LokiLocker, a Ransomware Similar to BlackBit Being Distributed in Korea

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.

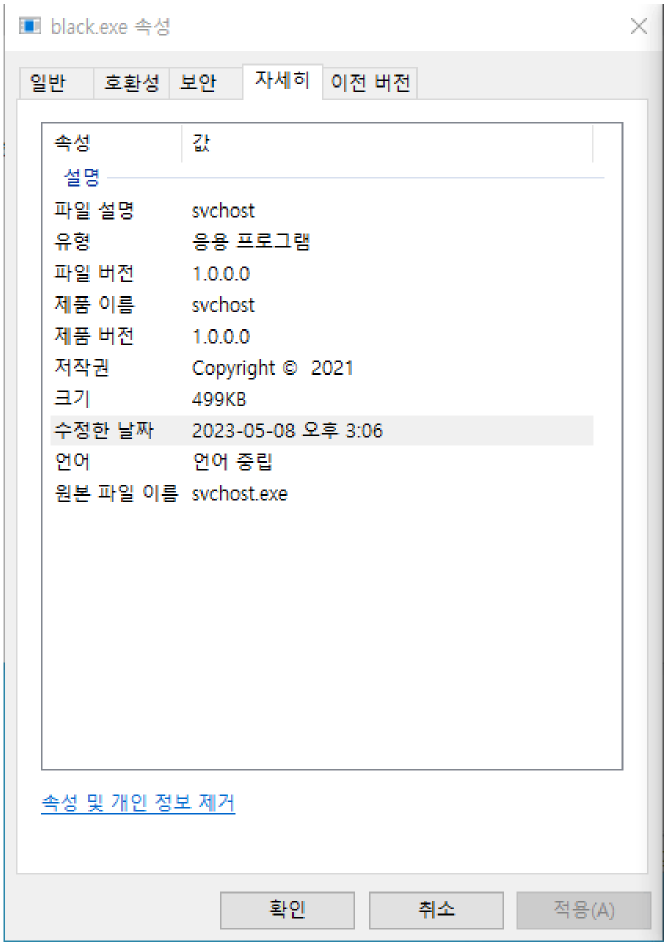
Similarities Between LokiLocker and BlackBit

- 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

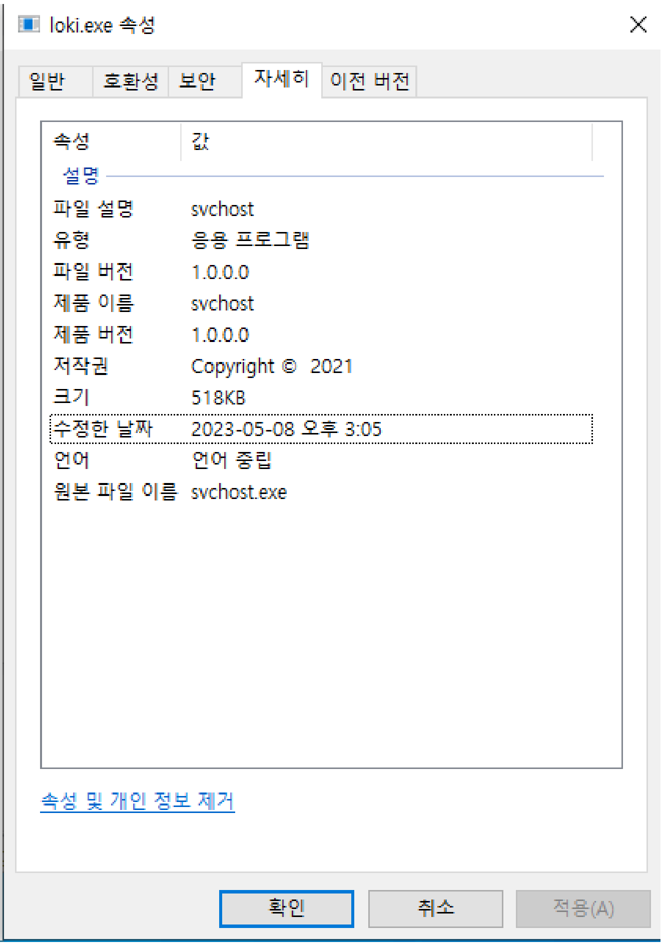
> BlackBit Ransomware Being Distributed in Korea

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.



