

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:53:42 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool AMTsol

Tool: AMTsol

Names	AMTsol Adupihan
Category	Malware
Type	Exfiltration
Description	<p>(Microsoft) Since the 2016 publication, Microsoft has come across an evolution of PLATINUM’s file-transfer tool, one that uses the Intel Active Management Technology (AMT) Serial-over-LAN (SOL) channel for communication. This channel works independently of the operating system (OS), rendering any communication over it invisible to firewall and network monitoring applications running on the host device. Until this incident, no malware had been discovered misusing the AMT SOL feature for communication.</p> <p>Upon discovery of this unique file-transfer tool, Microsoft shared information with Intel, and the two companies collaborated to analyze and better understand the purpose and implementation of the tool. We confirmed that the tool did not expose vulnerabilities in the management technology itself, but rather misused AMT SOL within target networks that have already been compromised to keep communication stealthy and evade security applications.</p>
Information	< https://www.microsoft.com/security/blog/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.amtsol >

Last change to this tool card: 28 December 2022

Download this tool card in [JSON](#) format

All groups using tool AMTsol

Changed	Name	Country	Observed
APT groups			

	Platinum		2009-Nov 2019	
--	--------------------------	---	---------------	--

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=454c7a03-4419-43d9-9671-5c70a4a81a8d>