Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:25:04 UTC

Tool: DoppelPaymer

Names	DoppelPaymer Pay OR Grief
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(CrowdStrike) We have dubbed this new ransomware DoppelPaymer because it shares most of its code with the BitPaymer ransomware operated by INDRIK SPIDER. However, there are a number of differences between DoppelPaymer and BitPaymer, which may signify that one or more members of INDRIK SPIDER have split from the group and forked the source code of both Dridex and BitPaymer to start their own Big Game Hunting ransomware operation.
Information	<https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.doppelpaymer>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DoppelPaymer>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool DoppelPaymer

Changed	Name	Country	Observed	
APT groups				
	Doppel Spider		2019-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6e1df6f2-f969-4cd0-bc33-e25588eb2672