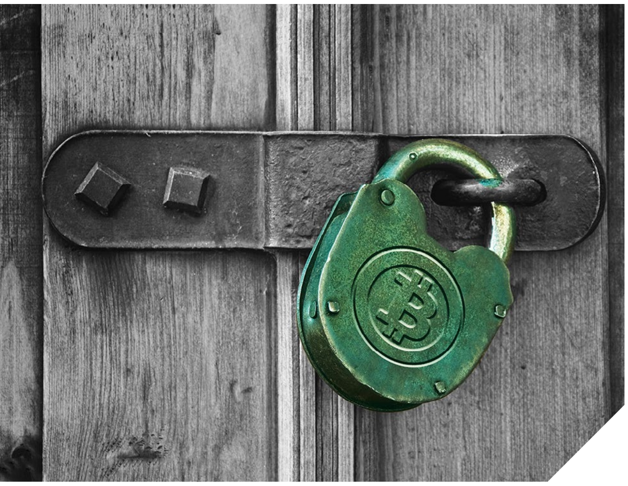


DDOS EXTORTION AND BITCOIN

by Neustar Engineering

DDos extortion is certainly not a new trick by the hacker community, but there have been several new developments to it recently. Notable among them is the use of Bitcoin as a method of payment. Neustar has several clients who have recently been victim to crude extortion plots using DDoS as punishment for not paying a ransom. In this blog post, we'll assess a recent plot involving the use of Bitcoin, profile the perpetrator, and outline solutions for any unfortunate victim of such a plot. (If you're the victim of an extortion plot, you should report it immediately to the appropriate law enforcement agency.)

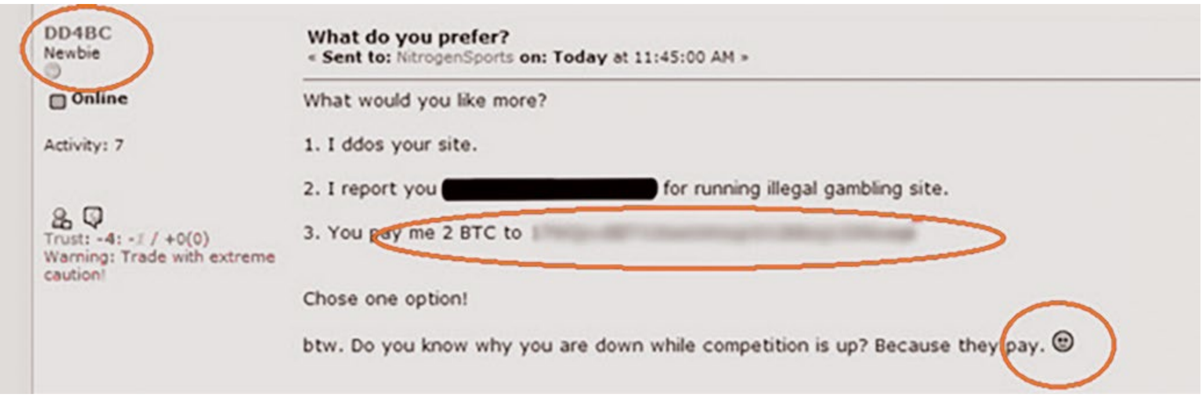
DD4BC (DDoS for Bitcoin) is a hacker (or hacker group) who has been found to extort victims with DDoS, demanding payment via Bitcoin. DD4BC seems to focus on the gaming and payment processing industries that use Bitcoin. The plots have several common characteristics. During these extortion acts, the hacker:

- Launches an initial DDoS attack (ranging from a few minutes to a few hours) to prove the hacker is able to compromise the victim's website
- Demands payment via Bitcoin while suggesting they're actually helping the site by pointing out their vulnerability to DDoS
- Threatens more virulent attacks in the future
- Threatens a higher ransom as the attacks progress (pay up now or pay more later)

Unprotected sites can be taken down by these attacks. A recent study by Arbor Networks concluded that a vast majority of DD4BCs actual attacks have been UDP Amplification attacks, exploiting vulnerable UDP Protocols such as NTP and SSDP. In the spectrum of cyber-attacks, UDP flooding via botnet is a relatively simple, blunt attack that simply overwhelms a network with unwanted UDP traffic. These attacks are not technically complex and are made easier with rentable botnets, booters, and scripts.

Example of a DDoS Extortion Attempt

Following is an example of a chat exchange between the hacker (screenname “DD4BC”) and the victim who has made the extortion plot public (screenname “Nitrogen Sports”). The following screenshot was taken from bitcointalk.org.



