Downloader.apk

Detected:

<https://www.virustotal.com/gui/file/286e2c552ecafa6a5f5c2aa624cf760db1952acf7a8634b4365cbf31c97fac85/detection>

286e2c552ecafa6a5f5c2aa624cf760db1952acf7a8634b4365cbf31c97fac85

Avira

|  |  |
| --- | --- |
| Name | Android |
| Date Discovered | Nov 23, 2015 |
| Type | Malware |
| Impact | Medium |
| Operating system | AndroidOS |

The file is a malicious Android application that undermines the security of the device or the privacy of the user. Typically, Android malware attempts to steal personal or account information, gain access to device functions via backdoors, send text messages or dial premium numbers, and lock or encrypt the device so the user has to pay to unlock the device.

Microsoft:

TrojanDropper:AndroidOS/SAgent.AN!MTB

[Detected by Microsoft Defender Antivirus](https://www.microsoft.com/en-us/windows/windows-defender?ocid=cx-wdsi-ency)

Aliases: No associated aliases

Summary

[Microsoft Defender for Endpoint](https://www.microsoft.com/en-us/security/business/threat-protection/endpoint-defender) detects and removes this threat.

This threat arrives on an Android device through various means, such as, but not limited to:

* Installation of apps from unknown or unverified download sites
* Exploitation of vulnerabilities
* Being dropped or downloaded by another malware

After it successfully installs and launches on the device, this threat has capabilities that might further compromise the device or the network the device is connected to.

HOTSUSHISTAR

Detected:

<https://www.virustotal.com/gui/file/6946bc153e41a0fc8e8c1eea0592d92750cecef3a05edaad67a9987847be41b6/detection>

|  |  |
| --- | --- |
| Name | PUA |
| Date Discovered | Mar 2, 2018 |
| Type | Potential Unwanted Application |
| Impact | Low |
| Operating system | Windows |

This class of detection flags, Potentially Unwanted Applications (PUA), may compromise the user's privacy and the security of the local system. These are legitimate applications that often try to use social engineering to make the user install additional offers during the installation of the software the user originally wanted. A PUA application classification is the result of software, an advert, or a website exhibiting one or more offending behaviors and/or properties. A full PUA list is available at <http://www.avira.com/en/potentially-unwanted-applications>. This detection doesn't mean that the file is malicious. However, if the file was installed on the system without the user's knowledge, the user's privacy or system security might be compromised. Disabling this detection is only recommended for advanced users who understand the risks and how to use these applications.

Disney plusHack

<https://www.virustotal.com/gui/file/3fb213290e01b1ea4c79c73d500e955f861c4861da4b1f5fa0d14f2d3c2cd7b1>

tic tac toe.apk

<https://www.virustotal.com/gui/file/adeeafa646e1411319d548b1c61d91e3d34a000217b49598e794cb11aea14d00>