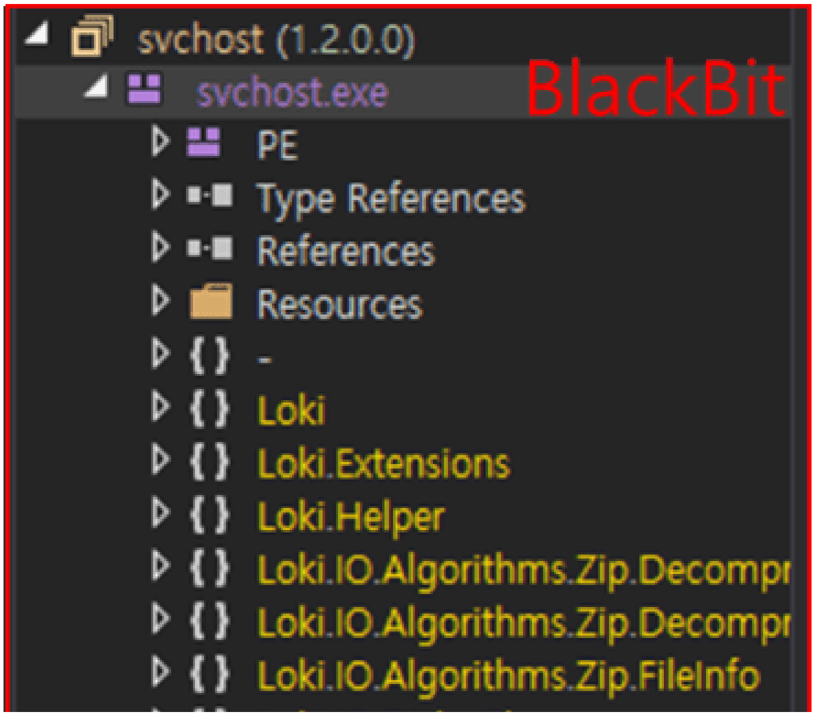
속성	값
설명	
파일 설명	svchost
유형	응용 프로그램
파일 버전	1.0.0.0
제품 이름	svchost
제품 버전	1.0.0.0
저작권	Copyright © 2021
크기	499KB
수정한 날짜	2023-05-08 오후 3:06
언어	언어 중립
원본 파일 이름	svchost.exe



