# Business services giant Conduent hit by Maze Ransomware

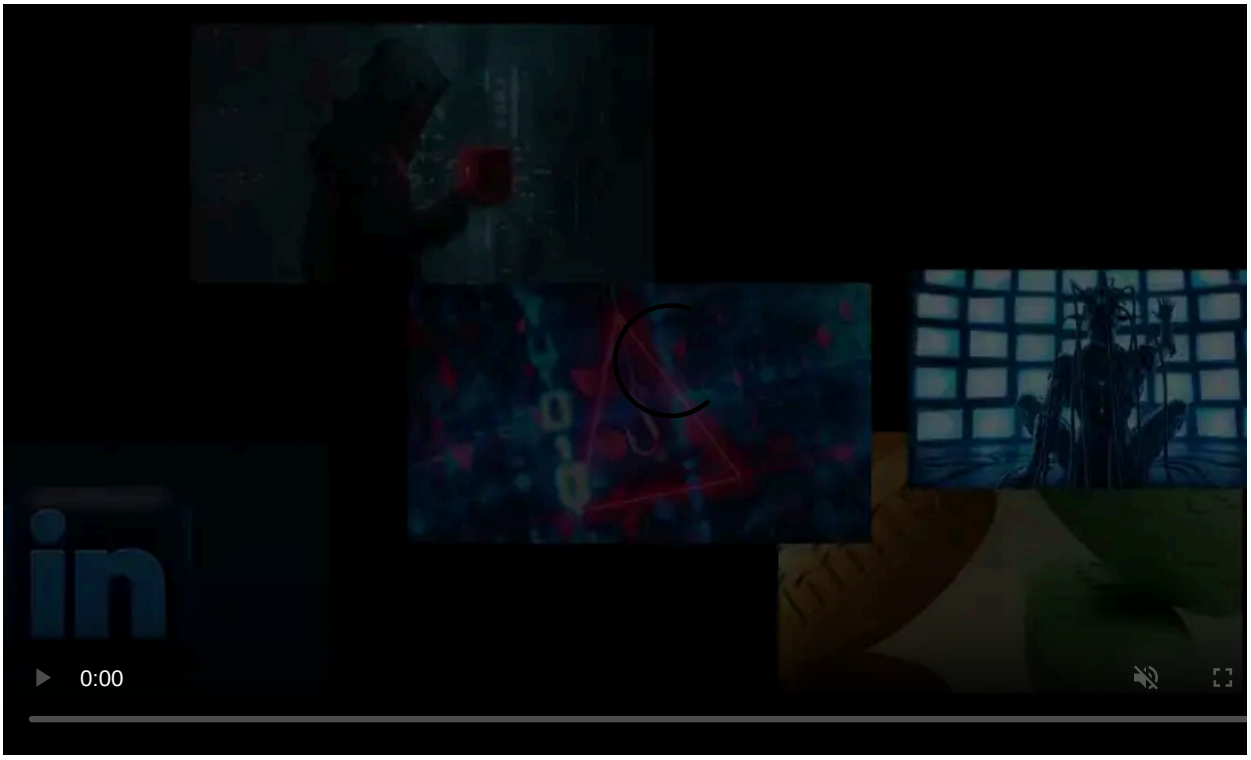
