Detecting a new ransomware strain, not asking for data ransom, but only needing the victim to join the Hacker's Discord server

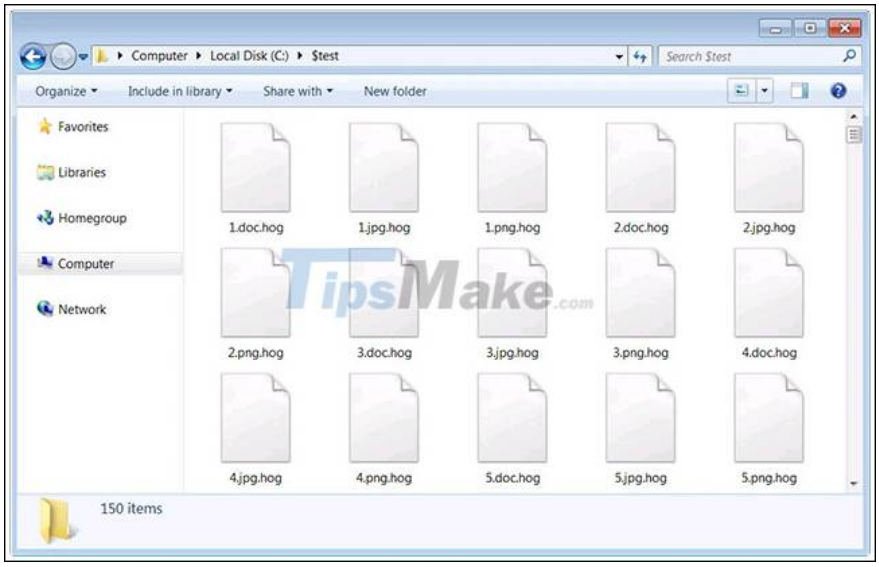
International security researchers have just stumbled upon a strain of ransomware that possesses rather strange behavior. Called 'Hog', this ransomware still enters the system and encrypts the victim's files.

However, it only accepts requests to decrypt the file if the victim participates in the Discord server controlled by the people behind the malware.

More specifically, security researcher from MalwareHunterTeam just found a decryptor developed for 'Hog ransomware', which requires victims to join the Discord server if they want their files to be resolved. code.

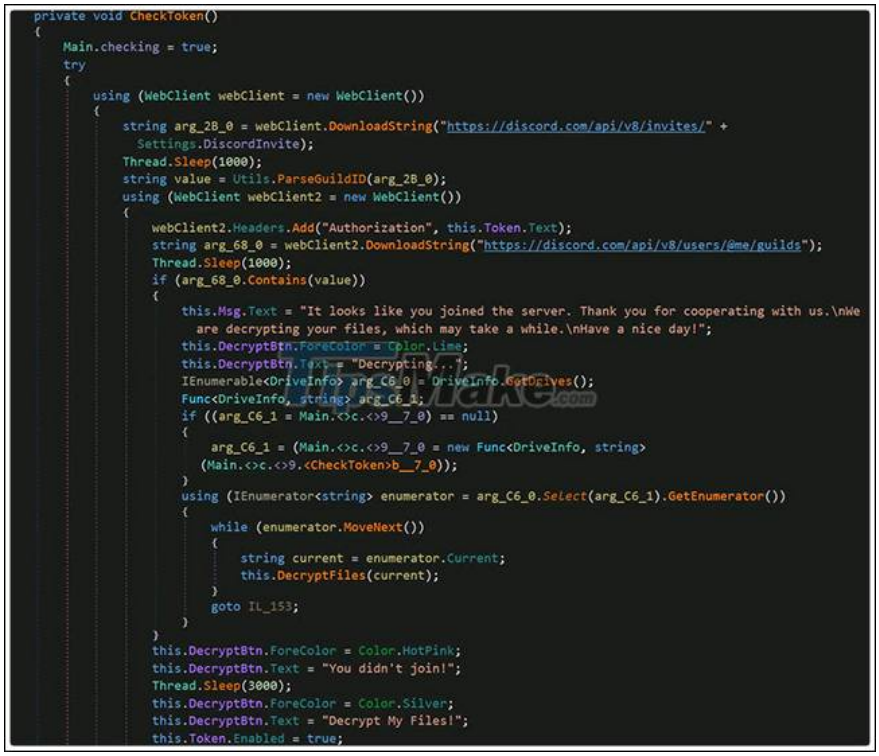
The encryptor of the malicious code was later discovered. When executed, it checks to see if a particular Discord server exists and, if so, will start encrypting the victim's file.

