Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:57:58 UTC

APT group: FIN7

Names	FIN7 *(FireEye)* Gold Niagara *(SecureWorks)* Calcium *(Symantec)* Navigator *(Fox-IT)* ATK 32 *(Thales)* APT-C-11 *(Qihoo 360)* ITG14 *(IBM)* TAG-CR1 *(Recorded Future)* GrayAlpha *(Recorded Future)* G0046 *(MITRE)*
Country	Russia
Motivation	Financial crime
First seen	2013
Description	FIN7 is a financially-motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. FIN7 is sometimes referred to as Carbanak, Anunak, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. The reports about arrests made of the mastermind of Carbanak instead of FIN7. However, security research teams keep referring to this arrest for all FIN7 activities since.
Observed	Sectors: Casinos and Gambling, Construction, Education, Energy, Financial, Government, High-Tech, Hospitality, Retail, Technology, Telecommunications, Transportation. Countries: Australia, France, Malta, UK, USA.
Tools used	7Logger, Anubis Backdoor, Astra, Bateleur, BIOLOAD, BIRDWATCH, Boostwrite, Carbanak, Cobalt Strike, CROWVIEW, DNSMessenger, Griffon, HALFBAKED, JSSLoader, Lizar, LOADOUT, Meterpreter, Mimikatz, NetSupport Manager, POWERPLANT, POWERSOURCE, RDFSNIFFER, Sardonic, SQLRAT.

Operations performed	Feb 2017	In late February 2017, FireEye as a Service (FaaS) identified a spear phishing campaign that appeared to be targeting personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. All of the observed intended recipients of the spear phishing campaign appeared to be involved with SEC filings for their respective organizations. <https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html>
	Mar 2017	Two recent fileless malware campaigns targeting financial institutions, government agencies and other enterprises have been linked to the same attack group. The campaigns, disclosed by Kaspersky Lab and Cisco's Talos research outfit in the last five weeks, made extensive use of fileless malware and known penetration testing tools and utilities to spy on organizations and move data and money off of networks. <https://threatpost.com/fileless-malware-campaigns-tied-to-same-attacker/124369/>
	Apr 2017	In a newly-identified campaign, FIN7 modified their phishing techniques to implement unique infection and persistence mechanisms. FIN7 has moved away from weaponized Microsoft Office macros in order to evade detection. This round of FIN7 phishing lures implements hidden shortcut files (LNK files) to initiate the infection and VBScript functionality launched by mshta.exe to infect the victim. <https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html>
	Jul 2017	Proofpoint researchers have uncovered that the threat actor commonly referred to as FIN7 has added a new Jscript backdoor called Bateleur and updated macros to its toolkit. <https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor>
	2017	Leveraging Shim Databases for Persistence A unique aspect of the incidents was how the group installed the CARBANAK backdoor for persistent access. Mandiant identified that the group leveraged an application shim database to achieve persistence on systems in multiple environments. The shim injected a malicious in-memory patch into the Services Control Manager ("services.exe") process, and then spawned a CARBANAK backdoor process.

	<https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html>
Jun 2017	Highly sophisticated fileless attack targeting restaurants across the US On June 7, 2017, Morphisec Lab identified a new, highly sophisticated fileless attack targeting restaurants across the US. The ongoing campaign allows hackers to seize system control and install a backdoor to steal financial information at will. It incorporates some never before seen evasive techniques that allow it to bypass most security solutions – signature and behavior based. <http://blog.morphisec.com/fin7-attacks-restaurant-industry>
Oct 2017	Attack to target banks and the enterprise Like clockwork, FIN7 again unleashed a new attack able to bypass almost every security solution. The attack, which took place between October 8 to 10, 2017, is yet another demonstration of the high-paced innovation by threat actors. <http://blog.morphisec.com/fin7-attack-modifications-revealed>
May 2018	New Attack Panel and Malware Samples Flashpoint analysts recently uncovered a new attack panel used by this group in campaigns they have called Astra. The panel, written in PHP, functions as a script-management system, pushing attack scripts down to compromised computers. <https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/>
2018	High-profile breaches including Red Robin, Chili's, Arby's, Burgerville, Omni Hotels and Saks Fifth Avenue, among many others. Fifth Avenue, Saks Off 5th, and Lord & Taylor department stores—all owned by The Hudson's Bay Company—acknowledged a data breach impacting more than five million credit and debit card numbers. The culprits? The same group that's spent the last few years pulling off data heists from Omni Hotels & Resorts, Trump Hotels, Jason's Deli, Whole Foods, Chipotle: A mysterious group known as Fin7. <http://blog.morphisec.com/fin7-not-finished-morphisec-spots-new-campaign>
Nov 2018	In this blog post, we present our findings on two campaigns, which occurred in the first and second weeks of November. These campaigns follow patterns similar to those presented by FireEye in August but with just enough variations to bypass many security vendors. <http://blog.morphisec.com/fin7-not-finished-morphisec-spots-new-campaign>

