Threat Agents/Groups Detected

For selected Attack Patterns

ML Supply Chain Compromise (attack-pattern--55e3e556-c45c-4b72-afa7-7a0ae7d31a9d) (AML.T0010)
Acquire Public ML Artifacts (attack-pattern--c6773651-9da7-453b-8a6f-60e04bd0b252) (AML.T0002)
Valid Accounts (attack-pattern--3e5f503f-f118-4eb3-9a53-8ebee49b1894) (AML.T0012)
Rogue Master (attack-pattern--b14395bd-5419-4ef4-9bd8-696936f509bb) (T0848)
Scheduled Task/Job (attack-pattern--35dd844a-b219-4e2b-a6bb-efa9a75995a9) (T1053)
Hardcoded Credentials (attack-pattern--c9a8d958-fcdb-40d2-af4c-461c8031651a) (T0891)
Data from Information Repositories (attack-pattern--3405891b-16aa-4bd7-bd7c-733501f9b20f) (T0811)

Earth Lusca (G1006): 100.0%

[Earth Lusca](https://attack.mitre.org/groups/G1006) is a suspected China-based cyber espionage group that has been active since at least April 2019. [Earth Lusca](https://attack.mitre.org/groups/G1006) has targeted organizations in Australia, China, Hong Kong, Mongolia, Nepal, the Philippines, Taiwan, Thailand, Vietnam, the United Arab Emirates, Nigeria, Germany, France, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations, telecommunications companies, religious movements banned in China, and cryptocurrency trading platforms; security researchers assess some [Earth Lusca](https://attack.mitre.org/groups/G1006) operations may be financially motivated. (Citation: TrendMicro EarthLusca 2022) [Earth Lusca](https://attack.mitre.org/groups/G1006) has used malware commonly used by other Chinese threat groups, including [APT41](https://attack.mitre.org/groups/G0096) and the [Winnti Group](https://attack.mitre.org/groups/G0044) cluster, however security researchers assess [Earth Lusca](https://attack.mitre.org/groups/G1006)'s techniques and infrastructure are separate. (Citation: TrendMicro EarthLusca 2022)

stix id: intrusion-set--cc613a49-9bfa-4e22-98d1-15ffbb03f034

Aliases: Earth Lusca, TAG-22, Charcoal Typhoon, CHROMIUM, ControlX

Domains: enterprise-attack, mobile-attack

x_mitre_version: 2.0