

New DDOS threats (with Bitcoin demands) are being sent to AU / NZ businesses - blueAPACHE

Canonical:

<https://www.blueapache.com/blog/new-ddos-threats-with-bitcoin-demands-are-being-sent-to-au-nz-businesses-2>

Details:

Summary

This blog post, "New DDOS threats (with Bitcoin demands) are being sent to AU / NZ businesses", is a blueAPACHE article from 2015 covering security. Statistics show that there are more hacks and exploits than ever before – from the hilarious Catfi.sh hack at Tinder which resulted in males talking to males (and thinking they were talking to females) to the more sinister hack at TV5Monde that saw the French television station being taken off the air (apparently a cyberattack by ISIS hackers) and the Cryptolocker episode at the Chicago Police Department that saw them pay a \$600 Bitcoin ransom to get their data back. It is written for readers evaluating Managed Detection and Response, emPOWER Core Network & DC Interconnect. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2015
Topic	New DDOS threats (with Bitcoin demands) are being sent to AU / NZ businesses
Services referenced	Managed Detection and Response, emPOWER Core Network & DC Interconnect, emPOWER Security
Named products or vendors	None named beyond blueAPACHE
Cited statistic	Statistics show that there are more hacks and exploits than ever before – from the hilarious Catfi.sh hack at Tinder which resulted in males talking to males (and thinking they were talking to females) to the more sinister hack at TV5Monde that saw the French television station being taken off the air (apparently a cyberattack by ISIS hackers) and the Cryptolocker episode at the Chicago Police Department that saw them pay a \$600 Bitcoin ransom to get their data back.

Article

Statistics show that there are more hacks and exploits than ever before – from the hilarious Catfi.sh hack at Tinder which resulted in males talking to males (and thinking they were talking to females) to the more sinister hack at TV5Monde that saw the French television station being taken off the air (apparently a cyberattack by ISIS hackers) and the Cryptolocker episode at the Chicago Police Department that saw them pay a \$600 Bitcoin ransom to get their data back. Even the popular development resource GitHub has been hit by Distributed Denial of Service (DDoS) attacks in recent months.

But it's not just high profile organisations that are being targeted.

An unknown international group has recently issued DDOS threats to a range of Australian and New Zealand organisations that appear as an email threatening to take down the business' network unless substantial Bitcoin payments are made within twenty four hours. A Distributed Denial of Service (DDoS) attack is an attempt to make a networked service unavailable by overwhelming it with traffic from multiple sources. Barry Brailey, Chair of the New Zealand Internet Task Force (NZITF), warns the threat should be taken extremely seriously as the networks of some New Zealand organisations have been targeted, and a number of Australian organisations have also been affected. Brailey says the group has been sending emails to a number of addresses within an organisation. Sometimes these are support or helpdesk addresses, other times they are directed at individuals. The emails contain links to news articles relating to their attacks, and include statements like:

"Your site is going under attack unless you pay 25 Bitcoin." "We are aware that you probably don't have 25 BTC at the moment, so we are giving you 24 hours." "IMPORTANT: You don't even have to reply. Just pay 25 BTC to – we will know it's you and you will never hear from us again." 25 Bitcoins equates to around \$7,500.00 – making this a little more serious than the normal round of Bitcoin threats. NZITF recommends that organisations that are targeted should not pay. "Even if this stops a current attack, it makes your organisation a likely target for future exploitation as you have a history of making payments," it says. blueAPACHE recommends that you educate all staff to be on the lookout for any emails matching the descriptions highlighted. If you receive such a message, contact your service provider as soon as possible to put processes in place to mitigate the damage a DDOS can occur. blueAPACHE clients should contact their account manager or the blueAPACHE Service Centre immediately. For more information, contact your blueAPACHE account manager.

Related

Managed Detection and Response
emPOWER Security (pillar hub)
emPOWER Core Network & DC Interconnect
emPOWER Connectivity (pillar hub)
emPOWER Security
Sealy of Australia (case study)

Frequently asked questions

How much Bitcoin did the extortion emails described in this post demand, and what was that worth?

