Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:02:35 UTC

Tool: MINEBRIDGE

Names	MINEBRIDGE MINEBRIDGE RAT GazGolder
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(FireEye) MINEBRIDGE is a 32-bit C++ backdoor designed to be loaded by an older, unpatched instance of the legitimate remote desktop software TeamViewer by DLL load-order hijacking. The backdoor hooks Windows APIs to prevent the victim from seeing the TeamViewer application. By default, MINEBRIDGE conducts command and control (C2) communication via HTTPS POST requests to hard-coded C2 domains. The POST requests contain a GUID derived from the system's volume serial number, a TeamViewer unique id and password, username, computer name, operating system version, and beacon interval. MINEBRIDGE can also communicate with a C2 server by sending TeamViewer chat messages using a custom window procedure hook. Collectively, the two C2 methods support commands for downloading and executing payloads, downloading arbitrary files, self-deletion and updating, process listing, shutting down and rebooting the system, executing arbitrary shell commands, process elevation, turning on/off TeamViewer's microphone, and gathering system UAC information. MINEBRIDGE's default method of communication is sending HTTPS POST requests over TCP port 443. This method of communication is always active; however, the beacon-interval time may be changed via a command. Before sending any C2 beacons, the sample waits to collect the TeamViewer generated unique id (<tv_id>) and password (<tv_pass>) via SetWindowsTextW hooks.
Information	<https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html> <https://www.zscaler.com/blogs/security-research/return-minebridge-rat-new-ttps-and-social-engineering-lures> <https://labs.sentinelone.com/breaking-ta505s-crypter-with-an-smt-solver/> <https://blog.morphisec.com/minebridge-on-the-rise-sophisticated-delivery-mechanism>

Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.minebridge>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:MINEBRIDGE>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool MINEBRIDGE

Changed	Name	Country	Observed	
APT groups				
	FIN11	[Unknown]	2016-Mar 2025	
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a84d3839-83ef-427c-b914-f46018515096