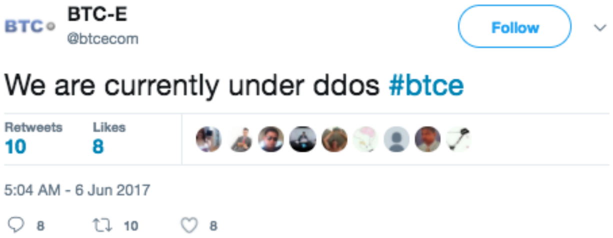
ERT Threat Alert

Cryptocurrencies Trade Under Fire

June 19, 2017

Abstract

Radware's Emergency Response Team (ERT) has been following a trend in outages effecting bitcoin exchanges over the last several weeks. Predicted by Radware last year[i], attacks against bitcoin exchanges and marketplaces seem correlated with currency value fluctuations and have exponentially grown due to the rise in value of bitcoin – hitting an all-time high of $2,995 USD on June 11[ii].



We are currently under ddos #btce

5:04 AM - 6 Jun 2017

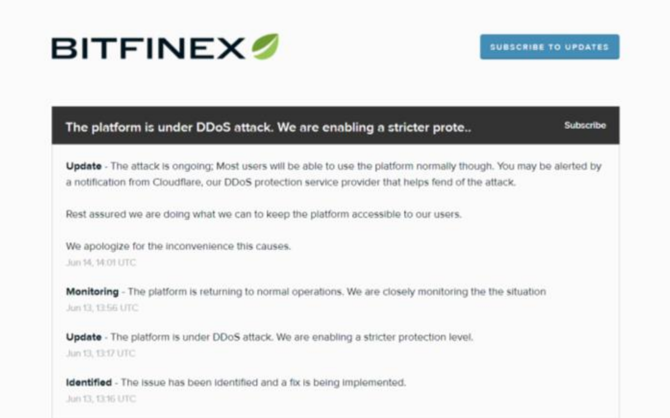
Figure 1: BTC-E suffers from a DDoS attack

Background

Obviously, bitcoin investors would like to see its value increase. Regardless, as its value increases, it becomes increasingly valuable to more people. This increased attention is creating profitable opportunities for cyber criminals. For example, the WannaCry[iii] campaign locked up computers around the world demanding bitcoin for a decryption key.

Since then, several crypto-currency exchanges around the world have been experiencing outages related to either a flood of natural traffic due to market fluctuations and demand or malicious traffic from denial-of-service attacks.

This past week, both Bitfinix and BTC-e announced[iv] that their networks were experiencing service degradation due to a denial-of-service attack. Coinbase reported experiencing issues with load times that resulted in users not being able to login or view the websites of the targeted exchanges.



The platform is under DDoS attack. We are enabling a stricter prote..

Update - The attack is ongoing; Most users will be able to use the platform normally though. You may be alerted by a notification from Cloudflare, our DDoS protection service provider that helps fend of the attack.

Rest assured we are doing what we can to keep the platform accessible to our users.

We apologize for the inconvenience this causes.
Jun 14, 14:01 UTC

Monitoring - The platform is returning to normal operations. We are closely monitoring the the situation
Jun 13, 13:56 UTC

Update - The platform is under DDoS attack. We are enabling a stricter protection level.
Jun 13, 13:17 UTC

Identified - The issue has been identified and a fix is being implemented.
Jun 13, 13:16 UTC

Figure 2: Bitfinex status page

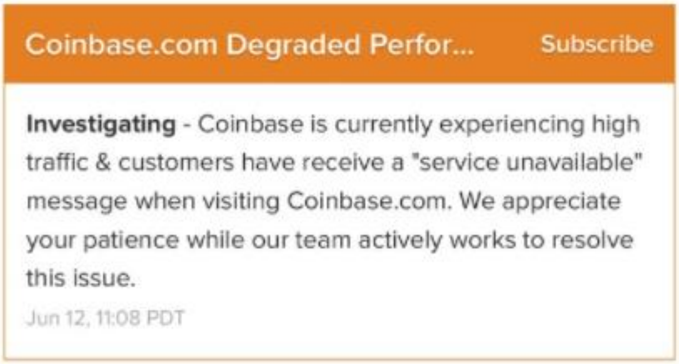
Bitcoin exchanges have also been the victim of multi-million dollar heists. In August, a Hong Kong-based Bitfinex[v] reported that hackers stole $71,000,000 USD. Last month, Bleeping Computers[vi] reported that South Korean bitcoin exchange Yapizon announced that their systems were breached and $5,500,000 USD was stolen.

