

# Indiabulls Group hit by CLOP Ransomware, gets 24h leak deadline

---

[bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/](https://bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/)

Lawrence Abrams

By

[Lawrence Abrams](#)

- June 22, 2020
- 06:50 PM
- 0



Indian conglomerate Indiabulls Group has allegedly been hit with a cyberattack from the CLOP Ransomware operators who have leaked screenshots of stolen data.

The Indiabulls Group is an Indian conglomerate with \$3.5 billion in revenue (2019), over 19,000 employees, and subsidiaries focusing on housing, personal finance and lending, infrastructure, and pharmaceuticals.

"The Indiabulls Group is a diversified financial services group with interests in housing finance, consumer finance and personal wealth. The Group also has a presence in Real Estate, Pharmaceuticals, Lighting and Infrastructure & Construction Equipment Leasing. The group has a net worth of more than ₹ 28,580 Cr. (as on 31st March, 2019)," states their [about page](#).

## CLOP Ransomware claims to have breached Indiabulls

---

The CLOP Ransomware operators claimed to have breached Indiabulls and have posted screenshots of files that they have allegedly stolen during the attack.

When performing a ransomware attack, the CLOP threat actors are known to steal unencrypted files before deploying the ransomware.

These files are then posted on their 'CLOP^ - LEAKS' data leak site with a threat that more data will be leaked if the ransom demand is not paid.

Today, the CLOP threat actors have uploaded screenshots of six stolen files with the message of "Contact us in 24H."

The leaked documents include a voucher, a letter, and four spreadsheets related to the Indiabulls Pharmaceuticals and Indiabulls Housing Finance Limited subsidiaries.

The screenshot shows a website header with the text '>\_ CLOP^ - LEAKS' and 'INDIABULLS.COM'. Below the header, there is a list of company details for Indiabulls:

- Type: Public company
- Industry: Financial Services
- Founded: January 2000
- Headquarters: Gurgaon, India
- Key people: Sameer Gehlaut (Chairman & Founder), Gagan Banga (Vice-Chairman & MD)
- Products: Financial Services, Real Estate, Pharmaceutical, Construction Equipment Leasing, LED Lights and Facilities sector
- Revenue: ₹ 25,000 crore (2019)
- Number of employees: 19,000 (2019)
- Website: www.Indiabulls.com

Below the company information, there is a section titled 'INDIABULLS CONTACT US IN 24H' and 'Screenshots:'. One of the screenshots is a 'VOUCHER' document from Indiabulls Pharmaceuticals. The voucher includes the following information:

- Reg Add : [REDACTED]
- BP Add : [REDACTED]
- Business Place: GSTIN: [REDACTED]
- INDIABULLS PHARMACEUTICALS LIMITED ( 7030 )
- M-62 & 63, 1st Floor, Connaught Place New Delhi 110001
- Document Date : [REDACTED]
- Posting Date : [REDACTED]
- Document Type : [REDACTED]
- Doc. Header Text : [REDACTED]
- STRN : [REDACTED]
- HSN/SAC : NOT UPDATED
- Gst Partner : NOT UPDATED
- Place of Supply : NOT UPDATED
- Vendor Reg. status : Registered
- GSTIN : [REDACTED]
- Reverse Charge : N
- Document Number : [REDACTED]
- Invoice No : [REDACTED]
- Self Invoice No : NOT UPDATED
- PAN : [REDACTED]

### Indiabulls leak on CLOP data leak site

It is not known how much CLOP is demanding for a ransom or when the attack occurred.

Cyberintelligence firm Bad Packets told BleepingComputer, though, that Indiabulls has an Citrix Netscaler ADC VPN gateway exposed, which is vulnerable to the CVE-2019-19781 vulnerability.

It is not known if this is how they were potentially breached.

Threat intel firm Bad Packets said that its internet-wide scans had discovered last year that the fintech company had run unpatched servers for a long time, leaving its systems exposed to attacks.

In March, the CLOP Ransomware operators also conducted an attack against U.S pharmaceutical company ExecuPharm when they stole 163GB of unencrypted files. Since then, the ransomware actors have leaked it all on their data leak site after not being paid.

BleepingComputer has contacted both CLOP and Indiabulls but has not received a response as of yet.

*H/T Cyble*

*Update 6/22/20: Added information about vulnerable Netscaler device.*

## **Related Articles:**

---

[SpiceJet airline passengers stranded after ransomware attack](#)

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

[Industrial Spy data extortion market gets into the ransomware game](#)

[New 'Cheers' Linux ransomware targets VMware ESXi servers](#)

[US Senate: Govt's ransomware fight hindered by limited reporting](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.