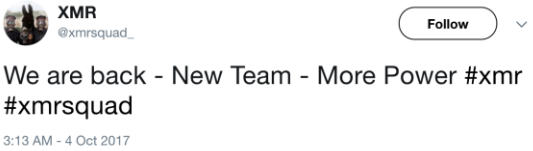
ERT Threat Alert

DDoS for Ransom (RDoS)

October 6, 2017

Abstract

Over the last few days Radware’s Emergency Response Team (ERT) has been tracking a number of RDoS (DDoS for Ransom) campaigns from groups claiming to be the Armada Collective and XMR Squad. XMR Squad has evidently been spamming (sending volumes of emails) ransom demands to multiple targets / prospective victims while in contrast, the Armada Collectives campaign has focused mostly on the financial sector in Central Europe.



XMR
@xmrsquad_

We are back - New Team - More Power #xmr #xmrsquad

3:13 AM - 4 Oct 2017

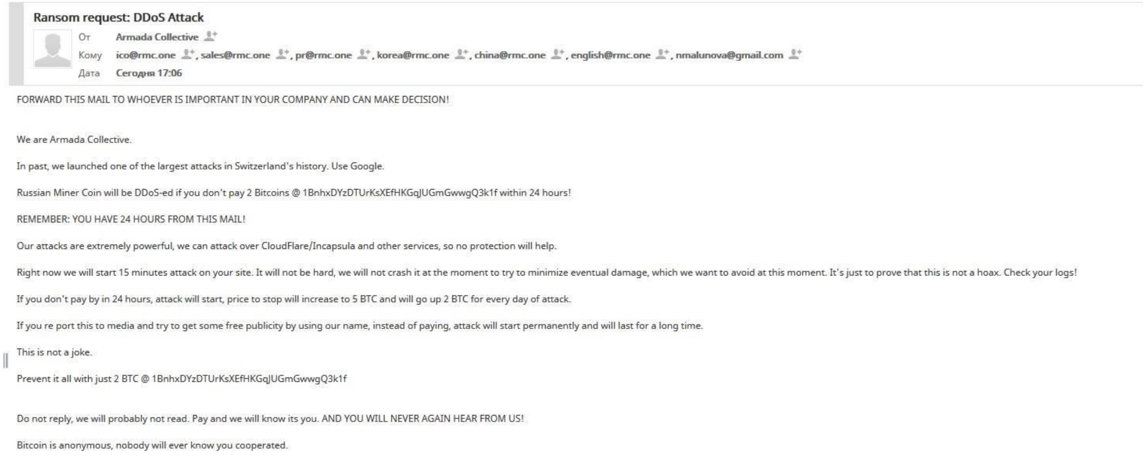
Figure 1: XMR Squad

Background

The original Armada Collective first surfaced in 2015 with a series of attacks on banks, e-commerce sites and hosting services in Russia, Thailand and Switzerland. The group would send ransom demands to a few companies in a single industry demanding Bitcoin under the threat of a largescale DDoS attack. To demonstrate their power, they would launch a sample attack. If the ransom was not paid in the allotted time, the target would face a persistent, multi-vector attack.

In the spring of 2016, after a lull in RDoS attacks, a new group emerged calling themselves the Armada Collective, but their modus operandi had changed. This group then targeted dozens of victims at once without launching a sample attack. RDoS campaigns can be financially rewarding to cyber-criminals for little to no investment. Because of this, many other hacking groups started imitating this new methodology The result was an explosion in RDoS cases from hackers using infamous names like Armada Collective and Anonymous to spread fear and gain credibility for their threat.

This week a group claiming to be the Armada Collective re-emerged in central Europe. This group closely followed the modus operandi of the original Armada Collective and has been observed targeting a handful of cryptocurrency companies. The group sent a ransom note to its victims that is very similar to the original Armada Collective ransom note. The group has demanded 2 Bitcoin under the threat of a DDoS and has been observed launching sample and follow through attacks.



Ransom request: DDoS Attack

От Armada Collective
Кому ico@rmc.one, sales@rmc.one, pr@rmc.one, korea@rmc.one, china@rmc.one, english@rmc.one, nmalunova@gmail.com
Дата Сегодня 17:06

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

In past, we launched one of the largest attacks in Switzerland's history. Use Google.

Russian Miner Coin will be DDoS-ed if you don't pay 2 Bitcoins @ 1BnhxDYzDTUrKsXEfHKGqJUGmGwwgQ3k1f within 24 hours!

