Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:58:54 UTC

Tool: IcedCoffee

Names	IcedCoffee
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Kaspersky) IcedCoffee is a fairly basic backdoor which uses WMI to collect a variety of system and user information from the system, which is then encoded with base64, encrypted with RC4 and submitted via HTTP POST to the C2 server. IcedCoffee has no built-in command capability, instead it may receive javascript files from the C2 server, which are deobfuscated and executed in memory, leaving nothing behind on disk for forensic analysis. IcedCoffee was not widely deployed, rather it was targeted at diplomats, including Ambassadors, of European governments.
Information	<https://securelist.com/shedding-skin-turlas-fresh-faces/88069/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:icedcoffee>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool IcedCoffee

Changed	Name	Country	Observed	
APT groups				
	Turla, Waterbug, Venomous Bear		1996-2024	

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