Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:37:49 UTC

Tool: PLAINTEE

Names	PLAINTEE
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Palo Alto) PLAINTEE is unusual in that it uses a custom UDP protocol for its network communications. PLAINTEE will create a unique GUID via a call to CoCreateGuid() to be used as an identifier for the victim. The malware then proceeds to collect general system enumeration data about the infected machine and enters a loop where it will decode an embedded config blob and send an initial beacon to the C2 server.
Information	<https://unit42.paloaltonetworks.com/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0254/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.plaintee>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PLAINTEE>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool PLAINTEE

Changed	Name	Country	Observed	
APT groups				
	Rancor		2017	

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