Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:06:25 UTC

Tool: BlackCoffee

Names	BlackCoffee PNGRAT ZoxPNG gresim
Category	Malware
Type	Backdoor
Description	(Novetta) ZoxPNG is a very simple RAT that uses the PNG image file format as the carrier for data going to and from the C2 server. ZoxPNG supports 13 commands natively. In addition, ZoxPNG has the ability to load and execute arbitrary code from the C2 server providing an almost unlimited feature set. For instance, ZoxPNG provides no functionality for key logging, screen grabbing or file execution. If an attacker required such functionality, the attacker would construct a simple shell-code binary which the ZoxPNG binary could execute thereby expanding the feature set of the Trojan. ZoxPNG does not contain any configuration information. The attacker using ZoxPNG must specify the C2 server address as a command line argument.
Information	<https://www.novetta.com/wp-content/uploads/2014/11/ZoxPNG.pdf> <https://www.fireeye.com/current-threats/apt-groups/rpt-apt17.html> <https://www.zdnet.com/article/fireeye-microsoft-wipe-technet-clean-of-malware-hidden-by-hackers/> <http://malware-log.hatenablog.com/entry/2015/05/18/000000_1>
MITRE ATT&CK	<https://attack.mitre.org/software/S0069/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.blackcoffee>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BLACKCOFFEE>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool BlackCoffee

Changed	Name	Country	Observed	
APT groups				
	APT 17, Deputy Dog, Elderwood, Sneaky Panda		2009-Jun 2024	
	APT 41		2012-Jul 2025	
	Axiom, Group 72		2008-2008/2014	
	Hidden Lynx, Aurora Panda		2009-2014	
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=12cdfcf1-3407-4838-9e6f-aae75fd69dac