Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:26:40 UTC

Tool: Byeby

Names	Byeby
Category	Malware
Type	Backdoor
Description	(Palo Alto) BYEBY was named based on a string within the malware itself. Most strings found within this malware are concatenated to 6 characters. One such example was an instance where a debug string contained 'BYE BY', which was likely a concatenated form of the phrase 'BYE BYE'. This malware is loaded as a DLL, with an export name of ServiceMain. The malware is configured to accept a number of commands. These appear to be Base64-encoded strings that, when decoded, provide their true meaning. Only the beginning of the commands are checked. The Base64-decoded strings have been included for the benefit of the reader.
Information	<https://unit42.paloaltonetworks.com/unit42-threat-actors-target-government-belarus-using-cmstar-trojan/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.byeby>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Byeby

Changed	Name	Country	Observed	
APT groups				
	Calypso		2016-Aug 2021	

	Vicious Panda		2015-Mar 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8ba1c2a6-3d3d-4dc7-82b4-6fb1913021ac