Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:37:44 UTC

Tool: GLOOXMAIL

Names	GLOOXMAIL Trojan.GTALK
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	GLOOXMAIL communicates with Google's Jabber/XMPP servers and authenticates with a hard-coded username and password. The malware can accept commands over XMPP that includes file upload and download, provide a remote shell, sending process listings, and terminating specified processes. The malware makes extensive use of the open source gloox library (<http://camaya.net/gloox/>, version 0.9.9.12) to communicate using the Jabber/XMPP protocol. All communications with the Google XMPP server are encrypted.
Information	<http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0026/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.glooxmail>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool GLOOXMAIL

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=54d56c5b-b85c-49b4-90de-91a60cb9041a