Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:52:36 UTC

Tool: BitRAT

Names	BitRAT
Category	Malware
Type	Backdoor, Info stealer, Credential stealer, Keylogger
Description	(Krabs on Security) As is the case with most HF malware, BitRAT is best described as an amalgamation of poorly pasted leaked source code slapped together alongside a fancy C# GUI. It makes heavy uses of libraries such as C++ Standard Library, Boost, OpenCV, and libcurl, as well as code copied directly from leaked malware source code or sites including StackOverflow. The choice of Camellia is somewhat unique, I have not seen this specific algorithm used in malware before.
Information	<https://krabsonsecurity.com/2020/08/22/bitrat-the-latest-in-copy-pasted-malware-by-incompetent-developers/> <https://krabsonsecurity.com/2020/09/04/bitrat-pt-2-hidden-browser-socks5-proxy-and-unknownproducts-unmasked/> <https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html> <https://www.fortinet.com/blog/threat-research/nft-lure-used-to-distribute-bitrat> <https://blog.qualys.com/vulnerabilities-threat-research/2023/01/03/bitrat-now-sharing-sensitive-bank-data-as-a-lure>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bit_rat>

Last change to this tool card: 15 February 2023

Download this tool card in JSON format

All groups using tool BitRAT

Changed	Name	Country	Observed
APT groups			

	Blind Eagle		2018-Nov 2024	
	OPERA1ER	[Unknown]	2016-Jul 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=041f9066-8f22-48b7-bb50-5d2ca3bf6410