Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:00:03 UTC

Tool: Metel

Names	Metel
Category	Malware
Type	Reconnaissance, Backdoor, Credential stealer, Info stealer
Description	(Kaspersky) Metel, the Russian word for blizzard, burrows its way into a financial organization using cleverly crafted spear phishing emails laced with malware, or luring victims to sites hosting the Niteris EK. The malware steals system information including process lists and screenshots, sending it to the attackers who evaluate whether the infected machine is interesting enough load the remainder of the Metel malware package. The malware contains more than 30 modules—some homemade, some taken from publicly available sources. The attackers also use legitimate pen-testing tools such as mimikatz, which is freely available and used by analysts to extract plaintext passwords, hashes, PIN codes and Kerberos tickets from the memory of Windows machines. Using this stolen data, the attackers are available to pivot internally, stealing credentials until they landed on a domain controller. With the reins of a domain controller, the attackers could extend their reach onto any machine.
Information	<https://threatpost.com/spree-of-bank-robberies-show-cybercriminals-borrowing-from-apt-attacks/116173/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Metel

Changed	Name	Country	Observed
APT groups			

	Corkow, Metel		2011	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a97eaa90-0c9a-4655-a212-01173f31b286