Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:43:30 UTC

APT group: RTM

Names	RTM *(ESET)* G0048 *(MITRE)*
Country	Russia
Motivation	Financial crime
First seen	2015
Description	(ESET) There are several groups actively and profitably targeting businesses in Russia. A trend that we have seen unfold before our eyes lately is these cybercriminals' use of simple backdoors to gain a foothold in their targets' networks. Once they have this access, a lot of the work is done manually, slowly getting to understand the network layout and deploying custom tools the criminals can use to steal funds from these entities. Some of the groups that best exemplify these trends are Buhtrap, Ratopak Spider, Cobalt Group and Corkow, Metel. The group discussed in this white paper is part of this new trend. We call this new group RTM; it uses custom malware, written in Delphi, that we cover in detail in later sections. The first trace of this tool in our telemetry data dates back to late 2015. The group also makes use of several different modules that they deploy where appropriate to their targets. They are interested in users of remote banking systems (RBS), mainly in Russia and neighboring countries. That this group is mostly targeting businesses is apparent from the processes they are looking for on a compromised system. They look for software that is usually only installed on accountants' computers, such as remote banking software or tools to help with accounts pay.
Observed	Countries: Czech, Germany, Kazakhstan, Russia, Ukraine.
Tools used	AtNow, RTM.
Information	<https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0048/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
