RATANKBA, Software S0241 | MITRE ATT&CK®

Archived: 2026-04-05 14:04:41 UTC

RATANKBA is a remote controller tool used by Lazarus Group. RATANKBA has been used in attacks targeting financial institutions in Poland, Mexico, Uruguay, the United Kingdom, and Chile. It was also seen used against organizations related to telecommunications, management consulting, information technology, insurance, aviation, and education. RATANKBA has a graphical user interface to allow the attacker to issue jobs to perform on the infected machines. [1] [2]

ID: S0241

ⓘ

Type: MALWARE

ⓘ

Platforms: Windows

Version: 1.1

Created: 17 October 2018

Last Modified: 25 April 2025

Version Permalink

Live Version

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	RATANKBA uses the `net user` command.[2]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	RATANKBA uses HTTP/HTTPS for command and control communication.[1][2]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	There is a variant of RATANKBA that uses a PowerShell script instead of the traditional PE form.[1][2]
		.003	Command and Scripting Interpreter: Windows Command Shell	RATANKBA uses cmd.exe to execute commands.[1][2]

Domain	ID		Name	Use
Enterprise	T1105		Ingress Tool Transfer	RATANKBA uploads and downloads information.[1][2]
Enterprise	T1057		Process Discovery	RATANKBA lists the system's processes.[1][2]
Enterprise	T1055	.001	Process Injection: Dynamic-link Library Injection	RATANKBA performs a reflective DLL injection using a given pid.[1][2]
Enterprise	T1012		Query Registry	RATANKBA uses the command `reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings"`. [2]
Enterprise	T1018		Remote System Discovery	RATANKBA runs the `net view /domain` and `net view` commands.[2]
Enterprise	T1082		System Information Discovery	RATANKBA gathers information about the OS architecture, OS name, and OS version/Service pack.[1][2]
Enterprise	T1016		System Network Configuration Discovery	RATANKBA gathers the victim's IP address via the `ipconfig -all` command.[1][2]
Enterprise	T1049		System Network Connections Discovery	RATANKBA uses `netstat -ano` to search for specific IP address ranges. [2]
Enterprise	T1033		System Owner/User Discovery	RATANKBA runs the `whoami` and `query user` commands.[2]
Enterprise	T1007		System Service Discovery	RATANKBA uses `tasklist /svc` to display running tasks.[2]
Enterprise	T1047		Windows Management Instrumentation	RATANKBA uses WMI to perform process monitoring.[1][2]

Source: https://attack.mitre.org/software/S0241