

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:45:40 UTC

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

Tool: Tyupkin

Names	Tyupkin Padpin
Category	Malware
Type	ATM malware
Description	(Lastline) For today's case study, we use a Tyupkin malware sample, a .Net application for bank automated teller machines (ATM) running on the Microsoft Windows operating system. Tyupkin's aim is to steal cash by sending a specific command to the cash dispenser of the compromised ATM. During the analysis, our sandbox will trick the malware into believing that our analysis environment is an ATM itself. We will achieve this by submitting our sample bundled with a few specific DLLs that provide programmer's interfaces to a Windows-based ATM, Extensions for Financial Services (XFS).
Information	<p><https://www.lastline.com/labsblog/tyupkin-atm-malware/></p> <p><https://archive.f-secure.com/weblog/archives/00002751.html></p> <p><https://securelist.com/tyupkin-manipulating-atm-machines-with-malware/66988/></p> <p><https://www.atmmarketplace.com/articles/can-the-atm-industry-stop-tyupkin-in-its-tracks/></p> <p><https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf></p>
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.tyupkin >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:tyupkin >

Last change to this tool card: 25 May 2020

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

All groups using tool Tyupkin

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=c524bf68-1845-457b-8cf3-cff7cae6714e>