground forum posts in September of 2014 to the exploit.in forum  
[<http://webcache.googleusercontent.com/search?q=cache:MoRFk9XkU40J:https://exploit.in/forum/pda/index.php/t84937.html+&cd=42&hl=en&ct=clnk&gl=us>]

**Figure 32:** Underground actors royalsales and royalhost are discussed by user Damascus and associated with BTC address

Damascus	9.12.2014, 01:24
I think we can safely put the status .. Purse btc he gave svezheregnuty for translation. A total of 2 steps: first - my translation of his second - 10 minutes Btc brought my purse through 1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL, which definitely belongs to the exchanger, which is evident in its operations. And so, that we have at the moment? - I supposedly said he needed btc, and he immediately merged them in immediately after the exchanger (in this it was possible to stop) - As soon as received the money, told me that walked away for 15 minutes while he waited Translation is started and after 10 minutes, and poured the money was gone - there was an hour and began to lie, he allegedly had with the phone and can not send wmq, supposedly in an hour all will be - then took longer than 2 hours, but the online and has not appeared	

## 17WQov8BTXJAemWmqn5XJ8ibiq13SNoaqs – Nitrogen Sports attack

- Received 0.23856426 BTC (\$57.49) from 1MiZX8F4pSwLUVUdMtj6NftV8JFMDGKEvK on 2014-09-29 11:21:36 , transferred this amount to 1FewXEfn3EofLuYsk72dNpVVTVCK9R2ct and 1MfNu4wYtEUwZKhDpXQhsTjsJqyuGwa32p 9/29/2014 2014-09-29 15:20:59. Taint analysis reveals that the aforementioned BTC-e address **1FsVcdeHbpvUVT3gjeuVR2ZSDnpcsJMsLL** has sent BTC to 17WQov as well [<https://blockchain.info/taint/17WQov8BTXJAemWmqn5XJ8ibiq13SNoaqs>]. Tracing these transactions eventually leads to address 3Bgk1oHeomvu6bo4q6RKA6xoA8X8B342Y7, which may be some type of mixing service [<https://blockchain.info/address/3Bgk1oHeomvu6bo4q6RKA6xoA8X8B342Y7>] that is receiving large transactions and moving large amounts of BTC to 3Q5r9gVn1Trj5TVPT5nKs3tKmnDcS9tBe2 in an initial transaction of 584.18 BTC. The address 3Q5r9g may be a repository [<https://blockchain.info/address/3Q5r9gVn1Trj5TVPT5nKs3tKmnDcS9tBe2>]. It has received funds in chunks of 20 BTC over the course of 22 transactions since April 1, 2015 for a total received amount of

964.181 BTC. This appears to be the final resting place for the largest chunk of BTC transferred through, since there are no outbound transactions listed as of this writing. A cleaner table can be found at [<https://www.walletexplorer.com/address/3Q5r9gVn1Trj5TVPT5nKs3tKmnDcS9tBe2>].

### **1E8R3cgmr2UcusyZ9k5KUvkj3fXYd9oWW6** – Holytransaction.com attack

- Received 2 BTC from 1Gc7bVikEMUpc3EwsVMLPgZXuyrtU49TMQ on 2015-02-16 17:25:02. Sent 2 BTC to 14gKfdNEgwaGFDU1N9apMSoJybwas7vkY9 (0.5 BTC), 1C82PwHJJjknk2uFFkq7CVM1yngGEQtGFJ (0.9999 BTC) and 1Gv1TD2zCE3jn4V3RgMF5gEy8DLGQPEgdn (0.5 BTC)

**Figure 33:** BTC address 1E8R3cgmr2UcusyZ9k5KUvkj3fXYd9oWW6 associated with Holytransaction campaign

Transactions (Oldest First)		Filter
6175c80266ab14abff484a9b9f22f8fd1105e21b8c41d31da443443b6c91668		2015-02-16 17:39:00
1E8R3cgmr2UcusyZ9k5KUvkj3fXYd9oWW6	→ 14gKfdNEgwaGFDU1N9apMSoJybwas7vkY9 1C82PwHJJjknk2uFFkq7CVM1yngGEQtGFJ 1Gv1TD2zCE3jn4V3RgMF5gEy8DLGQPEgdn	0.5 BTC 0.9999 BTC 0.5 BTC -2 BTC
73b64746ba500b0989843baeb6b9b72f8d5384f5e27b98b7366bd60319714ebc		2015-02-16 17:25:02
1Gc7bVikEMUpc3EwsVMLPgZXuyrtU49TMQ	→ 1E8R3cgmr2UcusyZ9k5KUvkj3fXYd9oWW6	2 BTC

### **16JEzTkXGeCFPrCoPo9hnSVZWLHMau31fg** – coin-sweeper.com attack and nicehash.com attack.

### **15QMfpfymmkj1AtEy9uvqvpgsTfDuGzJF** – no transactions, address was never used.

### **17aLGgw8AwJdqBtMMG1QtQJgNQQkiyEsp** – attack on blisterpool.com [<https://bitcoin-forums.net/index.php?topic=838783.0>].

- This BTC address was also used in an extortion letter for mmppool.org [<https://bitcoin-forums.net/index.php?topic=559011.460>] and in an extortion letter to Bitalo [<https://bitcointalk.org/index.php?topic=845595.msg9446027#msg9446027>]
- Received \$169.64 in four transactions between Nov 3 and Nov 7, 2014.
- Received from 1M71DBAyowNrFu9FGoztRAvr7m1iwGAVLL \$157.99 on 2014-11-03

**Figure 34:** BTC address 17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp associated with Blisterpool and mmpool.org campaign

- 2014-11-07: Received from 1Lb2FnMpRsmVZwdV1rGt1ysXyQ2aeBjbKk \$11.65

**Figure 35:** BTC address 17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp associated with Blisterpool and mmpool.org campaign

- 2014-11-04: Transferred to 1BqWPELcAs6v4ZmEQ8LT9qoVJ8kGkXFEC (0.076 BTC) and 1JiPSN2BqxwoWvucU7cpQ7tRywBiAqm65Y (0.6018 BTC)

