Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:00:53 UTC

APT group: FIN11

Names	FIN11 *(FireEye)* DEV-0950 *(Microsoft)* Lace Tempest *(Microsoft)* Chubby Scorpius *(Palo Alto)*
Country	[Unknown]
Motivation	Financial crime, Financial gain
First seen	2016
Description	(FireEye) Mandiant has also responded to numerous FIN11 intrusions, but we've only observed the group successfully monetize access in few instances. This could suggest that the actors cast a wide net during their phishing operations, then choose which victims to further exploit based on characteristics such as sector, geolocation or perceived security posture. Recently, FIN11 has deployed CLOP ransomware and threatened to publish exfiltrated data to pressure victims into paying ransom demands. The group's shifting monetization methods—from point-of-sale (POS) malware in 2018, to ransomware in 2019, and hybrid extortion in 2020—is part of a larger trend in which criminal actors have increasingly focused on post-compromise ransomware deployment and data theft extortion. Notably, FIN11 includes a subset of the activity security researchers call TA505, Graceful Spider, Gold Evergreen, but we do not attribute TA505's early operations to FIN11 and caution against using the names interchangeably. Attribution of both historic TA505 activity and more recent FIN11 activity is complicated by the actors' use of criminal service providers. Like most financially motivated actors, FIN11 doesn't operate in a vacuum. We believe that the group has used services that provide anonymous domain registration, bulletproof hosting, code signing certificates, and private or semi-private malware. Outsourcing work to these criminal service providers likely enables FIN11 to increase the scale and sophistication of their operations.
Observed	Sectors: Defense, Education, Energy, Financial, Hospitality, Retail, Telecommunications, Technology, Transportation. Countries: Worldwide.
Tools used	Amadey, AndroMut, AZORult, BLUESTEAL, Clop, EMASTEAL, FlawedAmmyy, FLOWERPIPE, FORKBEARD, Get2, JESTBOT, Meterpreter, MINEBRIDGE, MINEDOOR, MIXLABEL, NAILGUN, POPFLASH, SALTLICK, SCRAPMINT, SHORTBENCH, SLOWROLL, SPOONBEARD, TinyMet, VIDAR.

Operations performed	Dec 2019	Ransomware attack on Maastricht University <https://www.bleepingcomputer.com/news/security/ta505-hackers-behind-maastricht-university-ransomware-attack/>
	Mar 2020	U.S. pharmaceutical giant ExecuPharm has become the latest victim of data-stealing ransomware. ExecuPharm said in a letter to the Vermont attorney general's office that it was hit by a ransomware attack on March 13, and warned that Social Security numbers, financial information, driver licenses, passport numbers and other sensitive data may have been accessed. But TechCrunch has now learned that the ransomware group behind the attack has published the data stolen from the company's servers. <https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/>
	Oct 2020	Software AG IT giant hit with $23 million ransom by Clop ransomware <https://www.bleepingcomputer.com/news/security/software-ag-it-giant-hit-with-23-million-ransom-by-clop-ransomware/>
	Dec 2020	Global Accellion data breaches linked to Clop ransomware gang <https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/>
	Dec 2020	Singtel, QIMR Berghofer report Accellion-related data breaches <https://www.bleepingcomputer.com/news/security/singtel-qimr-berghofer-report-accellion-related-data-breaches/>
	Dec 2020	New Zealand Reserve Bank breached using bug patched on Xmas Eve <https://www.bleepingcomputer.com/news/security/new-zealand-reserve-bank-breached-using-bug-patched-on-xmas-eve/>
	Jan 2021	Australian securities regulator discloses security breach <https://www.bleepingcomputer.com/news/security/australian-securities-regulator-discloses-security-breach/>
	Jan 2021	Data breach exposes 1.6 million Washington unemployment claims <https://www.bleepingcomputer.com/news/security/data-breach-exposes-16-million-washington-unemployment-claims/>
	Feb 2021	Hacker Claims to Have Stolen Files Belonging to Prominent Law Firm Jones Day <https://www.wsj.com/articles/hacker-claims-to-have-stolen-files-belonging-to-prominent-law-firm-jones-day-11613514532>
	Feb 2021	Clop ransomware gang leaks online what looks like stolen Bombardier blueprints of GlobalEye radar snoop jet <https://www.theregister.com/2021/02/23/bombardier_clop_ransomware_leaks/>

