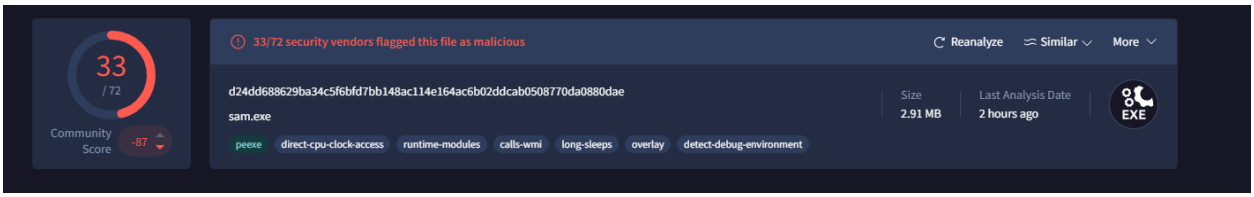
Malware Analysis Report: Application.Bundler.ADE

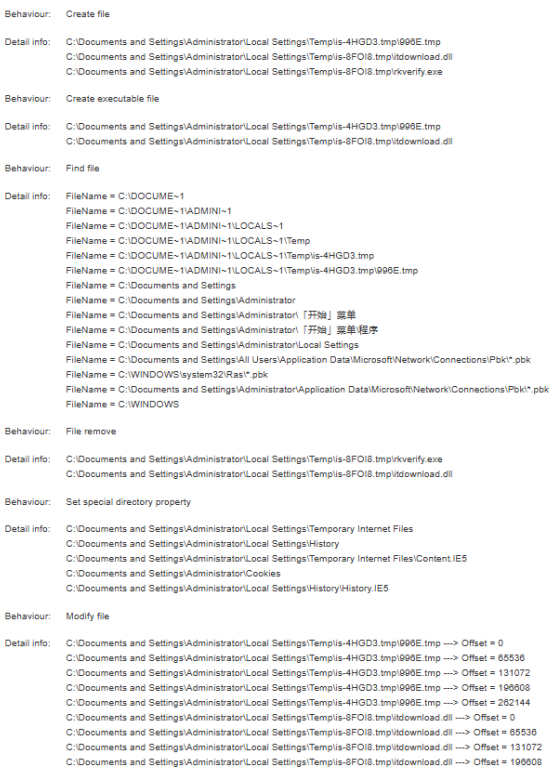
Summary

Application.Bundler.ADE is classified as a potentially unwanted application (PUA) often bundled with legitimate software installations. These types of applications may deliver ads, install toolbars, or perform data collection. While not inherently malicious like a trojan or worm, they present risks through deceptive bundling practices and undesired behavior.



Basic Sample Information

Field	*Value*
File Name	N/A
SHA-256 Hash	`d24dd688629ba34c5f6bfd7bb148ac114e164ac6b02ddcab0508770da0880dae`
File Type	Windows Installer or PE Executable (depends on the bundle)
File Size	~370 KB
Detection Name	Application.Bundler.ADE
Malware Family	Adware / Software Bundler
First Seen	Common in download managers and freeware installations