**Figure 36:** BTC address 17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp associated with Blisterpool and mmpool.org campaign**Figure 37:** 2014-11-07: Transferred to 1CoWRoiSixSGxLfiPe5QcLT7kddV26jZ8w (0.049 BTC) associated with Blisterpool and mmpool.org campaign

**132EdUarcghK2barhkxgaKQ2XqnchPbWSB** - mpex.co attack.

- 12/4/2014 10:35:13 PM (UTC) 1HoKWoK7X7cGJkWNgzvjRM1G7H3pvNmE9 paid 0.0217 BTC

**Figure 38:** BTC address 132EdUarcghK2barhxgaKQ2XqnchPbWSB associated with mpex.co campaign

fde70f43c190a02440e3d4d7f71881bca0d6f24e13724ebe382d03236aa4c487	2014-12-04 22:32:29
1HoKWoK7X7cGJkWNgjvjRM1G7H3pvNmE9	132EdUarcghK2barhxgaKQ2XqnchPbWSB
	0.0217 BTC

- 12/4/2014 22:33:03 **132EdUarcghK2barhxgaKQ2XqnchPbWSB** paid 0.0216 BTC to 1KzKw6ssAF1THNJHCED5XASnyupELbcrxM

**Figure 39:** BTC address 132EdUarcghK2barhxgaKQ2XqnchPbWSB associated with mpex.co campaign

416f15e1b56e326f1eb3e290f76108a691b1338fd71f17bd157cac06a83d9c6	2014-12-04 22:33:03
132EdUarcghK2barhxgaKQ2XqnchPbWSB	1KzKw6ssAF1THNJHCED5XASnyupELbcrxM
	0.0216 BTC

- A randomly selected sample of **132EdUarcghK2barhxgaKQ2XqnchPbWSB** transactions reveals numerous transfers to other BTC addresses until the transactions reach the address 16yzpVa3eR7xdXni1PGAW55X92HBkodZda and a SatoshiBONES (BTC based dice game) Hot Wallet address of 1bonesbTK2GjYasv5yzGPFCMAaQHup4vk. The 16yzp address was used to send BTC to the same SatoshiBONES Hot Wallet.

**Figure 40:** Transaction linked to DD4BC address involving BTC gambling

9a5a42f3f24a25b409aff30ff93c1acb81630d9775d738aed2f1ac5329894cdf	2014-12-04 23:22:44
15yTh12V4YY5Y6YbCetTKad9jbdnntsHUpb	16yzpVa3eR7xdXni1PGAW55X92HBkodZda 1bonesbTK2GjYas... (SatoshiBONES 0.09766pct)
	0.0196 BTC 0.001 BTC -0.0207 BTC

- This SatoshiBONES Hot Wallet was used in the December 2014 bet for a number less than 64, a category that includes a high payout (767.995 multiplier, and a low minimum bid of 0.001 BTC).

**Figure 41:** BTC gambling site that received funds from account associated with DD4BC through a transaction series



- At some point in the transaction chain, it is likely that the criminal, or the person who received the funds, is using a wallet compatible with the Satoshi Bones game, a list that is available at [<http://bitzillions.com/satoshibones/compatible>].
  - The list of compatible wallets includes Bitcoin-Qt/bitcoind (client), Electrum (client/server), Armory (client, Bitcoin client dependency), BitcoinJ (Client), MultiBit (Simplified payment verification/SPV client), Blockchain.info (Hybrid EWallet), Blockchain App for Android, iOS (Mobile app hybrid client), Strongcoin (Hybrid EWallet), BitcoinSpinner for Android (Client/server) and Bitcoin Wallet for Android (Simplified payment verification/SPV client).
  - The list of incompatible wallets [<http://bitzillions.com/satoshibones/incompatible>] includes Coinbase, Bitstamp, Instawallet, Mixing services, Other betting games, and Investment schemes.
- **8NeYaX6GCnibNkwyuGhGLuU2tYzbhvW7z** (online casino, name removed) - zero transactions
- **1NbhLM43duL2J2tBX2qQWBojEm5fNSoMEp** (slottyvegas and betatcasino.com) – zero transactions
- **12m5WBiRAm1Te4uj6tdcuVbmRA5h1P1Du5** – financial institution – zero transactions
- **1KU3TFMNxmE5UTMsjBmep34K6QJtJNJ6wD** – several financial institutions in Iceland
- **198QaeuJ6oMeuan2p5gyDx75odweMWzNXH** – unnamed victim – zero transactions

ASERT Threat Intelligence is interested in collecting any additional BTC addresses used in extortion campaigns that do not appear in this document.

## Examples of Extortion Mail

The volume of extortion mail has been high enough that some wise operational security teams have implemented mail monitoring rules to look for the usual array of wording in these messages as to provide timely situational awareness. In some cases, employees may delete such a message without notifying security teams that may not understand the context when they are then the victims of an unexpected DDoS attack. Robust situational awareness helps increase context and therefore preparedness before painful downtime leads to loss of revenue.

### Example 1 – Targeting an online casino

**From:** DD4BC Team [mailto:[dd4bct@gmail.com](mailto:dd4bct@gmail.com)]  
**Sent:** 10 April 2015 02:07 PM  
**To:** <REMOVED BY ASERT>  
**Subject:** Re: DDOS ATTACK!

Hitting [pokerstars.com](http://pokerstars.com) at the moment.  
 Good luck if you think you can stop what they can't.  
 But you still have time.

On Thu, Apr 9, 2015 at 3:46 PM, DD4BC Team <[dd4bct@gmail.com](mailto:dd4bct@gmail.com)> wrote:  
 Hello,

To introduce ourselves first:

<https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html>

<http://bitcoinbountyhunter.com/bitalo.html>

<http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info>

Or just google "DD4BC" and you will find more info.

Recently, we were DDoS-ing Neteller. You probably know it already.

So, it's your turn!

<site> is going under attack unless you pay 20 Bitcoin.

Pay to 18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother.

Right now we are running small demonstrative attack on your server.  
 Don't worry, it will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have 20 BTC at the moment, so we are giving you 48 hours to get it and pay us.

We do not know your exact location, so it's hard to recommend any Bitcoin exchanger, so use Google. Current price of 1 BTC is about 250 USD.

**IMPORTANT:** You don't even have to reply. Just pay 20 BTC to 18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z – we will know it's you and you will never hear from us again.