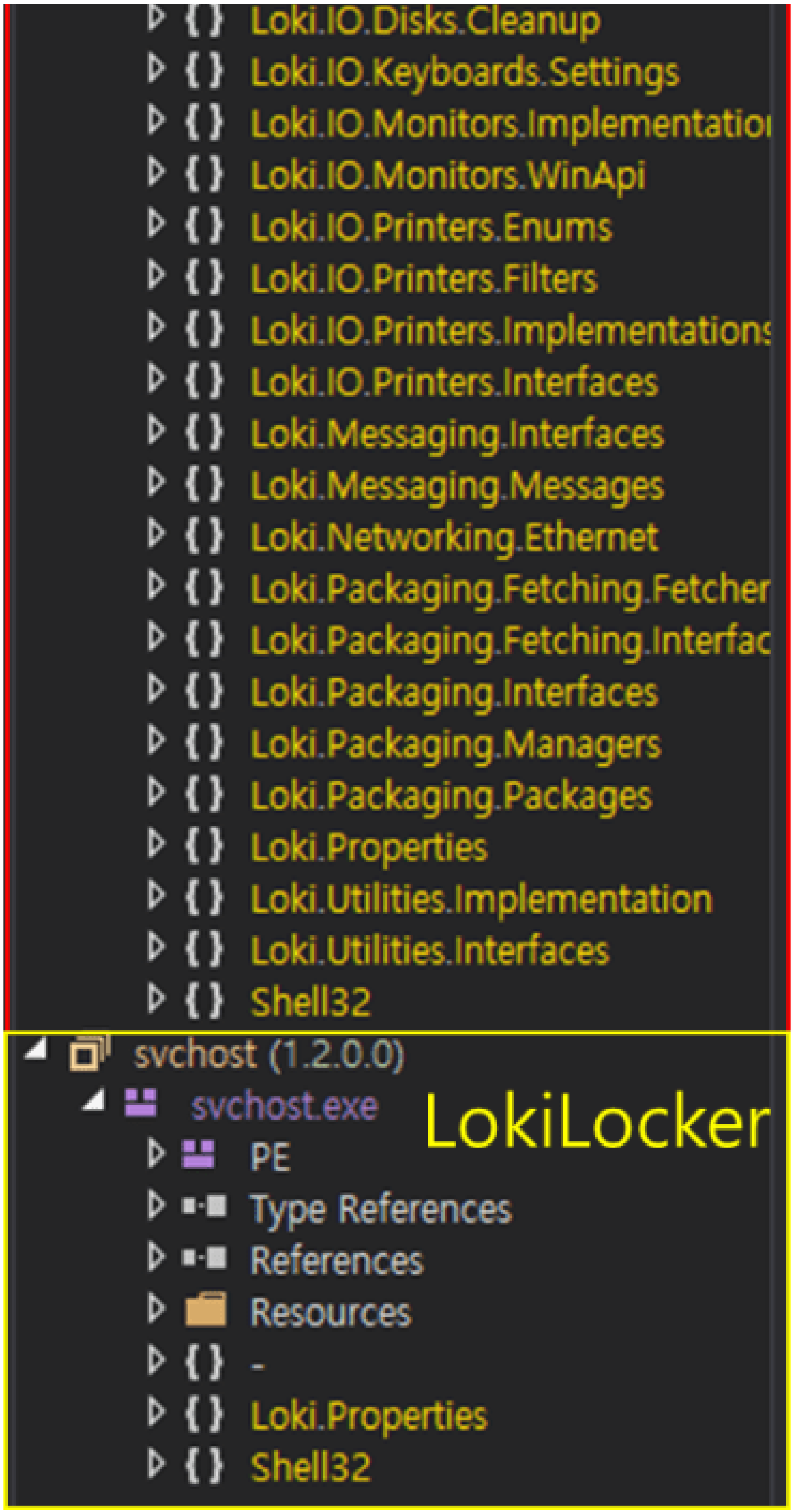
속성	값
설명	
파일 설명	svchost
유형	응용 프로그램
파일 버전	1.0.0.0
제품 이름	svchost
제품 버전	1.0.0.0
저작권	Copyright © 2021
크기	518KB
수정한 날짜	2023-05-08 오후 3:05
언어	언어 중립
원본 파일 이름	svchost.exe

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.



```
svchost (1.2.0.0)
  svchost.exe
    PE
    Type References
    References
    Resources
    { } -
    { } Loki
    { } Loki.Extensions
    { } Loki.Helper
    { } Loki.IO.Algorithms.Zip.Decompr
    { } Loki.IO.Algorithms.Zip.Decompr
    { } Loki.IO.Algorithms.Zip.FileInfo
```

