Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:52:11 UTC

Tool: HOMEFRY

Names	HOMEFRY
Category	Malware
Type	Credential stealer
Description	(FireEye) HOMEFRY: a 64-bit Windows password dumper/cracker that has previously been used in conjunction with AIRBREAK and BADFLICK backdoors. Some strings are obfuscated with XOR x56. The malware accepts up to two arguments at the command line: one to display cleartext credentials for each login session, and a second to display cleartext credentials, NTLM hashes, and malware version for each login session.
Information	<https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0232/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.homefry>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:HOMEFRY>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool HOMEFRY

Changed	Name	Country	Observed	
APT groups				
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	

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