Operation Harvest - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:18:15 UTC

APT group: Operation Harvest

Names	Operation Harvest *(McAfee)*
Country	China
Motivation	Information theft and espionage
First seen	2016
Description	(McAfee) Following a recent Incident Response, McAfee Enterprise‘s Advanced Threat Research (ATR) team worked with its Professional Services IR team to support a case that initially started as a malware incident but ultimately turned out to be a long-term cyber-attack. The diagram reflecting our outcome insinuated that Emissary Panda, APT 27, LuckyMouse, Bronze Union and APT 41 are the most likely candidates that overlap with the (sub-)techniques we observed.
Observed	
Tools used	BadPotato, Impacket, Mimikatz, nbtscan, PlugX, ProcDump, PsExec, RottenPotato, SMBExec, Winnti, WinRAR.
Information	<https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/operation-harvest-a-deep-dive-into-a-long-term-campaign/>

Last change to this card: 02 November 2021

Download this actor card in PDF or JSON format