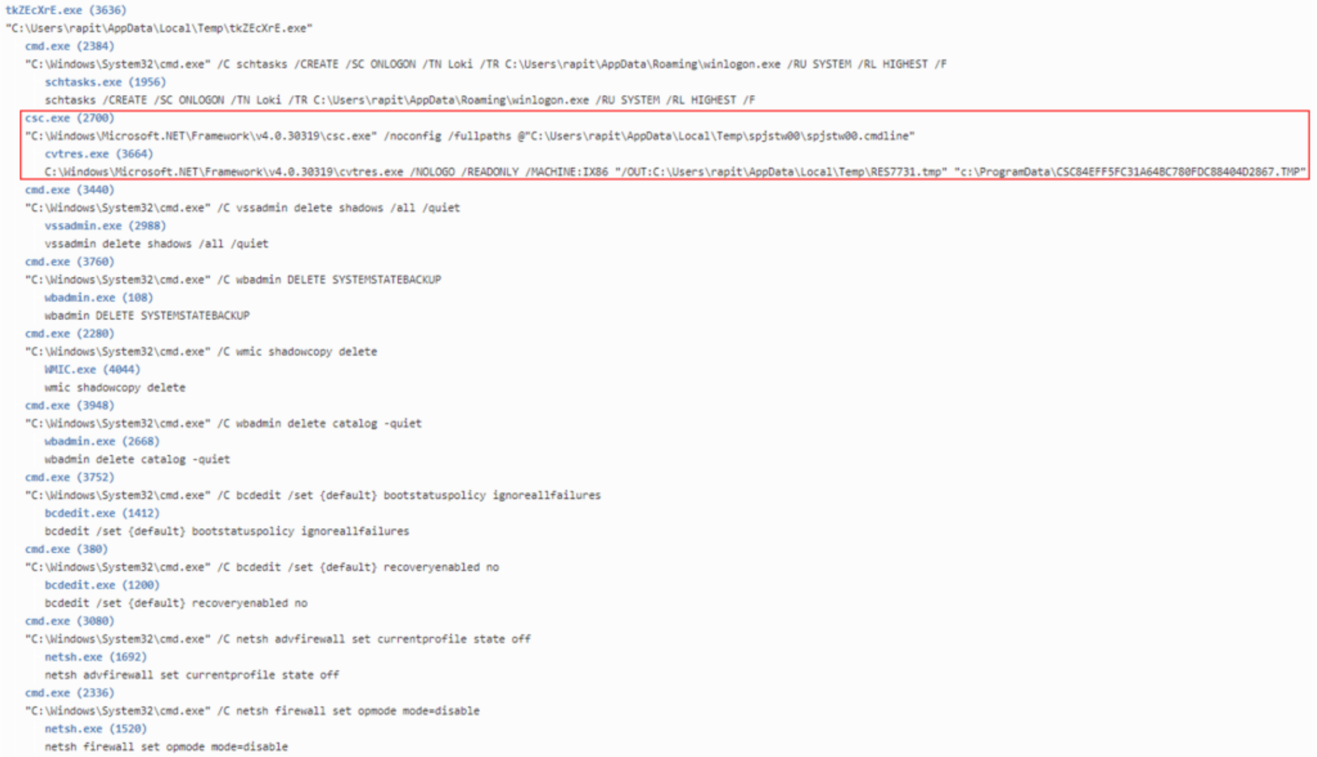


```
Loki.IO.Disks.Cleanup
Loki.IO.Keyboards.Settings
Loki.IO.Monitors.Implementatio
Loki.IO.Monitors.WinApi
Loki.IO.Printers.Enums
Loki.IO.Printers.Filters
Loki.IO.Printers.Implementations
Loki.IO.Printers.Interfaces
Loki.Messaging.Interfaces
Loki.Messaging.Messages
Loki.Networking.Ethernet
Loki.Packaging.Fetching.Fetcher
Loki.Packaging.Fetching.Interfac
Loki.Packaging.Interfaces
Loki.Packaging.Managers
Loki.Packaging.Packages
Loki.Properties
Loki.Utilities.Implementation
Loki.Utilities.Interfaces
Shell32
svchost (1.2.0.0)
  svchost.exe
    PE
    Type References
    References
    Resources
    -
    Loki.Properties
    Shell32
```