REMEMBER: YOU HAVE 24 HOURS FROM THIS MAIL!

Our attacks are extremely powerful, we can attack over CloudFlare/Incapsula and other services, so no protection will help.

Right now we will start 15 minutes attack on your site. It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by in 24 hours, attack will start, price to stop will increase to 5 BTC and will go up 2 BTC for every day of attack.

If you re port this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Prevent it all with just 2 BTC @ 1BnhxDYzDTUrKsXEfHKGqJUGmGwwgQ3k1f

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

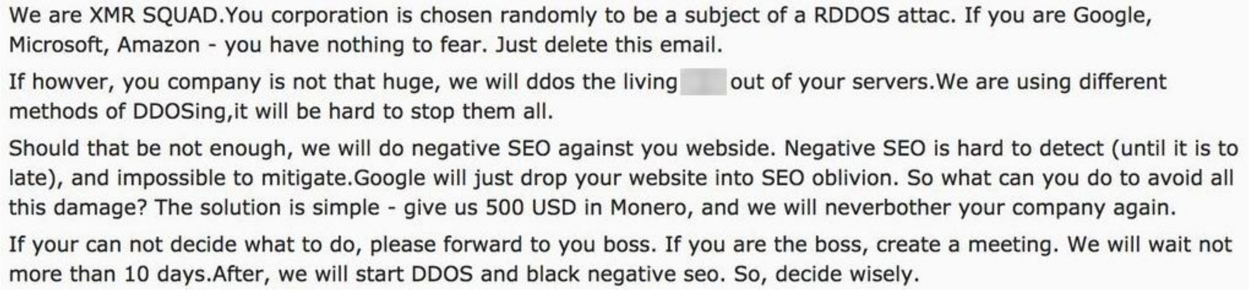
Figure 2: Ransom note sent to RMC from Armada Collective

Earlier this year Radware's ERT began tracking an RDoS group going by the name XMR Squad. This group was observed in May targeting companies in Germany and the United States. Targeted companies experienced a denial-of-service attack from the original XMR Squad if a ransom was not paid.

XMR Squad originally demanded 250 euros for testing their victim's DDoS mitigation system and followed through with their original threats. Shortly after their disappearance a different group going by the name XMR Squad appeared requesting 2-3 Bitcoins under a threat of a 300-600Gbps attack. The time for payment in that campaign was 24 hours.

More recently the group going by the name XMR Squad has not been following through with their original threats. Radware's ERT has received a large number of extortion letters from XMR Squad recently but never observed a sample or follow-through attack after the original group disappeared. The ransom demand in the most recent case was poorly written, looked nothing like prior demands and switched from BTC to Monero In addition, the window for payment was 10 days. This kind of time allows targeted victims time to put mitigation and an emergency plan in place.

It's believed that XMR Squad has no idea who they have ransomed in this current campaign. In their note they state, "If you are Google, Microsoft, Amazon – you have nothing to fear. Just delete this email." There is a low probability of XMR launching an attack during this campaign based on historical analysis, but with the Armada Collective launching attacks in central Europe again, those that receive any ransom note from an extortionist should take the proper steps to prepare for an attack in the event that XMR Squad changes their modus operandi.



We are XMR SQUAD.You corporation is chosen randomly to be a subject of a RDDOS attac. If you are Google, Microsoft, Amazon - you have nothing to fear. Just delete this email.

If howver, you company is not that huge, we will ddos the living [redacted] out of your servers.We are using different methods of DDOSing,it will be hard to stop them all.

Should that be not enough, we will do negative SEO against you webside. Negative SEO is hard to detect (until it is to late), and impossible to mitigate.Google will just drop your website into SEO oblivion. So what can you do to avoid all this damage? The solution is simple - give us 500 USD in Monero, and we will neverbother your company again.

If your can not decide what to do, please forward to you boss. If you are the boss, create a meeting. We will wait not more than 10 days.After, we will start DDOS and black negative seo. So, decide wisely.

