Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:09:11 UTC

Tool: Sysmain

Names	Sysmain
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Kaspersky) The autonomous part of Sysmain installs and registers itself to be persistent in the system. Then it gathers general information about the victims system, like • User- and computer names • Locale information • Network- and drive status • Default browsers • Running processes • File listing of the users profile directory. When ready, this data is submitted to one of the C&C-servers. After that, it checks periodically for new commands from C&C (pulling via HTTP). With a set of 11 commands, the malware is able to: • Execute shell-commands • Launch additional executables or libraries (sent by the attacker) • Collect arbitrary files for later exfiltration • Examine the victim’s filesystem. There are also commands used for maintenance purposes. Among others, there are commands to change the pubkey for C&C-communication or delete its traces in the registry.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Sysmain

Changed	Name	Country	Observed	
APT groups				
	Energetic Bear, Dragonfly		2010-Mar 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0290ce40-4114-48ba-a170-d1c40ca57a7d