Threat Group Cards: A Threat Actor Encyclopedia

Tool: ShimRAT

Names	ShimRAT Shim RAT
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Fox-IT) ShimRat is a custom developed piece of malware known as a 'RAT', Remote Administration Tool. It has among others standard capabilities for filesystem interaction.The malware was originally built in 2012 and its features were expanded over the years. The artifacts left in the first samples, are a good indicator that the project has been started in 2012. Multiple pdB paths were seen in the early versions of ShimRat. These PDB paths are not visible in the latest versions of ShimRat, due to how the samples are prepared. The PDB paths are either stripped or filled with different paths.
Information	<https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0444/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.shimrat>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool ShimRAT

Changed	Name	Country	Observed	
APT groups				
	Whitefly, Mofang	[Unknown]	2012-Jul 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=aac889bc-4215-404b-afa4-343364ff8cd4