Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:39:43 UTC

APT group: Chimera

Names	Chimera *(CyCraft)* Bronze Vapor *(SecureWorks)* Red Charon *(PWC)* THORIUM *(Microsoft)* Tumbleweed Typhoon *(Microsoft)* Nuclear Taurus *(Palo Alto)* G0114 *(MITRE)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2018	
Description	(CyCraft) For nearly two years, our team monitored several attacks that targeted Taiwan's semiconductor vendors. We believe these attacks originated from the same threat actor – Chimera – as these attacks utilized similar tactics, techniques and even the same customized malware. The actor likely harvested various valid credentials via phishing emails or data breaches as their starting point to conduct their cyber attack on the vendors. Cobalt Strike was later used as their main RAT tool. To avoid detection, the Cobalt Strike RAT was often masqueraded as a Google Chrome Update. The RAT would then connect back to their C2 server. As these servers were in a public cloud server, it made it difficult to track. Subsequently, by compromising the AD server, the delicate malware – SkeletonKeyInjector – was invoked to implant a general key to allow LM, persistence and defense evasion. Although this malware was discovered for the first time, we have high confidence that these attacks were conducted by the same threat actor. Based on the stolen data, we infer that the actor's goal was to harvest company trade secrets. The motive may be related to business competition or a country's industrial strategy.	
Observed	Sectors: Aviation, High-Tech. Countries: Netherlands, Taiwan and different geographical areas.	
Tools used	Cobalt Strike, SkeletonKeyInjector.	
Operations performed	Late 2017	Hackers spent 2+ years looting secrets of chipmaker NXP before being detected

		<https://arstechnica.com/security/2023/11/hackers-spent-2-years-looting-secrets-of-chipmaker-nxp-before-being-detected/>
	Late 2018	Operation “Skeleton Key” <https://cycraft.com/download/%5BTLP-White%5D20200415%20Chimera_V4.1.pdf>
	Oct 2019	NCC Group and Fox-IT have been tracking a threat group with a wide set of interests, from intellectual property (IP) from victims in the semiconductors industry through to passenger data from the airline industry. <https://blog.fox-it.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/>
Information	<https://cycraft.com/download/%5BTLP-White%5D20200415%20Chimera_V4.1.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0114/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