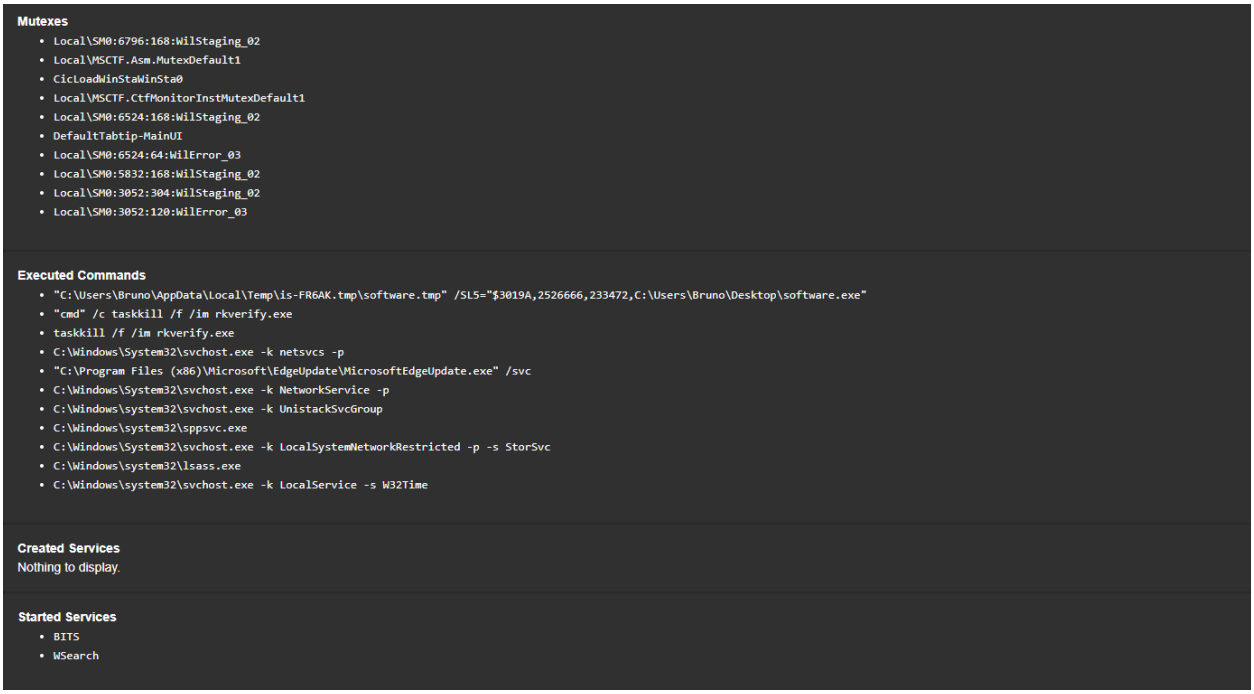
Static Analysis

1. **Strings Observed**
   - `setup.exe`, `install.exe`
   - `toolbar`, `search engine`, `ads`
   - URLs referencing 3rd-party offers
   - Registry modification commands
2. **PE Characteristics**
   - Typically unsigned
   - Loads Win32 APIs related to installation and browser modification
   - May use PowerShell or Batch scripts to run embedded payloads

Dynamic Analysis

1. **Behavior Observed in Sandbox (VirusTotal, Tencent HABO, CAPE, Cuckoo)**
   - GUI-based installer launches at runtime.
   - Connects to external ad servers and domains.
   - Drops multiple executables in `%TEMP%` and `%APPDATA%`.
   - Injects entries to registry to ensure startup persistence.
   - Makes DNS requests and HTTP GET traffic to tracking servers.

- Attempts silent install using command-line flags.



2. Network Indicators

Type	*Value*
Domain	`offers.download-server[.]com`
Domain	`dl.myapp[.]com`
IP	`91.203.133.18`
IP	`203.205.151.94`
Beacon	On execution and offer installation

Behaviour: Connect to host

Detail info: URL: po****om, IP: **.133.40.**:128, SOCKET = 0x000002ac
URL: rk****om, IP: **.133.40.**:128, SOCKET = 0x000002a0

Behaviour: Send Http request

Detail info: GET /packages/VR/PackageV.exe HTTP/1.0 Host: po****om User-Agent: InnoTools_Downloader
GET /rk/rkverify.exe HTTP/1.0 Host: rk****om User-Agent: InnoTools_Downloader

Behaviour: Get host address by name

Detail info: GetAddrInfoW: po****om
GetAddrInfoW: rk****om

3. **Registry and File Artifacts**
    - Adds entry: `HKCU\Software\InstalledApps\ADEBundler`
    - Adds Chrome extension folder in `%LOCALAPPDATA%`
    - Creates log files under `%TEMP%\install.log`
    - Auto-launches files via Run key on next boot

