Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:59:17 UTC

APT group: Tiny Spider

Names	Tiny Spider *(CrowdStrike)*	
Country	[Unknown]	
Motivation	Financial crime	
First seen	2015	
Description	(ForcePoint) It all starts with the delivery of a small loader called TinyLoader, an obfuscated executable withsimple–yet powerful –downloader functionality. Upon execution, it will first brute force its own decryption key (a 32-bit value, meaning this takes a fraction of second on modern PCs) before using this to decrypt the main program code. The core functionality of the decrypted code is communication with a set of hardcoded C2 servers by IP and port. If the C2 is active, it will provide what is effectively a piece of shellcode, encrypted by another 32-bit constant. This shellcode is not 'fire and forget': it instead sees the loader establish a semi-interactive two-way communication with the C2. Note that the earliest traits and mentions of TinyLoader go back to as far as 2015.	
Observed	Sectors: Retail. Countries: Worldwide.	
Tools used	PinkKite, PsExec, TinyPOS, TinyLoader.	
Operations performed	2017	A new family of point-of-sale malware, dubbed PinkKite, has been identified by researchers who say the malware is tiny in size, but can delivered a hefty blow to POS endpoints. <https://threatpost.com/new-pos-malware-pinkkite-takes-flight/130428/>
Information	<https://www.forcepoint.com/sites/default/files/resources/files/report-tinypos-analysis-en.pdf>	

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=ca6c6c94-9ef8-4aa4-8d9e-ad943b9fbe23