DD4BC, Armada Collective Inspire Cyber Extortion Copycats

By SecurityWeek News on December 07, 2015

Cyber extortion is expected to gain traction among cybercriminals after attack groups such as DD4BC (DDoS "4" Bitcoin) and Armada Collective successfully boosted revenue by extorting organizations, according to threat intelligence company Recorded Future.

Over the past year, the DD4BC group attempted to extort numerous companies, many in the financial services sector, by warning the of an imminent powerful DDoS attack that would be launched against their infrastructure unless they agreed to pay a specific ransom. Following the warning email, a small attack, typically of 10-15 Gbps and lasting only several minutes was launched, to prove the threat was real.

Armada Collective operated in a similar manner, first sending threat emails and small attacks to prove it was capable of launching DDoS attacks, and some suggested that DD4BC might have rebranded. The group also asked for a small amount of Bitcoin from companies willing to pay the ransom to avoid being attacked.

In September, Akamai's Prolexic Security Engineering and Response Team (PLXsert) revealed that between September 2014 and August 2015 DD4BC launched a total of 141 attacks against organizations in North America, Europe, Asia and Australia. They also revealed that the group's largest attack peaked at 56 Gbps and that NTP (22%), SSDP (15%), UDP (15%) and SYN (13%) floods were used to disrupt targets.

Akamai also observed a 13.34 Gbps average peak bandwidth for all attacks, which was quite low, considering that the group was claiming to be capable of launching 400-500 Gbps attacks. The security researchers also revealed that attackers initially asked between 25 ($6,000) and 100 ($24,000) Bitcoin from companies to prevent being hit by the DDoS attacks, but that they also started threatening to expose a targeted organization via social media, to bring harm to the brand.

Following the September report from Akamai, the activity of DD4BC has decreased significantly, and Recorded Future suggests that the cybercriminals in the group might be in fear of being caught. Furthermore, they suggest that those behind Armada Collective might have been thinking exactly the same after the recent incident with ProtonMail.

The encrypted email service provider was targeted by the group in early November, yet the attack against it was much powerful than what DD4BC or Armada Collective ever showed before. Initial investigation led to the conclusion that the service might have been attacked by a state-sponsored actor, especially with Armada Collective emailing ProtonMail to explain that they did not launch the second attack, and that it was much powerful than any DDoS they would be able to produce.

Based on all this data, Recorded Future suggests that other groups are already copying this modus operandi, looking to achieve the same level of success that DD4BC and Armada Collective had. Moreover, they claim that a recent set of attacks against Greek banks, carried out by a group calling themselves Armada Collective, might have been performed by entirely different people.

The ransom was much higher than those requested by DD4BC and Armada Collective, namely 20,000 BTC, about $7.2 Million, which is atypical. Moreover, after ProtonMail paid the ransom, Armada Collective emailed them back to deny responsibility for the attack, and Recorded Future notes that they even returned the ransom.

The threat intelligence company also notes that there has been an increase in requests on the Dark Web for information on how to perform DDoS attacks, a clear indicator that others are also considering cyber extortion to boost their revenue. Script kiddies are suspected to be interested in this method the most, and the fact that all suspects arrested in the recent TalkTalk breach are very young appears to confirm this.

“Nevertheless, the DDoS threat landscape continues to evolve. While cyber extortion has been around for quite some time, the adoption of Bitcoin as a method of ransom will continue to attract new miscreants into the DDoS space,” Recorded Future said.

Related: The Rise of Cyber Extortion

Previous Columns by SecurityWeek News:
DD4BC, Armada Collective Inspire Cyber Extortion Copycats
EFF Launches Security Vulnerability Disclosure Program
Rootnik Trojan Modifies Legitimate Root Tool to Hack Android Devices
Let's Encrypt Enters Public Beta
International Operation Disrupts Dorkbot Botnet

Tags:
NEWS & INDUSTRY Cybercrime

ALSO ON SECURITYWEEK PROVIDES INFORMATION SECURITY NEWS AND ANALYSIS. WHAT'S THIS?

Linux Machines Powered Nearly Half of DDoS Attacks in Q3: Kaspersky
1 comment • a month ago
Lange — Watch out world Linux is slowly movin to the number 1 OS YEA

Security Flaws in LastPass Exposed User Passwords
1 comment • 20 days ago
Mr.Nunya — "In the client-side attack scenario, in which the attacker has access to the victim's machine..." SO in other words, …

Changing the Economics of Cybersecurity
1 comment • 22 days ago
Murali — I agree to certain extend but in the SaaS and BYOD environment how do we really control the end point (employees …

Industry Reactions to Hacking Back: Feedback Friday
1 comment • 25 days ago
Brandon Bain — Great article! We've often heard, "The best defense is a good offense" but it's difficult to apply that to …

Subscribe Add Disqus to your site Privacy DISQUS

Most Recent Most Read

- To Improve Security Effectiveness, Look Inside
- Iran Made 53 Arrests Linked to IS Since 2014: Police
- DD4BC, Armada Collective Inspire Cyber Extortion Copycats
- EFF Launches Security Vulnerability Disclosure Program
- FireEye Patches Critical Flaw Found by Google Researchers
- What's the Real Cost to Us of an Ad-Funded Web?
- Rootnik Trojan Modifies Legitimate Root Tool to Hack Android Devices
- Russian Hackers Using Bootkit to Steal Payment Data
- Serious Flaws Found in Honeywell Gas Detectors
- 650,000 Affected by JD Wetherspoon Data Breach

Popular Topics

Information Security News
IT Security News
Risk Management
Cybercrime
Cloud Security
Application Security
Smart Device Security

Security Community

IT Security Newsletters
IT Security White Papers
Suits and Spooks
ICS Cyber Security Conference
CISO Forum
InfosecIsland.Com

Stay Intouch

Twitter
Facebook
LinkedIn Group
Cyber Weapon Discussion Group
RSS Feed
Submit Tip
Security Intelligence Group

About SecurityWeek

Team
Advertising
Events
Writing Opportunities
Feedback
Contact Us