Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:13:35 UTC

APT group: GCMAN

Names	GCMAN *(Kaspersky)* G0036 *(MITRE)*
Country	Russia
Motivation	Financial crime
First seen	2016
Description	(Kaspersky) A second group, which we call GCMAN because the malware is based on code compiled on the GCC compiler, emerged recently using similar techniques to the Corkow, Metel Group to infect banking institutions and attempt to transfer money to e-currency services. The initial infection mechanism is handled by spear-phishing financial institution targets with e-mails carrying a malicious RAR archive to. Upon opening the RAR archive, an executable is started instead of a Microsoft Word document, resulting in infection. Once inside the network, the GCMAN group uses legitimate and penetration testing tools such as Putty, VNC, and Meterpreter for lateral movement. Our investigation revealed an attack where the group then planted a cron script into bank's server, sending financial transactions at the rate of $200 per minute. A time-based scheduler was invoking the script every minute to post new transactions directly to upstream payment processing system. This allowed the group to transfer money to multiple e-currency services without these transactions being reported to any system inside the bank.
Observed	Sectors: Financial. Countries: Russia.
Tools used	GCMAN, Meterpreter, PuTTY, VNC and malicious RAR archives.
Information	<https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0036/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
