Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:53:21 UTC

Tool: Kurton

Names	Kurton
Category	Malware
Type	Backdoor, Tunneling, Info stealer
Description	This family of malware is a backdoor that tunnels its connection through a preconfigured proxy. The malware communicates with a remote command and control server over HTTPS via the proxy. The malware installs itself as a Windows service with a service name supplied by the attacker but defaults to IPRIP if no service name is provided during install.
Information	<https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> <http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.kurton>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Kurton

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	

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