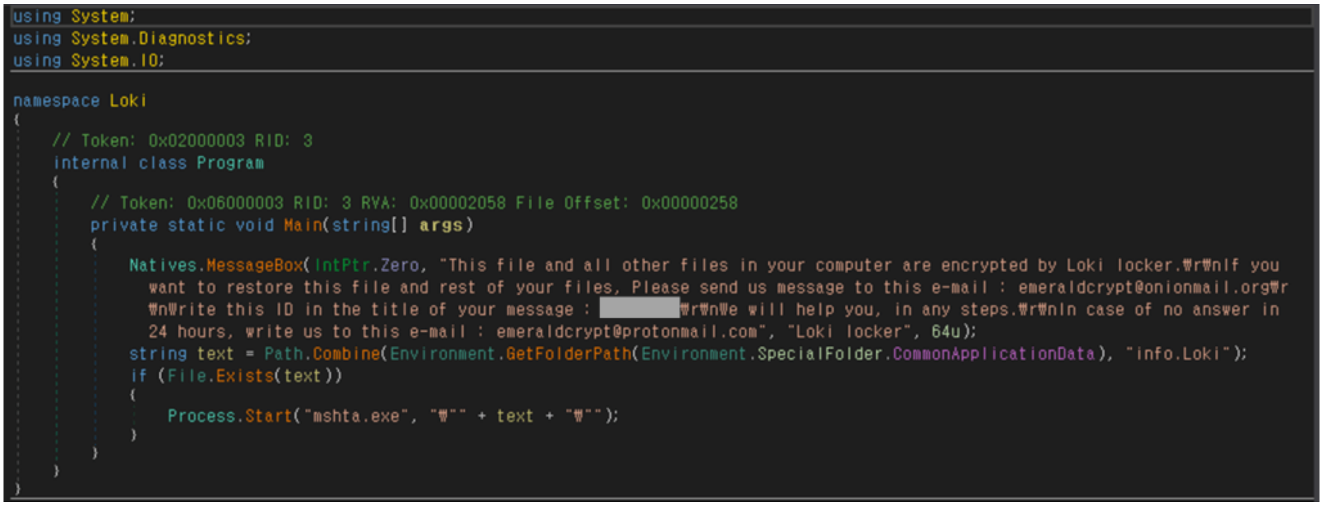
LokiLocker

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.



```
tkZEcXrE.exe (3636)
"C:\Users\rapit\AppData\Local\Temp\tkZEcXrE.exe"
  cmd.exe (2384)
  "C:\Windows\System32\cmd.exe" /C schtasks /CREATE /SC ONLOGON /TN Loki /TR C:\Users\rapit\AppData\Roaming\winlogon.exe /RU SYSTEM /RL HIGHEST /F
    schtasks.exe (1956)
    schtasks /CREATE /SC ONLOGON /TN Loki /TR C:\Users\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\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\rapit\AppData\Local\Temp\RES7731.tmp" "c:\ProgramData\CSC84EFF5FC31A64BC780FDC88404D2867.TMP"
  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 wbadmin DELETE SYSTEMSTATEBACKUP
    wbadmin.exe (108)
    wbadmin DELETE SYSTEMSTATEBACKUP
  cmd.exe (2280)
  "C:\Windows\System32\cmd.exe" /C wmic 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
```

