Boss Spider, Gold Lowell - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:48:04 UTC

APT group: Boss Spider, Gold Lowell

Names	Boss Spider *(CrowdStrike)* Gold Lowell *(SecureWorks)* CTG-0007 *(SecureWorks)*	
Country	Iran	
Motivation	Financial gain	
First seen	2015	
Description	(SecureWorks) In late 2015, Secureworks Counter Threat Unit (CTU) researchers began tracking financially motivated campaigns leveraging SamSam ransomware (also known as Samas and SamsamCrypt). CTU researchers associate this activity with the Gold Lowell threat group. Gold Lowell typically scans for and exploits known vulnerabilities in Internet-facing systems to gain an initial foothold in a victim's network. The threat actors then deploy the SamSam ransomware and demand payment to decrypt the victim's files. The consistent tools and behaviors associated with SamSam intrusions since 2015 suggest that Gold Lowell is either a defined group or a collection of closely affiliated threat actors. Applying security updates in a timely manner and regularly monitoring for anomalous behaviors on Internet-facing systems are effective defenses against these tactics. Organizations should also create and test response plans for ransomware incidents and use backup solutions that are resilient to corruption or encryption attempts.	
Observed	Sectors: Education, Government, Healthcare.	
Tools used	Mimikatz, PsExec, SamSam, SDelete.	
Counter operations	Nov 2018	Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses <https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public>

Information	<https://www.secureworks.com/research/samsam-ransomware-campaigns> <https://www.crowdstrike.com/blog/an-in-depth-analysis-of-samsam-ransomware-and-boss-spider/>

Last change to this card: 26 April 2021

Download this actor card in PDF or JSON format
