

Clop Releases Exfiltrated Data On Surface Web Domain

- On July 19, 2023, the Clop (Cl0p) extortion collective released stolen PricewaterhouseCoopers (PwC) data on a newly registered website with a '[.]com' domain. Clop previously published PwC data to its Tor-based leak site, "CLOP^_ - LEAKS". Analysis is ongoing to determine if the contents of the leaks match.
- The data has been published on the surface web in four parts, with each path a direct download link. The domain was registered on July 18, 2023, leveraging infrastructure appearing to be operating within the Russian Federation.
- PwC acknowledged it was compromised as part of Clop's May 2023 campaign exploiting CVE-2023-34362 in the MOVEit file transfer tool. At the time of writing, reports indicate that in excess of 375 organizations have been compromised as part of Clop's campaign.
- While it is unclear why Clop has chosen PwC's data to be leaked in this way, it is most likely a result of a lack of engagement from the victim coupled with the organizations' high profile which will likely draw significant public and media attention.
- **ZeroFox assesses Clop is most likely experimenting with a new shaming tactic to pressure victims into paying ransom demands. It is very likely that Clop operatives believe the threat of leaking data on surface web domains will exert greater pressure on victims by potentially garnering a broader audience—including media attention—and resulting in greater reputational damage to the victim's brand. The success of this tactic—for future use by Clop as well as other collectives—very likely depends on public reaction to the leak and how victims respond.**


FILES PART1
<https://pwcclinetsanddocuments.com/pwc/1.zip>
<https://pwcclinetsanddocuments.com/pwc/1.x01>
<https://pwcclinetsanddocuments.com/pwc/1.x02>
<https://pwcclinetsanddocuments.com/pwc/1.x03>
<https://pwcclinetsanddocuments.com/pwc/1.x04>
<https://pwcclinetsanddocuments.com/pwc/1.x05>
<https://pwcclinetsanddocuments.com/pwc/1.x06>
<https://pwcclinetsanddocuments.com/pwc/1.x07>
<https://pwcclinetsanddocuments.com/pwc/1.x08>
<https://pwcclinetsanddocuments.com/pwc/1.x09>
<https://pwcclinetsanddocuments.com/pwc/1.x10>
<https://pwcclinetsanddocuments.com/pwc/1.x11>
<https://pwcclinetsanddocuments.com/pwc/1.x12>
<https://pwcclinetsanddocuments.com/pwc/1.x13>
<https://pwcclinetsanddocuments.com/pwc/1.x14>
<https://pwcclinetsanddocuments.com/pwc/1.x15>
<https://pwcclinetsanddocuments.com/pwc/1.x16>
<https://pwcclinetsanddocuments.com/pwc/1.x17>
<https://pwcclinetsanddocuments.com/pwc/1.x18>
<https://pwcclinetsanddocuments.com/pwc/1.x19>
<https://pwcclinetsanddocuments.com/pwc/1.x20>
<https://pwcclinetsanddocuments.com/pwc/1.x21>
<https://pwcclinetsanddocuments.com/pwc/1.x22>
<https://pwcclinetsanddocuments.com/pwc/1.x23>
<https://pwcclinetsanddocuments.com/pwc/1.x24>
<https://pwcclinetsanddocuments.com/pwc/1.x25>
<https://pwcclinetsanddocuments.com/pwc/1.x26>

FILES PART2
<https://pwcclinetsanddocuments.com/pwc/2.zip>
<https://pwcclinetsanddocuments.com/pwc/2.x01>

FILES PART3
<https://pwcclinetsanddocuments.com/pwc/3.zip>

FILES PART4
<https://pwcclinetsanddocuments.com/pwc/4.zip>
<https://pwcclinetsanddocuments.com/pwc/4.x01>
<https://pwcclinetsanddocuments.com/pwc/4.x02>
<https://pwcclinetsanddocuments.com/pwc/4.x03>

Source: Clop's '[.]com' domain hosting PwC's data

Recommendations

- Subscribe to ZeroFox Advanced Dark Web Intelligence for updates on new ransomware targets.
- Utilize the ZeroFox Platform's Intelligence Search interface to investigate Indicators of Compromise and metadata related to Ransomware.
- Patch vulnerable MOVEit Transfer versions.
- Reset service account credentials for affected systems and MOVEit Service Accounts.