Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:30:52 UTC

Tool: TONESHELL

Names	TONESHELL
Category	Malware
Type	Backdoor
Description	(Trend Micro) The TONESHELL malware is the main backdoor used in this campaign. It is a shellcode loader that loads and decodes the backdoor shellcode with a 32-byte key in memory. In the earlier version of TONESHELL, it has the capabilities from TONEINS malware, including establishing persistence and installing backdoors. However, the more recent version of TONESHELL is a standalone backdoor without any installer capabilities (such as the file ~$Talk points.docx). It is also obfuscated in a similar fashion to TONEINS malware, indicating that the actors continue to update the arsenal and separate the tools in order to bypass detection.
Information	<https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.toneshell>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool TONESHELL

Changed	Name	Country	Observed	
APT groups				
	CeranaKeeper		2022-2023	
	Mustang Panda, Bronze President		2012-Jun 2025	

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