Ransom DDoS Extortion Actor "Fancy Lazarus" Returns

p **proofpoint.com**/us/blog/threat-insight/ransom-ddos-extortion-actor-fancy-lazarus-returns

Blog

Threat Insight

Ransom DDoS Extortion Actor "Fancy Lazarus" Returns

June 10, 2021 Axel F

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

In mid-to-late August 2020, Akamai and the U.S. Federal Bureau of Investigation (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.
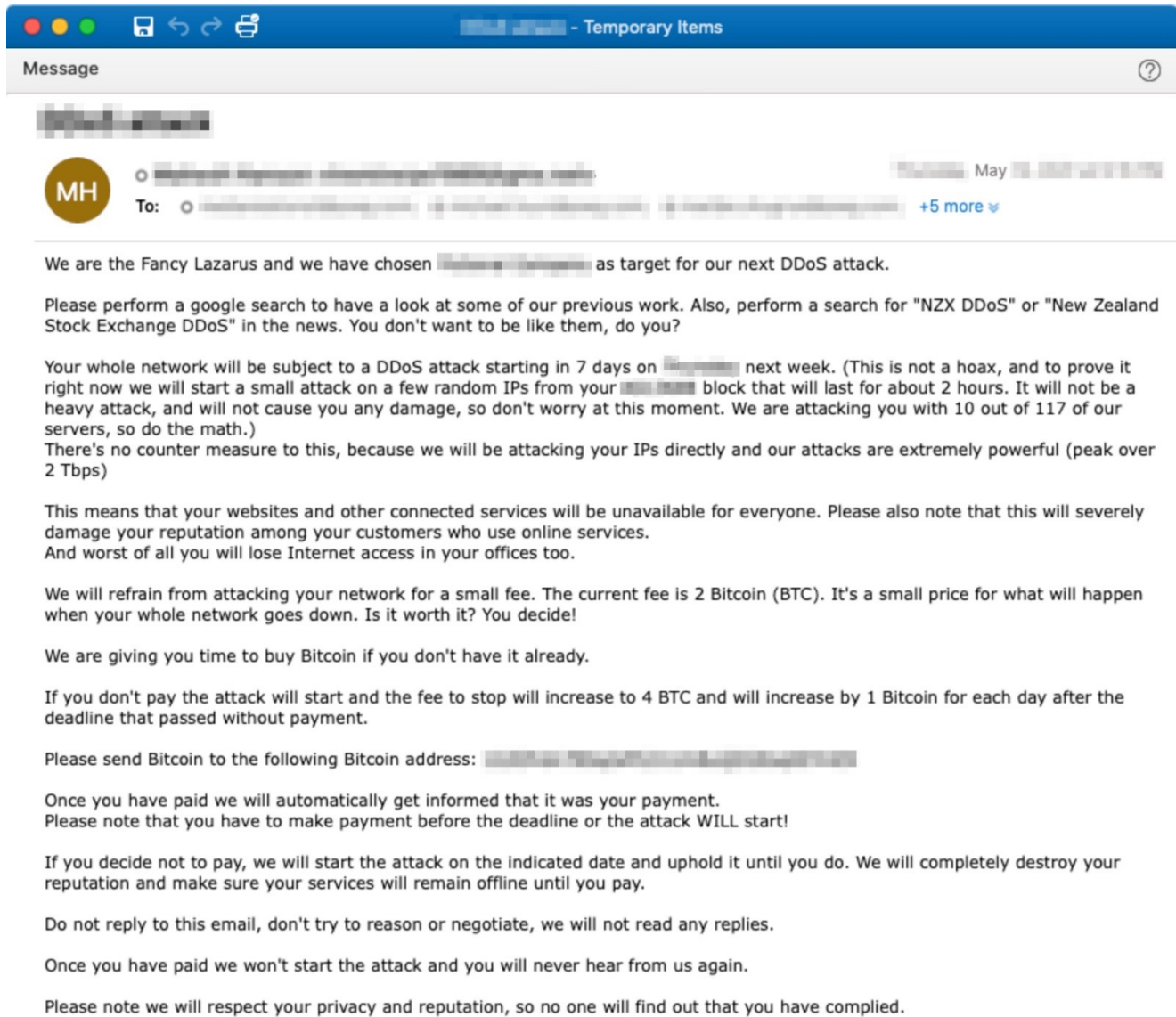
Figure 1. Example of current emails being sent by "Fancy Lazarus."

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.

EDIT (Added on 06/11/21)

A recent report by Akamai also notes a resurgence of this activity since May 2021 and provides a great amount of details and examples on the specific nature of the DDoS traffic.

Is your organization protected from extortion threat actors? Learn about Ransomware Attacks.

Subscribe to the Proofpoint Blog