Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:21:34 UTC

Tool: Helminth

Names	Helminth
Category	Malware
Type	Backdoor
Description	Helminth is a backdoor that has at least two variants - one written in VBScript and PowerShell that is delivered via a macros in Excel spreadsheets, and one that is a standalone Windows executable.
Information	<https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/> <https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html> <https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/> <http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0170/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.helminth>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Helminth>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Helminth

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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