Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:45:45 UTC

Tool: GrimPlant

Names	GrimPlant Elephant Implant
Category	Malware
Type	Reconnaissance, Backdoor, Tunneling
Description	(SOC Investigation) GrimPlant capabilities: • Gather IP address, hostname, OS, username, home dir • Execute commands received remotely and return results to C2 • Use gRPC (HTTP/2+SSL) for C2 communication
Information	<https://www.socinvestigation.com/ukraines-cert-warns-russian-threat-actors-for-fake-av-updates/> <https://blog.malwarebytes.com/threat-intelligence/2022/04/new-uac-0056-activity-theres-a-go-elephant-in-the-room/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.grimplant>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool GrimPlant

Changed	Name	Country	Observed	
APT groups				
	SaintBear, Lorec53		2021-Oct 2022	

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