## Abstract

Over the last week, Radware's Emergency Response Team (ERT) has been tracking a DDoS-for-ransom campaign (RDoS) from a group claiming to be Phantom Squad, a group that made public threats to DDoS Steam, Xbox Live and PlayStation Network in December of 2015.

An RDoS campaign is a distributed denial-of-service (DDoS) attack motivated by monetary gain. Attackers typically start with an email or a post threatening to launch an attack at a certain day and time unless a ransom is paid, usually in Bitcoin. In some cases, attackers will launch a sample attack on the victim's network as evidence that the threat is real.

The group posing as Phantom Squad began spamming out ransom demands on September 19th and has reportedly targeted thousands of companies throughout Europe, Asia and the United States. The group is currently requesting .2 BTC under the threat of a DDoS attack to be launched on September 30th if the ransom is not paid.

Due to the number of victims in this campaign and low ransom demand, it's unlikely that this group posing as Phantom Squad will follow through on their threats. To date, no sample attacks have been reported against targeted networks. Furthermore, to launch a series of denial-of-service attacks of this scale, 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. Companies should be advised to not pay the ransom demands.

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

We are Phantom Squad

Your network will be DDoS-ed starting Sept 30st 2017 if you don't pay protection fee - 0.2 Bitcoin @

If you don't pay by Sept 30st 2017, attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

This is not a joke.

Figure 1: Ransom demand from 'Phantom Squad'

## Reasons for Concern

In 2016, ransom was the #1 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 has witnessed an emerging trend of hackers (and copycats) who extort organizations by posing an imminent threat of DDoS attacks. As IoT botnets have become more powerful, Radware has witnessed an increase in the number of RDoS 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 modus operandi and spam similar ransom threats using other group names, with no intention of launching an attack. In 2016, many opportunists emerged using infamous names like the Armada Collective, Anonymous and Lizard Squad to spread fear and gain credibility for their threats. This year, Radware has witnessed groups pretending to be Fancy Bear, Armada Collective, Anonymous and Phantom Squad.

## Targets

Currently, Radware has witnessed ransom letters targeting companies in the following industries:

- Manufacturing
- Technology
- Education

## Attack Vectors

Most of these RDoS groups that actually launch attacks run 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 include floods using the following protocols:

- SSDP
- NTP
- DNS
- UDP
- TCP RST
- TCP SYN
- SYN Flood
- SYN ACK
- SSYN
- ICMP

## Delivery Methods

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

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

- "Real" groups prove their competence by launching a “demo attack; 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 and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - 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, it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.