FIN6, Skeleton Spider - Threat Group Cards: A Threat Actor Encyclopedia

APT group: FIN6, Skeleton Spider

Names	FIN6 *(FireEye)* Skeleton Spider *(CrowdStrike)* Gold Franklin *(Secureworks)* White Giant *(PWC)* ITG08 *(IBM)* ATK 88 *(Thales)* TAG-CR2 *(Recorded Future)* TAAL *(Microsoft)* Storm-0538 *(Microsoft)* Camouflage Tempest *(Microsoft)* G0037 *(MITRE)*
Country	[Unknown]
Motivation	Financial crime, Financial gain
First seen	2015
Description	FIN6 is a cybercrime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors. (FireEye) FIN6 is a cybercriminal group intent on stealing payment card data for monetization. In 2015, FireEye Threat Intelligence supported several Mandiant Consulting investigations in the hospitality and retail sectors where FIN6 actors had aggressively targeted and compromised point-of-sale (POS) systems, making off with millions of payment card numbers. Through iSIGHT, we learned that the payment card numbers stolen by FIN6 were sold on a “card shop” — an underground criminal marketplace used to sell or exchange payment card data.
Observed	Sectors: Chemical, Energy, Hospitality, Manufacturing, Retail.

Tools used	AbaddonPOS, Anchor, BlackPOS, CmdSQL, Cobalt Strike, FlawedAmmyy, Grateful POS, JSPSPY, LockerGoga, Magecart, Meterpreter, Mimikatz, More_eggs, Ryuk, SCRAPMINT, TerraStealer, Vawtrak, Windows Credentials Editor, Living off the Land.	
Operations performed	2018	Based on Visa Payment Fraud Disruption's (PFD) analysis of eCommerce compromises throughout 2018, FIN6's focus on the CNP environment has only amplified, suggesting that the cybercrime group has fully incorporated targeting CNP environments into their criminal methodology. <https://usa.visa.com/dam/VCOM/global/support-legal/documents/fin6-cybercrime-group-expands-threat-To-ecommerce-merchants.pdf>
	Jan 2019	Over the past 8-10 weeks, Morphisec has been tracking multiple sophisticated attacks targeting Point of Sale thin clients globally. More specifically, on the 6th of February we identified an extremely high number of prevention events stopping Cobalt Strike backdoor execution, with some of the attacks expressly targeting Point of Sale VMWare Horizon thin clients. <http://blog.morphisec.com/new-global-attack-on-point-of-sale-systems>
	Jan 2019	Hackers have infected the systems of Altran Technologies with malware that spread through the company network, affecting operations in some European countries. To protect client data and their own assets, Altran decided to shut down its network and applications. <https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/>
	Mar 2019	One of the largest aluminum producers in the world, Norsk Hydro, has been forced to switch to partial manual operations due to a cyber attack that is allegedly pushing LockerGoga ransomware. <https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/>
	Apr 2019	The Securonix Threat Research Team has been closely monitoring the LockerGoga targeted cyber sabotage/ransomware (TC/R) attacks impacting Norsk Hydro (one of the largest aluminum companies worldwide), Hexion/Momentive (a chemical manufacturer), and other companies' IT and operational technology (OT) infrastructure, causing over US$40 million in damages. <https://www.securonix.com/securonix-threat-research-detecting-lockergoga-targeted-it-ot-cyber-sabotage-ransomware-attacks/>

	Aug 2019	Based on our investigation and analysis of its adversarial tactics, techniques and procedures (TTPs), we believe ITG08 is actively attacking multinational organizations, targeting specific employees with spear phishing emails advertising fake job advertisements and repeatedly deploying the More_eggs Jscript backdoor malware. <https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/>
	Sep 2019	Hackers have breached the infrastructure of Volusion, a provider of cloud-hosted online stores, and are delivering malicious code that records and steals payment card details entered by users in online forms. <https://www.zdnet.com/article/hackers-breach-volusion-and-start-collecting-card-details-from-thousands-of-sites/> <https://www.zdnet.com/article/card-data-from-the-volusion-web-skimmer-incident-surfaces-on-the-dark-web/>
	Mar 2020	In a new and dangerous twist to this trend, IBM X-Force Incident Response and Intelligence Services (IRIS) research believes that the elite cybercriminal threat actor ITG08, also known as FIN6, has partnered with the malware gang behind one of the most active Trojans — TrickBot — to use TrickBot's new malware framework dubbed "Anchor" against organizations for financial profit. <https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/>
Counter operations	Oct 2021	Europol detains suspects behind LockerGoga, MegaCortex, and Dharma ransomware attacks <https://therecord.media/europol-detains-suspects-behind-lockergoga-megacortex-and-dharma-ransomware-attacks/>
Information	<https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html> <https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf> <https://dti.domaintools.com/Skeleton-Spider-Trusted-Cloud-Malware-Delivery/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0037/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format