By Lawrence Abrams

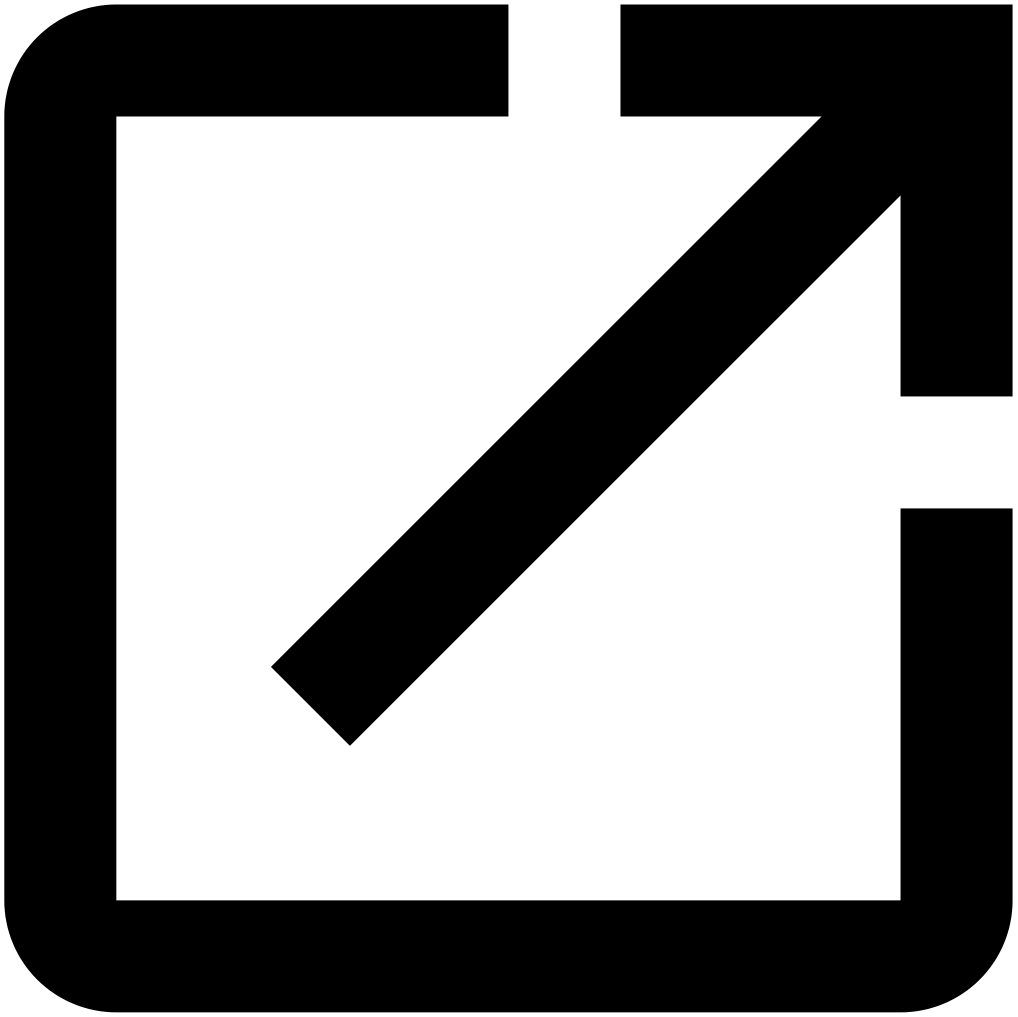
Published: 2020-06-04 · Archived: 2026-04-05 16:22:41 UTC