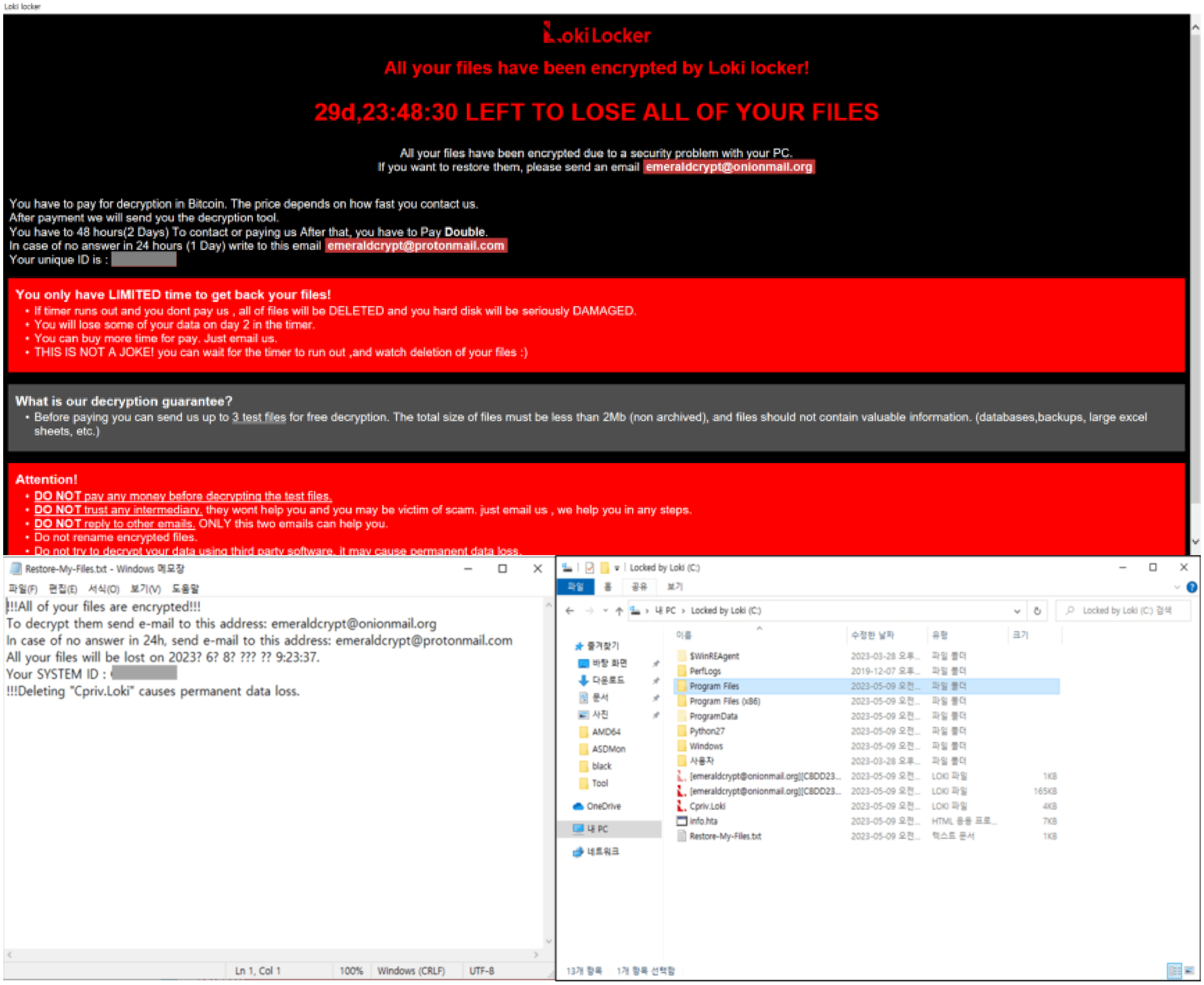


```
using System;
using System.Diagnostics;
using System.IO;

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.



Loki locker

LokiLocker

All your files have been encrypted by Loki locker!

29d,23:48:30 LEFT TO LOSE ALL OF YOUR FILES

All your files have been encrypted due to a security problem with your PC.
If you want to restore them, please send an email emeraldcrypt@onionmail.org

You have to pay for decryption in Bitcoin. The price depends on how fast you contact us.
After payment we will send you the decryption tool.
You have to 48 hours(2 Days) To contact or paying us After that, you have to Pay **Double**.
In case of no answer in 24 hours (1 Day) write to this email emeraldcrypt@protonmail.com
Your unique ID is : [redacted]

You only have LIMITED time to get back your files!

- If timer runs out and you dont pay us , all of files will be DELETED and you hard disk will be seriously DAMAGED.
- You will lose some of your data on day 2 in the timer.
- You can buy more time for pay. Just email us.
- THIS IS NOT A JOKE! you can wait for the timer to run out ,and watch deletion of your files :)

What is our decryption guarantee?

- Before paying you can send us up to 3 test files for free decryption. The total size of files must be less than 2Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

Attention!

- **DO NOT** pay any money before decrypting the test files.
- **DO NOT** trust any intermediary. they wont help you and you may be victim of scam. just email us , we help you in any steps.
- **DO NOT** reply to other emails. ONLY this two emails can help you.
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.

Restore-My-Files.txt - Windows 메모장

```
!!!All of your files are encrypted!!!
To decrypt them send e-mail to this address: emeraldcrypt@onionmail.org
In case of no answer in 24h, send e-mail to this address: emeraldcrypt@protonmail.com
All your files will be lost on 2023? 6? 8? ??? ?? 9:23:37.
Your SYSTEM ID : [redacted]
!!!Deleting "Cpriv.Loki" causes permanent data loss.
```

Locked by Loki (C:)

이름	수정한 날짜	유형	크기
$WinREAgent	2023-03-28 오후...	파일 폴더	
PerfLogs	2019-12-07 오후...	파일 폴더	
Program Files	2023-05-09 오전...	파일 폴더	
Program Files (x86)	2023-05-09 오전...	파일 폴더	
ProgramData	2023-05-09 오전...	파일 폴더	
Python27	2023-05-09 오전...	파일 폴더	
Windows	2023-05-09 오전...	파일 폴더	
사용자	2023-03-28 오후...	파일 폴더	
[emeraldcrypt@onionmail.org][C8DD23...	2023-05-09 오전...	LOKI 파일	1KB
[emeraldcrypt@onionmail.org][C8DD23...	2023-05-09 오전...	LOKI 파일	165KB
Cpriv.Loki	2023-05-09 오전...	LOKI 파일	4KB
info.hta	2023-05-09 오전...	HTML 응용 프로...	7KB
Restore-My-Files.txt	2023-05-09 오전...	텍스트 문서	1KB

13개 항목 1개 항목 선택함

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