Abstract
With the value of bitcoin increasing in recent weeks, Radware is witnessing an increase in cyber-attacks driven by financially-motivated and ransom-based attacks. A group claiming to be the Armada Collective has sent out ransom notes to seven banks in South Korea. They are requesting $315,000 USD and threatening to knock the networks of these institutions offline on June 26, 2017 if the ransom is not paid. The group has launched sample 5Gbps cyber-attacks against these victims. Radware research is concerned these initial assaults could be followed by additional attacks throughout the world.

What is RDoS (Ransom DDoS)?
An RDoS is a distributed denial-of-service (DDoS) attack motivated by monetary gain. Attacks typically start with a letter or even a Twitter post threatening to launch an attack at a certain day and time unless a ransom is paid. To validate the threat, attackers will often launch a sample attack on the victim's network.

This method was initially introduced by DD4BC and has been replicated by the Armada Collective since 2015. Armada would accompany their ransom notes with a short "demo" attack. Armada Collective's attacks were methodical and achieved high success rates. Consequently, many hacker groups now imitate this modus operandi and spread similar ransom threats using other group names with no intention of launching an attack.

According to Radware's *2016-2017 Global Application and Network Security Report*, ransom is the #1 motivation behind cyber-attacks. One out of six organizations worldwide reported having received at least one such ransom note.[i]

Who is Armada Collective?
In 2014, a bitcoin extortionist group called DD4BC emerged. This group targeted institutions around the world with threats of DDoS attacks if a ransom in bitcoin was not paid. Two core members of DD4Bc were ultimately arrested in December 2015, but this did not stop the growth of ransom-based DDoS attacks.

In September 2015, a new group called the Armada Collective emerged targeting banks, e-commerce and hosting services in Russia, Thailand, Switzerland, and more. In November 2015, The Armada Collective launched one of their most famous campaigns. The group targeted several email service providers like ProtonMail, NeomailBox, VFEmail, HushMail, FastMail, Zoho, and Runbox.

Armada Collective had a very specific pattern of blackmailing only a handful of victims at a time. They would send their target a letter demanding a ransom be paid in bitcoin. To underscore the threat, the group would launch a sample attack for 15 to 30 minutes against the victims' network. If the ransom was not paid in the allotted time, the ransom would increase and the targets would face largescale and persistent multi-vector attacks.

This threat should be taken seriously, as it mirrors the same pattern as the original Armada Collective. In 2015, The Armada Collective would target a handful of companies in the same industry. When they attacked the email service providers, they only ransomed seven companies. This week, the group claiming to be the Armada Collective is only targeting eight financial institutions.

Copycats
In the spring of 2016, after a lull in RDoS attacks, a group emerged calling themselves the Armada Collective, but their modus operandi had clearly changed. This group claiming to be Armada Collective was no longer targeting a small number of victims but instead were targeting dozens of victims at once without launching a sample attack. As a result, these attackers were able to make thousands of dollars by taking advantage of public fear and a notorious name. Several other copycat groups that emerged in 2016 leveraging this method included New World Hackers and Lizard Squad.

RDoS in 2017

Other groups emerged in 2017, including XMR Squad and zzb00t. XMR Squad targeted companies in Germany and the United States[ii]. Companies like DHL, Hermes, AldiTalk, Freenet and Snipes all experienced denial-of-service attacks in the wake of not paying a ransom of 2-3 bitcoin to XMR Squad.

At the same time, there are several fake RDoS groups like Meridian Collective and Fancy Bear that are spamming extortion emails. Meridian Collective threatened to attack several corporations on June 16, 2017 if their ransom was not paid. These targeted corporations ultimately did not pay the ransom and were not attacked. To launch a series of denial-of-service attacks, the group will require vast resources. Therefore, when a group sends dozens of extortion letters, they typically will not follow through with a cyber-attack.

The name Armada Collective returned this week leveraging the same techniques as the original group. Armada Collective has sent out ransom letters to at least seven South Korean banks threatening to attack on June 26. This group is requesting approximation $315,000 USD from its victims. If payment is not rendered by the 26th, this group is threating to increase the ransom and knock the organizations offline.

$1M Ransom Paid by Navanna

Earlier this month, a hosting service in South Korea - Nayana[iii] - paid hackers $1,000,000 USD after becoming infected with a variant of ransomware called Erebus. It is believed that because this company paid the ransom, other criminals have chosen to target South Korean companies.

Delivery Methods

The main delivery method for RDoS is email. There are exceptions. Recently, the group XMR Squad and ZZb00t ran a ransom campaign using a Twitter account to deliver their ransom note.

Attack Vectors

Most of these RDoS groups are running their own network stressers, however some leverage publicly-available stressers to conduct their campaigns. When experiencing an RDoS attack, expect 100+ Gbps and multi-vector attacks simultaneously. The attack is likely to be persistent and last for days. Attack vectors used by Armada Collective include floods using the following protocols:

NTP: The attacker sends spoofed NTP packets, containing monlist request code, to the vulnerable NTP servers. Monlist is a command requesting a list of the last 600 hosts who connected to the addressed NTP server. The NTP servers then send large replies to the spoofed IP, the victim, thus flooding the victim. This attack generates a great deal of traffic and can easily cause DoS.

ICMP: Internet Control Message Protocol (ICMP) is a connectionless protocol used for IP operations, diagnostics, and errors. An ICMP Flood - sending an abnormally large number of ICMP packets of any type (especially network latency testing “ping” packets) - can overwhelm a target server that attempts to process every incoming ICMP request, until a denial-of-service condition for the target server.

SYN: A SYN flood overwhelms a target machine by sending thousands of connection requests to it using spoofed IP addresses. This causes the target machine to attempt to open a connection for each malicious request and subsequently wait for an ACK packet that never arrives. A server under a SYN flood attack will continue to wait for a SYN-ACK packet for each connection request, as the delay could be normal and related to network congestion. However, because a SYN-ACK packet never arrives for any of the connection requests; the massive number of half-open connections quickly fills up the server’s TCB table before it can time any connections out. This process continues for as long as the flood attack continues.

RDoS Groups (Fake/Real)

- DD4BC
- Armada Collective
- RedDoor
- exBTC
- Kadyrovtsy
- Borya Collective
- Lizard Squad (fake)
- Stealth Ravens
- XMR Squad
- ZZb00t
- FancyBear
- Xball
- Meridian Collective

Dealing with a Ransom Letter

Companies should be advised not to pay an extortionist and seek professional assistance for mitigating RDoS attacks. Such a threat usually provokes the need for a scrubbing service, ACL/BGP reconfiguration, as well as the usual DDoS protection essentials to assure uptime and SLA.

Evaluation – Is It Real or Fake

Although it is almost impossible to determine whether a ransom note comes from a competent hacker group or an amateur unit, there are several indicators to distinguish between the two:

- The fake groups often request a different amount of money than the original
- "Real" groups prove their competence; fake groups exclude the "demo" attack
- These groups do not have official websites or target lists
- When hackers launch real RDoS attacks, they normally target less than a dozen companies under the same industry
- Look for suspicious indicators. Is this group known for DDoS attacks? In the case of Fancy Bear, they do not launch DDoS attacks

Effective DDoS Protection Essentials:

- **Hybrid DDoS Protection** - (on-premise + cloud) – for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - to promptly protect from unknown threats and 0-day attacks
- **A Cyber-Security Emergency Response Plan** - that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further security measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

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://www.radware.com/ert-report-2016/
[ii] https://www.link11.com/en/press/detail/new-round-of-ddos-blackmailing-by-xmr-squad-allegedly/
[iii] http://www.bbc.com/news/technology-40340820