




| Horizon Report

Eastern European Threat Actor Extorts Hosting Providers Using DDoS Attacks

Date	December 07, 2015
Report ID	HR-20151207-001
Impact	 Targeted and Compromised Organizations HIGH  Other organizations MEDIUM

1. Overview
2. Analysis
3. Indicators
4. Area 1 Guidance

Overview

Risk: **HIGH**

A threat actor, identified as Armada Collective, intimidates hosting providers with DDoS attacks unless a certain ransom is paid in Bitcoin.

This threat actor sends extortion emails identifying their group to hosting provider employees. In their emails, they detail DDoS threats, ransom payments and a provider-specific Bitcoin address where payment should be sent. Armada Collective has been observed targeting hosting providers since November 2015. Some of these providers are Area 1 partners. The attacks seem to follow the same modus operandi as the “DDoS 4 Bitcoin” (DD4BC) attacks in 2014, which affected more than 140 companies[1].

Actor Attribution

Armada Collective may be a copycat group or a conglomerate of groups related to DD4BC located in Eastern Europe.

[1] Case Study: Summary of Operation DD4BC. Akamai. <https://www.stateoftheinternet.com/resources-web-security-threat-advisories-2015-dd4bc-case-study-ddos-attacks-bitcoin-extortion-ransom.html>. September 09, 2015.

1. Overview
 - 2. Analysis**
 3. Indicators
 4. Area 1 Guidance
-

Analysis

Target

Armada Collective targets hosting, email, and other service providers. The hosting providers threatened by the actor include some of Area 1's partners. Armada Collective launched barrages of extortion emails to various principals and admin accounts.

Emails

Emails originated from a mail.ru email account and were traced to AS47764 (Limited Liability Company Mail.ru, according to WHOIS data.) The emails were nearly identical and claimed DDoS attack capabilities of up to 1Tbps. Demands appeared to range from 20 – 50 bitcoins and gave victims between 3-8 days to remit payment. Costs to end the DDoS attacks increased if the deadline was missed and would continue to increase every hour thereafter.

Attacks

Along with the extortion email, the threat actor launched a smaller-scale DDoS on the hosting provider to establish credibility of the threat. They also threatened to contact customers to explain why the hosting provider's service was down and recommend that they use another service, driving away business.

To date, no victim of Armada Collective attacks has experienced a DDoS heavier than 15Gbps. Also, each victim had been given an extension of 3-4 days to pay the extortion nearing the deadline.

Business Impact

-  Denial of service to customers

1. Overview
 - 2. Analysis**
 3. Indicators
 4. Area 1 Guidance
-

Analysis

Cases

It should be noted – and information regarding this attack is readily available – that Armada Collective initially targeted private email providers, including CERN based ProtonMail^[2]. Under duress, ProtonMail acquiesced to the demands and paid the ransom, however the attacks continued and actually strengthened. What remains unclear is whether the continued attacks were due to copycat groups or Armada Collective itself, as ProtonMail was somewhat public about the incident and Armada Collective denied involvement in the continued attacks.

[2] “DD4BC, Armada Collective, and the Rise of Cyber Extortion.” Recorded Future, <https://www.recordedfuture.com/dd4bc-cyber-extortion/>. December 7, 2015.

1. Overview
 2. Analysis
 - 3. Indicators**
 4. Area 1 Guidance
-

Indicators

Identifying Information

The following information may be able to be used to identify the threat actor. The actor may, and is expected to, stop using this identifying information in the future to maintain operational security.

Email Address

collective_armada@mail[.]ru

continued on next page

...

1. Overview
2. Technical Analysis
3. Indicators
4. **Area 1 Guidance**

Area 1 Guidance

Actions

- ✓ Do not pay the ransom. Funding the threat actor's operation may provide incentive for further attacks against you and peer providers in the future.
- ✓ Ensure that your Anti-DDoS solution is in working order.
- ✓ In the case that your organization experiences a DDoS attack, route the targeted domains to a null IP address.
- ✓ In order to minimize points of entry for any attacks, ensure that unnecessary and legacy internet services are disabled.

Defensive Guidance

- If your customers experience DDoS attacks over web port 80, consider using a Content Distribution Network (CDN) service such as Akamai or CloudFlare.