When successfully encrypting a victim's file, the malicious code appends the .hog extension to the file extension as shown below, and automatically extracts the decoder component.



After Hog has encrypted the target device, it will immediately launch the DECRYPT-MY-FILES.exe decoder from the Windows Startup folder.

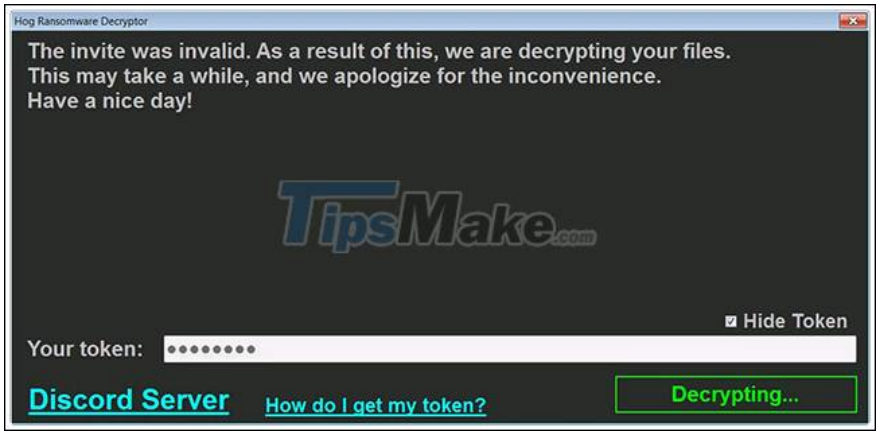
This decoder will explain the victim in detail what happened to them, and then prompt the victim to enter the Discord user token created specifically for them.



```
private void CheckToken()
{
    Main.checking = true;
    try
    {
        using (WebClient webClient = new WebClient())
        {
            string arg_2B_0 = webClient.DownloadString("https://discord.com/api/v8/invites/" +
              Settings.DiscordInvite);
            Thread.Sleep(1000);
            string value = Utils.ParseGuildID(arg_2B_0);
            using (WebClient webClient2 = new WebClient())
            {
                webClient2.Headers.Add("Authorization", this.Token.Text);
                string arg_68_0 = webClient2.DownloadString("https://discord.com/api/v8/users/@me/guilds");
                Thread.Sleep(1000);
                if (arg_68_0.Contains(value))
                {
                    this.Msg.Text = "It looks like you joined the server. Thank you for cooperating with us.\nWe
                      are decrypting your files, which may take a while.\nHave a nice day!";
                    this.DecryptBtn.ForeColor = Color.Lime;
                    this.DecryptBtn.Text = "Decrypting...";
                    IEnumerable<DriveInfo> arg_C6_0 = DriveInfo.GetDrives();
                    Func<DriveInfo, string> arg_C6_1;
                    if ((arg_C6_1 = Main.<>c.<>9__7_0) == null)
                    {
                        arg_C6_1 = (Main.<>c.<>9__7_0 = new Func<DriveInfo, string>
                      (Main.<>c.<>9.<CheckToken>b__7_0));
                    }
                    using (IEnumerator<string> enumerator = arg_C6_0.Select(arg_C6_1).GetEnumerator())
                    {
                        while (enumerator.MoveNext())
                        {
                            string current = enumerator.Current;
                            this.DecryptFiles(current);
                        }
                        goto IL_153;
                    }
                }
                this.DecryptBtn.ForeColor = Color.HotPink;
                this.DecryptBtn.Text = "You didn't join!";
                Thread.Sleep(3000);
                this.DecryptBtn.ForeColor = Color.Silver;
                this.DecryptBtn.Text = "Decrypt My Files!";
                this.Token.Enabled = true;
```

If you don't already know, Discord is a voice and text chat system that allows you to communicate with others. Anyone can create a discussion host whatever they want. You can find people to talk to about Valkyrie and form teams at most times of the day. Learn more about Discord in THIS article.

The Discord token allows the ransomware to authenticate against the Discord APIs as users and check if they join their server, as shown by the source code below.



If the victim joined the server or the server doesn't exist, the ransomware decrypts the victim's files using the static key embedded in the ransomware.

While this appears to be a ransomware in development, it does show a tendency for threat actors to start using Discord more often for malicious activities.

Another ransomware named Humble was recently spotted by Trend Micro, using a webhook to post details about the new victims to the hackers' Discord server.

In addition, Discord is often used by threat agents to spread malware or collect stolen data.

In the face of this situation, it is important that administrators and network security tools increase the deployment of Discord traffic monitoring for early detection of threats or unusual behavior.