Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:23:50 UTC

Tool: MgBot

Names	MgBot BLame Mgmbot POCOSTICK
Category	Malware
Type	Backdoor
Description	(Malwarebytes) MgBot uses several anti-analysis and anti-virtualization techniques. The code is self modifying which means it alters its code sections during runtime. This makes static analysis of the sample harder. MgBot tries to avoid running in known virtualized environment such as VmWare, Sandboxie and VirtualBox. To identify if it's running in one of these environments, it looks for the following DLL files: vmhgfs.dll, sbiedll.dll and vboxogl.dll and if it finds any of these DLLs, it goes to an infinite loop without doing any malicious activity.
Information	<https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/> <https://vb2020.vblocalhost.com/uploads/VB2020-43.pdf> <https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1146>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.mgbot>

Last change to this tool card: 28 December 2024

Download this tool card in JSON format

All groups using tool MgBot

Changed	Name	Country	Observed

APT groups

	Bronze Highland		2012-Jul 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ff3865c1-fb45-4197-89a2-2cce3bed17bb