# Cl0p

## Target Bio

**Names/Alias:** Cl0p, TA505, Graceful Spider, Spandex Tempest, FIN11
**Affiliations:** LockBit, Hive, Locky Ransomware, REvil
**Motivation:** Financial gain
**First Activity:** 2014
**Structure:** Centralized
**Country of Basis:** Russia, Confederacy of Independent States
**Targets:** Enterprise, government, education, healthcare
**Methodology:** Ransomware, zero-day attacks, phishing
**Most Recent Development:** Oracle E-business breach


## BLUF

Cl0p specializes in finding and exploiting zero-day vulnerabilities in target organizations systems by utilizing a blend of remote access tools and Cl0p branded ransomware to extract and encrypt the targets data for extortion purposes. Their tendency to exploit zero-day vulnerabilities makes proactive defense difficult, yet crucial in mitigating attack risks.

## Background

Cl0p is a Russian speaking cyber-criminal group based in either Russia or the Confederacy of Independent States [1][2][3] and has been active since 2014. The groups name is a reference to both the Russian word for bedbug and a common online exploit of changing letters for numbers to avoid detection [1]. Cl0p operates simultaneously as a ransomware as a service provider and an individual attacker, primarily utilizing a mixture of stolen credentials and zero-day exploits on their targets [1][2][3][4]. They have been responsible for numerous attacks on many different organizations over the last 6 years, the most recent being the compromise of Oracle E-Business assets [1][2][4][5]

## Summary (General Overview)

Originating in 2014, Cl0p is now regarded as “one of the largest phishing and malspam distributors worldwide” and is responsible for more than 10,000 security breaches globally as of 2023, including incidents involving British Airways, the BBC, and UCLA. The U.S. Department of Health and Human Services has reported that operators have observed payouts to Cl0p reaching up to $500 million USD. The group has gained notoriety for exploiting zero-day vulnerabilities and using double extortion tactics, such as in their recent breach of Oracle E-Business services, which leveraged an exploit chain involving the UiServlet component to enable remote code execution. In addition to conducting their own attacks, Cl0p provides services to other cybercriminal organizations, including botnet operators, initial access brokers, and Ransomware-as-a-Service providers. They avoid targeting Russia or former Soviet states, and their malware does not function on systems using the Russian language; however, there is no indication of political or ideological motivation behind this, as Cl0p has consistently stated that their operations are driven solely by financial gain.

# Details & References

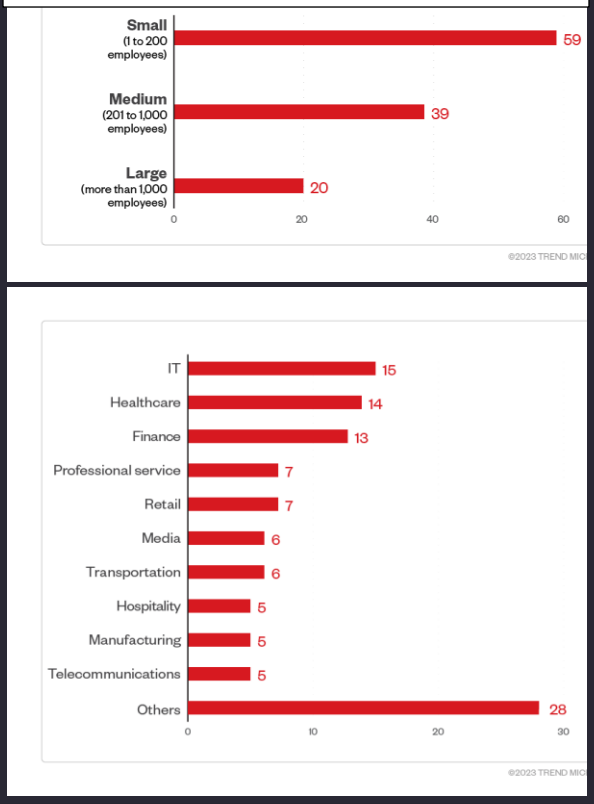
## Analysis Summary

After being founded in 2014, Cl0p's TTP's have evolved from sophisticated phishing campaigns and attacks, to methods that are aimed at targeting zero-day vulnerabilities within systems to extract data and extort their victims [7]. In their most recent breach (Oracle E-Business), they chained multiple vulnerabilities together to accomplish this goal [1][2][3][4][5][6]. This methodology puts them in a unique position within the cyber threat community, as most other attackers tend to utilize known vulnerabilities in unpatched software to exploit their targets [1][4].

Cl0p claims to have always been exclusively financially motivated. They have stated that they have no interest in anything other than monetary gain. A combination of open-source intelligence and Student Security Operations Center (SSOC) dark web reconnaissance has revealed that to be true thus far. They don't have any ideals, beliefs, or grand themes driving their actions other than money. They view themselves as an 'after the fact' pen-testing service, exploiting organizations to buy their data back, then providing highly detailed documentation of the vulnerability that was exploited, how it was manipulated, and mitigation measures to not only fix the current vulnerability, but also to protect against future attacks.

Throughout the years since its founding, Cl0p has continued to evolve their TTP's to compromise systems and exploit businesses; The only thing that hasn't changed is their motive, that being financial gain [3][7]. Cl0p's offensive adaptability and flexibility, along with their monetary goal solidifies them as a major threat to businesses around the world. Cl0p's focus on zero-day exploits make proactive defense against them extremely difficult but also vitally important. To combat Cl0p and similar threats, organizations should adopt a robust security framework and implement proven best practices, including comprehensive employee training, multi-factor authentication (MFA), secure system configuration, timely patching, continuous log auditing, and regular security testing such as red-team exercises and penetration assessments [6][7]. These preventative measures strengthen an organization's resilience against zero-day exploits and ransomware, reducing overall risk, minimizing attack surface, and improving security posture.

### Targeted Business Demographics




Source: Ransomware Spotlight: Clop | Trend Micro (US)

## References


[1] Cl0p ransomware: The skeezy invader that bites while you sleep

[2] Ransomware Gang Haunted US Firms Long Before MOVEit Hack

[3] Profile: TA505/Cl0p Ransomware

[4] *2025 Threat Hunting Report - CrowdStrike*

[5] Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign

[6] #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

[7] Ransomware Spotlight: Clop | Trend Micro (US)

[8] https://www.hhs.gov/sites/default/files/clop-ransomware-analyst-note-tlpclear.pdf?utm_source=copilot.com