EMBARGO – Thursday, June 10, 5:00 AM EST

Ransom DDoS Extortion Actor "Fancy Lazarus" Returns

Key Takeaways

- The ransom distributed denial of service extortion threat actor known as "Fancy Lazarus" is back, taking aim at an increasing number of industries, including the energy, financial, insurance, manufacturing, public utilities, and retail sectors.
- There is no known connection between this group and the APT actors with the same names.
- These latest campaigns have some differences to previous campaigns, including a change to the group's name, the amount of Bitcoin being ransomed, and variations in the email body content.
- While it is not possible for organizations or companies to avoid being the target of such attacks, there are indications that most such threats either do not materialize into an actual attack or they are successfully mitigated.

Overview

As of May 12, 2021, Proofpoint researchers are tracking renewed distributed denial of service (DDoS) extortion activity targeting an increasing number of industries, including the energy, financial, insurance, manufacturing, public utilities, and retail by the threat actor "**Fancy Lazarus.**" Proofpoint researchers have observed the activity primarily at U.S. companies or those with a global footprint. The actor took over a month-long break from April to May 2021 before returning with new campaigns that include some changes to the group's tactics, techniques, and procedures:

- New name: The group, who have previously identified themselves as "Fancy Bear", "Lazarus," "Lazarus Group," and "Armada Collective," among others, is now going by "Fancy Lazarus." There is no known connection between this group and the APT actors with the same names.
- New price: The extortion emails now have adjusted ransom pricing, lowering it from ransoms as high as ten Bitcoin (BTC) to its current two BTC starting price. This change is likely to account for Bitcoin's fluctuating value.
- Variation in email content: In terms of email body content, the specific variant is reminiscent of the original variants from August 2020 with some minor changes and evolutions. It is interesting that the group is still going back and tweaking the original email, potentially indicating its effectiveness. Between August 2020 and now, however, they have tried completely different text in the emails.

Background

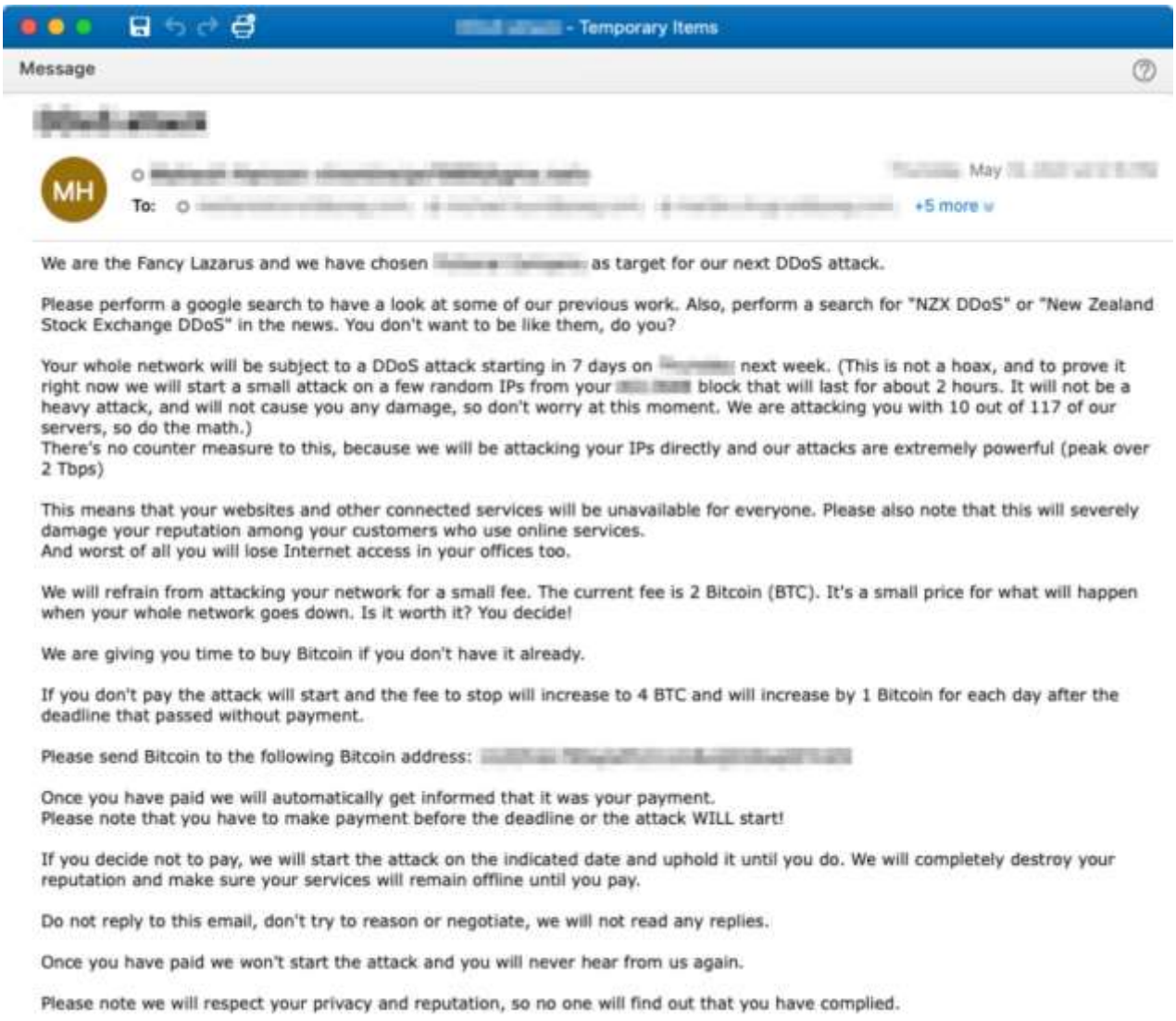
EMBARGO – Thursday, June 10, 5:00 AM EST