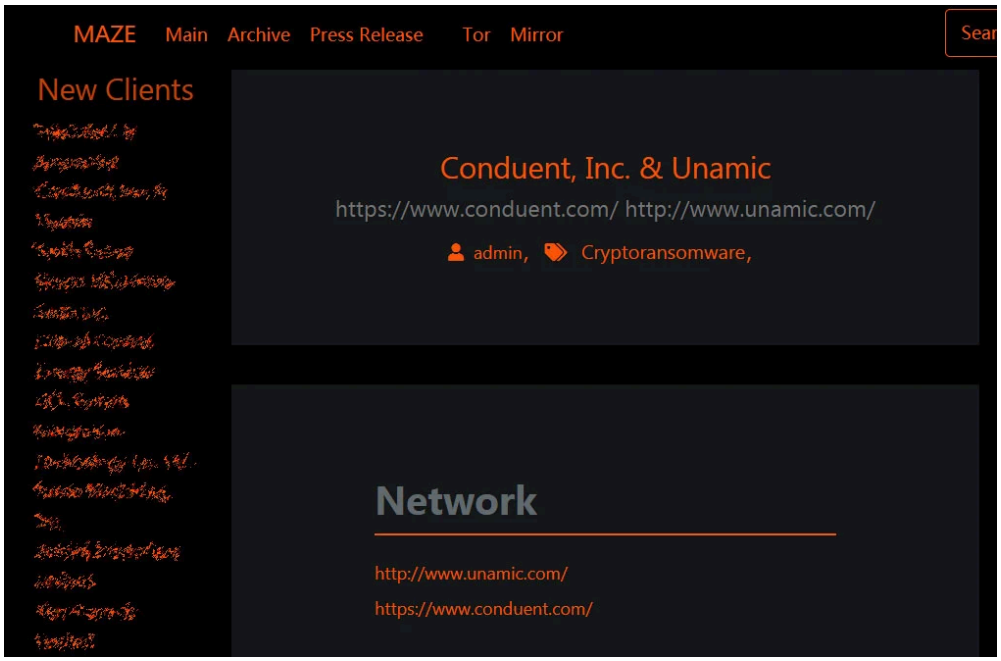

The Maze Ransomware operators are claiming to have successfully attacked business services giant Conduent, where they stole unencrypted files and encrypted devices on their network.

Conduent is a New Jersey, USA based business services firm with 67,000 employees and a 2019 business revenue of $4.47 billion.

Today, Maze Ransomware posted a new entry to their data leak site that states that they breached the network for Conduent in May 2020.


0:00

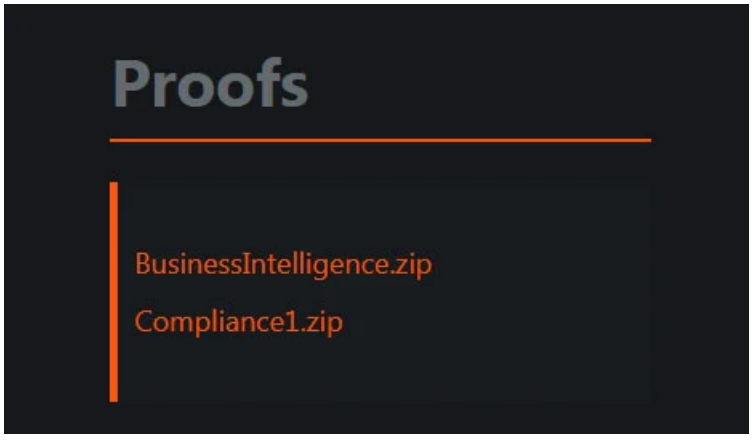





**Conduent entry on Maze leak site**

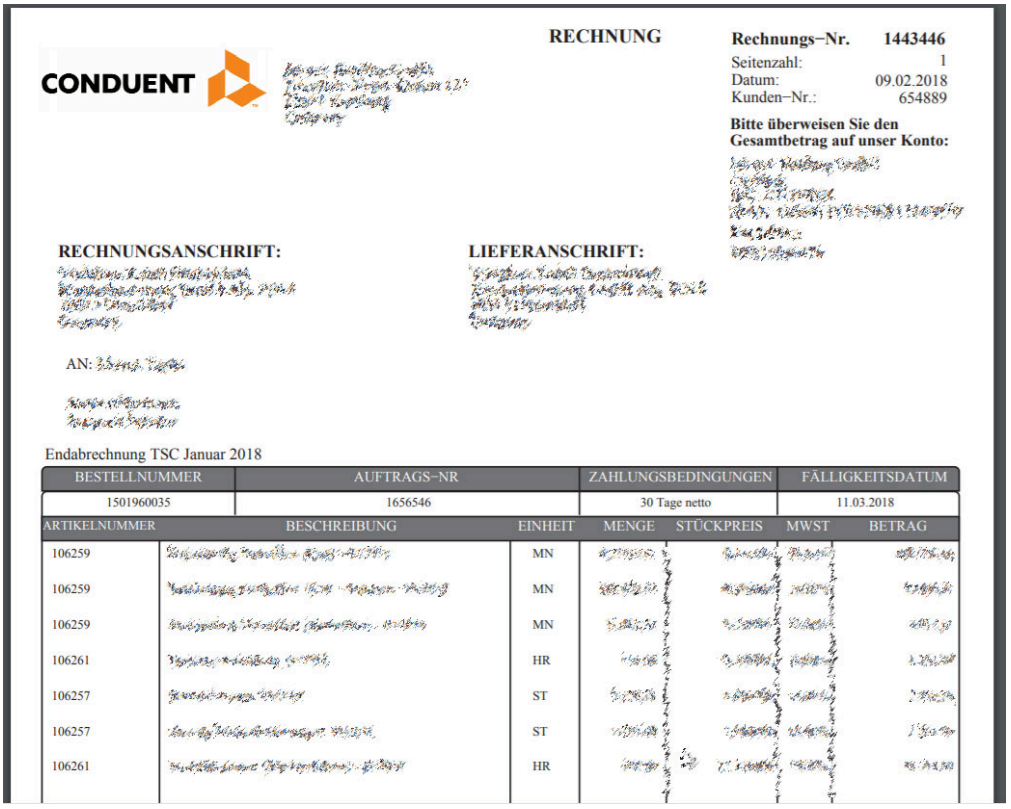
When conducting an attack, the Maze Ransomware operators steal unencrypted files before deploying the ransomware. This stolen data and the threat of publicly releasing it is then used as leverage to 'persuade' the victim to pay a ransom.

