Ransom DDoS Update: The Hunt For Unprotected Assets

"Fantasy APT Seeking Unprotected Assets"

JUNE 11, 2021

In the past few weeks, Radware's Cloud DDoS Protection Service has been seeing a significant increase in DDoS activity and has been rapidly onboarding new customers in distress. Several internet service providers (ISPs) and cloud service providers (CSPs) have reported receiving ransom letters followed by DDoS attacks that impacted their services and availability. Going by the name "Fancy Lazarus," the action radius of this extortion group has been extending to organizations of all sizes across the world and in all verticals. No target is too small or too big.

A DDoS extortion group identifies and targets organizations with unprotected assets and invites them to pay a ransom while threatening with devastating DDoS attacks.

Background

"Fantasy APT looking for unprotected assets," sounds like a classified advertisement you typically find in the newspaper. While it might sound entertaining, it very much describes the latest tactics employed by DDoS extortionists. It has been almost a year since a malicious actor, going by the names "Fancy Bear" and "Lazarus Group," started targeting finance, travel and e-commerce organizations in what has been one of the most extensive and longest-running DDoS extortion campaigns in history.

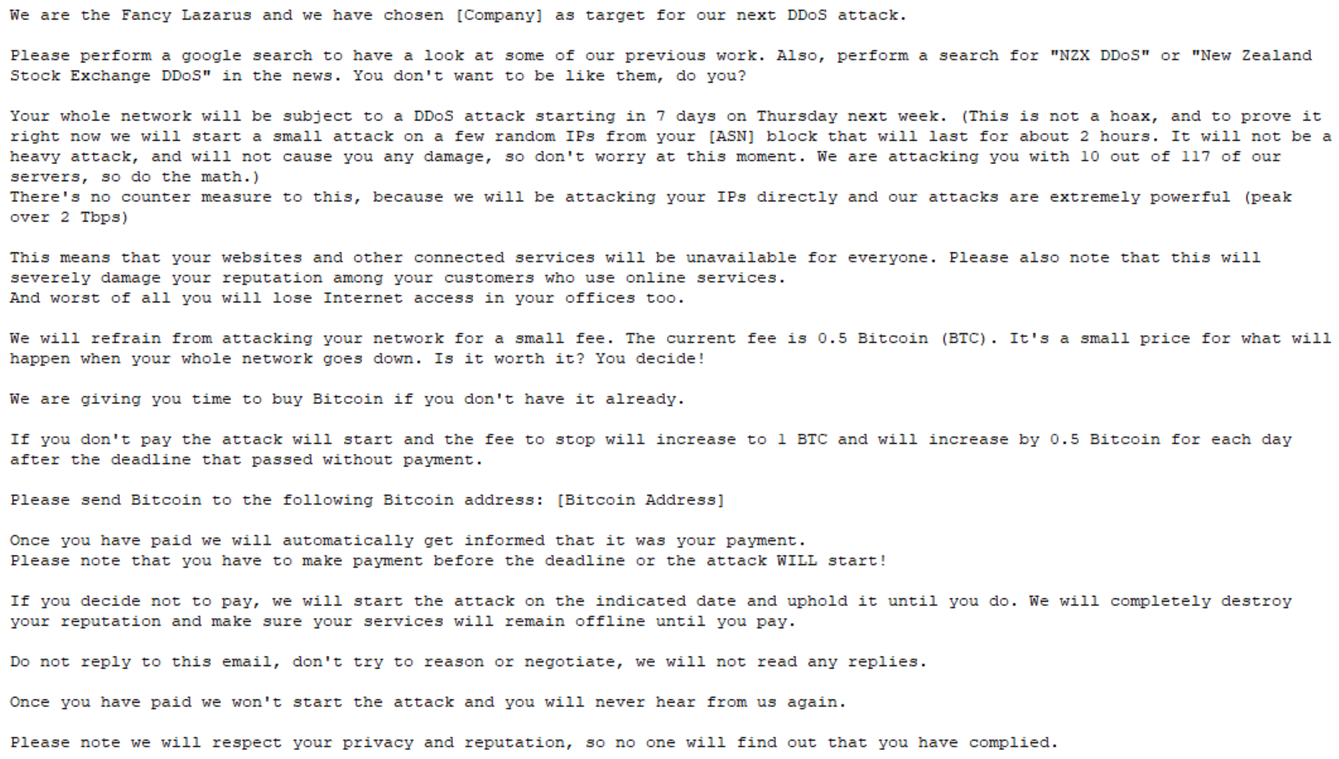
In a ransom DDoS **update**, Radware covered the tactic of circling back and how extortionists were trying to accelerate their campaign to profit from the surge in Bitcoin. In that update, we noted that ransom DDoS, which have historically been short-term events, have become a persistent threat and should now be considered an integral part of the DDoS threat landscape.

