Amadey Bot Disguised as a Famous Korean Messenger Program Being Distributed

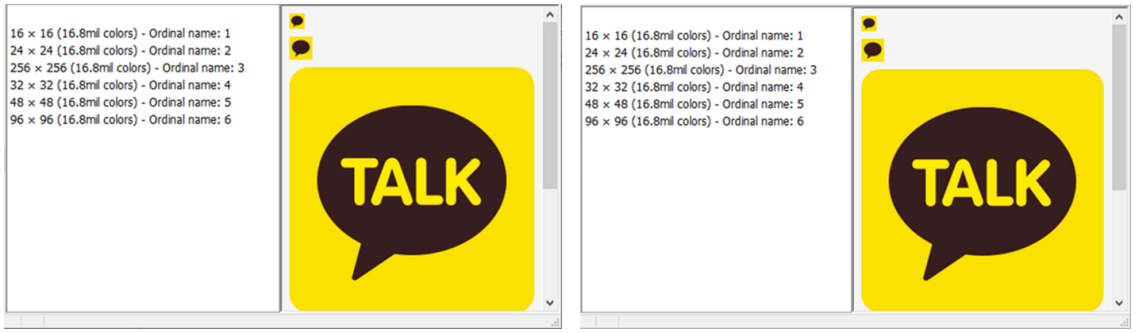
By ATCP

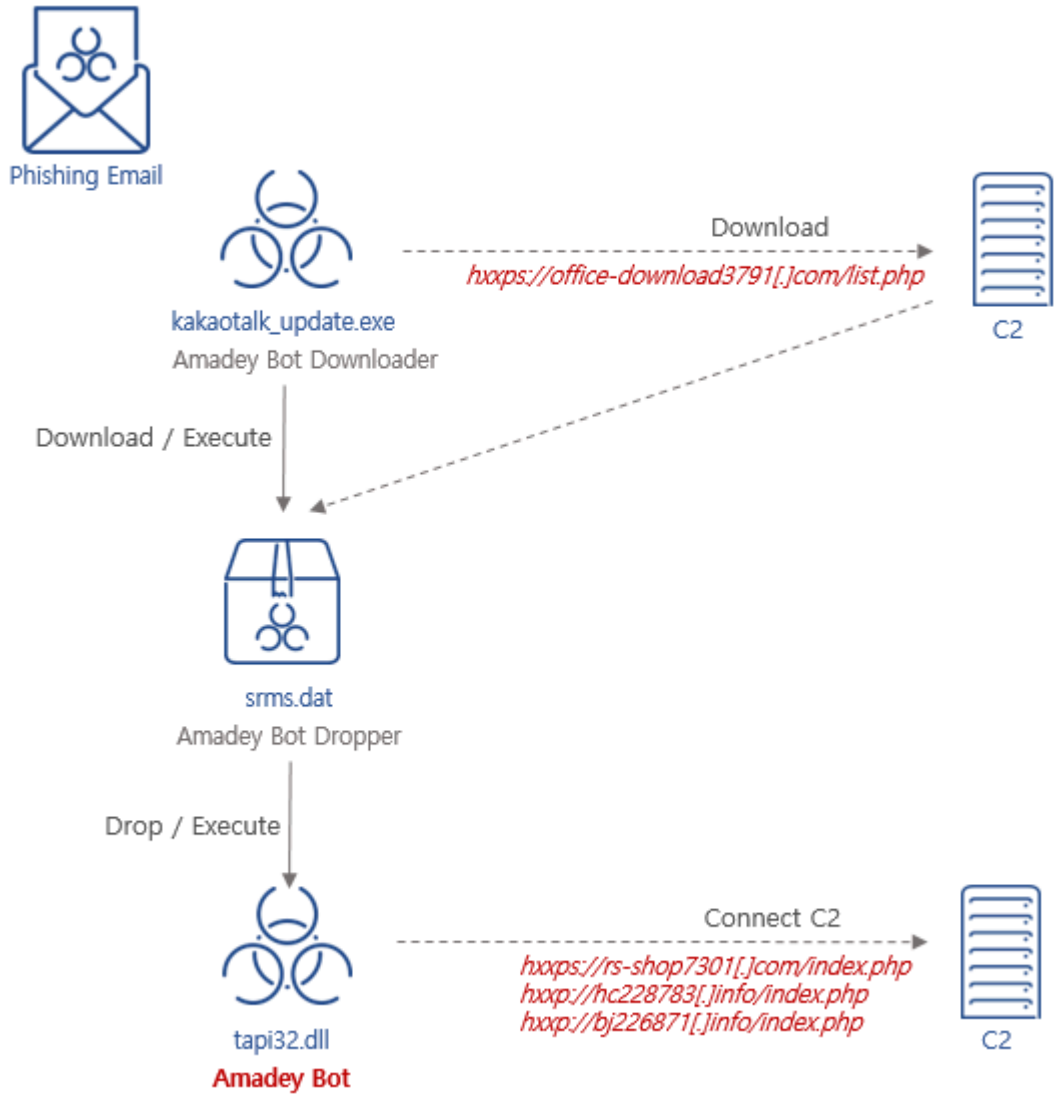
Published: 2022-10-16 · Archived: 2026-04-10 02:13:32 UTC

