Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:12:35 UTC

Tool: MSUpdater

Names	MSUpdater
Category	Malware
Type	Dropper, Backdoor, Info stealer, Exfiltration
Description	(ZScaler) The malware dropped and launched from the PDF exploit has been seen to be virtual machine (VM) aware in order to prevent analysis within a sandbox. The Trojan functionality is decrypted at run-time, and includes expected functionality, such as, downloading, uploading, and executing files driven by commands from the C&C. Communication with the C&C is over HTTP but is encoded to evade detection. The Trojan file name (e.g., 'msupdate.exe') and the HTTP paths used in the C&C (e.g., '/microsoftupdate/getupdate/default.aspx') are used to stay under the radar by appearing to be related to Microsoft Windows Update - hence the name given to this Trojan.
Information	<https://www.zscaler.com/blogs/research/msupdater-trojan-and-link-targeted-attacks> <https://cybersecurity.att.com/blogs/labs-research/msupdater-trojan-found-using-cve-2012-0158-space-and-missile-defense-conference>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:msupdater>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool MSUpdater

Changed	Name	Country	Observed	
APT groups				
	Putter Panda, APT 2		2007	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e288f4fe-9d9f-4f36-be19-6895ad1ada0c