We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated. If you need to contact us, feel free to use some free email service.

But if you ignore us, and don't pay within 48 hours, long term attack will start, price to stop will go to 50 BTC and will keep increasing for every hour of attack.

**ONE MORE TIME:** It's a one-time payment. Pay and you will not hear from us ever again!

### **Example 2: Generic message [<http://pastebin.com/5KTqJztB>]**

Hello,

To introduce ourselves first:

<https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html>

<http://bitcoinbountyhunter.com/bitalo.html>

<http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info>

Or just google "DD4BC" and you will find more info.

So, it's your turn!

Your sites are going under attack unless you pay 15 Bitcoin.

Pay to 15QMfpfyymmkgj1AtEy9uvqvpgsTfDuGzJF

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother. Or at least not with cheap protection like CloudFlare – it will not help at all, but we will instantly crash your site and increase the price.

Right now we are running small demonstrative attack.  
Don't worry, it will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have 15 BTC at the moment, so we are giving you 24 hours to get it and pay us.

Find the best exchanger for you on <http://howtobuybitcoins.info>  
You can pay directly through exchanger to our BTC address, you don't even need to have BTC wallet.

Current price of 1 BTC is about 230 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

**IMPORTANT:** You don't even have to reply. Just pay 15 BTC to 15QMfpfymmkgj1AtEy9uvqvpqgsTfDuGzJF – we will know it's you and you will never hear from us again.

We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated. If you need to contact us, feel free to use some free email service. Or contact us via Bitmessage: BM-NC1jRewNdHxX3jHrufjxDsRWXGdNisY5

But if you ignore us, and don't pay within 24 hours, long term attack will start, price to stop will go to 30 BTC and will keep increasing for every hour of attack.

**IMPORTANT:** It's a one-time payment. Pay and you will not hear from us ever again!

We do bad things, but we keep our word.

Thank you.

### **Example 3: Attack on Holytransaction**

```
Received: from mxback1o.mail.yandex.net ([127.0.0.1])
    by mxback1o.mail.yandex.net with LMTP id sP4giQdm
    for <francesco@noveltylab.com>; Sun, 15 Feb 2015 15:34:34 +0300
Received: from forward3o.mail.yandex.net (forward3o.mail.yandex.net [37.140.190.32])
    by mxback1o.mail.yandex.net (nwsmtplib/Yandex) with ESMTP id vb88BeHrHw-YYm8iDNN;
    Sun, 15 Feb 2015 15:34:34 +0300
X-Yandex-Front: mxback1o.mail.yandex.net
X-Yandex-TimeMark: 1424003674
X-Yandex-Spam: 1
Received: from mxfront8o.mail.yandex.net (mxfront8o.mail.yandex.net [37.140.190.12])
    by forward3o.mail.yandex.net (Yandex) with ESMTP id 336D446818E2
    for <francesco@noveltylab.com>; Sun, 15 Feb 2015 15:34:34 +0300 (MSK)
```

```

Received: from mxfront8o.mail.yandex.net ([127.0.0.1])
    by mxfront8o.mail.yandex.net with LMTP id My9kOXKd;
    Sun, 15 Feb 2015 15:34:32 +0300
Received: from www.safe-mail.net (www.safe-mail.net [212.29.227.230])
    by mxfront8o.mail.yandex.net (nwsmtplib/Yandex) with ESMTPS id qTsey5a6uI-YVtaL3au;
    Sun, 15 Feb 2015 15:34:31 +0300
    (using TLSv1 with cipher AES256-SHA (256/256 bits))
    (Client certificate not present)
Authentication-Results: mxfront8o.mail.yandex.net; spf=pass (mxfront8o.mail.yandex.net: domain of
Safe-mail.net designates 212.29.227.230 as permitted sender) smtp.mail=dd4bc@Safe-mail.net
Received: by tapuz.safe-mail.net with Safe-mail (Exim 4.63)
    (envelope-from <dd4bc@Safe-mail.net>)
    id 1YMyP6-00080A-HX; Sun, 15 Feb 2015 07:34:28 -0500
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofw;
    s=N1-0105; d=Safe-mail.net;
    b=La+UKjT7/nH2Ab8Avv46nsIDfogedbybzHtyz1KPTqkwfi+AxmcV8McDupKM5zaX6
    NAdzXVAhzrxeitZswZNpTmMTy18uyJrlgonOTsY7ejwZQ5Ro7TGxQ1bsB0iRc9Vc
    RtwWaTpKb07tlDuNVGmWDDTjZhRGZl3rs62ewZFT09I=;
Received: from pc ([5.149.250.53]) by Safe-mail.net with https
Subject: DDOS ATTACK!
Date: Sun, 15 Feb 2015 12:34:28 +0000
From: "DD4BC Team" <dd4bc@Safe-mail.net>
To: support@holytransaction.com, admin@holytransaction.com, webmaster@holytransaction.com
CC: contact@noveltylab.com, andrey@noveltylab.com
X-SMType: Regular
X-SMRef: N1-tGUXt_r_px
Message-ID: <N1-tGUXt_r_px@Safe-mail.net>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-SMSignature: PFBB0JO90+zZxKD6X7VvQH+Aa/LZvu26Jhb6umQtzzqauUCIu+6FpM43qU6wZpVt
    bCWEV429c5frPXGSyMTuG7f1pqVx4fgt7sfJgkM78X+R4212HRpNXX0iwjqSBBLG
    5lahqqIGsBk97AFchutJYQZJElaOn9EI9nQOseM1h0=
X-Yandex-Forward: a2248a66577f514e9e4344383293bf4f
X-Yandex-Forward: 1ead9c3167a0c8e31703bffb04c820d9
X-Yandex-Forward: 06f0ea25a70affc3af5f029335033671
X-Yandex-Forward: c519b137cc93bac9021526ee62354407
Return-Path: contact@noveltylab.com
X-Yandex-Forward: 3f4450736ec7fd9a924515bf049e1b90
X-Yandex-Filter: 2090000000002889126

```

Hello,

Your site is extremely vulnerable to DDoS attacks.

I want to offer you info how to properly setup your protection, so that you can't be ddosed.