In mid-to-late August 2020, Akamai and the U.S. Federal Bureau of Investigations (FBI) alerted organizations to a spate of ransom denial-of-service extortion emails from this group. According to the published reports, this group took aim at thousands of organizations from multiple global industry verticals. In each case the threat actor demanded Bitcoin payment or else a small-scale denial-of-service attack would be launched with a more substantial attack mere days later.

Campaign Details

The campaigns always begin with sensational emails. The current iteration, as illustrated in Figure 1, starts with an announcement of the name the group uses currently and an acknowledgement that they are targeting a specific company. They then threaten a DDoS attack in seven days, and, to prove it is not a hoax, mention a "small attack" that will be launched on a specific IP, subnet, or Autonomous System. The emails claim that the max attack speed will be "2 Tbps." They also warn about potential damage to the target company's reputation and loss of internet access at their offices almost certainly to further coerce the victim into complying with their demands.

EMBARGO – Thursday, June 10, 5:00 AM EST



- Temporary Items

Message

MH

To: +5 more

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

Please perform a google search to have a look at some of our previous work. Also, perform a search for "NZX DDoS" or "New Zealand Stock Exchange DDoS" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in 7 days on next week. (This is not a hoax, and to prove it right now we will start a small attack on a few random IPs from your block that will last for about 2 hours. It will not be a heavy attack, and will not cause you any damage, so don't worry at this moment. We are attacking you with 10 out of 117 of our servers, so do the math.)
There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services.
And worst of all you will lose Internet access in your offices too.

We will refrain from attacking your network for a small fee. The current fee is 2 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to 4 BTC and will increase by 1 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following 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!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. 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 we will respect your privacy and reputation, so no one will find out that you have complied.

Figure 1. Example of current emails being sent by "Fancy Lazarus."

Each of the campaigns is also characterized by the following elements:

- **Recipients:** The emails are typically sent to well researched recipients, such as individuals listed as contacts in Border Gateway Protocol (BGP) or Whois information for company networks. The emailed individuals also work in areas such as communications, external relations, investor relations. Additionally, extortion emails are often sent to email aliases such as help desk, abuse, administrative contacts, or customer service.
- **Email body:** There are three email variants sent to the same recipients conveying the same information, except with the email body in plain text, HTML, or as a JPG image attachment. This is a likely an attempt to evade detections.
- **Sender emails:** Each sender email is different and unique to the targeted company. Previously the sender often contained "Fancy Bear," "F.B.," "Armada Collective," "A.C.," "Lazarus," or "Lazarus Group," and even at times included the targeted company's

highest-ranking person such as the CEO's name. In the most current campaign, a random "First name Last name" format is used and the names appear fictional.

- **Sender email provider:** Each email is created at one of the various free email services.
- **Payment:** Proofpoint has observed ransom demands of two BTC, which roughly equated to $76,000 USD on May 26, 2021. The price doubles to four BTC after the deadline and increases by one BTC each day after that. The Bitcoin addresses are unique to each potential target.

Conclusion

While Proofpoint does not have visibility into the actual "Fancy Lazarus" DDoS attacks and whether they are carried out, FBI reporting indicates that many affected companies that pass the threatened deadline either do not see any additional activity or the activity is successfully mitigated. There are, however, several prominent institutions that have either received attack demonstrations or reported an impact to their operations, so it is important for companies and organizations to be prepared by having appropriate mitigations in place such as using a DoS protection service and having disaster recovery plans at the ready.