Feb 2021	Kroger data breach exposes pharmacy and employee data <https://www.bleepingcomputer.com/news/security/kroger-data-breach-exposes-pharmacy-and-employee-data/>
Mar 2021	Cybersecurity firm Qualys is the latest victim of Accellion hacks <https://www.bleepingcomputer.com/news/security/cybersecurity-firm-qualys-is-the-latest-victim-of-accellion-hacks/>
Mar 2021	Ransomware gang leaks data stolen from Colorado, Miami universities <https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-stolen-from-colorado-miami-universities/>
Mar 2021	Energy giant Shell discloses data breach after Accellion hack <https://www.bleepingcomputer.com/news/security/energy-giant-shell-discloses-data-breach-after-accellion-hack/>
Mar 2021	Ransomware gang urges victims' customers to demand a ransom payment <https://www.bleepingcomputer.com/news/security/ransomware-gang-urges-victims-customers-to-demand-a-ransom-payment/>
Mar 2021	Ransomware group targets universities in Maryland, California in new data leaks <https://www.zdnet.com/article/ransomware-group-targets-universities-of-maryland-california-in-new-data-leaks/>
Mar 2021	Ransomware gang leaks data from Stanford, Maryland universities <https://www.bleepingcomputer.com/news/security/ransomware-gang-leaks-data-from-stanford-maryland-universities/>
Apr 2021	More Accellion Health Data Breaches Revealed <https://www.healthcareinfosecurity.com/more-accellion-health-data-breaches-revealed-a-16350>
Jun 2021	Clop ransomware is back in business after recent arrests <https://www.bleepingcomputer.com/news/security/clop-ransomware-is-back-in-business-after-recent-arrests/>
Oct 2021	Clop ransomware gang is leaking confidential data from the UK police <https://securityaffairs.co/wordpress/125792/cyber-crime/clop-ransomware-uk-police.html>
Nov 2021	Marine services provider Swire Pacific Offshore hit by ransomware <https://www.bleepingcomputer.com/news/security/marine-services-provider-swire-pacific-offshore-hit-by-ransomware/>
Apr 2022	Clop ransomware gang is back, hits 21 victims in a single month <https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-is-back-hits-21-victims-in-a-single-month/>

Aug 2022	Hackers attack UK water supplier but extort wrong company <https://www.bleepingcomputer.com/news/security/hackers-attack-uk-water-supplier-but-extort-wrong-company/> <https://therecord.media/ransomware-group-may-have-stolen-customer-bank-details-from-british-water-company/>
Sep 2022	FIN11 is Back : Impersonates Popular Video Conference Application <https://www.cyfirma.com/outofband/fin11-is-back-impersonates-popular-video-conference-application/>
Dec 2022	Cl0p Ransomware Targets Linux Systems with Flawed Encryption <https://www.sentinelone.com/labs/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor-available/>
Feb 2023	Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day <https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/>
Mar 2023	Clop ransomware gang begins extorting GoAnywhere zero-day victims <https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-begins-extorting-goanywhere-zero-day-victims/>
Mar 2023	Clop ransomware claims Saks Fifth Avenue, retailer says mock data stolen <https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-saks-fifth-avenue-retailer-says-mock-data-stolen/>
Mar 2023	City of Toronto confirms data theft, Clop claims responsibility <https://www.bleepingcomputer.com/news/security/city-of-toronto-confirms-data-theft-clop-claims-responsibility/>
Mar 2023	Procter & Gamble confirms data theft via GoAnywhere zero-day <https://www.bleepingcomputer.com/news/security/procter-and-gamble-confirms-data-theft-via-goanywhere-zero-day/>
Mar 2023	UK Pension Protection Fund latest victim of GoAnywhere hack <https://therecord.media/uk-pension-protection-fund-clop-goanywhere-fortra>
Mar 2023	Crown Resorts confirms ransom demand after GoAnywhere breach <https://www.bleepingcomputer.com/news/security/crown-resorts-confirms-ransom-demand-after-goanywhere-breach/>
Mar 2023	Tasmania officials: 16,000 student documents leaked by Clop ransomware group <https://therecord.media/tasmania-government-ransomware-clop-student-documents>
Apr 2023	Microsoft: Clop and LockBit ransomware behind PaperCut server hacks <https://www.bleepingcomputer.com/news/security/microsoft-clop-and-lockbit-ransomware-behind-papercut-server-hacks/>