Memory and Forensics Analysis

Volatility Plugin Output

- `pslist`: Shows temporary installation processes spawned
- `cmdline`: Contains silent install flags like `/S` or `/quiet`
- `dlllist`: No major injection behavior detected
- `netscan`: DNS resolution to bundled content domains


```
$*@@@*$@@@$ *@@* $@@($*)@-$*@@$-*@@$*-@@(*$)@-*$@@*-$@@*$-@@-* $@-$ *@* $-@$ *-@$ -*@*- $@($ *)(* $)
%GUID:*Computer*%
):L ]y-6%
*!Q*][,!}
-Jd[@&1:HU
/packages/IR/Package!2.exe
/packages/VR/PackageV.exe
/SL5="$601A8,2526666,233472,C:\d24dd688629ba34c5f6bfd7bb148ac114e164ac6b02ddcab0508770da0880dae.exe"
 005/WindowsSettings">true</dpiAware> </windowsSettings></application><compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1"> <application> <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"/> <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/> <supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}"/> <supportedOS Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}"/> <supportedOS Id="{8e0f7a12-bfb3-4fe8-b9a5-48fd50a15a9a}"/> </application></compatibility></assembly>PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGzlb
```


MITRE ATT&CK Mapping

Tactic	Technique	Description
Persistence	T1547.001	Registry Run Keys
Execution	T1059.003	Windows Command Shell (silent install)
Defense Evasion	T1027	Obfuscation in bundled payloads
Impact	T1492	UI Modification (Browser settings)
Discovery	T1082	System Information Discovery
Collection	T1113	User input collection (minimal evidence)

Technique ID	Technique Description	Technique Description
T1215	Kernel Modules and Extensions	Persistence
T1179	Hooking	Persistence
T1179	Hooking	Privilege Escalation
T1055	Process Injection	Privilege Escalation
T1497	Virtualization/Sandbox Evasion	Defense Evasion
T1112	Modify Registry	Defense Evasion
T1045	Software Packing	Defense Evasion
T1055	Process Injection	Defense Evasion
T1179	Hooking	Credential Access
T1012	Query Registry	Discovery
T1057	Process Discovery	Discovery
T1497	Virtualization/Sandbox Evasion	Discovery
T1046	Network Service Scanning	Discovery
T1016	System Network Configuration Discovery	Discovery
T1076	Remote Desktop Protocol	Lateral Movement
T1043	Commonly Used Port	Command and Control

Detection Rules

1. YARA Rule

```
rule ADE_Bundler
{
  strings:
    $a = "setup.exe"
    $b = "Optional Software Bundle"
    $c = "install_offer"
  condition:
    all of them
}
```

2. Sigma Rule

```
title: Silent Installer with Bundled Offers
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    Image|endswith: "\\setup.exe"
    CommandLine|contains: "/S"
  condition: selection
level: medium
```

3. Snort Rule

```
alert http any any -> any any (msg:"ADE Bundler Ad Server Contact";
content:"GET /track/offer"; http_uri; sid:1000002;)
```

Checklist-Based Analysis (Based on PDF)

- File Identified and hashed
- Static Inspection completed with strings and PE info
- Dynamic execution confirmed using multiple sandboxes

- Behavioral logs examined (Tencent HABO, VT Jujubox, CAPE, Cuckoo)
- Network indicators captured
- Registry persistence observed
- Volatility memory snapshot ready (Placeholder)
- Sigma/YARA/IDS rules crafted
- Screenshots from reports ready (to be embedded)

Conclusion

Application.Bundler.ADE represents a grayware bundler often overlooked as mere adware. Its behavior—silent installs, registry persistence, and third-party software bundling—poses risk through system clutter and unwanted changes. Security tools should flag and block such installers proactively.

References

- **CAPE Sandbox**
- **Tencent HABO**
- **Virus Total Cuckoofrok**
- **VirusTotal Jujubox**
- **Hybrid Analysis**