Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:50:49 UTC

Tool: Ranbyus

Names	Ranbyus
Category	Malware
Type	Banking trojan, Backdoor, Info stealer, Credential stealer, Botnet
Description	(ESET) This banking trojan doesn't have web-injection functionality and instead implements a targeted attack on specific banking/payment software. Win32/Spy.Ranbyus collects information about the infected system (active processes, OS version and so on) and forwards it to its command center. The main functionality for stealing money is based on a set of various form grabbers for specific payment software.
Information	<https://www.welivesecurity.com/2012/12/19/win32spy-ranbyus-modifying-java-code-in-rbs/> <https://www.welivesecurity.com/2012/06/05/smartcard-vulnerabilities-in-modern-banking-malware/> <http://www.xylibox.com/2013/01/trojanwin32spyranbyus.html> <https://www.johannesbader.ch/2015/05/the-dga-of-ranbyus/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ranbyus>

Last change to this tool card: 22 May 2020

Download this tool card in JSON format

All groups using tool Ranbyus

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

1 group listed (0 APT, 0 other, 1 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a3572c1a-b6eb-4dda-aff7-2158f479b17b