Over three weeks ago, DDoS extortionists have been sending ransom letters to ISPs and CSPs posing as "Fancy Lazarus." In an attempt to instill fear in their victims and pressuring them to comply with their demands, the actors created a new "super" APT moniker, a polynomial consisting of an equal part "Fancy Bear," the **Russian APT** and a part "Lazarus," the **North Korean APT.**

In their letter, the extortionists allow their victims seven days to purchase Bitcoin and pay the ransom before beginning DDoS attacks. The fee increases each day after the deadline passes without payment. The ransom demand varies between targets and seems to be adjusted to the target's reputation and size. The ransom demand is also more "acceptable" compared to the huge demands of 10 - 20 bitcoin ($370,000 and $740,000 at the time of publication) in the August campaigns. Demands now vary between 0.5 ($18,500), 2 ($75,000) and 5 BTC ($185,000) and increase by the same amount for every day the deadline was missed.

In the last few weeks, our cloud services have had numerous emergency onboardings with the mention of a ransom letter. Most of the onboardings were new customers, others were existing customers seeking to protect new assets. We did not get notified of a ransom letter received by protected customers. Because there is an array of DDoS protection services/solutions in the marketplace, Radware believes the threat actors are specifically targeting unprotected assets and organizations. These malicious actors can leverage BGP routing information to detect if targets are protected by always-on cloud mitigation services.

Reports from victims impacted by follow-up attacks of this extortion campaign confirm this observation. Most ISPs and CSPs victims did have DDoS mitigation solutions to protect their customers. However, they were not prepared for large, globally-distributed attacks targetting their DNS services and saturating their internet uplinks.



We are the Fancy Lazarus and we have chosen [Company] 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 Thursday 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 [ASN] 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 0.5 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 1 BTC and will increase by 0.5 Bitcoin for each day after the 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!

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.

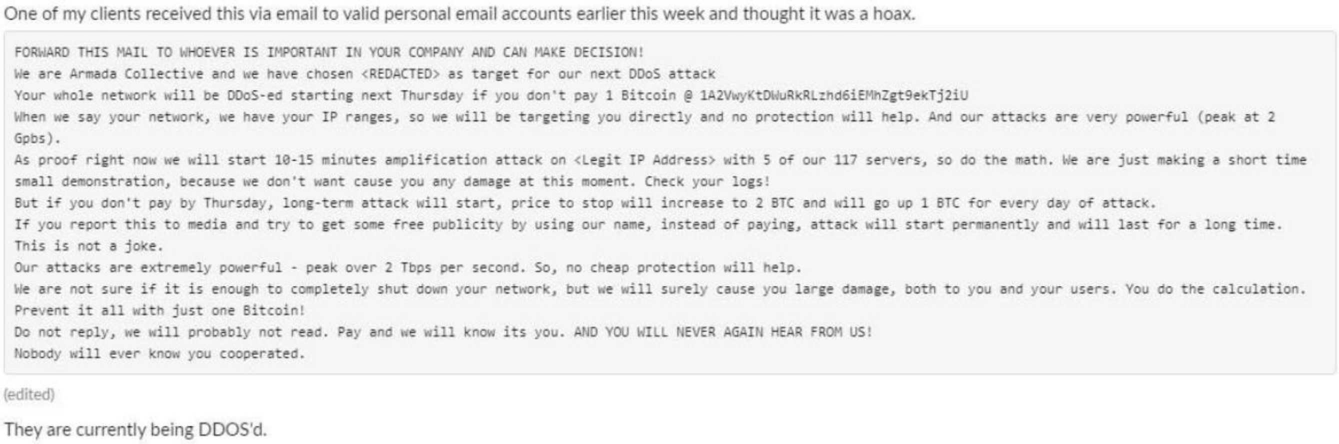
Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

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: Letter circulating in several forums and received by ransom DDoS victims

In their current message, the extortionists are claiming to use 10 out of a total of 117 attack servers to perform "not that heavy" DDoS attacks and provide proof of the legitimacy of their claims. Ransom letters in the earlier campaigns between August and December did not mention the fraction and total number of servers. In November of 2020, there was one **tweet** revealing a campaign from a group claiming to be the "Armada Collective" that was targeting smaller ISPs. The message mentioned a demonstration DDoS attack using five of the 117 attack servers (see Figure 2).



