Subgroup: Earth Freybug - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Subgroup: Earth Freybug

Names	Earth Freybug *(Trend Micro)*
Country	China
Motivation	Information theft and espionage
First seen	2012
Description	A subgroup of APT 41. (Trend Micro) Earth Freybug is a cyberthreat group that has been active since at least 2012 that focuses on espionage and financially motivated activities. It has been observed to target organizations from various sectors across different countries. Earth Freybug actors use a diverse range of tools and techniques, including LOLBins and custom malware. This article provides an in-depth look into two techniques used by Earth Freybug actors: dynamic-link library (DLL) hijacking and application programming interface (API) unhooking to prevent child processes from being monitored via a new malware we've discovered and dubbed UNAPIMON.
Observed	
Tools used	UNAPIMON, Living off the Land.
Information	<https://www.trendmicro.com/en_us/research/24/d/earth-freybug.html>

Last change to this card: 22 April 2024

Download this actor card in PDF or JSON format