Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:55:27 UTC

Tool: RomeoBravo

Names	RomeoBravo BravoNC
Category	Malware
Type	Backdoor
Description	(SecurityWeek) A new sample of WannaCry emerged in late March, and five organizations were infected with it. The RomeoAlfa and BravoNC backdoors were employed in these attacks, with the former used to drop WannaCry onto the compromised computers of at least two victims. AlphaNC is believed to be an evolution of Duuzer, a sub-family of the Destover wiping tool used in the Sony attacks. These attacks hit organizations spanning a range of sectors and geographies, but Symantec found evidence of the tools used in the February attacks on the computers compromised in March and April as well. The BravoNC Trojan was used to deliver WannaCry to the computers of at least two other victims, the security researchers say. The malware connects to a C&C server hosted at the same IP address as the IP address used by Destover and Duuzer samples, and which was also referred to in a Blue Coat report last year.
Information	<https://www.securityweek.com/wannacry-highly-likely-work-north-korean-linked-hackers-symantec-says> <https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-RAT-and-Staging-Report.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bravonc>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool RomeoBravo

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=38bd5c63-903d-4124-bb78-987dcc03937c