One of my clients received this via email to valid personal email accounts earlier this week and thought it was a hoax.

```
FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!
We are Armada Collective and we have chosen <REDACTED> as target for our next DDoS attack
Your whole network will be DDoS-ed starting next Thursday if you don't pay 1 Bitcoin @ 1A2VwyKtDWuRkRLzhd6iEMhZgt9ekTj2iU
When we say your network, we have your IP ranges, so we will be targeting you directly and no protection will help. And our attacks are very powerful (peak at 2
Gpbs).
As proof right now we will start 10-15 minutes amplification attack on <Legit IP Address> with 5 of our 117 servers, so do the math. We are just making a short time
small demonstration, because we don't want cause you any damage at this moment. Check your logs!
But if you don't pay by Thursday, long-term attack will start, price to stop will increase to 2 BTC and will go up 1 BTC for every day of attack.
If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.
This is not a joke.
Our attacks are extremely powerful - peak over 2 Tbps per second. So, no cheap protection will help.
We are not sure if it is enough to completely shut down your network, but we will surely cause you large damage, both to you and your users. You do the calculation.
Prevent it all with just one Bitcoin!
Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!
Nobody will ever know you cooperated.
```

(edited)

They are currently being DDOS'd.

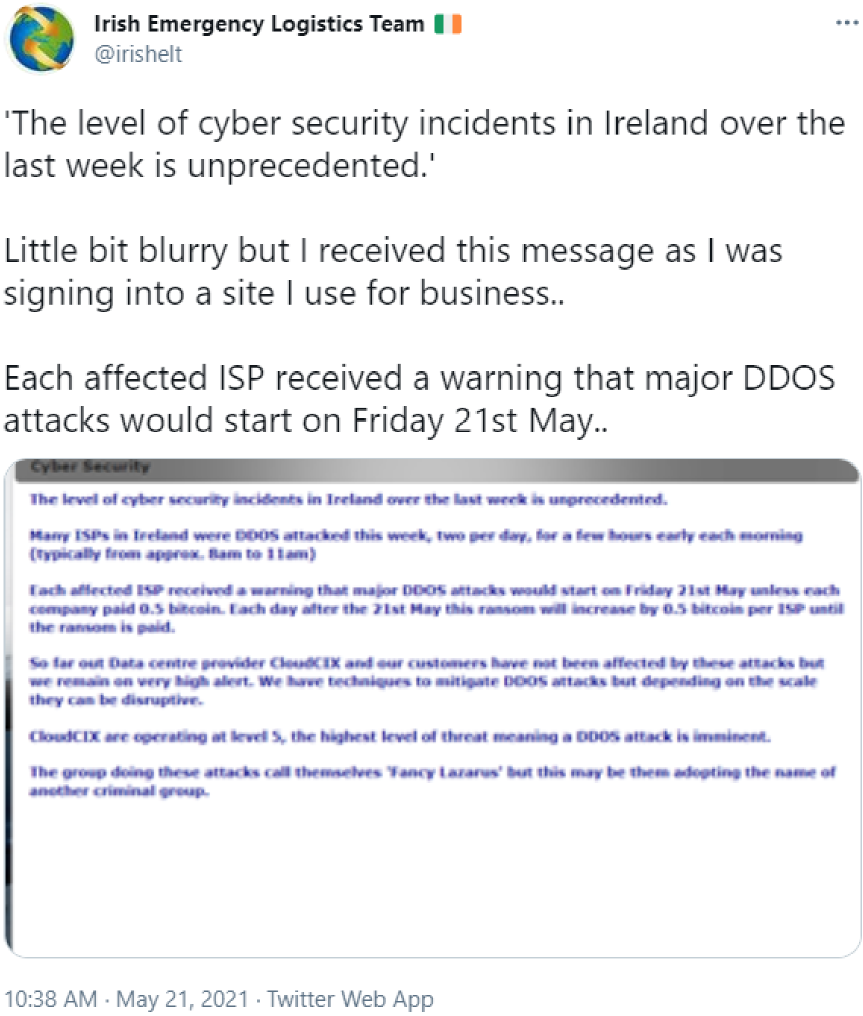
Figure 2: Ransom Letter from Armada Collective in November of 2020

ISP and CSP Targeted by Ransom DDoS

On May 19th, Danish Computerworld **reported** that Copenhagen ISP Gigabit was hit by a DDoS attack that took their network down for almost three hours. According to the Danish **media**, the attack was between 50 - 200Gbps. The Danish ISP confirmed being approached by a hacker group calling itself "Fancy Lazarus" before the attacks started. Once the company had returned to full operation, Gigabit immediately prepared a detailed logbook and reported it to law enforcement, including the Center for Cybersecurity (CFCS).

