Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:40:51 UTC

Tool: RogueRobin

Names	RogueRobin RogueRobinNET
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration, Tunneling
Description	(Palo Alto) In our original blog on DarkHydrus, we analyzed a PowerShell-based payload we named RogueRobin. While performing the analysis on the delivery documents using the .sct file AppLocker bypass, we noticed the C# payload was functionally similar to the original RogueRobin payload. The similarities between the PowerShell and C# variants of RogueRobin suggests that the DarkHydrus group ported their code to a compiled variant. The C# variant of RogueRobin attempts to detect if it is executing in a sandbox environment using the same commands as in the PowerShell variant of RogueRobin. The series of commands, as seen in Table 2, include checks for virtualized environments, low memory, and processor counts, in addition to checks for common analysis tools running on the system. The Trojan also checks to see if a debugger is attached to its processes and will exit if it detects the presence of a debugger.
Information	<https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/> <https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0270/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.roguerobin> <https://malpedia.caad.fkie.fraunhofer.de/details/win.roguerobin>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:RogueRobin>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool RogueRobin

Changed	Name	Country	Observed	
APT groups				
	DarkHydrus, LazyMeerkat		2016-Jan 2019	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=87ad16c6-a771-4f89-bdd3-c5e2ad4f3354