DDoS Attack Group Extortion sent requests to extort money to thousands of companies

A group of DDoS Extortion attackers, known as Phantom Squad, have sent many spam messages to thousands of companies, threatening DDoS attacks on September 30 if victims don't pay.

A group of misleading attackers (translating from DDoS Extortion) using the name Phantom Squad sent many spam messages to thousands of companies worldwide, threatening DDoS attacks on September 30 if the victim did not pay money.

The e-mail was first discovered by researcher Derrick Farmer and is believed to have started from September 19 until now.

Hacker only asks for a $ 700 ransom

Email threatens to require companies to pay 0.2Bitcoin (about $ 720) or prepare the website to collapse. Usually these emails are sent to few companies so that bad guys attack when they don't pay.

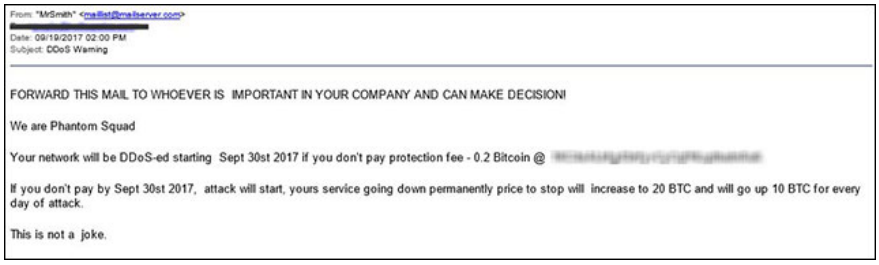
This time the attacker sent many people at the same time, the familiar type of spam to spread malware. Therefore, some experts claim that they are not able to perform DDoS attacks on many of these targets in a day, perhaps just a threat and hope the victim will pay.

Deflection is not the sharpest tool

The number of spam emails surprised many experts. Its impact can be found on social networks and webmaster forums, where sysadmin seek help.

'Recycle' email snippet

Radware engineers also received similar emails, so much so that they had to issue a security warning. Researcher Daniel Smith at Radware also points out that they may not be the real Phantom Squad. This is a DDoS attack group that has reduced many game networks in 2015.


From: "MrSmith" <[redacted]>
[redacted]
Date: 09/19/2017 02:00 PM
Subject: DDoS Warning

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 @ [redacted]

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.

Email segment with fairly simple content of the attacker

Smith noticed that the extortion note was similar to the note used by the Armada Collective group in June 2017. This case turned out to be harmless.

Experts say they cannot attack DDoS

This shows evolution in DDoS extortion attacks (RDoS) when attackers move from small groups of businesses to large groups in hopes of receiving money from many victims.

'The attacker can earn thousands of dollars through public fear. Some copycat groups emerged from 2016 and 2017 like New World Hackers, Lizard Squad, LilzSec, Fancy Bear and Anonymous, 'Smith said. 'In order for a denial of service to be in need of great resources. When sending so many emails, they cannot perform the attack. '