On October 17th, 2022, the Korean Internet & Security Agency (KISA) published a security notice titled “Advising Caution on Cyber Attacks Exploiting the Kakao Service Malfunction Issue’, and according to the notice, malware disguised as a KakaoTalk installation file (KakaoTalkUpdate.zip etc.) is being distributed via email.

- KISA security notice: https://www.boho.or.kr/data/secNoticeView.do?bulletin_writing_sequence=66958

The ASEC analysis team was able to secure a file that seems to be of the type while monitoring relevant samples. This malware has the same filename and icon as the actual messenger program, which prompts ordinary users to launch it.

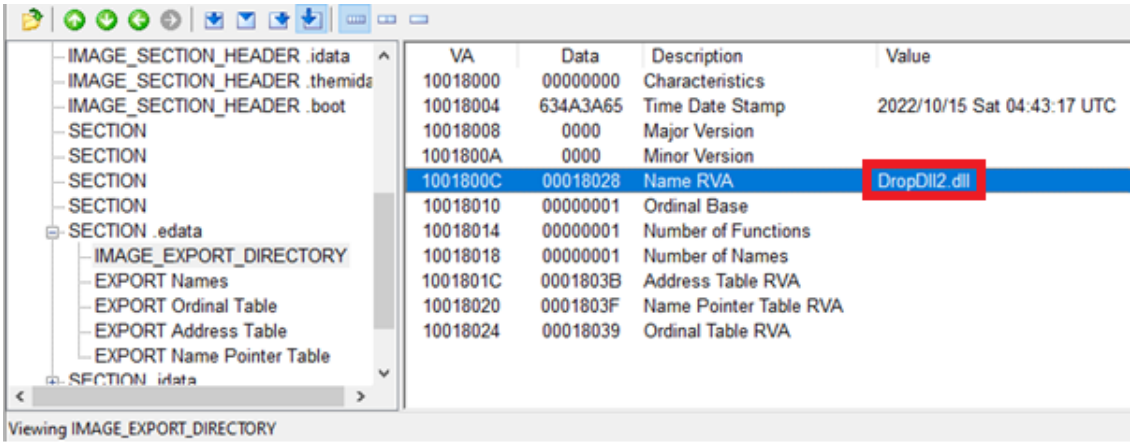