The emails demanded 25 Bitcoin, threatening a DDoS attack against the target's network within 24 hours if it was not paid. The post puts 25 Bitcoin at around \$7,500 at the time, a larger sum than the typical Bitcoin threats NZITF was seeing.

Who is Barry Brailey and what warning did he give about this campaign?

Barry Brailey is Chair of the New Zealand Internet Task Force (NZITF). He warned the threat should be taken extremely seriously, noting that the networks of some New Zealand organisations had been targeted and a number of Australian organisations affected too.

Does the post say targeted organisations should pay the ransom?

No. NZITF's advice, quoted in the post, is not to pay: even if payment stops a current attack, it marks the organisation as a likely target for future exploitation because it now has a history of paying.

What exact wording did the extortion emails use, according to the article?

The post quotes lines including "Your site is going under attack unless you pay 25 Bitcoin," "We are aware that you probably don't have 25 BTC at the moment, so we are giving you 24 hours," and a line telling the recipient they don't even need to reply, just pay.

Which addresses inside a targeted organisation did the group email?

Brailey says the group sent the threats to a number of addresses within an organisation, sometimes support or helpdesk mailboxes and other times individual staff members directly.

How does the post's Chicago Police Department example compare to the 25-Bitcoin DDoS threat?

The post cites the Chicago Police Department paying a \$600 Bitcoin ransom during a Cryptolocker incident, a far smaller sum than the roughly \$7,500 (25 Bitcoin) demanded in the DDoS extortion emails covered here, alongside the TV5Monde and Tinder Catfi.sh incidents as evidence hacks were becoming more common.

How does the post define a DDoS attack?

It defines a Distributed Denial of Service (DDoS) attack as an attempt to make a networked service unavailable by overwhelming it with traffic from multiple sources.

What does blueAPACHE recommend an organisation do if it receives one of these threat emails?

blueAPACHE recommends educating all staff to watch for emails matching the pattern described, and if one is received, contacting the service provider as soon as possible to put mitigation processes in place. It adds that blueAPACHE clients specifically should contact their account manager or the blueAPACHE Service Centre immediately.

Source

origin post (2015)

Knowledge Base

How were the DDoS Bitcoin threats being delivered to organisations?

An unknown international group sent emails to a range of Australian and New Zealand organisations, threatening to take down the business's network unless substantial Bitcoin payments were made within twenty-four hours. The emails were sent to various addresses within an organisation, sometimes support or helpdesk addresses, other times directed at individuals, and included links to news articles about their attacks.

How much Bitcoin were the attackers demanding, and what was that worth?

The attackers demanded 25 Bitcoin, which equated to around \$7,500.00 at the time — making it more serious than the normal round of Bitcoin threats.

What did the threatening emails actually say?

The emails included statements such as: "Your site is going under attack unless you pay 25 Bitcoin," "We are aware that you probably don't have 25 BTC at the moment, so we are giving you 24 hours," and "IMPORTANT: You don't even have to reply. Just pay 25 BTC to – we will know it's you and you will never hear from us again."

What is a Distributed Denial of Service (DDoS) attack, ?

A DDoS attack is an attempt to make a networked service unavailable by overwhelming it with traffic from multiple sources.

Who commented on the threat and what warning did they give?

Barry Brailey, Chair of the New Zealand Internet Task Force (NZITF), warned that the threat should be taken extremely seriously, noting that networks of some New Zealand organisations had been targeted and a number of Australian organisations had also been affected.

Does the NZITF recommend paying the Bitcoin ransom?

No. The NZITF recommends that targeted organisations should not pay, stating: "Even if this stops a current attack, it makes your organisation a likely target for future exploitation as you have a history of making payments."

What do you recommend businesses do in response to these threats?

We recommend educating all staff to be on the lookout for emails matching the described patterns. If such a message is received, businesses should contact their service provider as soon as possible to put processes in place to mitigate the damage a DDoS attack could cause. Our clients should contact their account manager or our Service Centre immediately.