Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:01:25 UTC

Tool: ShadyRAT

Names	ShadyRAT
Category	Malware
Type	Backdoor, Info stealer
Description	(Trend Micro) This notorious data-stealing spying Trojan also used blogging platforms as a C&C channel, except that the commands are encrypted and encoded into HTML comments, interspersed with what appears to be legitimate content. This makes the traffic look like it comes from a real user visiting a blog with a regular web browser. In fact, the page is not being displayed at all on the infected system; the Trojan just decodes the information within the comments and is able to understand the commands the attacker is sending. On a cursory look to the actual blog, a visitor would never spot any of this, since the comments are never displayed on the browser either. This is a perfect vehicle for these attackers, who are trying to stay undetected for as long as possible. ShadyRAT was the first major targeted attack that was spotted in the wild, and this technique was possibly a contributing factor. The network traffic looks perfectly tame to any traffic observer or security device. On top of this, ShadyRAT was also able to decrypt and decode C&C commands hidden within JPG files using the LSB technique as seen in the first entry of this series. A shady one indeed.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-concealing-code-and-cc-traffic/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool ShadyRAT

Changed	Name	Country	Observed

APT groups

	Comment Crew, APT 1		2006-May 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=851d2801-ccbb-48b1-869d-2ba82ad45c9d