Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:11:41 UTC

Tool: Kwampirs

Names	Kwampirs
Category	Malware
Type	Backdoor, Worm
Description	Kwampirs is a family of malware which uses SMB to spread. It typically will not execute or deploy in environments in which there is no publicly available admin$ share. It is a fully featured backdoor which can download additional modules. Typical C2 traffic is over HTTP and includes 'q=[ENCRYPTED DATA]' in the URI.
Information	<https://symantec-blogs.broadcom.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia> <https://lab52.io/blog/orangeworm-group-kwampirs-analysis-update/> <https://blog.reversinglabs.com/blog/unpacking-kwampirs-rat>
MITRE ATT&CK	<https://attack.mitre.org/software/S0236/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.kwampirs>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Kwampirs

Changed	Name	Country	Observed	
APT groups				
	Orangeworm	[Unknown]	2015-Jan 2020	

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