2018/2019	In 2018-2019, researchers of Kaspersky Lab's Global Research and Analysis Team analyzed various campaigns that used the same Tactics Tools and Procedures (TTPs) as the historic FIN7, leading the researchers to believe that this threat actor had remained active despite the 2018 arrests. In addition, during the investigation, we discovered certain similarities to other attacker groups that seemed to share or copy the FIN7 TTPs in their own operations. <https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/>
Jan 2019	The shared codebase with recent tools attributed to FIN7, together with the same techniques and backdoor, allows to attribute this new loader to the cybercrime group. The timestamps, together with simpler functionality, suggest BIOLOAD is a preceding iteration of BOOSTWRITE. Since the loader is specifically built for each targeted machine and requires administrative permissions to deploy, it suggests the group gathers information about its targets' networks. <https://www.fortinet.com/blog/threat-research/bioload-fin7-boostwrite-lost-twin.html>
Oct 2019	In this blog, we reveal two of FIN7's new tools that we have called BOOSTWRITE and RDFSNIFFER. <https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html>
Mar 2020	A US hospitality provider has recently been the target of an incredibly rare BadUSB attack, ZDNet has learned from cyber-security firm Trustwave. The attack happened after the company received an envelope containing a fake BestBuy gift card, along with a USB thumb drive. <https://www.zdnet.com/article/rare-badusb-attack-detected-in-the-wild-against-us-hospitality-provider/>
Jul 2020	Collaboration between FIN7 and the RYUK group <https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/>
Dec 2020	This report presents an attack chain that was intercepted and prevented within a customer's network in December 2020, then will focus on a component from a typical FIN7 attack chain - JSSLoader. <https://blog.morphisec.com/the-evolution-of-the-fin7-jssloader>

	Jun 2021	Cybercrime Group FIN7 Using Windows 11 Alpha-Themed Docs to Drop Javascript Backdoor <https://www.anomali.com/blog/cybercrime-group-fin7-using-windows-11-alpha-themed-docs-to-drop-javascript-backdoor>
	Oct 2021	FIN7 Recruits Talent For Push Into Ransomware <https://geminiadvisory.io/fin7-ransomware-bastion-secure/>
	Jan 2022	FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7 <https://www.mandiant.com/resources/evolution-of-fin7>
	Mar 2023	FIN7 tradecraft seen in attacks against Veeam backup servers <https://labs.withsecure.com/publications/fin7-target-veeam-servers>
	Late 2023	Threat Group FIN7 Targets the U.S. Automotive Industry <https://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry>
	Apr 2024	FIN7 Uses Trusted Brands and Sponsored Google Ads to Distribute MSIX Payloads <https://www.esentire.com/blog/fin7-uses-trusted-brands-and-sponsored-google-ads-to-distribute-msix-payloads>
	Jul 2024	FIN7: The Truth Doesn't Need to be so STARK <https://www.team-cymru.com/post/fin7-the-truth-doesn-t-need-to-be-so-stark>
	Jul 2024	FIN7 hosting honeypot domains with malicious AI DeepNude Generators – New Silent Push research <https://www.silentpush.com/blog/fin7-malware-deepfake-ai-honeypot/>
	Jul 2024	FIN7 Deploys Anubis Backdoor to Hijack Windows Systems via Compromised SharePoint Sites <https://thehackernews.com/2025/04/fin7-deploys-anubis-backdoor-to-hijack.html>
Counter operations	Aug 2018	Three Members of Notorious International Cybercrime Group “Fin7” In Custody for Role in Attacking Over 100 U.S. companies <https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100>
	May 2020	Another Alleged FIN7 Cybercrime Gang Member Arrested <https://www.bankinfosecurity.com/another-alleged-fin7-cybercrime-gang-member-arrested-a-14345>

	Apr 2021	FIN7 sysadmin behind “billions in damage” gets 10 years <https://blog.malwarebytes.com/reports/2021/04/fin7-sysadmin-behind-billions-in-damage-gets-10-years/>
	Jun 2021	FIN7 manager sentenced to 7 years for role in global hacking scheme <https://therecord.media/fin7-manager-sentenced-to-7-years-for-role-in-global-hacking-scheme/>
Information	<https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html> <https://atr-blog.gigamon.com/2017/07/25/footprints-of-fin7-tracking-actor-patterns-part-1> <https://atr-blog.gigamon.com/2017/07/26/footprints-of-fin7-tracking-actor-patterns-part-2> <https://exchange.xforce.ibmcloud.com/threat-group/guid:5b8c11d520f9e15fcb51ed77c3cae246> <https://www.prodaft.com/m/reports/FIN7_TLPCLEAR.pdf> <https://www.sentinelone.com/labs/fin7-reboot-cybercrime-gang-enhances-ops-with-new-edr-bypasses-and-automated-attacks/> <https://www.recordedfuture.com/research/grayalpha-uses-diverse-infection-vectors-deploy-powernet-loader-netsupport-rat>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0046/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
