Abstract
Over the last week, Radware's Emergency Response Team (ERT) has been tracking an emerging ransom denial-of-service (RDoS) campaign from a group identifying itself as Fancy Bear. The group has been distributing extortion emails to payment processing vendors in multiple locations across the globe.

Figure 1: Fancy Bear RDoS note

Background
In RDoS attacks, the perpetrators send a letter threatening to attack an organization—rendering its business, operations or capability unavailable—unless a ransom is paid by the deadline. This extortion method has grown in popularity every year since 2010 and typically come in the form of a volumetric distributed denial-of-service (DDoS) attack. However, it is increasingly in vogue to find techniques that are more piercing and more efficient without generating large volumes. The most advanced attacks combine both volumetric and non-volumetric cyber-attack techniques. The success of such cyber-extortion campaigns has led to many copycats that simply distribute emails at all directions hoping to be paid.

At the end of April, a group claiming to be Fancy Bear began sending out extortion attempts. The extortionist behind this campaign attempted to intimidate their victims by using the name of APT28 (Fancy Bear) and an infamous cyber-espionage group. APT28 is believed to be a nation state-level attacker that uses zero-day exploits and spear phishing attacks to spread malware. RDoS attacks were not the typical modus operandi for Fancy Bears' attacks to date.

However starting in November, Fancy Bear's name is appearing on extortion letters in this new RDoS campaign. This time, Fancy Bear is requesting between 1-2 bitcoins with the ransom increasing by one bitcoin every day without payment.

What is RDoS
RDoS campaigns are extortion-based distributed denial-of-service attacks 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 RDoS attacks were methodical and achieved high success rates. Today, many hacker groups imitate this modus operandi and spread similar ransom threats using other group names as a form of intimidation with no intention (or limited capacity) of launching an attack.

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. 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 model and spam similar ransom threats using other group names, with no intention of launching an attack.

We are the Fancy Bear and we have chosen your company as target for our next DDoS attack.

Please perform a google search for "Fancy Bear" and "Mirai Botnet" to have a look at some of our previous "work".

Your network will be subject to a DDoS attack starting at [Ransom Deadline]

(This is not a hoax, and to prove it right now we will start a small attack on xxx.xxx.xxx.xxx and xxx.xxx.xxx.xxx that will last for 30 minutes. It will not be heavy attack, at this moment.)

What does this mean?

This means that your website and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation amongst your users / customers.

How do I stop this?

We are willing to refrain from attacking your servers for a small fee. The current fee is 1 Bitcoin (BTC). The fee will increase by 1 Bitcoins for each day after [Ransom Deadline] that has passed without payment.

Please send the bitcoin to the following Bitcoin address:

[Bitcoin Address]

Once you have paid we will automatically get informed that it was your payment. Please note that you have to make payment before the deadline or the attack WILL start!

What if I don't pay?

If you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution (Cloudflare, Incapsula and similar services are useless). We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again!

Please note that Bitcoin is anonymous and no one will find out that you have complied.

Figure 2: Current Fancy Bear extortion email

Targets

Currently the group claiming to be Fancy Bear is targeting a limited number of financial services organizations – payment processers under the threat of an attack from the Mirai Botnet. Each letter contains a unique bitcoin address. In the note, Fancy Bear listed the IP address of the victim and targeted them with a sample attack. As of this moment, no follow through attacks have been observed.

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 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

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.

Organizations Under Attack Should Consider

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 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 RDoS 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.