Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:17:07 UTC

Tool: Nibatad

Names	Nibatad
Category	Malware
Type	Loader, Downloader
Description	(Symantec) In some attacks, Whitefly has used a second piece of custom malware, Trojan.Nibatad. Like Vcrodat, Nibatad is also a loader that leverages search order hijacking, and downloads an encrypted payload to the infected computer. And similar to Vcrodat, the Nibatad payload is designed to facilitate information theft from an infected computer. While Vcrodat is delivered via the malicious dropper, we have yet to discover how Nibatad is delivered to the infected computer. Why Whitefly uses these two different loaders in some of its attacks remains unknown. And while we have found both Vcrodat and Nibatad inside individual victim organizations, we have not found any evidence of them being used simultaneously on a single computer.
Information	<https://symantec-blogs.broadcom.com/blogs/threat-intelligence/whitefly-espionage-singapore?es_p=8774683>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Nibatad

Changed	Name	Country	Observed	
APT groups				
	Whitefly, Mofang	[Unknown]	2012-Jul 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=083cff3b-8471-4192-8f4d-9dc8e52b0659