BlackTech, Circuit Panda, Radio Panda

Archived: 2026-04-05 22:00:25 UTC

APT group: BlackTech, Circuit Panda, Radio Panda

Names	BlackTech *(Trend Micro)* Circuit Panda *(CrowdStrike)* Radio Panda *(CrowdStrike)* Palmerworm *(Symantec)* TEMP.Overboard *(FireEye)* T-APT-03 *(Tencent)* Red Djinn *(PWC)* Manga Taurus *(Palo Alto)* Earth Hundun *(Trend Micro)* Canary Typhoon *(Microsoft)* G0098 *(MITRE)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2010
Description	(Trend Micro) BlackTech is a cyber espionage group operating against targets in East Asia, particularly Taiwan, and occasionally, Japan and Hong Kong. Based on the mutexes and domain names of some of their C&C servers, BlackTech's campaigns are likely designed to steal their target's technology. Following their activities and evolving tactics and techniques helped us uncover the proverbial red string of fate that connected three seemingly disparate campaigns: PLEAD, Shrouded Crossbow, and of late, Waterbear.
Observed	Sectors: Construction, Financial, Government, Healthcare, Media, Technology. Countries: China, Hong Kong, Japan, Taiwan, USA.
Tools used	BendyBear, BIFROST, Bluether, DRIGO, Flagpro, Gh0stTimes, IconDown, KIVARS, PLEAD, XBOW, Living off the Land.

Operations performed	2010	Operation “Shrouded Crossbow” This campaign, first observed in 2010, is believed to be operated by a well-funded group given how it appeared to have purchased the source code of the BIFROST backdoor, which the operators enhanced and created other tools from. Shrouded Crossbow targeted privatized agencies and government contractors as well as enterprises in the consumer electronics, computer, healthcare, and financial industries. <https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/>
	2012	Operation “PLEAD” PLEAD is an information theft campaign with a penchant for confidential documents. Active since 2012, it has so far targeted Taiwanese government agencies and private organizations.
	2014	Operation “Waterbear” Waterbear has actually been operating for a long time. The campaign’s name is based on its malware’s capability to equip additional functions remotely.
	Jul 2018	ESET researchers have discovered a new malware campaign misusing stolen digital certificates. We spotted this malware campaign when our systems marked several files as suspicious. Interestingly, the flagged files were digitally signed using a valid D-Link Corporation code-signing certificate. The exact same certificate had been used to sign non-malicious D-Link software; therefore, the certificate was likely stolen. <https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/>
	Apr 2019	At the end of April 2019, ESET researchers utilizing ESET telemetry observed multiple attempts to deploy Plead malware in an unusual way. Specifically, the Plead backdoor was created and executed by a legitimate process named AsusWSPanel.exe. This process belongs to the Windows client for a cloud storage service called ASUS WebStorage. <https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/>
	Dec 2019	[…] in one of its recent campaigns, we’ve discovered a piece of Waterbear payload with a brand-new purpose: hiding its network behaviors from a specific security product by API hooking techniques. In our analysis, we have discovered that the security vendor is APAC-based, which is consistent with BlackTech’s targeted countries.

		<https://blog.trendmicro.com/trendlabs-security-intelligence/waterbear-is-back-uses-api-hooking-to-evade-security-product-detection/>
	2020	The addition of a US target to this campaign suggests the group is expanding campaigns to embrace a wider, more geographically diverse set of targets in their quest to steal information – although the full motivations remain unclear. <https://www.zdnet.com/article/these-hackers-have-spent-months-hiding-out-in-company-networks-undetected/>
	Aug 2020	BendyBear: Novel Chinese Shellcode Linked With Cyber Espionage Group BlackTech <https://unit42.paloaltonetworks.com/bendybear-shellcode-blacktech/>
	Oct 2020	Flagpro: The new malware used by BlackTech <https://insight-jp.nttsecurity.com/post/102hf3q/flagpro-the-new-malware-used-by-blacktech>
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/> <https://www.trendmicro.com/en_us/research/24/d/earth-hundun-waterbear-deuterbear.html> <https://www.trendmicro.com/en_us/research/24/e/earth-hundun-2.html>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0098/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=mangataurus>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
