Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:04:24 UTC

Tool: pngdowner

Names	pngdowner
Category	Malware
Type	Backdoor, Credential stealer
Description	(CrowdStrike) he pngdowner malware is a simple tool constructed using Microsoft Visual studio and implemented via single C++ source code file. Initially, the malware will perform a connectivity check to a hard-coded URL (http://www.microsoft.com), using a constant user agent Mozilla/4.0 (Compatible; MsIE 6.0;). If this request fails, the malware will attempt to extract proxy details and credentials from Windows Protected storage, and from the IE Credentials store using publicly known methods, using the proxy credentials for subsequent requests if they enable outbound HTTP access. An initial request is then made to the hard-coded C2 server and initial URI – forming a URL of the form (in this sample) http://login.stream-media.net/files/xx11/index.asp?95027775, where the numerical parameter represents a random integer. A hard-coded user agent of myagent is used for this request, and subsequent communication with the C2 server.
Information	<https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf> <https://www.iocbucket.com/iocs/7f7999ab7f223409ea9ea10cff82b064ce2a1a31>
MITRE ATT&CK	<https://attack.mitre.org/software/S0067/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.pngdowner>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool pngdowner

Changed	Name	Country	Observed

APT groups

	Putter Panda, APT 2		2007	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=37964559-63c8-4384-ad64-fdb22fd4796d