DD4BC
Newbie

Online

Activity: 7

Trust: -4: -1 / +0(0)
Warning: Trade with extreme caution!

What do you prefer?
« **Sent to:** NitrogenSports **on: Today** at 11:45:00 AM »

What would you like more?

1. I ddos your site.

2. I report you [redacted] for running illegal gambling site.

3. You pay me 2 BTC to [redacted]

Chose one option!

btw. Do you know why you are down while competition is up? Because they pay. ☺

Profile of the Extorting Hacker

The hacker goes by the name DD4BC (DDoS for Bitcoin) and provides a Bitcoin account address for the transfer of funds. As for the hacker’s gender, evidence suggests that most hackers tend to be male, although female hackers seem to be growing in number. At a recent MIT hackathon, only 15% of the participants were female. An earlier study concluded that around 91% of hackers were male. Visitors to Hacker News were 77% male in 2012. Based on the available data, it’s a solid assumption that DD4BC is a male, but we cannot be sure from the communications.

The hacker refers to himself in the singular (“me”) rather than in the plural (“we”), indicating a lone-wolf actor. His poor grammar and misspelled words suggest that English is not his first language. If true, the hacker has probably learned English in school, suggesting some formal education. He also demonstrates a level of immaturity with a smiley face emoticon. The levity suggests that the hacker does not fully comprehend the seriousness of the crime being committed, but rather considers this a game.

The hacker’s extortion is two-fold. He threatens not only a DDoS attack, but also to report the site for alleged illegality to some redacted authority. He’s familiar with the gaming platform and its competitors. He’s also familiar with the payment processors that serve the industry. He seems focused on Bitcoin gaming operators and payment processors, although recent attacks have expanded into the financial industry at large.

The Arbor Networks report traced DD4BC Bitcoin payments back to an online wallet for a gaming/gambling platform called SatoshiBONES. This online wallet is compatible with other Bitcoin and gaming platforms. Although the attacks target clients around the world, the initial attacks were mainly against European sites and during hours that would indicate a European actor.

Overall Assessment of the Extortion

The hacker is most likely a gamer or online gambler who uses Bitcoin as the preferred payment method because of its inherent anonymity. The hacker is most likely a male under 27 years of age, living in Europe and working independently. The extortion may be an attempt to replenish his Bitcoin account.

DDoS Mitigation Options

The good news for online businesses that fall victim to such plots is that there are legitimate and robust modes of protection available that do not require paying the ransoms demanded by extorting hackers.

- On-Demand Cloud is a set of cloud-based services used to mitigate an attack. The service is typically a large scrubbing network that is managed by a Security Operations Center (SOC). When under attack, all client traffic is redirected to the scrubbing network; countermeasures are applied to remove the DDoS traffic. Legitimate traffic is forwarded to the protected website.
- Specialized **DDoS appliances** exist that can mitigate a variety of attacks. These appliances can be quite effective in some cases, but they are limited to the circuit capacity feeding into the web server or network. Any large flood that overwhelms the IP connection capacity will render the appliance ineffective.
- Hybrid DDoS Protection combines an appliance with an on-demand cloud service. This is the best—but most expensive—option. An on-network DDoS appliance is combined with a cloud-based scrubbing service to provide a one-two punch to handle all types of DDoS attacks. Low-volume attacks are thwarted by the appliance while large-volume attacks are handled by the scrubbing cloud via redirection.
- Always-Routed Cloud. Frequently attacked online businesses can consider a constant redirection to a scrubbing network. This can be expensive and will add latency that may not be necessary in non-attack conditions.
- **Content Delivery Networks** (CDNs) can provide some protection, in the form of absorption and/or rate limiting. Some of the low-cost CDNs have a protection mode that can impact the user experience by delaying website load times or presenting CAPTCHA user challenges. Automated protections can be bypassed by clever attackers. Origin servers can also be vulnerable if not protected.

In summary, any business that values its online presence should prepare for a potential DDoS attack. Because hackers are constantly preying on unprotected websites and other online properties, if you leave your site unprotected, you may find yourself at the mercy of an extortionist. Choose a DDoS mitigation option that fits your environment and sign up pre- emptively, during non-attack conditions. Once an attack is in progress, your reputation will suffer and losses will mount as you scramble to stop the attack using expensive emergency mitigation services. Neustar has a variety of services to help protect your domain, including from DDoS attack. ■

For more information visit:
www.neustar.biz/services/ddos-protection

neustar