Calypso RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:37:25 UTC

Tool: Calypso RAT

Names	Calypso RAT
Category	Malware
Type	Backdoor
Description	(Positive Technologies) The dropper extracts the payload as an installation BAT script and CAB archive, and saves it to disk. The payload inside the dropper has a magic header that the dropper searches for. The dropper encrypts and decrypts data with a self-developed algorithm that uses CRC32 as a pseudorandom number generator (PRNG). The algorithm performs arithmetic (addition and subtraction) between the generated data and the data that needs to be encrypted or decrypted. Now decrypted, the payload is saved to disk at %ALLUSERSPROFILE;\TMP_%d%d, where the last two numbers are replaced by random numbers returned by the rand() function. Depending on the configuration, the CAB archive contains one of three possibilities: a DLL and encrypted shellcode, a DLL with encoded loader in the resources, or an EXE file. We were unable to detect any instances of the last variant.
Information	<https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Calypso RAT

Changed	Name	Country	Observed	
APT groups				
	Calypso		2016-Aug 2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f2340394-4915-485e-b3f8-5aeafdb7794c