May 2023	Microsoft links Clop ransomware gang to MOVEit data-theft attacks <https://www.bleepingcomputer.com/news/security/microsoft-links-clop-ransomware-gang-to-moveit-data-theft-attacks/> <https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-starts-extorting-moveit-data-theft-victims/>
May 2023	Missouri warns that health info was stolen in IBM MOVEit data breach <https://www.bleepingcomputer.com/news/security/missouri-warns-that-health-info-was-stolen-in-ibm-moveit-data-breach/>
May 2023	US govt contractor Serco discloses data breach after MoveIT attacks <https://www.bleepingcomputer.com/news/security/us-govt-contractor-serco-discloses-data-breach-after-moveit-attacks/>
May 2023	Colorado warns 4 million of data stolen in IBM MOVEit breach <https://www.bleepingcomputer.com/news/security/colorado-warns-4-million-of-data-stolen-in-ibm-moveit-breach/>
May 2023	Russian cyber thieves linked to personal data breach at North Carolina hospitals <https://news.yahoo.com/russian-cyber-thieves-linked-personal-202630737.html>
May 2023	Sony confirms data breach impacting thousands in the U.S. <https://www.bleepingcomputer.com/news/security/sony-confirms-data-breach-impacting-thousands-in-the-us/>
May 2023	Third Flagstar Bank data breach since 2021 affects 800,000 customers <https://www.bleepingcomputer.com/news/security/third-flagstar-bank-data-breach-since-2021-affects-800-000-customers/>
May 2023	Maine govt notifies 1.3 million people of MOVEit data breach <https://www.bleepingcomputer.com/news/security/maine-govt-notifies-13-million-people-of-moveit-data-breach/>
May 2023	Amazon confirms employee data breach after vendor hack <https://www.bleepingcomputer.com/news/security/amazon-confirms-employee-data-breach-after-vendor-hack/>
May 2023	Auto parts giant AutoZone warns of MOVEit data breach <https://www.bleepingcomputer.com/news/security/auto-parts-giant-autozone-warns-of-moveit-data-breach/>
Jun 2023	Delta Dental of California data breach exposed info of 7 million people <https://www.bleepingcomputer.com/news/security/delta-dental-of-california-data-breach-exposed-info-of-7-million-people/>
Jun 2023	MOVEIt breach impacts GenWorth, CalPERS as data for 3.2 million exposed <https://www.bleepingcomputer.com/news/security/moveit-breach-impacts-genworth-calpers-as-data-for-32-million-exposed/>

