Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:42:47 UTC

APT group: Lead

Names	Lead *(Microsoft)* TG-3279 *(SecureWorks)* Casper *(BlackBerry)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2016
Description	(Microsoft) In the past few years, Lead's victims have included: • Multinational, multi-industry companies involved in the manufacture of textiles, chemicals, and electronics • Pharmaceutical companies • A company in the chemical industry • University faculty specializing in aeronautical engineering and research • A company involved in the design and manufacture of motor vehicles • A cybersecurity company focusing on protecting industrial control systems During these intrusions, Lead's objective was to steal sensitive data, including research materials, process documents, and project plans. Lead also steals code-signing certificates to sign its malware in subsequent attacks. In most cases, Lead's attacks do not feature any advanced exploit techniques. The group also does not make special effort to cultivate victims prior to an attack. Instead, the group often simply emails a Winnti installer to potential victims, relying on basic social engineering tactics to convince recipients to run the attached malware. In some other cases, Lead gains access to a target by brute-forcing remote access login credentials, performing SQL injection, or exploiting unpatched web servers, and then they copy the Winnti installer directly to compromised machines.
Observed	Sectors: Online video game companies, Pharmaceutical, Technology, Telecommunications. Countries: Japan, USA.
Tools used	Cobalt Strike, Winnti.

Information	<https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