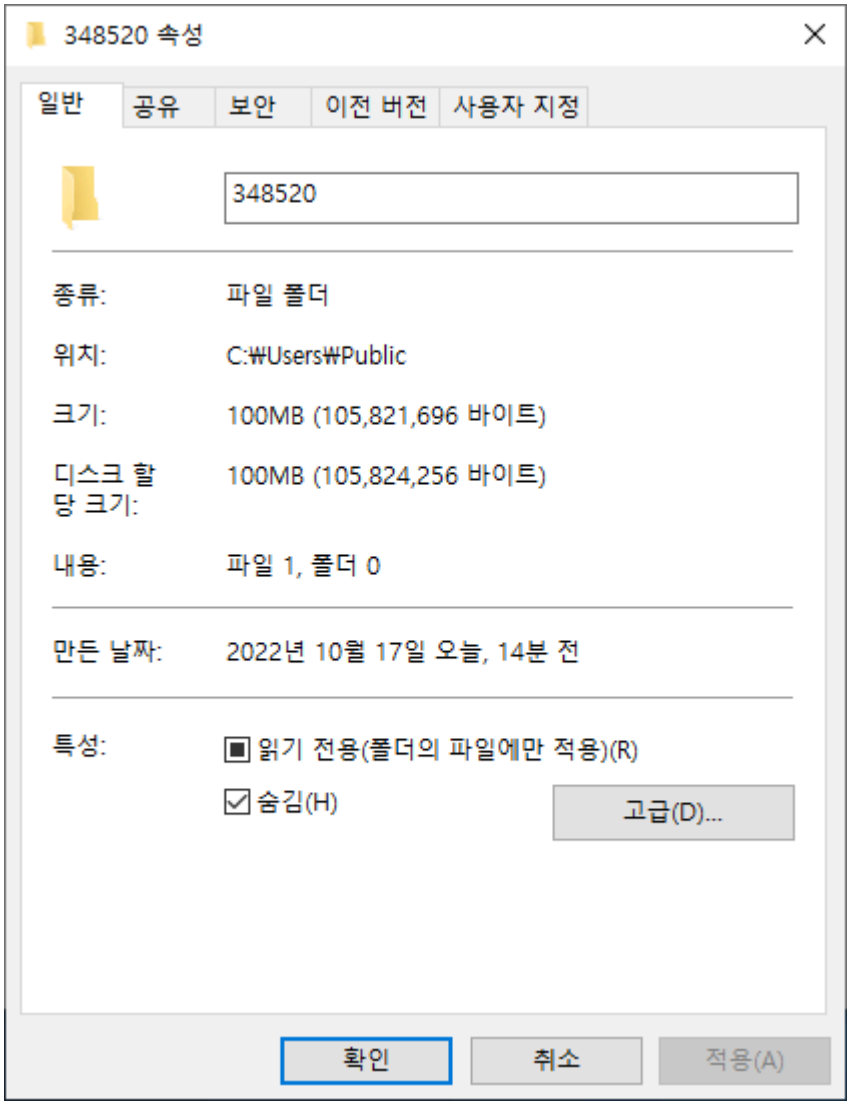


Upon initial execution of the kakaotalk_update.exe malware which is seen to have been attached to emails, it runs recursion on the process and injects itself into the process. The injected process connects to the C2 server and downloads a zip file with additional compressed malware to a shared folder path, before executing the following command.

- cmd.exe /c rundll32.exe “C:\users\public\srms.dat” Run
- cmd.exe /C timeout /t 5 /nobreak & Del /f /q “C:\Users\[Username]\Desktop\kakaotalk_update.exe”

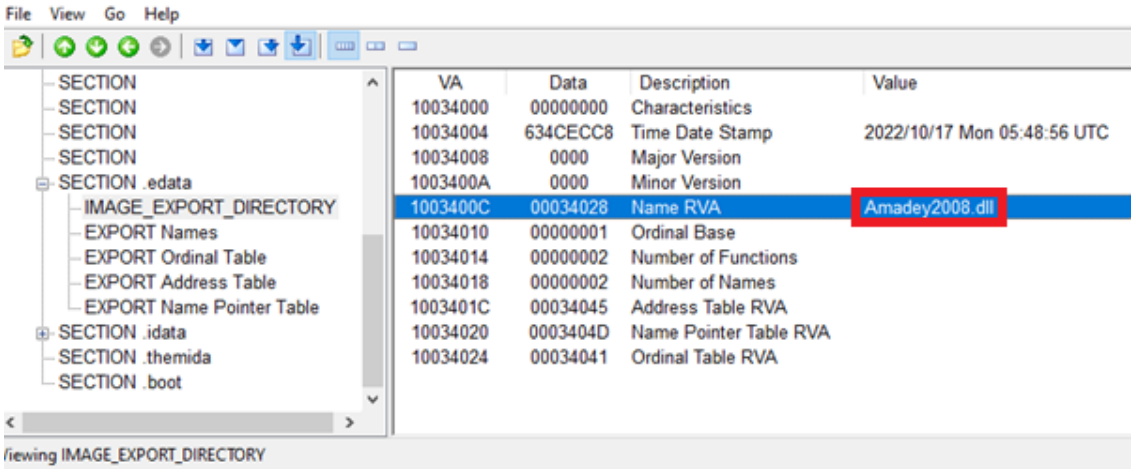
The downloaded and executed file with the name of “srms.dat” is a dropper (See Figure 3) that creates a DLL that behaves as the AmadeyBot malware.