If you want info on fixing it, pay me 1.5 BTC to 1E8R3cggnr2Ucusyz9k5KUvkj3fxYd9oWW6

**Example 4: Attack temporarily stopped**

```

Received: from mxback10h.mail.yandex.net ([127.0.0.1])
    by mxback10h.mail.yandex.net with LMTP id hZA4o5yh
    for <francesco@noveltylab.com>; Sun, 15 Feb 2015 20:42:35 +0300
Received: from forward2h.mail.yandex.net (forward2h.mail.yandex.net [84.201.187.147])
    by mxback10h.mail.yandex.net (nwsmt/ Yandex) with ESMTP id zmnJCtme3t-gZV8An0Y;
    Sun, 15 Feb 2015 20:42:35 +0300
X-Yandex-Front: mxback10h.mail.yandex.net
X-Yandex-TimeMark: 1424022155
X-Yandex-Spam: 1
Received: from mxfront7h.mail.yandex.net (mxfront7h.mail.yandex.net [84.201.186.11])
    by forward2h.mail.yandex.net (Yandex) with ESMTP id 8AE907011A5
    for <francesco@noveltylab.com>; Sun, 15 Feb 2015 20:42:35 +0300 (MSK)
Received: from mxfront7h.mail.yandex.net ([127.0.0.1])
    by mxfront7h.mail.yandex.net with LMTP id Y4zpR2jt;
    Sun, 15 Feb 2015 20:42:34 +0300
Received: from www.safe-mail.net (www.safe-mail.net [212.29.227.230])
    by mxfront7h.mail.yandex.net (nwsmt/ Yandex) with ESMTPS id ew3lf1WEgd-gXXGJWpE;
    Sun, 15 Feb 2015 20:42:33 +0300
    (using TLSv1 with cipher AES256-SHA (256/256 bits))
    (Client certificate not present)
Authentication-Results: mxfront7h.mail.yandex.net; spf=fail (mxfront7h.mail.yandex.net: domain of
Safe-mail.net does not designate 212.29.227.230 as permitted sender) smtp.mail=dd4bc@Safe-mail.net
Received: by tapuz.safe-mail.net with Safe-mail (Exim 4.63)
    (envelope-from <dd4bc@Safe-mail.net>)
    id 1YN3DD-0005Us-R9; Sun, 15 Feb 2015 12:42:31 -0500
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws;
    s=N1-0105; d=Safe-mail.net;
    b=DbSYiNzZa+fn/4HHPHj5YyLfQnLs1uFiXmSkKQqWf1ke9L0loLcplg7Pt7Kzvrom
    9Hsn7nB3Yo6IHpfkObu7HSXjmT7V7YP1OIUZbDzGLmpxjVZhcBCV7FRstuyP+iYR
    I81lns5+I11EP/bNnV8nOwrxCktcyW5QJcSDICGcCy4=;
Received: from pc ([5.149.250.53]) by Safe-mail.net with https
Subject: Re: DDOS ATTACK!
Date: Sun, 15 Feb 2015 17:42:31 +0000
From: "DD4BC Team" <dd4bc@Safe-mail.net>
To: support@holytransaction.com, admin@holytransaction.com, webmaster@holytransaction.com
CC: contact@noveltylab.com, andrey@noveltylab.com
X-SMType: Regular
X-SMRef: N1-k-aoA4Bpyi
Message-Id: <N1-k-aoA4Bpyi@Safe-mail.net>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-SMSignature: UoLdia4npzhTAJu/ytxW1S1Q1Cg2HykmNsSQKqOtQTX61DB6iG0p/auR8CdgDxp
    yyE3Yuht+pwV+vXFL9w1Pys/xXCg/SfrPChVfW6YySB1gUQBndLz1ca2RxQzeUcB
    YsIw6YdiulCp0yvoTa/a4YlG0WFfSh8YL3BJuOI1sLg=
X-Yandex-Forward: a2248a66577f514e9e4344383293bf4f
X-Yandex-Forward: 1ead9c3167a0c8e31703bffb04c820d9

```

X-Yandex-Forward: 06f0ea25a70affc3af5f029335033671  
 X-Yandex-Forward: c519b137cc93bac9021526ee62354407  
 Return-Path: contact@noveltylab.com  
 X-Yandex-Forward: 3f4450736ec7fdda924515bf049e1b90  
 X-Yandex-Filter: 2090000000002889126

btw. Attack temporarily stopped.

If payment not received within 6 hours, attack restarts and price will double up.

----- Original Message -----

**From:** "DD4BC Team" <dd4bc@Safe-mail.net>  
**To:** support@holytransaction.com, admin@holytransaction.com, webmaster@holytransaction.com  
**Cc:** contact@noveltylab.com, andrey@noveltylab.com  
**Subject:** DDOS ATTACK!  
**Date:** Sun, 15 Feb 2015 12:34:28 +0000

Hello,

Your site is extremely vulnerable to DDoS attacks.

I want to offer you info how to properly setup your protection, so that you can't be ddosed.

If you want info on fixing it, pay me 1.5 BTC to 1E8R3cggnr2Ucusyz9k5KUvkj3fXYd9oWW6

### Example 5: Threat of increasing extortion

```
Received: from mxback8m.mail.yandex.net ([127.0.0.1])
    by mxback8m.mail.yandex.net with LMTP id ieBgk4QX
    for <francesco@noveltylab.com>; Mon, 16 Feb 2015 17:14:03 +0300
Received: from forward5m.mail.yandex.net (forward5m.mail.yandex.net [37.140.138.5])
    by mxback8m.mail.yandex.net (nwsmtplib/Yandex) with ESMTP id zbvYgUDKqI-E2l400de;
    Mon, 16 Feb 2015 17:14:02 +0300
X-Yandex-Front: mxback8m.mail.yandex.net
X-Yandex-TimeMark: 1424096042
X-Yandex-Spam: 1
Received: from mxfront5m.mail.yandex.net (mxfront5m.mail.yandex.net [37.140.138.55])
    by forward5m.mail.yandex.net (Yandex) with ESMTP id 4F33629A09F8
    for <francesco@noveltylab.com>; Mon, 16 Feb 2015 17:13:50 +0300 (MSK)
Received: from mxfront5m.mail.yandex.net ([127.0.0.1])
    by mxfront5m.mail.yandex.net with LMTP id xAkYEmSh;
    Mon, 16 Feb 2015 17:13:49 +0300
Received: from www.safe-mail.net (www.safe-mail.net [212.29.227.230])
    by mxfront5m.mail.yandex.net (nwsmtplib/Yandex) with ESMTPS id DrviR47bbY-DmquWYNY;
    Mon, 16 Feb 2015 17:13:48 +0300
    (using TLSv1 with cipher AES256-SHA (256/256 bits))
    (Client certificate not present)
Authentication-Results: mxfront5m.mail.yandex.net; spf=pass (mxfront5m.mail.yandex.net: domain of
Safe-mail.net designates 212.29.227.230 as permitted sender) smtp.mail=dd4bc@Safe-mail.net
Received: by tapuz.safe-mail.net with Safe-mail (Exim 4.63)
    (envelope-from <dd4bc@Safe-mail.net>)
```

