Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:23:41 UTC

Tool: HammerDuke

Names	HammerDuke HAMMERTOSS NetDuke tDiscoverer
Category	Malware
Type	Backdoor, Loader
Description	(F-Secure) HammerDuke is a simple backdoor that is apparently designed for similar use cases as SeaDuke. Specifically, the only known infection vector for HammerDuke is to be downloaded and executed by CozyDuke onto a victim that has already been compromised by that toolset. This, together with HammerDuke's simplistic backdoor functionality, suggests that it is primarily used by the Dukes group as a secondary backdoor left on CozyDuke victims after CozyDuke performed the initial infection and stole any readily available information from them. HammerDuke is however interesting because it is written in .NET, and even more so because of its occasional use of Twitter as a C&C communication channel. Some HammerDuke variants only contain a hardcoded C&C server address from which they will retrieve commands, but other HammerDuke variants will first use a custom algorithm to generate a Twitter account name based on the current date. If the account exists, HammerDuke will then search for tweets from that account with links to image files that contain embedded commands for the toolset to execute. HammerDuke's use of Twitter and crafted image files is reminiscent of other Duke toolsets. Both OnionDuke and MiniDuke also use date-based algorithms to generate Twitter account names and then searched for any tweets from those accounts that linked to image files. In contrast however, for OnionDuke and MiniDuke the linked image files contain embedded malware to be downloaded and executed, rather than instructions.
Information	<https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf> <https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/apt29-

	hammertoss-stealthy-tactics-define-a.pdf> <https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0037/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tdiscoverer>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:HammerDuke>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool HammerDuke

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1e6b6d4a-107d-4162-a46f-364df9138fc0