Jun 2023	Hackers steal data of 45,000 New York City students in MOVEit breach <https://www.bleepingcomputer.com/news/security/hackers-steal-data-of-45-000-new-york-city-students-in-moveit-breach/>
Jun 2023	Siemens Energy confirms data breach after MOVEit data-theft attack <https://www.bleepingcomputer.com/news/security/siemens-energy-confirms-data-breach-after-moveit-data-theft-attack/>
Jul 2023	Shell Becomes Latest Cl0p MOVEit Victim <https://www.darkreading.com/attacks-breaches/shell-latest-cl0p-moveit-victim>
Jul 2023	Radisson Hotels, major insurance firms become latest MOVEit victims to disclose breaches <https://therecord.media/radisson-hotels-major-insurance-firms-disclose-moveit-incidents>
Jul 2023	Shutterfly says Clop ransomware attack did not impact customer data <https://www.bleepingcomputer.com/news/security/shutterfly-says-clop-ransomware-attack-did-not-impact-customer-data/>
Jul 2023	BlackCat, Clop claim ransomware attack on cosmetics maker Estée Lauder <https://therecord.media/blackcat-clop-claim-cyberattack-on-estee-lauder>
Jul 2023	Clop now leaks data stolen in MOVEit attacks on clearweb sites <https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/>
Jul 2023	Medical files of 8M-plus people fall into hands of Clop via MOVEit mega-bug <https://www.theregister.com/2023/07/27/maximus_deloitte_moveit_hack/>
Jul 2023	Welltok data breach exposes data of 8.5 million US patients <https://www.bleepingcomputer.com/news/security/welltok-data-breach-exposes-data-of-85-million-us-patients/>
Aug 2023	Clop ransomware now uses torrents to leak data and evade takedowns <https://www.bleepingcomputer.com/news/security/clop-ransomware-now-uses-torrents-to-leak-data-and-evade-takedowns/>
Sep 2023	Johnson & Johnson discloses IBM data breach impacting patients <https://www.bleepingcomputer.com/news/security/johnson-and-johnson-discloses-ibm-data-breach-impacting-patients/>
Sep 2023	CL0P Seeds ^_- Gotta Catch Em All! <https://unit42.paloaltonetworks.com/cl0p-group-distributes-ransomware-data-with-torrents/>
Nov 2023	Microsoft: SysAid zero-day flaw exploited in Clop ransomware attacks <https://www.bleepingcomputer.com/news/security/microsoft-sysaid-zero-day-flaw-exploited-in-clop-ransomware-attacks/>

	Feb 2024	French unemployment agency data breach impacts 43 million people <https://www.bleepingcomputer.com/news/security/french-unemployment-agency-data-breach-impacts-43-million-people/>
	Dec 2024	Clop ransomware claims responsibility for Cleo data theft attacks <https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-cleo-data-theft-attacks/>
	Dec 2024	Clop ransomware is now extorting 66 Cleo data-theft victims <https://www.bleepingcomputer.com/news/security/clop-ransomware-is-now-extorting-66-cleo-data-theft-victims/>
	Dec 2024	Food giant WK Kellogg discloses data breach linked to Clop ransomware <https://www.bleepingcomputer.com/news/security/food-giant-wk-kellogg-discloses-data-breach-linked-to-clop-ransomware/>
	Mar 2025	Retail giant Sam's Club investigates Clop ransomware breach claims <https://www.bleepingcomputer.com/news/security/retail-giant-sams-club-investigates-clop-ransomware-breach-claims/>
Counter operations	Jun 2021	Operation "Cyclone" Ukraine arrests Clop ransomware gang members, seizes servers <https://www.bleepingcomputer.com/news/security/ukraine-arrests-clop-ransomware-gang-members-seizes-servers/> <https://www.interpol.int/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring>
	Jun 2023	US govt offers $10 million bounty for info on Clop ransomware <https://www.bleepingcomputer.com/news/security/us-govt-offers-10-million-bounty-for-info-on-clop-ransomware/>
Information	<https://www.fireeye.com/blog/threat-research/2020/10/fin11-email-campaigns-precursor-for-ransomware-data-theft.html> <https://cybernews.com/security/cl0p-hacker-hides-in-ukraine/> <https://therecord.media/clop-moveit-zero-day-dustin-childs-interview> <https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html>	

Last change to this card: 30 June 2025

Download this actor card in PDF or JSON format
