Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:33:33 UTC

Tool: BrutishCommand

Names	BrutishCommand
Category	Malware
Type	Dropper
Description	(Palo Alto) The BrutishCommand loader uses a very interesting method to decrypt the FakeM functional code. The main function in this loader checks the command line arguments passed to it, and if there are none present it will obtain a random number between 0-9 and create a new process using the same executable with this random number as a command line argument. If the executable has a command line argument, the Trojan subjects the value to a hashing algorithm and compares the hash to 0x20E3EEBA. If the value matches the static hash, the executable will subject the command line argument to a second algorithm that will produce a value that the Trojan will use as the decryption key to decrypt the embedded FakeM shellcode. It essentially brute forces its own decryption key by rerunning itself over and over until it runs with the correct value is provided on the command line. Unit 42 had not seen this technique used by other malware families and it introduces a challenging hurdle when attempting to analyze or debug the loader Trojan.
Information	<https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:BrutishCommand>

Last change to this tool card: 13 June 2020

Download this tool card in JSON format

All groups using tool BrutishCommand

Changed	Name	Country	Observed

APT groups

	Scarlet Mimic		2015-Aug 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3e2c0fb6-a852-47dd-9638-4a04399adbf9