Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:20:52 UTC

Tool: Syscon

Names	Syscon SYSCON Sanny
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Trend Micro) Bots can use various methods to establish a line of communication between themselves and their command-and-control (C&C) server. Usually, these are done via HTTP or other TCP/IP connections. However, we recently encountered a botnet that uses a more unusual method: an FTP server that, in effect, acts as a C&C server. Using an FTP server has some advantages. It is less common, and this fact may allow it to slip unnoticed by administrators and researchers. However, this also leaves the C&C traffic open for monitoring by others, including security researchers. In addition, thanks to a coding mistake by the attackers, this particular backdoor does not always run the right commands.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/syscon-backdoor-uses-ftp-as-a-cc-channel/> <https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0464/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.syscon>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Syscon

Changed	Name	Country	Observed	
APT groups				
	Honeybee	[Unknown]	2017	
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=60d69ed9-e971-40af-9ea7-658d46c130c4