Denial-of-service attacks on bitcoin exchanges are not new. They happen often[vii], but recent outages come at bitcoin's peak and were followed by a decline in value after the attacks. Outages caused by a flood of traffic from legitimate users or malicious traffic prevent users from accessing their mobile apps, websites and API. As a result, these users panic as the price of the coin fluctuates while they are locked out.

Attack Types and Reasons for Concern

- Denial of Service
- Cyber-ransom
- User account seizure

Leading bitcoin exchanges typically excel in service availability, so much so that some users have turned into full-time traders, providing them a platform to store and trade thousands of dollars of cryptocurrency in real time. System overloads need to be avoided so that traders' real-time market interactions are not interrupted. When a trading platform goes down, users are unable to access their wallets and fear that bitcoin's value will fluctuate, resulting in the company suffering reputation damage.



Coinbase.com Degraded Perfor... Subscribe

Investigating - Coinbase is currently experiencing high traffic & customers have receive a "service unavailable" message when visiting Coinbase.com. We appreciate your patience while our team actively works to resolve this issue.

Jun 12, 11:08 PDT

Figure 3: Coinbase outage

Status Pages:

- https://status.kraken.com/ - Degraded System Service – 6-17
- https://status.coinbase.com/ - Minor Service Outage – 6-17
- https://bitfinex.statuspage.io/ - Under attack – 6-17

What's Expected Next

Bitcoin is slowly becoming accepted around the world. With this acceptance comes more users and this demand puts a strain on the networks. Ramping and manipulations to influence the BTC/USD exchange are only the beginning; a high bandwidth attack from a botnet could take the exchange down. Some of these services are dealing with hundreds of thousands of requests at a time and can even fail from a burst of legitimate traffic as a result of a change in value.

In addition, as the value and popularity of the currency rises, Radware expects more ransomware and RDoS[viii] campaigns. Bitcoin is the preferred currency for cyber criminals on the Darknet and it's also the currency of choice for extortionists. It is expected that as bitcoin continues to rise in value, cyber criminals will continue to rely on cryptocurrencies as a means for payment. The wallets and exchanges that house the currency will also be targeted at a persistent rate.

Exchanges might experience denial-of-service attacks by hacktivist seeking to compromise or seize accounts. In the past, hacktivists groups such as Anonymous launched denial-of-service attacks against PayPal after refusing to process payment for Wikileaks.

Organizations Under Attack Should Consider

Effective DDoS protection solutions:

- A hybrid DDoS protection solution that combines on-premise detection and mitigation with cloud-based protection for volumetric attacks. It provides quick detection, immediate mitigation and prevents internet pipe saturation.
- Solution must distinguish between legitimate and malicious traffic, protect the SLA and block the attack.
- An integrated, synchronized DDoS protection solution that can protect from multi-vector attacks combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- A cyber-security emergency response plan that includes an emergency response team and DDoS protection solutions and process in place. Identify areas where help is needed from a third party.

Effective Web Application protection elements (against web intrusions, defacement and data leakage)**:**

- IP-agnostic device fingerprinting – Having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time
- Automatic and real time generation of policies to protect from Zero-day, unknown attacks
- Shortest time from deployment to a full coverage of OWASP Top-10

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud based DDoS protection solutions protect against attacks in real time and help ensure service availability.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you’re under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today’s attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware’s Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

[i] https://blog.radware.com/security/2016/07/bitcoin-exchanges-attack/
[ii] https://www.coinbase.com/charts
[iii] https://blog.radware.com/security/2017/06/smb-vulnerabilities-wannacry-adylkuzz-sambacry/
[iv] https://www.infosecurity-magazine.com/news/worlds-largest-bitcoin-exchange/
[v] https://www.bloomberg.com/news/articles/2016-08-05/hacked-bitcoin-exchange-says-it-will-spread-losses-among-users
[vi] https://www.bleepingcomputer.com/news/security/hacked-south-korean-bitcoin-exchange-loses-5-5-million/
[vii] https://themerkle.com/top-5-cryptocurrency-exchanges-hit-by-ddos-attacks/
[viii] https://security.radware.com/ddos-threats-attacks/cyber-ransom-spring-2017/