Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:08:23 UTC

Tool: MoneyTaker

Names	MoneyTaker
Category	Malware
Type	Banking trojan
Description	(Group-IB) In an attack on a Russian bank through the AWS CBR, hackers used a tool called MoneyTaker v5.0, which the group has been named after. Each component of this modular program performs a certain action: searches for payment orders and modifies them, replaces original payment details with fraudulent ones, and then erases traces. The success of replacement is due to the fact that at this stage the payment order has not yet been signed, which will occur after payment details are replaced. In addition to hiding the tracks, the concealment module again substitutes the fraudulent payment details in a debit advice after the transaction back with the original ones. This means that the payment order is sent and accepted for execution with the fraudulent payment details, and the responses come as if the payment details were the initial ones. This gives cybercriminals extra time to mule funds before the theft is detected.
Information	<https://www.group-ib.com/blog/moneytaker>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool MoneyTaker

Changed	Name	Country	Observed	
APT groups				
	MoneyTaker		2016	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=37a3a707-92e1-4ac7-bd2d-7a1779e5b3bb