Norlys, another Danish ISP, was attacked in the early hours of May 20th. Large amounts of traffic were directed towards the company's DNS servers and impacted their customers' TV and internet services. The DDoS attack lasted for three hours and it took Norlys until that afternoon to recover all operations.

On May 21st, the Irish Emergency Logistics Team reported unprecedented levels of cybersecurity incidents in Ireland. According to a warning posted by CloudCIX, a leading Irish internet exchange and CSP, many ISPs in Ireland were the target of several DDoS attacks lasting a few hours each morning. Each affected ISP received a warning of a major DDoS attack that would start on May 21st unless the company paid 0.5 bitcoin.



Irish Emergency Logistics Team
@irishelt

'The level of cyber security incidents in Ireland over the last week is unprecedented.'

Little bit blurry but I received this message as I was signing into a site I use for business..

Each affected ISP received a warning that major DDOS attacks would start on Friday 21st May..

Cyber Security

The level of cyber security incidents in Ireland over the last week is unprecedented.

Many ISPs in Ireland were DDOS attacked this week, two per day, for a few hours early each morning (typically from approx. 8am to 11am)

Each affected ISP received a warning that major DDOS attacks would start on Friday 21st May unless each company paid 0.5 bitcoin. Each day after the 21st May this ransom will increase by 0.5 bitcoin per ISP until the ransom is paid.

So far out Data centre provider CloudCIX and our customers have not been affected by these attacks but we remain on very high alert. We have techniques to mitigate DDOS attacks but depending on the scale they can be disruptive.

CloudCIX are operating at level 5, the highest level of threat meaning a DDOS attack is imminent.

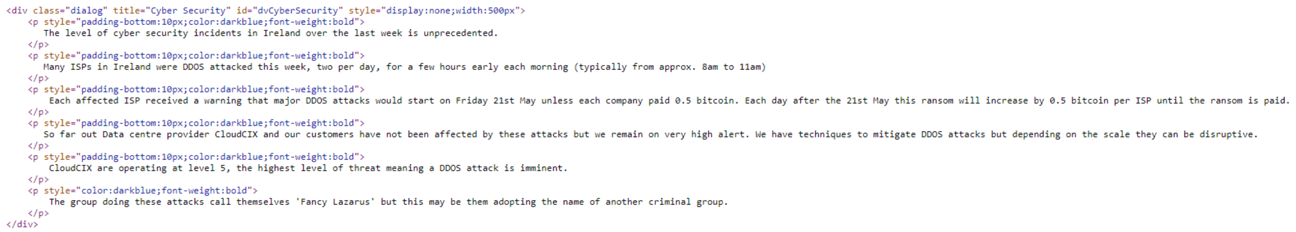
The group doing these attacks call themselves 'Fancy Lazarus' but this may be them adopting the name of another criminal group.

10:38 AM · May 21, 2021 · Twitter Web App

Figure 3: Message from Irish Emergency Logistics Team on Twitter about Irish ISPs affected by ransom letters

A message announcing "CloudCIX are operating at level 5, the highest level of threat meaning a DDoS attack is imminent," was spread across several Irish websites via JavaScript popups, as found in the HTML source of an Irish freight provider's login page (see Figure 4).

