Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:51:33 UTC

Tool: FormerFirstRAT

Names	FormerFirstRAT FF-RAT ffrat
Category	Malware
Type	Backdoor, Exfiltration
Description	(Palo Alto) This remote administration tool (RAT) is referred to as “FormerFirstRAT” by its authors. FormerFirstRAT communicates using unencrypted HTTP over port 443; the use of mismatching ports and communication protocols is not uncommon in targeted attack campaigns. In addition, port / protocol mis-match traffic can be an indicator of bad activity. The remote server has the ability to respond and provide instructions to the RAT. We have identified the following functionalities: • Modify sleep timer between requests • Execute a command and return the command output • Browse the file system • Download files • Delete files • Exfiltrate victim information
Information	<https://unit42.paloaltonetworks.com/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.former_first_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:formerfirstrat>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool FormerFirstRAT

Changed	Name	Country	Observed	
APT groups				
	Bookworm		2015	
	DragonOK		2015-Jan 2017	
	RedAlpha		2015-2021	
	Samurai Panda		2009	
	Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens		2010-Oct 2018	

5 groups listed (5 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=d04ba5af-cabc-4710-bf6e-84688a211480