ERT Threat Alert
Global RDoS Campaign – Fancy Bear
October 25, 2019

Abstract

Over the last week, Radware's Emergency Response Team (ERT) has been tracking an emerging global ransom denial of service (RDoS) campaign from a group identifying itself as the Russian cyber espionage group, Fancy Bear. This campaign is similar to the one Radware reported on two years ago[1]. This new group has been distributing extortion emails to financial institutions globally for the past week. As of this moment, victims are still receiving ransom notes.

Background

In mid-October 2019, Radware's ERT began mitigating sample attacks launched by an RDoS group claiming to be Fancy Bear. The extortionists currently behind this campaign attempted to intimidate their victims by using the name of APT28 (Fancy Bear), an infamous cyber-espionage group. APT28 is a Russian-backed cyber espionage group that is also known as Pawn Storm, Sofacy Group, Tsar Team and Fancy Bear and is notorious for international hacking related to influence and disinformation operations. RDoS attacks are not the modus operandi for Fancy Bears' to date.

Starting in October 2019, almost 2 years after the first major campaign leveraged the name, Fancy Bear began appearing on extortion letters again in a new RDoS campaign. This time, Fancy Bear is requesting 2 bitcoins, $17,400 at the time of delivery, with the ransom increasing by one bitcoin every day without payment.

Subject: DDoS attack

We are the Fancy Bear and we have chosen [Victim] as target for our next DDoS attack.

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

Your network will be subject to a DDoS attack starting at [Deadline] (in X days).

(This is not a hoax, and to prove it right now we will start a small attack on your [Target] that will last for 30 minutes. It will not be heavy attack, and will not cause you any damage so don't worry, 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 will refrain from attacking your servers for a small fee. The current fee is 2 Bitcoin (BTC). The fee will increase by 1 Bitcoin for each day after deadline that passed without payment.

Please send 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 on 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, Sucuri, Imperva 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 1: 2019 Fancy Bear Extortion Letter (Current)

[1] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/fancybear/

ERT Threat Alert
Global RDoS Campaign – Fancy Bear
October 25, 2019

What is an RDoS Campaign?

RDoS campaigns are extortion-based distributed denial-of-service (DDoS) attacks motivated by monetary gain. Attacks typically start with the perpetrators sending a letter threatening to attack an organization—rendering its business, operations or capability unavailable—unless a ransom is paid by the deadline. To validate the threat, attackers will often launch a sample attack on the victim's network.

This extortion method has grown in popularity every year since 2010 and typically comes in the form of a volumetric distributed denial-of-service (DDoS) attack. The method was initially introduced by DD4BC and has been replicated by several groups over the years. RDoS group will typical accompany their ransom demand with a short "demo" attack.

Prior RDoS groups were methodical and achieved high success rates. However, today many groups imitate prior tactics and techniques. They spread similar ransom threats using other group names as a form of intimidation with no intention (or limited capacity) of launching an attack.

Targets

Currently the group claiming to be Fancy Bear is targeting a number of financial services organizations around the world. Attacks have been observed in South America, Africa, Northern Europe and parts of Asia. In the note, the attackers list a specific IP address of the victim network and target it with a sample attack. The selection of the specific IP address shows that the attackers are researching targeted network for maximum impact. As of this moment, sample attack range between 40-60gbps. No follow-up attacks have been observed.

Attack Methods

Most of these DDoS-for-ransom groups that launch attacks are running their own botnet, however some leverage publicly available stressers to conduct campaigns. When experiencing a RDoS attack from this type of group, expect 40-60Gbps and multiple vectors of attacks simultaneously. A sample attack is likely to last anywhere between 15 minutes to a few hours. In the past, Radware's ERT has mitigated follow-up attacks that have been persistent and lasted for days. Current attack vectors in this campaign include floods using the following protocols:

- SSDP
- NTP
- DNS
- CLDAP
- WSD
- ARMS
- SYN
- ICMP

The group carrying out the recent wave of RDoS attacks under the name Fancy Bear are currently launching large scale, multi-vector demo DDoS attacks when sending victims the ransom note. One of the more notable attack vectors from this campaign was the use of Web Service Dynamic Discovery (WSD) protocol, UDP/3702 for amplification. While this attack vector has been known since the beginning of the year, no one publicly spoke about it until the third quarter when details began to slowly emerge that botherders had employed a new attack vector into their amplification toolkit.

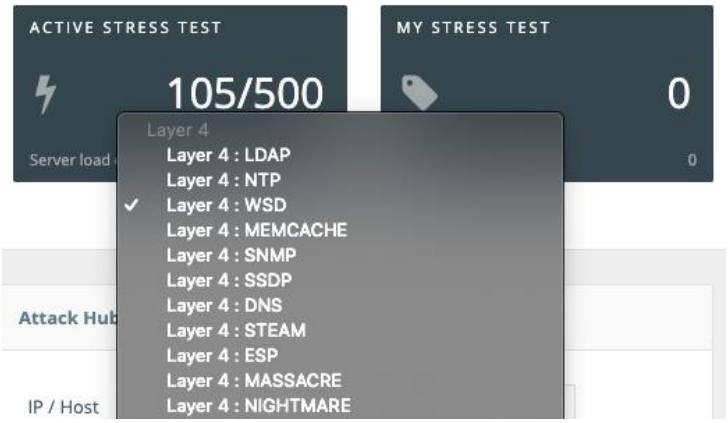

Figure 2: WSD Attack Vector Offered via DDoS-for-Hire

Another notable attack vector from this campaign is the newly discovered vector that allows attackers the ability to abuse Apple's Remote Management Service (ARMS) to launch an amplified denial-of-service attack. By sending malicious datagrams to exposed ARMS services on UDP/3283, attackers could gain an amplification factor of 35.5 to 1.

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, experienced hacker group or an amateur unit - some units emerged under the guise of notorious hacking crews. While these fake groups send emails nearly identical to real ransom letters, there are several 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 real DDoS for ransom attacks, they normally target many companies under the same industry
5. Look for suspicious indicators. Is this group known for DDoS attacks?

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 3: 2017 Fancy Bear Extortion Letter

Effective DDoS Protection Essentials

- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks. In this current campaign Radware's ERT has been able to mitigate all vectors of attacks from the Fancy Bear RDoS group.
- **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
- **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 **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats. 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.