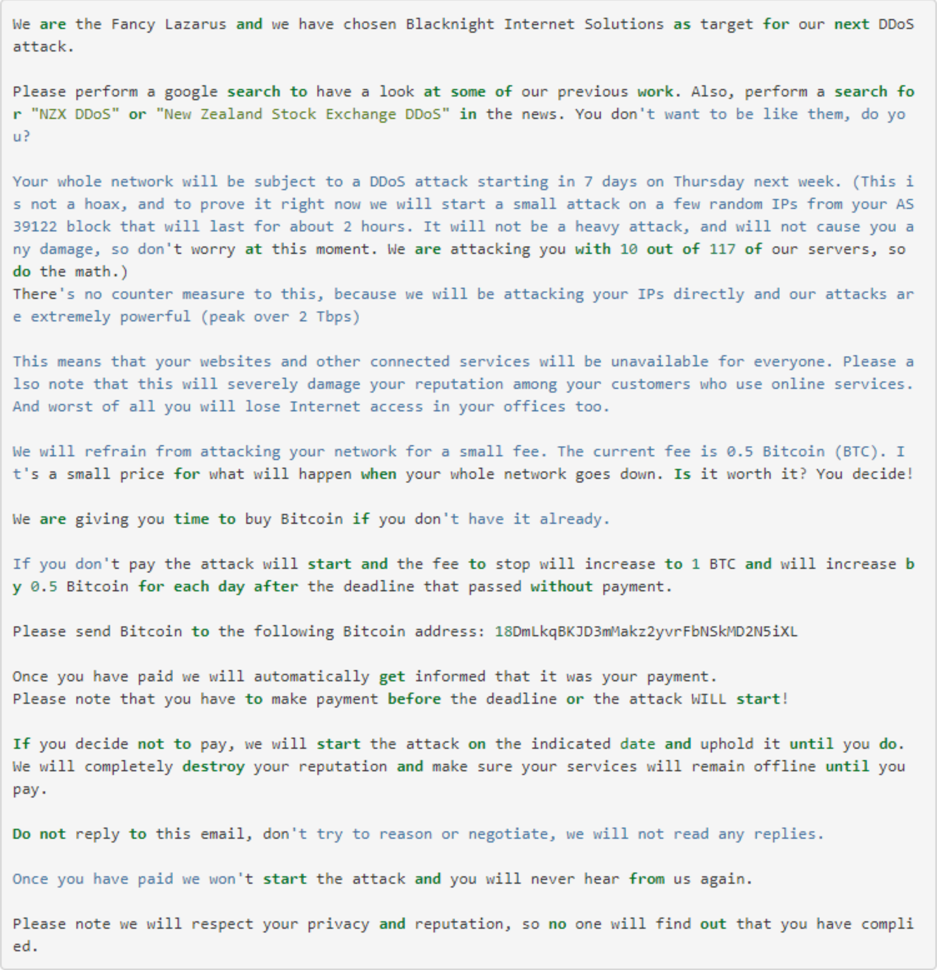
`



```
<div class="dialog" title="Cyber Security" id="dvCyberSecurity" style="display:none;width:500px">
    <p style="padding-bottom:10px;color:darkblue;font-weight:bold">
      The level of cyber security incidents in Ireland over the last week is unprecedented.
    </p>
    <p style="padding-bottom:10px;color:darkblue;font-weight:bold">
      Many ISPs in Ireland were DDOS attacked this week, two per day, for a few hours early each morning (typically from approx. 8am to 11am)
    </p>
    <p style="padding-bottom:10px;color:darkblue;font-weight:bold">
       Each affected ISP received a warning that major DDOS attacks would start on Friday 21st May unless each company paid 0.5 bitcoin. Each day after the 21st May this ransom will increase by 0.5 bitcoin per ISP until the ransom is paid.
    </p>
    <p style="padding-bottom:10px;color:darkblue;font-weight:bold">
      So far out Data centre provider CloudCIX and our customers have not been affected by these attacks but we remain on very high alert. We have techniques to mitigate DDOS attacks but depending on the scale they can be disruptive.
    </p>
    <p style="padding-bottom:10px;color:darkblue;font-weight:bold">
       CloudCIX are operating at level 5, the highest level of threat meaning a DDOS attack is imminent.
    </p>
    <p style="color:darkblue;font-weight:bold">
       The group doing these attacks call themselves 'Fancy Lazarus' but this may be them adopting the name of another criminal group.
    </p>
</div>
```

