GCMAN: how to steal $200 per minute

By Kaspersky

Published: 2017-09-13 · Archived: 2026-04-05 22:48:20 UTC

VIRUS DEFINITION

Virus Type: Advanced Persistent Threat, Trojan, Malware, APT, ATM, Banking Trojans, spear-phishing, cybercrime

What is GCMAN?

GCMAN is a group that uses APT techniques and legitimate penetration testing tools to infect computer networks and attempt to steal funds by transferring money from financial institutions to e-currency services. The malware was compiled with the help of the GCC compiler, a rarity among malware writers.

What it can do?

The initial infection mechanism is handled by spear-phishing. A financial institution is targeted with e-mails carrying a malicious RAR archive. When the RAR archive is opened an executable is started instead of a Microsoft Word document, resulting in infection. The group also plants a cron script into the bank's server to generate financial transactions at the rate of $200 per minute.

Who are the victims of its attacks?

The victims are limited to financial institutions.

Am I at risk?

You are in a risk group if your organisation falls into the category above. Make sure you are using advanced anti-malware solutions and taking advice from a reliable security company.

How do I know if I’m infected?

Kaspersky Lab products successfully detect and block the malware used by GCMMAN threat actors with the following detection names:

Backdoor.Win32.GCMan; Backdoor.Win64.GCMan; Trojan-Downloader.Win32.GCMan

The company is has also released crucial Indicators of Compromise (IOC) and other data to help organizations search for traces of these attack groups in their corporate networks.

How can I protect myself?

The only way to discover an attempted break in or a successful penetration of the perimeter is to analyze the behavior patterns and to try to spot an attack by identifying an attacker in a flow of typical corporate network activity.

To be on the safe side make sure you are using advanced anti-malware solutions such as Kaspersky Next EDR Optimum. Also pay attention to your cybersecurity awareness to make sure that you can identify phishing emails in your email box.

To raise the level of protection, it is recommended that organizations use System Watcher that includes the BSS (Behavior Stream Signatures) module. This is included in all modern products and solutions.

Of course, just offering a multitude of powerful endpoint security layers is not enough. Spear-phishing, one of the most popular techniques for initial infection, makes reliable mail security a must. Kaspersky Security for Mail Servers scans incoming emails for both malicious attachments and URLs, significantly reducing the chances of malware reaching its victims.

Recommended products:

- Kaspersky Premium Antivirus
- Download Kaspersky Premium Antivirus with 30-Day Free Trial
- Kaspersky VPN - Download and Try for Free
