

THE STATE OF SECURITY ([HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/](http://www.tripwire.com/state-of-security/))

News. Trends. Insights.

[HOME \(HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY\)](http://www.tripwire.com/state-of-security/) » [LATEST SECURITY NEWS \(HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/LATEST-SECURITY-NEWS/\)](http://www.tripwire.com/state-of-security/topics/latest-security-news/) » [Full Investigation Threatened Against DD4BC Attack Group](#)

Full Investigation Threatened Against DD4BC Attack Group



([HTTP://WWW.TRIPWIRE.COM/STATE-OF-](http://www.tripwire.com/state-of-security/contributors/david-bisson/)

[SECURITY/CONTRIBUTORS/DAVID-BISSON/](http://www.tripwire.com/state-of-security/contributors/david-bisson/))

DAVID BISSON ([HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/DAVID-BISSON/](http://www.tripwire.com/state-of-security/contributors/david-bisson/))

AUG 28, 2015 |

[LATEST SECURITY NEWS \(HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/LATEST-SECURITY-NEWS/\)](http://www.tripwire.com/state-of-security/topics/latest-security-news/)



SECURITY
NEWS

(<http://www.tripwire.com/state-of-security/latest-security-news/full-investigation-threatened-against-dd4bc-attack-group/>)

◀ 17 ◀ 66 ◀ 29 ◀ 11

A group of security researchers and law enforcement officials are threatening to launch a full investigation into the DDoS for Bitcoins (DD4BC) attack group if it continues to target banks.

DD4BC (<http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/dd4bc-group-targets-companies-with-ransom-driven-ddos-attacks/>) is known for launching small- to mid-size DDoS attacks against its victims and threatening even larger, more prolonged attack campaigns unless they pay a ransom in Bitcoin. In addition to targeting banks, the group has went after well known Bitcoin exchanges. Two in particular, Bitalo and Bitmain, have helped fund a bounty for any information regarding DD4BC (<http://bitcoinbountyhunter.com/bitalo.html>).

According to Roland Dobbins of Arbor Network's security engineering and response team, the law enforcement and security communities are interested in bringing down the group before it has the opportunity to target any more financial organizations.

"There is a very, very active posse who are trying to identify the actor, and intelligence agencies in some jurisdictions are after DD4BC," Dobbins recently told the AusNOG conference (<http://www.ausnog.net/>) in Melbourne, Australia, as reported by *The Register*

(http://www.theregister.co.uk/2015/08/28/irate_security_posse_intel_spooks_in_ddos_hushed_hacker_hunt/). "There is no jurisdictional taskforce setup yet as far as I know, but there are some closed, vetted operational security groups trying to track down the threat actor. I think DD4BC is one person who is reasonably tech savvy but not an innovator. The attacker will escalate the probe into a full investigation if they continue to hit banks."

Abusable
SSDP
Services

UDP/80 – UDP/1900, ~119 bytes
 Spoofed Source: 172.19.234.6
 Destinations: Multiple SSDP Services
 SSDP query: *M-Search enumeration*

172.19.234.6/

One of DD4BC's tactics: SSDP Reflection/Amplification Attacks (Source: Roland Dobbins (<https://app.box.com/s/2kpbqfdl1ko3qhfh4y8ekd1rvj24vfd>))

News of a possible investigation into DD4BC follows the release of Verisign's Q2 DDoS Trends Report (http://www.verisign.com/en_US/security-services/ddos-protection/ddos-report/index.xhtml?cmp=LK-RP-TRENDS4), which in part analyzes DD4BC and observes that the group is likely comprised of relatively few people. The report estimates that DD4BC probably has five members or fewer (<http://www.scmagazine.com/dd4bc-are-ddos-attack-driving-force-new-report-claims/article/435244/>).

Other notable findings (http://www.circleid.com/posts/20150827_ddos_for_bitcoin_increasingly_targets_financial_industry/) of the report include the fact that attacks over five Gbps accounted for approximately 20% of all DDoS campaigns and that 34 percent more attacks were mitigated in the first half of 2015 than in the same period of 2014.

◀ 17 ▶ 66 ▶ 29 ▶ 11

TAGS AusNOG (<http://www.tripwire.com/state-of-security/tag/ausnog/>), Bitalo (<http://www.tripwire.com/state-of-security/tag/bitalo/>), Bitcoin (<http://www.tripwire.com/state-of-security/tag/bitcoin/>), Bitmain (<http://www.tripwire.com/state-of-security/tag/bitmain/>), DD4BC (<http://www.tripwire.com/state-of-security/tag/dd4bc/>), DDoS (<http://www.tripwire.com/state-of-security/tag/ddos/>), Verisign (<http://www.tripwire.com/state-of-security/tag/verisign/>)

Login

There are no comments posted yet. Be the first one!

