Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:11:21 UTC

Tool: AppleJeus

Names	AppleJeus
Category	Malware
Type	Reconnaissance, Downloader
Description	(Kaspersky) The main purpose of Updater.exe is to collect the victim's host information and send it back to the server. Upon launch, the malware creates a unique string with the format string template "%09d-%05d" based on random values, which is used as a unique identifier of the infected host. This malware collects process lists, excluding "[System Process]" and "System" processes and gets the exact OS version from the registry value at "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion". It seems that such values only exist from Windows 10, so we assume that the author developed and tested it on Windows 10. At the end of the installation process, the installer immediately runs the Updater.exe module with the "CheckUpdate" parameter. This file looks like a regular tool and most likely will not arouse the suspicion of system administrators. After all, it even contains a valid digital signature, which belongs to the same vendor. But the devil is in the detail, as usual. The code writer developed this project under the codename "jeus", which was discovered in a PDB path included in the updater and used as unique HTTP multipart message data separator string. Because of this, and the fact that the attacked platforms include Apple macOS, we decided to call this Operation AppleJeus.
Information	<https://securelist.com/operation-applejeus/87553/> <https://us-cert.cisa.gov/ncas/current-activity/2021/02/17/north-korean-malicious-cyber-activity-applejeus>
MITRE ATT&CK	<https://attack.mitre.org/software/S0584/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.applejeus> <https://malpedia.caad.fkie.fraunhofer.de/details/osx.applejeus>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:AppleJeus>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool AppleJeus

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2ef2a76e-950e-49fd-be23-a1f1d5c61f5e