WMI Ghost - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:06:37 UTC

Tool: WMI Ghost

Names	WMI Ghost Wimmie Syndicasec
Category	Malware
Type	Backdoor, Exfiltration
Description	(Trend Micro) The malware used in the Luckycat campaign, detected by Trend Micro as TROJ_WIMMIE or VBS_WIMMIE, connects to a C&C server via HTTP over port 80. It is notable because it uses Windows Management Instrumentation (WMI) to establish persistence. VBS_WIMMIE registers a script that works as a backdoor to the WMI event handler and deletes files associated with it or TROJ_WIMMIE. As a result, the backdoor cannot be detected by antivirus software through simple file scanning.The compromised computer posts data to a PHP script that runs on the C&C server, usually count.php. The initial communication results in the creation of a file on the C&C server that contains information on the compromised computer. Although the file is empty, the file name contains the hostname of the compromised computer, followed by its MAC address, along with the campaign code the attackers use to identify which malware attack caused the compromise: ~[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE] The attacker then creates a file with a name that ends in @.c, which contains a command. [HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE]@.c The compromised computer then downloads the file and executes the specified command, which may include any of the following: • Get external IP address • Execute shell command • Download file • Upload file The compromised computer then sends the output to the C&C server and deletes the command file.

Information	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf> <https://secrary.com/ReversingMalware/WMIGhost/> <https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.wmighost>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool WMI Ghost

Changed	Name	Country	Observed	
APT groups				
	Lotus Blossom, Spring Dragon, Thrip		2012-Aug 2024	
	Lucky Cat		2011	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=79ca754c-8547-4c75-b7c9-836e9bf0034f