Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:41:39 UTC

Tool: Tonnerre

Names	Tonnerre
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Check Point) The malware contains 5 Delphi forms, with each one responsible for a different capability: Form1 – Malware Installation and upgrading process. Form2 – Collects files from predefined folders – Documents, Downloads, Pictures and more. Form3 – Connects to an FTP server to exfiltrate collected data and get further commands. Form4 – Collects files from removable devices for exfiltration. Form5 – Uses the lame command line tool to record sound.
Information	<https://research.checkpoint.com/2021/after-lightning-comes-thunder/> <https://download.bitdefender.com/resources/files/News/CaseStudies/study/393/Bitdefender-Whitepaper-Iranian-APT-Makes-a-Comeback-with-Thunder-and-Lightning-Backdoor-and-Espionage-Combo.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tonnerre>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Tonnerre

Changed	Name	Country	Observed	
APT groups				
	Infy, Prince of Persia		2007-Feb 2017	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=bdbeb269-24c2-494e-a6c0-aba5a0cb6e59