8.t Dropper - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:29:14 UTC

Tool: 8.t Dropper

Names	8.t Dropper 8.t RTF exploit builder 8t_dropper RoyalRoad
Category	Malware
Type	Dropper
Description	8T_Dropper has been used by Chinese threat actor TA428 in order to install Cotx RAT onto victim's machines during Operation LagTime IT. According to Proofpoint the attack was developed against a number of government agencies in East Asia overseeing government information technology, domestic affairs, foreign affairs, economic development, and political processes. The dropper was delivered through an RTF document exploiting CVE-2018-0798.
Information	<https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.8t_dropper>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool 8.t Dropper

Changed	Name	Country	Observed	
APT groups				
	Bronze Butler, Tick, RedBaldNight, Stalker Panda		2006-Apr 2021	
	Goblin Panda, Cycldek, Conimes		2013-Jun 2020	
	Icefog, Dagger Panda		2011-2018/2019	

	Naikon, Lotus Panda		2010-Apr 2022	
	Rancor		2017	
	RedFoxtrot		2014-Aug 2021	
	SharpPanda, Sharp Dragon		2018-Mar 2024	
	TA428		2013-Jan 2022	
	Tonto Team, HartBeat, Karma Panda		2009-Apr 2023	
	Tropic Trooper, Pirate Panda, APT 23, KeyBoy		2011-Jun 2023	
	Vicious Panda		2015-Mar 2020	

11 groups listed (11 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fc849859-2aa0-4b98-8573-36d9041fd1c2