Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:18:38 UTC

APT group: Calypso

Names	Calypso *(Positive Technologies)* Bronze Medley *(SecureWorks)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2016	
Description	(Positive Technologies) The PT Expert Security Center first took note of Calypso in March 2019 during threat hunting. Our specialists collected multiple samples of malware used by the group. They have also identified the organizations hit by the attackers, as well as the attackers' C2 servers. Our data indicates that the group has been active since at least September 2016. The primary goal of the group is theft of confidential data. Main targets are governmental institutions in Brazil, India, Kazakhstan, Russia, Thailand, and Turkey. Our data gives reason to believe that the APT group is of Asian origin.	
Observed	Sectors: Government. Countries: Afghanistan, Belarus, Brazil, India, Kazakhstan, Kyrgyzstan, Mongolia, Russia, Thailand, Turkey, Ukraine.	
Tools used	Byeby, Calypso RAT, DCSync, DoublePulsar, EarthWorm, EternalBlue, EternalRomance, FlyingDutchman, Hussar, Mimikatz, nbtscan, netcat, OS_Check_445, PlugX, Quarks PwDump, SysInternals, TCP Port Scanner, Whitebird, ZXPortMap, Living off the Land.	
Operations performed	Mar 2021	Exchange servers under siege from at least 10 APT groups <https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/>
	Aug 2021	4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan <https://www.recordedfuture.com/chinese-APT-groups-target-afghan-telecommunications-firm/>

Information	<https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/>

Last change to this card: 02 November 2021

Download this actor card in PDF or JSON format
