Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:23:10 UTC

APT group: MoneyTaker

Names	MoneyTaker *(Group-IB)*
Country	Russia
Motivation	Financial crime
First seen	2016
Description	(Group-IB) In less than two years, this group has conducted over 20 successful attacks on financial institutions and legal firms in the USA, UK and Russia. The group has primarily been targeting card processing systems, including the AWS CBR (Russian Interbank System) and purportedly SWIFT (US). Given the wide usage of STAR in LATAM, financial institutions in LATAM could have particular exposure to a potential interest from the MoneyTaker group. Although the group has been successful at targeting a number of banks in different countries, to date, they have gone unreported. In addition to banks, the MoneyTaker group has attacked law firms and also financial software vendors. In total, Group-IB has confirmed 20 companies as MoneyTaker victims, with 16 attacks on US organizations, 3 attacks on Russian banks and 1 in the UK.
Observed	Sectors: Financial. Countries: Russia, UK, USA.
Tools used	Citadel, Kronos, Metasploit, MoneyTaker, Screenshotter.
Information	<https://www.group-ib.com/blog/moneytaker>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format