Afterward, using rundll32.exe, it creates and runs the AmadeyBot with the filename “tapi32.dll” as shown below, then deletes itself.

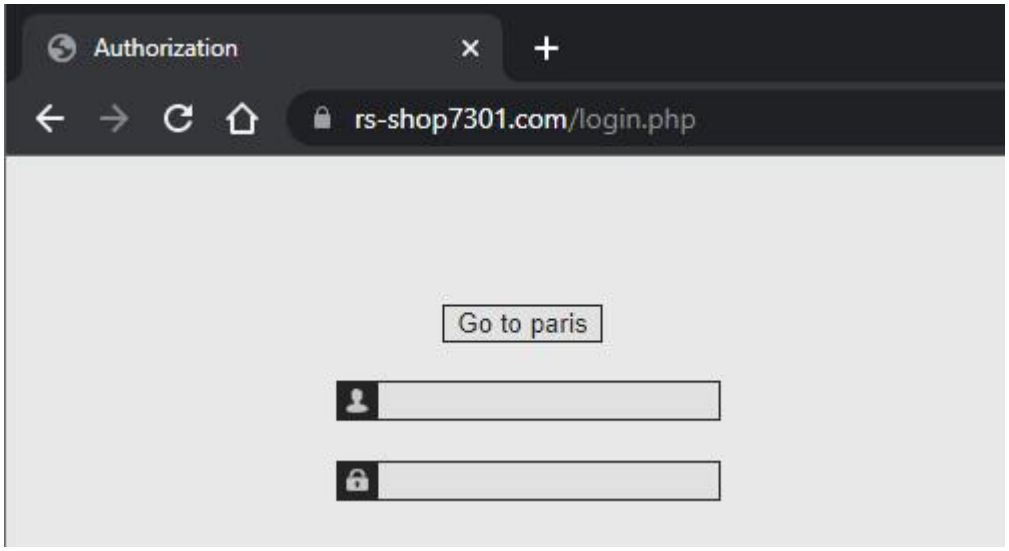
- rundll32.exe “C:\users\public\348520\tapi32.dll”,Run
- rundll32.exe “C:\users\public\348520\tapi32.dll”,Start
- cmd.exe /C timeout /t 5 /nobreak & Del /f /q “C:\users\public\srms.dat”



As shown in Figure 7, the executed Amadey Bot **transmits information from the user PC including the infected system’s ID, Amadey version, admin privilege status, architecture, Windows version, PC name, and username to the C2 server.**

Body

Name	Value
id	3505014108
vs	2.00
ar	0
bi	1
lv	0
os	1
av	0
pc	DESKTOP-UGGTH7R
un	kk



Detailed analysis on the Amadey Bot malware can be found in the following ASEC blog posts.

- **Amadey Bot Being Distributed Through SmokeLoader (Link)**
- **[Warning] 'Amadey' Malware Targeting Korean Cryptocurrency Companies (Link)**

AhnLab's anti-malware software, V3, detects and blocks the malware above using the aliases below.

[File Detection]
– Downloader/Win.Amadey.R5282269 (2022.10.17.03)
– Trojan/Win.Amadey.C5282244 (2022.10.17.03)
– Dropper/Win.Amadey.C5282248 (2022.10.17.03)

MD5

00a7588c41c5a1183f098901d30df09a

0184b0f6403420f7134a3e4a37498754

ccd5a8f11035b888a7a3de6035ac272e

Additional IOCs are available on AhnLab TIP.

URL

https[:]//office-download3791[.]com/list[.]php

https[:]//rs-shop7301[.]com/index[.]php

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/40483/