Figure 4: Javascript popup announcing CloudCIX operating at level 5

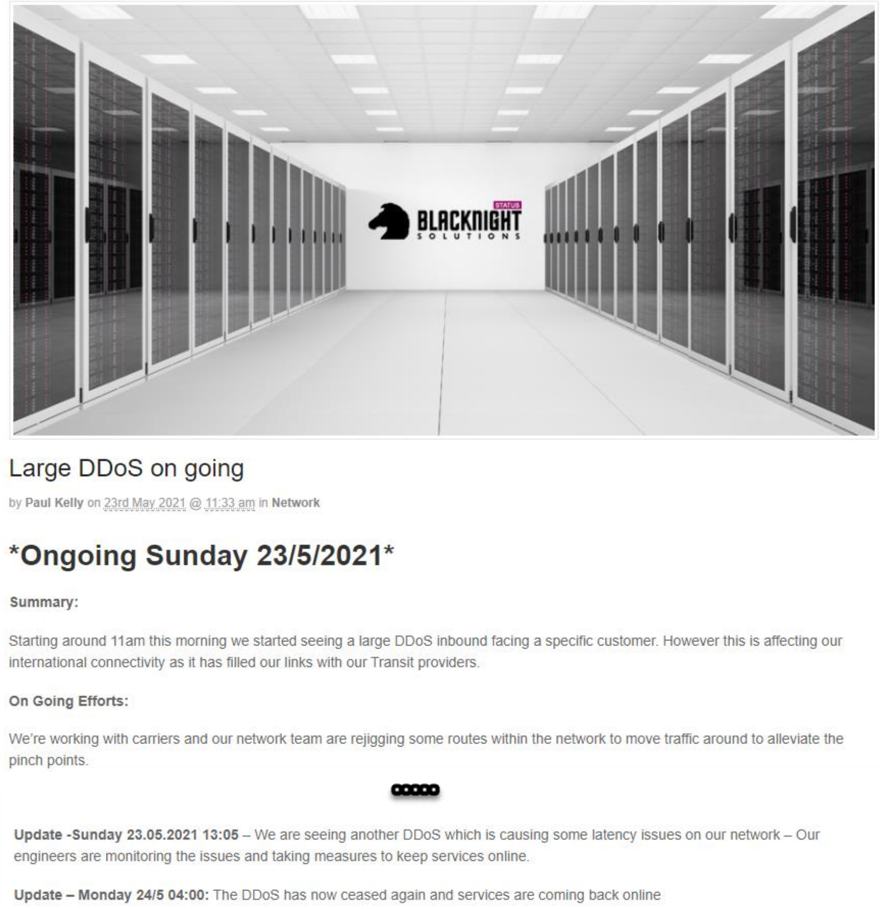
Zero.bs **published** a ransom note from "Fancy Lazarus" addressed to Blacknight Solutions, threatening to start an attack unless 0.5 bitcoin was paid.



```
We are the Fancy Lazarus and we have chosen Blacknight Internet Solutions 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 Thursday 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 AS 39122 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 0.5 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 1 BTC and will increase by 0.5 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: 18DmLkqBKJD3mMakz2yvrFbNSkMD2N5iXL

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 5: Ransom letter addressed to Blacknight Solutions (source: zero.bs)

On May 23rd, Blacknight Solutions **announced** a large DDoS attack on their network. The DDoS ceased in the early morning hours of the next day (see Figure 6).



Large DDoS on going

by **Paul Kelly** on 23rd May 2021 @ 11:33 am in **Network**

Ongoing Sunday 23/5/2021

Summary:

Starting around 11am this morning we started seeing a large DDoS inbound facing a specific customer. However this is affecting our international connectivity as it has filled our links with our Transit providers.

On Going Efforts:

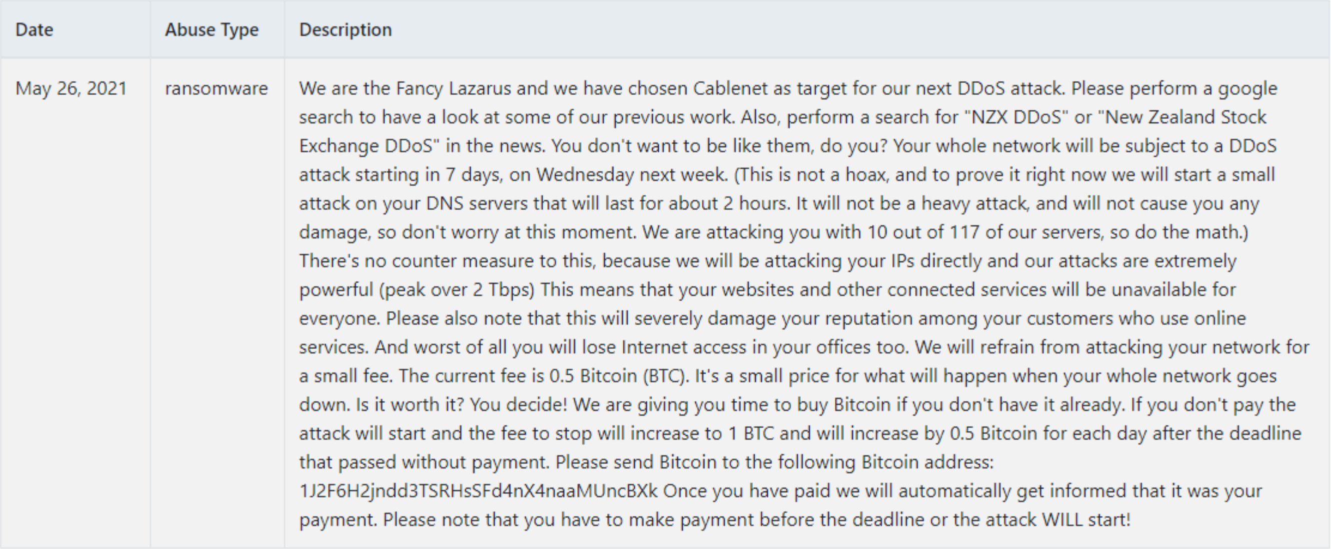
We're working with carriers and our network team are rejigging some routes within the network to move traffic around to alleviate the pinch points.

Update -Sunday 23.05.2021 13:05 – We are seeing another DDoS which is causing some latency issues on our network – Our engineers are monitoring the issues and taking measures to keep services online.

Update – Monday 24/5 04:00: The DDoS has now ceased again and services are coming back online

Figure 6: Blacknight Solutions status page about large DDoS attack

Another ransom message was **reported** on Bitcoin Abuse on May 26th. Again, the message originated from a group calling themselves "Fancy Lazarus" and demanded a ransom of 0.5 bitcoin from Cablenet, a internet service provider based in Cyprus.



Date	Abuse Type	Description
May 26, 2021	ransomware	We are the Fancy Lazarus and we have chosen Cablenet 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 Wednesday next week. (This is not a hoax, and to prove it right now we will start a small attack on your DNS servers 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 0.5 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 1 BTC and will increase by 0.5 Bitcoin for each day after the deadline that passed without payment. Please send Bitcoin to the following Bitcoin address: 1J2F6H2jndd3TSRHsSFd4nX4naaMUncBXk 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!

Figure 7: Bitcoin Abuse report of DDoS ransom letter targeting Cablenet

