Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:01:31 UTC

Tool: Sality

Names	Sality Sector Kuku SalLoad Kookoo SaliCode Kukacka
Category	Malware
Type	Botnet, Worm, Downloader, Loader
Description	(Cylance) The Sality virus infects local executables, removable storage, and remotely shared drives. It creates a peer-to-peer botnet which facilitates the downloading and execution of other malware. Sality can perform malicious code injection and modify its entry point to force code execution. This malware remains viable by adopting the successful strategies of other threats, implementing techniques like rootkit/backdoor capability, keylogging, and worm-like propagation.
Information	<https://threatvector.cylance.com/en_us/home/cylance-vs-sality-malware.html> <https://www.botconf.eu/wp-content/uploads/2015/12/OK-P18-Kleissner-Sality.pdf> <https://en.wikipedia.org/wiki/Sality>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sality>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Sality>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool Sality

Changed	Name	Country	Observed

Other groups

	Salty Spider		2003-Dec 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ccf23a1f-eec2-465a-89a8-fc38dfbfeea8