Earth Lusca - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:58:52 UTC

APT group: Earth Lusca

Names	Earth Lusca *(Trend Micro)* Bronze University *(SecureWorks)* Chromium *(Microsoft)* Charcoal Typhoon *(Microsoft)* Red Dev 10 *(PWC)* Red Scylla *(PWC)* G1006 *(MITRE)*
Country	China
Motivation	Information theft and espionage, Financial gain
First seen	2019
Description	(Trend Micro) In this tech brief, we are going to expose a threat actor originating from China. Since the malware being used by the group, such as ShadowPad and Winnti, overlapped with other threat actors, its activities were attributed to other groups such as APT 41, Earth Baku, Sparkling Goblin, and the “Winnti” cluster in different reports. Our research reveals the different TTPs and the independent set of infrastructure that made us consider it a separate threat actor from the other known actors mentioned. Some reports named this threat actor “RedHotel, TAG-22” or “Fishmonger.” We decided to separate it from the Winnti umbrella and track this threat actor under the name “Earth Lusca.” Our investigation of Earth Lusca started in mid-2021, when we discovered a campaign targeting customer service companies in China via a watering hole attack. Eventually, our monitoring and research lead to the publication of a blog post on a previously-unreported malware known as BIOPASS RAT. We continued monitoring the threat actor, eventually discovering a few more targeted operations against various targets worldwide. In this research, we will expose all of the groups TTPs and its current operations. During our investigation, we also managed to reach some of the victims and gather interesting information from compromised servers that were used as watering holes. We were able to learn Earth Lusca’s reconnaissance and lateral movement techniques while working with our local incident response service team via our XDR system.

Observed	Sectors: Casinos and Gambling, Education, Government, Media, Telecommunications and Covid-19 research organizations, religious movements that are banned in Mainland China, pro-democracy and human rights political organizations and various cryptocurrency trading platforms. Countries: Australia, China, France, Germany, Hong Kong, Japan, Mongolia, Nepal, Nigeria, Philippines, Taiwan, Thailand, UAE, USA, Vietnam.	
Tools used	AntSword, BadPotato, Behinder, BIOPASS RAT, Cobalt Strike, Doraemon, EarthWorm, FRP, fscan, FunnySwitch, HUC Port Banner Scanner, lcx, KTLVdoor, Mimikatz, nbtscan, PipeMon, ShadowPad Winnti, SprySOCKS, Winnti, WinRAR.	
Operations performed	Early 2023	Earth Lusca Employs New Linux Backdoor, Uses Cobalt Strike for Lateral Movement <https://www.trendmicro.com/en_us/research/23/i/earth-lusca-employs-new-linux-backdoor.html>
	Dec 2023	Earth Lusca Uses Geopolitical Lure to Target Taiwan Before Elections <https://www.trendmicro.com/en_us/research/24/b/earth-lusca-uses-geopolitical-lure-to-target-taiwan.html>
	Sep 2024	Earth Lusca Uses KTLVdoor Backdoor for Multiplatform Intrusion <https://www.trendmicro.com/en_us/research/24/i/earth-lusca-ktlvdoor.html>
Information	<https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf> <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G1006/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