POST A NEW COMMENT

Enter text right here!

Comment as a Guest, or login:

[illegible]

Displayed next to your comments.

Not displayed publicly.

If you have a website, link to it here.

Subscribe to

Submit Comment

None



About David Bisson



(<http://www.tripwire.com/state-of-security/contributors/david-bisson/>)

David Bisson (<http://www.tripwire.com/state-of-security/contributors/david-bisson/>) has contributed 321 posts to The State of Security.

View all posts by David Bisson (<http://www.tripwire.com/state-of-security/contributors/david-bisson/>) >

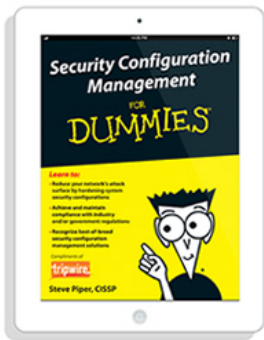
Follow @DMBisson

The State of Security Newsletter

Receive the latest security stories, trends and insights directly in your inbox each week.

Sign Up

FREE EBOOK



(http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-

[bnr&utm_content=pdf&utm_campaign=scm-for-dummies](http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)
Security Configuration Management

For Dummies (http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)

Download Now (http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)

Latest Security News (/state-of-security/topics/latest-security-news/)

Full Investigation Threatened Against DD4BC Attack Group AUG 28, 2015

FireEye Intern Pleads Guilty to Selling Dendroid Malware on Darkode AUG 27, 2015

Report: Phishing Scams Cost Companies Millions Per Year AUG 26, 2015

GitHub Restores Service Following DDoS Attack AUG 26, 2015

VoIP Scam Lands Three Men in Jail AUG 25, 2015

POPULAR

FEATURED

RECENT



Agora, the dark web's biggest marketplace, shuts over Tor privacy fears
(<http://www.tripwire.com/state-of-security/security-data-protection/agora-the-dark-webs-biggest-marketplace-shuts-over-tor-privacy-fears/>)

AUGUST 27, 2015

(<http://www.tripwire.com/state-of-security/security-data-protection/agora-the-dark-webs-biggest-marketplace-shuts-over-tor-privacy-fears/>)



Asymmetric Network Defense: It's 1904 All Over Again (<http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/asymmetric-network-defense-its-1904-all-over-again/>)

AUGUST 23, 2015

(<http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/asymmetric-network-defense-its-1904-all-over-again/>)



British Travel Company Breached, Hundreds of Customers' Information Exposed
(<http://www.tripwire.com/state-of-security/latest-security-news/british-travel-company-breached-hundreds-of-customers-information-exposed/>)

AUGUST 24, 2015

(<http://www.tripwire.com/state-of-security/latest-security-news/british-travel-company-breached-hundreds-of-customers-information-exposed/>)



BSides: Broadening the Horizons of Information Security (<http://www.tripwire.com/state-of-security/featured/bsides-broadening-the-horizons-of-information-security/>)

AUGUST 23, 2015

(<http://www.tripwire.com/state-of-security/featured/bsides-broadening-the-horizons-of-information-security/>)



FireEye Intern Pleads Guilty to Selling Dendroid Malware on Darkode
(<http://www.tripwire.com/state-of-security/latest-security-news/fireeye-intern-pleads-guilty-to-selling-dendroid-malware-on-darkode/>)

AUGUST 27, 2015

(<http://www.tripwire.com/state-of-security/latest-security-news/fireeye-intern-pleads-guilty-to-selling-dendroid-malware-on-darkode/>)

Tweets

Follow



Tripwire, Inc. @TripwireInc

36m

Android Dolphin, Mercury Browsers Vulnerable to Remote Attacks
[tripwire.me/1JVkSCj](#) via @DMBisson #security #infosec
Show Summary



Tripwire, Inc. @TripwireInc

2h

A Shopping Cart Is Not Just For Groceries [tripwire.me/1JNNgWZ](#) via @FisherIDAM #security #identity
Show Summary



Tripwire, Inc. @TripwireInc

4h

Ticking the Box Is Not Enough [tripwire.me/1NyUWNf](#) via @SBLTD #security #infosec
Show Summary




Tripwire, Inc. @TripwireInc

6h

Exploiting the Social Media Security Conundrum
[tripwire.me/1K25Z17](#) via @Peter_Skaronis #security #infosec

Tweet to @TripwireInc




Tripwire

6,139 likes

Like Page

Share

Be the first of your friends to like this



Topics (/state-of-security/topics/)

- Government >
- Incident Detection >
- IT Security and Data Protection >
- Latest Security News >
- Off Topic >
- Regulatory Compliance >
- Risk-Based Security for Executives >
- Security Awareness >
- Security Slice >
- This Week in Security >
- Tripwire News >
- Vulnerability Management >