id 1YNM0e-0000tC-FT; Mon, 16 Feb 2015 09:13:40 -0500  
 DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws;  
     s=N1-0105; d=Safe-mail.net;  
     b=djr4T1MZtv8t//I4PJkAFdP03peQhkK4BBUImL4UtkaiSwXa88dh6jTyO50S051t  
     7miI5y4epCOHv9ksSMruLLys9m9Qf+rewKJjo9VwTH8/T5u/K0DEwNysBJGKm5a  
     x1lR9HfiaFY2i6GFWi101zbIzbbqx8+KG571Y9OcbM8=;  
 Received: from pc ([5.149.250.53]) by Safe-mail.net with https  
 Subject: Re: DDOS ATTACK!  
 Date: Mon, 16 Feb 2015 14:13:40 +0000  
 From: "DD4BC Team" <dd4bc@Safe-mail.net>  
 To: support@holytransaction.com, admin@holytransaction.com, webmaster@holytransaction.com  
 CC: contact@noveltylab.com, andrey@noveltylab.com  
 X-SMType: Regular  
 X-SMRef: N1-wpQ47UW3DF  
 Message-ID: <N1-wpQ47UW3DF@Safe-mail.net>  
 MIME-Version: 1.0  
 Content-Type: text/plain; charset=us-ascii  
 Content-Transfer-Encoding: 7bit  
 X-SMSignature: tYr6sEhTEOWzxSRh8GqAKnUBFd6isT1/ripsybiHMf3Tm/CPcys1VmaNfxxaFXm  
     zLq6U/mFHiuVotFsQh7o0rDEGyw0sejX+0tczA0+5v2QE8mBNjVl3+fGrCZFwUtm  
     Vp4CJ71apVbROUqK7x5xvBtZmcQWUQz91h3L9d+4v8M=  
 X-Yandex-Forward: a2248a66577f514e9e4344383293bf4f  
 X-Yandex-Forward: 1ead9c3167a0c8e31703bff04c820d9  
 X-Yandex-Forward: 06f0ea25a70affc3af5f029335033671  
 X-Yandex-Forward: c519b137cc93bac9021526ee62354407  
 Return-Path: contact@noveltylab.com  
 X-Yandex-Forward: 3f4450736ec7fdda924515bf049e1b90  
 X-Yandex-Filter: 2090000000002889126

Return site back online without paying me first, it's going down again (protection will not help) and price to stop it increases to 3 BTC. And will keep doubling for every day of attack.

----- Original Message -----

From: "DD4BC Team" <dd4bc@Safe-mail.net>  
 To: support@holytransaction.com, admin@holytransaction.com, webmaster@holytransaction.com  
 Cc: contact@noveltylab.com, andrey@noveltylab.com  
 Subject: DDOS ATTACK!  
 Date: Sun, 15 Feb 2015 12:34:28 +0000

Hello,

Your site is extremely vulnerable to DDoS attacks.

I want to offer you info how to properly setup your protection, so that you can't be ddosed.

If you want info on fixing it, pay me 1.5 BTC to 1E8R3cgmr2Ucusyz9k5KUvkj3fXYd9oWW6

## Example 6:

From: DD4BC Team [mailto:[dd4bcteam@keemail.me](mailto:dd4bcteam@keemail.me)]  
Sent: 21. mai 2015 15:23  
To:  
Subject: DDOS ATTACK!

Hello,

To introduce ourselves first:

hXXp://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks

hXXp://bitcoinbountyhunter.com/bitalo.html

hXXp://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info

Or just google "DD4BC" and you will find more info.

So, it's your turn!

Your sites are going under attack unless you pay 25 Bitcoin.

Pay to 1KU3TFMNxmE5UTMsjBmep34K6QJtJNJ6wD

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother. Or at least not with cheap protection like CloudFlare or Incapsula...but you can try. :)

Right now we are running small demonstrative attack on one of your IPs - <REMOVED> Don't worry, it will not be hard and will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have 25 BTC at the moment, so we are giving you 24 hours to get it and pay us.

Find the best exchanger for you on hXXp://howtobuybitcoins.info or hXXp://localbitcoins.com You can pay directly through exchanger to our BTC address, you don't even need to have BTC wallet.

Current price of 1 BTC is about 230 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

**IMPORTANT:** You don't even have to reply. Just pay 25 BTC to 1KU3TFMNxmE5UTMsjBmep34K6QJtJNJ6wD – we will know it's you and you will never hear from us again.

We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated.

If you need to contact us, feel free to use some free email service. Or contact us via Bitmessage: BM-NC1jRewNdHxX3jHrufjxDsRWXGdNisY5

But if you ignore us, and don't pay within 24 hours, long term attack will start, price to stop will go to 50 BTC and will keep increasing for every hour of attack.

**IMPORTANT:** It's a one-time payment. Pay and you will not hear from us ever again!

We do bad things, but we keep our word.

## Areas for Future Research and Investigation

### Threat Actors Use of Perfect-Privacy.org / secure-mail.cc and/or secure-mail.biz

The threat actor joining the IRC channel of an extorted target in November 2014 used an IP address 176.10.116.169 (listed as a tor node), which also associates itself with the perfect-privacy.org VPN service [<https://www.robtex.com/en/advisory/ip/176/10/116/169/>].

The three extortion letters for holytransaction.com (Feb 15 and 16, 2015) appeared to originate from an IP address 5.149.250.53.