Reasons For Concern

A ransom DDoS group is identifying and targeting organizations with unprotected assets with ransom letters and threats of devastating DDoS attacks. The action radius of the extortionists has been extending rapidly to organizations of all sizes across the world and in all verticals. If your organization has a critical service exposed or loss of connectivity impacts your business, you are a potential target for these extortionists.

Back in January, we said ransom DDoS had become a persistent threat and we do not expect this to change anytime soon. As long as there are victims to extort, campaigns will keep emerging.

Recommendations

Radware recommends organizations, ISPs and CSPs of any size and vertical to assess the protection of their internet connections and plan against globally distributed DDoS attacks aimed at DNS servers and attempting to saturate internet uplinks.

On-premise or local DDoS detection and mitigation is adequate for latency sensitive services and applications, but it only protects local infrastructure against attacks that are below the capacity of the internet links. Once attacks grow beyond the bandwidth of those connections, an upstream solution is required to block attacks while allowing only legitimate traffic to the organization. Large and globally distributed DDoS attacks can only be effectively mitigated by stopping malicious traffic closest to its source and never allowing multiple geographically distributed traffic streams to flock. Globally distributed and anycasted protection services are most effective against these kinds of DDoS attacks.

Ransom DDoS Update: The Hunt For Unprotected Assets

"Fantasy APT Seeking Unprotected Assets"

JUNE 11, 2021

Cloud DDoS services will introduce latency, which can be unacceptable for certain applications and services during normal operating conditions. Hybrid DDoS protection provides the best of both worlds with on-premise protection against all types of DDoS attacks while automatically diverting to a Cloud DDoS mitigation service when the attacks risk saturating the internet link. While diverted to the cloud, additional latency will be incurred, but the service will remain available, while in peace time there is no additional latency.

More information on different deployment options for different use cases can be found in this **blog**.

Our DDoS response guide outlines steps that allow you to minimize the impact of a DDoS attack and how to recover quickly. Download your guide **here**.

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **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
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

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 **Radware's Security Research Center.** 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.