Threat Group Cards: A Threat Actor Encyclopedia

Tool: IRAFAU

Names	IRAFAU
Category	Malware
Type	Backdoor
Description	(Fortinet) The backdoor, which we now call “IRAFAU” from a decrypted string found during analysis, comes as a file packed with what looks to be modified UPX. Regardless, unpacking it is simple. Once unpacked, the backdoor malware’s behavior was not obvious because its strings were still encrypted and APIs used had been dynamically imported. So, the first thing this malware does is to initialize a structure where it stores the decrypted strings that will be used in the next function calls. This includes the command and control server string, function pointers, and dynamically imported APIs that will be used throughout its execution. This structure is passed as a parameter to subsequent functions.
Information	<https://www.fortinet.com/blog/threat-research/cve-2017-11826-exploited-in-the-wild-with-politically-themed-rtf-document>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool IRAFAU

Changed	Name	Country	Observed	
APT groups				
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

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