Received: from pc ([5.149.250.53]) by Safe-mail.net with https

This IP address is associated with an array of perfect-privacy.org (VPN provider), secure-mail.cc and secure-mail.biz sites, but has also been historically associated with the server ns1.clickicexmlfeed[.]com. This domain, when pasted into a browser window, results in a series of redirects that leads a user (at least on OSX) to a popup message that Flash Player is out of date. This is a very typical malware delivery tactic. The IP address has been associated with various types of malicious activity in the past however, therefore actual correlation with specific threat actors is unlikely.



The chain of activity leading to the above message started with ns1.clickicexmlfeed.com, which apparently redirected to [http://ww9.clickicexmlfeed\[.\]com/](http://ww9.clickicexmlfeed[.]com/), which bounced the connection to some type of redirector system, which then displayed various types of messages (take a survey, download a mac cleanup program, flash update).

The link for the Flash update program is

[http://checksoft.how2safeupdate\[.\]org/?pcl=9t20A908UewesRb6CGyj7YVBoZ44Pc25dumgPuPFhXk.&cid=DV338cf932f36911e4b1a70a92e2e1261797f1ad784b05&v\\_id=7VdJpiSOfsIDvl-NKvWYccJ1Zk5ZT3dOKVxJ1HkI8\\_A](http://checksoft.how2safeupdate[.]org/?pcl=9t20A908UewesRb6CGyj7YVBoZ44Pc25dumgPuPFhXk.&cid=DV338cf932f36911e4b1a70a92e2e1261797f1ad784b05&v_id=7VdJpiSOfsIDvl-NKvWYccJ1Zk5ZT3dOKVxJ1HkI8_A).

This appears to be a shady redirector service.

Clickice itself has been written about in the past [<http://www.spider.io/blog/2013/12/cyber-criminals-defraud-display-advertisers-with-tdss/>] in conjunction with the TDSS clickfraud malware. Links to the DD4BC group are extremely tenuous however; this IP address appears to be part of infrastructure used by numerous criminal actors for various services, based on its presence in the Spamhaus XBL, SBL, and abuseat.org CBL. Additionally, a tor node has been observed on this IP address, making any attempts at attribution extremely difficult.

**Table 1:** Resolutions for IP address 5.149.250.53

ns3.perfect-privacy.com	ns.secure-mail.biz	ns.perfect-privacy.com
ns3.secure-mail.biz	ns1.perfect-privacy.com	ns4.perfect-privacy.com
ns1.secure-mail.biz	ns2.perfect-privacy.com	ns3.perfect-privacy.com
ns4.perfect-privacy.com	ns2.secure-mail.biz	ns2.perfect-privacy.com
ns1.perfect-privacy.com	ns1.clickicexmlfeed.com	

### Forensics Analysis on Compromised Infrastructure

As DD4BC leverages network infrastructure for attack, there may be logs or other meaningful indicators that can be extracted for research and investigation purposes. Organizations that have unwittingly engaged in these DDoS attacks have an opportunity to provide insight to law enforcement and researchers who are working to attribute and bring DD4BC to justice. In the case of layer 7 attacks, there may be logs of value that can reveal further insight into the attackers infrastructure. Unfortunately, in the case of the voluminous SSDP, NTP and other reflection/amplification attacks, logs aren't going to be as useful due to the spoofed address techniques in use by the attacker(s) and whatever services are being leveraged.

### Attribution Research

Attribution is sometimes a very helpful process to help locate miscreants and bring them to justice. In other cases, the attention of being identified is enough to cause an attacker to modify their behavior. Professional criminals aren't as likely to change their ways however, and won't be scared off as easily. Although we cannot be absolutely certain of this assessment, we believe that DD4BC is one person. The volume of attacks, frequency of attacks, the lack of follow through in several cases, and the fact that the earlier extortion mails tend to be written in first-person singular are all factors in this assessment. Later extortion mails used the phrasing "we", perhaps in an attempt to overstate the threat and therefore increase extortion payments by positioning the threat actor as part of a group, however the continually observed TTPs still suggest a singular threat actor at play.

[Dd4bcteam@gmail.com](mailto:Dd4bcteam@gmail.com) (owner name: "Dd Bcteam"  
[\[http://www.emailsherlock.com/emailsearch/dd4bcteam@gmail.com/\]](http://www.emailsherlock.com/emailsearch/dd4bcteam@gmail.com/))

[Dd4bc@outlook.com \[http://www.emailsherlock.com/emailsearch/dd4bc@outlook.com/\]](http://www.emailsherlock.com/emailsearch/dd4bc@outlook.com/) reveals a Guy Fawkes mask as associated with the e-mail address.

Fullcontact

Fullscreen

Logout

Fullname: DD4BC Team

Twitter: <https://twitter.com/dd4bc>

Twitterimage:

Klout: <http://klout.com/dd4bc>

The klout site reveals the text “Erasmus of Rotterdam”

Erasmus of Rotterdam

11

Twitter

Sign in to view what Erasmus of Rotterdam has been up to on their social channels!

The twitter link [twitter.com/dd4bc] only reveals one tweet, related to a raid of Neteller. Neteller was a victim of DD4BC.

[Tweets & replies](#) [Photos & videos](#)

 **Erasmus of Rotterdam** @dd4bc · Apr 2  
@NETELLER

UK Police raid popular online payment processor Neteller for money laundering charges.



[View more photos and videos](#)

1 1

While there may be no direct connection between the user “ambiorx” who allegedly compromised one of the bitcoin sites and stole all bitcoins, and the DD4BC threat actor(s), the association between the DDoS attack and the apparently opportunistic currently compromise may be worthy of further investigation.

[<https://www.snip2code.com/Snippet/353351/excoin+&cd=2&hl=en&ct=clnk&gl=us>] includes a variety of data about the Ambiorx user, gathered from the excoin staff. This message is reproduced here:

#### “WHAT HAPPENED?

The purpose of this document is to help us better understand who was behind the coordinated attacks on Excoin in January and February 2015. We have reason to believe this person/group still poses a threat to the Blackcoin community as a whole and we wish to prevent such attacks in the future. I will reference a lot of different material to help us infer who might be responsible. These documents are attached or linked to in the post. Please comment if you find certain elements to be misleading or if you wish to state additional information. The text will be edited accordingly. I will hand over control of this document to a community leader who wishes to handle the investigation.

