Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:01:32 UTC

Tool: FlawedGrace

Names	FlawedGrace GraceWire
Category	Malware
Type	Backdoor, Downloader
Description	(Proofpoint) FlawedGrace is a remote access trojan (RAT) named after debugging artifacts (class names) left in the analyzed sample. The malware is written in C++. It is a very large program and makes extensive use of object-oriented and multithreaded programming techniques. This makes reverse engineering and debugging the malware both difficult and time consuming. The coding style and techniques suggest that FlawedGrace was not written by the same developer as ServHelper. FlawedGrace uses a complicated binary protocol for its command and control. It can use a configurable port for communications, but all samples we have observed to date have used port 443. Figure 8 shows an example of the first four messages between an infected system and C&C server. FlawedGrace also uses a series of commands, provided below for reference: • target_remove • target_update • target_reboot • target_module_load • target_module_load_external • target_module_unload • target_download • target_upload • target_rdp • target_passwords • target_servers • target_script

	• destroy_os • desktop_stat
Information	<https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505> <https://www.msreverseengineering.com/blog/2019/1/14/a-quick-solution-to-an-ugly-reverse-engineering-problem>
MITRE ATT&CK	<https://attack.mitre.org/software/S0383/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.flawedgrace>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool FlawedGrace

Changed	Name	Country	Observed	
APT groups				
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2e3f838e-197c-412f-a98d-4b3ad248baa6