Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:13:53 UTC

Tool: NewCT

Names	NewCT CT
Category	Malware
Type	Loader
Description	(FireEye) The first-stage payload for RATs called “CT/NewCT” used by both the Moafee and DragonOK attack groups employs an evasive “CPU core check” technique. The payload attempts to detect the number of processor cores in the running environment, by calling the 'GetSystemInfo' API, which returns a structure with system data, including number of cores. If only one core is detected, it quits. This probably is an attempt to detect virtualized environments such as sandboxes, as well as other analysis environments used by reverse engineers, which often tend to be configured with a single core. If the CPU core check detects more than one core, it implants the NewCT2 RAT in %temp%\MSSoap.DLL(some variants will use BurnDCSrv.DLL and IntelAMTPP.DLL) and executes the written file.
Information	<https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.new_ct>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:newct>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool NewCT

Changed	Name	Country	Observed
APT groups			

	DragonOK		2015-Jan 2017	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6b4292bd-b44f-4f30-82f9-2ee15bdac87e