Every detail mentioned here must be independently verified by the community so we can move forward in an orderly manner. I do not wish to play the role of moderator in this discussion. We are asking for the community to fill in the blanks and help us in locating those responsible.

#### **Relevant documents:**

- login-times-ambiorx.txt

This document contains timestamps (UTC) from our server when ambiorx logged onto exco.in

- zeded-excoin-irc-log.txt

- syllabear-excoin-irc-log.txt

Provided to us by freenode user Zeded is a log that goes back to December (many thanks! I banned him at the end of the log by accident, sorry!) The timezone used is unclear but likely to be easily determined with help from the second log.

Syllabear has a more detailed log (thank you for your help, as well) in the AEST timezone and this goes back to January 19th.

- blackcoin-irc-log.txt

This channel log was provided to me by #Blackcoin chanop Seopkip via Gritt-N-Auld. Thank you both. This log goes back to March 2014.

- insite-chat-logs.txt

These are logs from the web chat I found archived on Google, from January 24 to Feb 09. I will inquire if obtaining a full log from the server is a possibility.

Also referenced:

- <http://otc.evilbs.com/>

This site archives IRC nicks and IPs on relevant channels, useful for connecting shared accounts.

### **Basic facts:**

Username: ambiorx

Email: exco@comtecservices.be (feel free to write them a lovely message)

IP Addresses used on Excoin:

141.101.105.65

141.134.108.38

62.210.170.27

171.25.193.20

194.150.168.95

82.116.120.3

### **Identified DDOS IP Addresses:**

104.131.204.15

104.131.213.10

104.154.38.52

107.170.150.138

130.211.185.192

146.148.40.57

172.245.55.112

184.172.15.235

50.97.173.18

5.255.253.51

66.249.69.136

66.249.69.88

66.249.75.104

66.249.75.184

66.249.75.216

66.249.75.88

66.249.79.111

66.249.79.119

66.249.79.127

66.249.79.135

66.249.79.4

66.249.79.95

### **IRC Records:**

ambiorx (8d866c26@gateway/web/freenode/ip.141.134.108.38)

The first recorded data we have of ambiorx begins on January 14th with account creation on server.

IP: 141.134.108.38

Wed, 14 Jan 2015 22:40:59 UTC +00:00

Their first IRC presence begins ten days later on January 24th..

Saturday, January 24th, 2015 ~ 9:09 AM

5:49 PM <ambiorx> Hello

5:50 PM <ambiorx> someone from excoin here?

5:50 PM <ambiorx> support?

Their first webchat presence begins (as far as our logs can tell) on February 1st

ambiorx 2015-02-01 04:07:45 UTC admin here?

ambiorx 2015-02-01 04:08:56 UTC got a deposit that's not credited to my Excoin balance...

ambiorx 2015-02-01 04:17:06 UTC And just created a ticket FYI

Starting with logs in December you will notice anonymous connections from tor, with nicks lurking in our channel. Normally this is not cause for suspicion but the pattern of these handles are troubling, and they permanently parted from the channel once ambiorx completed their attack.

The suspected handles:

coxbird, arrakian, scytale, facedancer

SyllaBear's #Excon log,

January 21 (note the times)

08:51 |-] arrakian [~arrakian@gateway/tor-sasl/arrakian] has quit [Write error: Connection reset by peer]

08:51 |-] scytale [~scytale@gateway/tor-sasl/scytale] has quit [Read error: Connection reset by peer]

23rd

00:34 |-] facedancer [~arrakian@gateway/tor-sasl/arrakian] has joined #excoin

00:35 |-] arrakian [~arrakian@gateway/tor-sasl/arrakian] has quit [Ping timeout: 250 seconds]

00:35 |-] scytale [~scytale@gateway/tor-sasl/scytale] has quit [Ping timeout: 250 seconds]

4th (Gritt and Syllabear were edited out of this excerpt)

09:31 |-] ambiorx [8d866c26@gateway/web/freenode/ip.141.134.108.38] has joined #excoin

09:31 < ambiorx> Excoin is offline?!

09:32 < ambiorx> blackwavelabs as well

09:34 < ambiorx> arturo you know more about this?

09:34 |-] arrakian [~arrakian@gateway/tor-sasl/arrakian] has joined #excoin

Last sign of ambiorx – Feb 8th

12:08 |-] ambiorx [8d866c26@gateway/web/freenode/ip.141.134.108.38] has quit [Client Quit]

12:08 |-] arrakian [~arrakian@gateway/tor-sasl/arrakian] has quit [Quit: Leaving]

### The tor connection

What is the significance of these sign in/out? It seems likely that these were nicks designed to monitor rooms and keep their own personal logs. These handles were not just in #excoin, but also #blackcoin and can be found lurking in other crypto channels such as #viacoin, #stellar, #cann.

Ambiorx makes no appearance in #blackcoin but arrakian's name appears in the channel over 2,000 times. Unless I missed something, they have never said a word except to collect rain. Same for scytale though their name appears less, ~700 times. Many of these nicks/bots use names that originate from the novel and film, Dune.

The #blackcoin log mentions on Nov. 27th: [20:40] \* arrakian is now known as hayt  
[otc.evilbs.com](http://otc.evilbs.com/?hayt&tz=America/Los_Angeles&l=100) links hayt with jacarutu: [http://otc.evilbs.com/?hayt&tz=America/Los\\_Angeles&l=100](http://otc.evilbs.com/?hayt&tz=America/Los_Angeles&l=100)  
 Jacarutu shares a name with this blackcoin twitter: <https://twitter.com/jacarutu> (NOT CONFIRMED)  
 Many of those handles also trace back to a 'milbot' – which was created by Sevith: <https://twitter.com/xSevithx> (NOT CONFIRMED)

I have compiled a list of suspicious nicks that I have linked with otc.evilbs.com and our DDOS IPs. I apologize if a few of these are incorrect and I encourage you to prove me wrong:

muddo  
 bloodshoteyes  
 finiternity  
 Valexus  
 whywefight  
 rake\_boss  
 Valexus  
 koreandog  
 cryptovexed  
 marc\_ffmz  
 AstralF0x  
 shovel\_boss  
 lenar  
 mortale  
 \_wewincoins-com  
 PCFiL  
 Wenter  
 perrier  
 Argamas  
 vlurk  
 kalisto  
 yescrypto

### Traces of Ambiorx

So what happens when you search for Ambiorx? Well, it's a misspelling of a Belgian leader for one. And the main IP originates from Belgium so that may be a nice red herring or laziness. The e-mail address they used was a very selective one. I can find no useful information on that domain.

