Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:41:42 UTC

Tool: TINYTYPHON

Names	TINYTYPHON
Category	Malware
Type	Backdoor
Description	TINYTYPHON is a backdoor that has been used by the actors responsible for the MONSOON campaign. The majority of its code was reportedly taken from the MyDoom worm.
Information	<https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0131/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tinytyphon>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:TINYTYPHON>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool TINYTYPHON

Changed	Name	Country	Observed	
APT groups				
	Operation HangOver, Monsoon, Viceroy Tiger		2010-Jan 2020	
	Patchwork, Dropping Elephant		2013-Jun 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=05e9fde6-0d47-42c4-a579-d3c5c2e3a87d