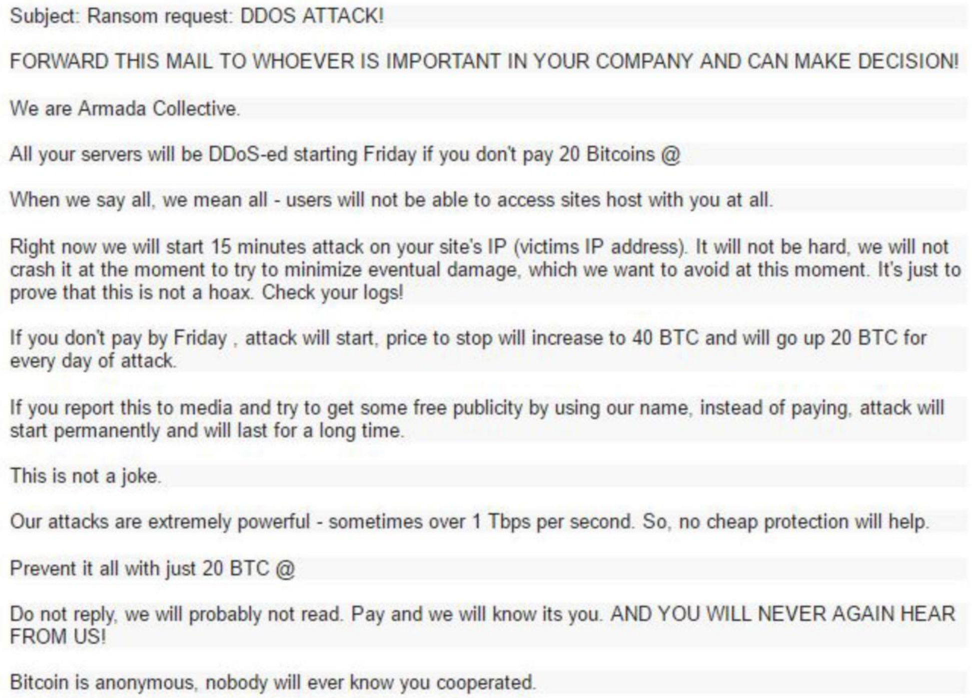
Figure 3: Ransom demand from XMR Squad (Reddit)

Reasons for Concern

In 2016, ransom was the number one motivation behind cyber-attacks; half of organizations were subject to this extortion threat, according to Radware's *2016-2017 Global Application & Network Security Report.* In parallel to the ransomware plague, Radware witnessed an emerging trend of hackers (and copycats) that extort organizations by posing an imminent threat of DDoS attacks – one out of six organizations was a victim. As IoT botnets have become more powerful, Radware has witnessed an increase in the number of DDoS for ransom attacks (RDoS attacks) threats that companies have received in 2017.

RDoS campaigns can be financially rewarding to a cyber-criminal who enjoys making large amounts of money for little to no investment. Because of this, many hacking groups now imitate this model and spam similar ransom threats using other group names, with no intention of launching an attack.

The main reason for concern with the recent campaign is the pattern of not following through with an attack has been broken. The Armada Collective has recently demonstrated that its threats are serious by launching sample attacks and following through with the original threat. This demonstrates a shift in the RDoS threat landscape. Companies targeted should take these threats seriously as the group claiming to be the Armada Collective is launching attacks again.



Subject: Ransom request: DDOS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @

When we say all, we mean all - users will not be able to access sites host with you at all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by Friday , attack will start, price to stop will increase to 40 BTC and will go up 20 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Prevent it all with just 20 BTC @

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

Figure 4: Original Armada Collective Demand (2015)

Targets

Armada Collective

- Financial Services in Central Europe (Crypto Currencies)
- Countries which seem to have a lot of focus on them:
  - Slovakia
  - Slovenia
  - Eastern-Europe / Former Soviet Union (FSU) Crypto Currency companies

XMR Squad

- Global Spamming

Attack Vectors

Most of these DDoS for ransom groups that actually launch attacks are running their own **network stressers**, however some leverage publicly-available stressers to conduct campaigns. When experiencing a DDoS for ransom attack, expect 100+ Gbps and multi-vector attacks simultaneously. The attack is likely to be persistent and last for days. Attack vectors include floods using the following protocols:

- SSDP
- NTP
- DNS
- UDP
- TCP RST
- TCP SYN

- SYN Flood
- SYN ACK
- SSYN
- ICMP

Dealing with a Ransom Letter

Companies are 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 hacking group or an amateur unit, there are several indicators to distinguish between the two:

- The fake RDoS 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 ransomware 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-premises + **cloud DDoS protection**) – 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 **DDoS protection** 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.