Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:33:24 UTC

APT group: RATicate

Names	RATicate *(Sophos)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2019
Description	(Sophos) In a series of malspam campaigns dating back to November of 2019, an unidentified group sent out waves of installers that drop remote administration tool (RAT) and information stealing malware on victims' computers. We've identified five separate campaigns between November, 2019 and January, 2020 in which the payloads used similar packing code and pointed to the same command and control (C&C) infrastructure. The campaigns targeted industrial companies in Europe, the Middle East, and the Republic of Korea. This leads us to believe that they are all the work of the same actors—a group we've dubbed RATicate. A new campaign we believe connected to the same actors leverages concern about the global COVID-19 pandemic to convince victims to open the payloads. This is a shift in tactics, but we suspect that this group constantly changes the way they deploy malware—and that the group has conducted campaigns prior to this past November.
Observed	Sectors: Industrial, Manufacturing, Media, Telecommunications. Countries: Romania, Japan, Kuwait, South Korea, Switzerland, UK and Europe and Middle East.
Tools used	Agent Tesla, BetaBot, BlackRAT, Formbook, GuLoader, LokiBot, NetWire RC, njRAT, NSIS, RemcosRAT.
Information	<https://news.sophos.com/en-us/2020/05/14/raticate/> <https://news.sophos.com/en-us/2020/07/14/raticate-rats-as-service-with-commercial-crypter/>

Last change to this card: 15 July 2020

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=30e5ac74-bfff-470f-ba68-a9f34ea7c57b