Sites where ambiorx has appeared recently:

<http://otc.evilbs.com/?Ambiorx>  
<https://xrptalk.org/topic/4271-cryptsy-not-accounting-for-lost-xrp/>  
<https://bitcointa.lk/threads/ann-pmtocoins-com-new-exchange-trading-helixcoin.252816/page-11>  
<http://myr.nonce-pool.com/index.php?page=statistics&action=blocks&height=113214&prev=1>  
<https://www2.coinmine.pl/drk/index.php?page=statistics&action=blocks&height=23406&next=1>  
<http://steamcommunity.com/profiles/76561197997458320> (NOT CONFIRMED)

This includes a full name and city. I stress this may not be related.

<http://www.swtor.com/community/member.php?u=356263> (NOT CONFIRMED)

You must be registered to view the details of this. It's from 2012. A place of work is mentioned but this account is not confirmed to be related yet. An excerpt:

"About Ambiorx  
Biography  
I'm a social guy who likes to play mmorpg's, my first was Start Wars Galaxies (still miss)  
Location  
near Antwerp, Belgium  
Interests  
Star Wars, scuba diving, Motogg and last but not least: my wife and kids!!  
Occupation ---removed until confirmation---"

### **Where we go from here?**

We have a list of IPs, suspicious nicks, and a possible lead in Belgium but otherwise very little is known. I encourage others to comb through logs and help shed some more light on all these nicks populating IRC. The attack on Excoin was no doubt the work of a botnet and if we can confirm a connection between them then Blackcoin needs to be protected and freenode needs to be informed of all these bogus accounts. We greatly appreciate your assistance.

-Arturo"

## **Mitigation**

Even though DD4BC seemingly can't deliver on the threatened hundreds of gb/sec promised in extortion emails it often doesn't matter. Much lower volume attacks often succeed due to the unpreparedness of defenders [7]. On the other hand, well prepared organizations shouldn't have any trouble defending against these as well as much larger attacks that may come from DD4BC, copycat, or other adversaries. ASERT originally warned about the potential scale of reflection/amplification attacks well over a year ago [1]. Subsequently, ASERT provided its customers as well as the community at large with insights and a prolific amount of information regarding reflection/amplification attacks [2] [3] [4] [5] [6]. These materials provide in-depth information about how these attacks work, why they work, and precisely how to easily mitigate them using Arbor products and services as well as other network-based mitigation strategies.

## **Conclusion**

All indicators suggest that attacks by DD4BC will continue. Other indicators suggest that copycat attackers have already emerged and are actively engaged in attack campaigns. A perfect storm of network architecture weaknesses due to misconfiguration, ease of launching attacks, unprepared targets, and anonymized digital currency sets the stage for lucrative criminal gain with minimal risk to the perpetrators. The key is to be prepared, because even if DD4BC is prosecuted, attacks will likely increase in intensity and volume over time as trends from the last several years indicate. As a result of the painful downtime experienced by the targets in these campaigns, organizations should realize that defenses should be instituted sooner rather than later and begin taking steps to avoid devastating service disruptions. Organizations that are threatened should also report the threats and attacks to their law enforcement contacts, and we invite such organizations to share meaningful attack data with Arbor ASERT if possible.

## References

- [1] Soluk, Kirk. (2014, February 14). NTP Attacks: Welcome to The Hockey Stick Era. <http://www.arbornetworks.com/asert/2014/02/ntp-attacks-welcome-to-the-hockey-stick-era/>
- [2] ASERT Threat Intelligence. (2014, March). ASERT Threat Intelligence Brief 2014-05 – Comprehensive Insight and Mitigation Strategies for NTP Reflection/Amplification Attacks. Available to Arbor Customers Upon Request.
- [3] Dobbins, Roland. (2014, August). When the Sky is Falling, Network-Scale Mitigation of High-Volume Reflection/Amplification DDoS Attacks. <https://www.brighttalk.com/webcast/9053/122257>
- [4] Dobbins, Roland. (2014, October). Presentation – When the Sky is Falling: Network-Scale Mitigation of High-Volume Reflection/Amplification DDoS Attacks. <https://app.box.com/s/r7an1moswtc7ce58f8gg>
- [5] Dobbins, Roland. (2015, May 12). How to Become an Internet Supervillain in Three Easy Steps. <http://asert.arbornetworks.com/how-to-become-an-internet-supervillain-in-three-easy-steps/>
- [6] Dobbins, Roland. (2009 – Present). Public Folder of Best Current Practices (BCPs) tutorials and techniques for network operators. <https://app.box.com/s/4h2l6f4m8is6jnwk28cg>
- [7] Dobbins, Roland. (2014). Presentation - Breaking the Bank; An Analysis of the 2012 – 2014 ‘Operation Ababil’ Financial Industry DDoS Attack Campaign. <https://app.box.com/s/ko8lk4vlh1835p36na3u>

## About ASERT

The Arbor Security Engineering & Response Team (ASERT) at Arbor Networks delivers world-class network security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions that are referred to as "super remediations," and represent the best in information security. This is a reflection of having both visibility and remediation capabilities at a majority of service provider networks globally.

ASERT shares operationally viable intelligence with hundreds of international Computer Emergency Response Teams (CERTs) and with thousands of network operators via intelligence briefs and security content feeds. ASERT also operates the world's largest distributed honeynet, actively monitoring Internet threats around the clock and around the globe via ATLAS®, Arbor's global network of sensors: <http://atlas.arbor.net>. This mission and the associated resources that Arbor Networks brings to bear to the problem of global Internet security is an impetus for innovation and research.

To view the latest research, news, and trends from Arbor, ASERT and the information security community at large, visit our Threat Portal at <http://www.arbornetworks.com/threats/>.