Background

Apparently, ransom cyber threats are not only about encrypting files. Over the past week, there has been an exponential increase in DDoS for ransom threats. This is an increasingly popular tactic of extortion and financial gain for hackers and hacktivists alike - "if payment isn't received, a cyber-attack will be launched that can result in damaged reputation and lost customers/revenue."

This method was initially introduced by DD4BC and replicated by the Armada Collective in late 2015. Armada accompanied their ransom notes with a short "demo" attack. When the time for payment expired, Armada took down the victims' data centers with traffic volumes typically exceeding 100Gbps.

The Armada Collective's attacks were gradual and methodical and achieved high success rates. Consequently, many hacking groups now imitate this modus operandi and spread similar ransom threats while the major groups continue to launch their threats and attacks.

Handling a Ransom Note

Although it is almost impossible to determine whether a ransom note comes from a competent, experienced hacker group or an amateur unit - some units emerged under the guise of a notorious DDoS for ransom group – **do not decry a ransom note**. While these fake groups send emails nearly identical to real ransom letters, there are a number of indicators to distinguish between the two:

1. The fake groups often request a different amount of money
2. "Real" groups prove their competence; fake groups exclude the "demo" attack
3. These groups do not have official accounts, websites or target lists
4. When hackers launch a real ransom attack, they normally target many companies under the same industry (see the ProtonMail case study)

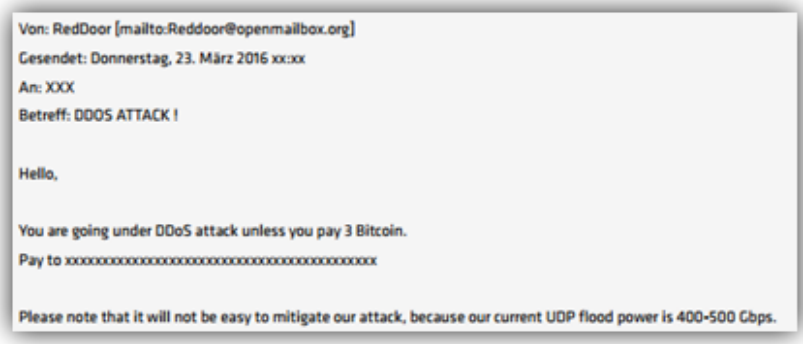
It is recommended to have several experts examining the ransom letters in order to ascertain its origin.

Ransom DDoS Groups

- DD4BC
- Armada Collective
- RedDoor
- ezBTC Squad

Delivery Methods

The main delivery method from a DDoS for ransom group is via email. There are exceptions to this rule however. Recently, the group ezBTC Sqaud attempted to run a ransom campaign using a Twitter account to deliver their ransom note. Below are just a few examples an organization could experience when being targeted by a ransom campaign.


Von: RedDoor [mailto:Reddoor@openmailbox.org]
Gesendet: Donnerstag, 23. März 2016 xx:xx
An: XXX
Betreff: DDOS ATTACK !

Hello,

You are going under DDoS attack unless you pay 3 Bitcoin.
Pay to xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps.

Figure 1: DDoS Threat Message by "Reddoor"

From: "Armada Collective" armadacollective@openmailbox.org
To: abuse@victimdomain; support@victimdomain; info@victimdomain
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 @ XXX

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 @ XXX

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: DDoS Threat Message by "Armada Collective"

Figure 3: DDoS Threat Message by "ezBTC Sqaud"

Attack Vectors

Most of these DDoS for ransom groups are running their own network stressers, however some leverage publicly available stressers to conduct their campaigns. When experiencing a DDoS for ransom attack, expect +100Gbps 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

Full list of DDoS tools and techniques at Radware's DDoSPedia

Targeted Industries

- Financial
- E-Commerce
- Web services
- Retail

Organizations Under Attack Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe
- A hybrid solution that includes on-premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A solution that provides protection against sophisticated web-based attacks and website intrusions to prevent defacement and information theft.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.
- Monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

In addition, we recommend inspecting and patching your network often is necessary in order to defend against these types of risks and threats as they evolve.

Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

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.