Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:08:01 UTC

Tool: BONDUPDATER

Names	BONDUPDATER Poison Frog Glimpse
Category	Malware
Type	Backdoor, Info stealer
Description	(Palo Alto) BONDUPDATER is a PowerShell-based Trojan first discovered by FireEye in mid-November 2017, when OilRig targeted a different Middle Eastern governmental organization. The BONDUPDATER Trojan contains basic backdoor functionality, allowing threat actors to upload and download files, as well as the ability to execute commands. BONDUPDATER, like other OilRig tools, uses DNS tunneling to communicate with its C2 server. During the past month, Unit 42 observed several attacks against a Middle Eastern government leveraging an updated version of the BONDUPDATER malware, which now includes the ability to use TXT records within its DNS tunneling protocol for its C2 communications.
Information	<https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/> <https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html> <https://www.boozallen.com/s/insight/blog/dark-labs-discovers-apt34-malware-variants.html> <https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0360/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.bondupdater>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BONDUPDATER>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool BONDUPDATER

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5ca10b6c-95cb-4ff3-abb0-afc59394a633