As 'proof' that the threat actors breached Conduent, 1GB worth of files were posted that allegedly was stolen during the ransomware attack.




**Alleged proof of the attack**

The posted files are called 'BusinessIntelligence.zip' and 'Compliance1.zip' and include various financial spreadsheets, customer audits, invoices, commission statements, and other miscellaneous documents.



RECHNUNG

CONDUENT

Rechnungs–Nr. 1443446
Seitenzahl: 1
Datum: 09.02.2018
Kunden–Nr.: 654889

Bitte überweisen Sie den Gesamtbetrag auf unser Konto:

RECHNUNGSANSCHRIFT:

LIEFERANSCHRIFT:

AN:

Endabrechnung TSC Januar 2018

| BESTELLNUMMER | AUFTRAGS–NR | ZAHLUNGSBEDINGUNGEN | FÄLLIGKEITSDATUM |
|---|---|---|---|
| 1501960035 | 1656546 | 30 Tage netto | 11.03.2018 |

| ARTIKELNUMMER | BESCHREIBUNG | EINHEIT | MENGE | STÜCKPREIS | MWST | BETRAG |
|---|---|---|---|---|---|---|
| 106259 | | MN | | | | |
| 106259 | | MN | | | | |
| 106259 | | MN | | | | |
| 106261 | | HR | | | | |
| 106257 | | ST | | | | |
| 106257 | | ST | | | | |
| 106261 | | HR | | | | |

Due to the varied types of data already posted by the Maze gang, Conduent must disclose it as a data breach to their clients and employees.

In a statement to BleepingComputer, Conduent confirmed that they suffered a ransomware attack on May 29th, 2020 that impacted services for approximately 10 hours.

"Conduent's European operations experienced a service interruption on Friday, May 29, 2020. Our system identified ransomware, which was then addressed by our cybersecurity protocols. This interruption began at 12.45 AM CET on May 29th with systems mostly back in production again by 10.00 AM CET that morning, and all systems have since then been restored. This resulted in a partial interruption to the services that we provide to some clients. As our investigation continues, we have on-going internal and external security forensics and anti-virus teams reviewing and monitoring our European infrastructure."

## Possible breach through Citrix Netscaler vulnerability

Threat intelligence company Bad Packets stated that for at least eight weeks, between December 17, 2019, and at least February 14, 2020, Conduent had a Citrix server exposed that was vulnerable to the CVE-2019-19781 vulnerability.

This vulnerability was patched in January 2020 and allowed attackers to perform remote code execution on vulnerable devices.

Using these devices as a staging area, attackers would then spread laterally throughout the internal network as they compromise further devices.

The CVE-2019-19781 vulnerability is known to be used by threat actors in the past to breach networks and deploy ransomware.

In a report highlighting human-operated ransomware, the Microsoft Threat Protection Intelligence Team states that DoppelPaymer and RobbinHood have been seen utilizing the vulnerability to breach corporate networks.

In April 2020, when we broke the news that Maze breached IT services company Cognizant, Bad Packets also found vulnerable Citrix NetScaler gateways on their network.

> Hmm... was it those vulnerable Citrix (NetScaler) gateways?
>
> — Bad Packets Report (@bad_packets) April 18, 2020

While it is not confirmed if this vulnerability was used as part of this attack, the Maze Ransomware operators have been known to use vulnerabilities to gain access to networks in the past.

**Updated 6/4/20 1:52 PM EST:** Added more information about Citrix Netscaler devices being used by Conduent in the past.
**Updated 6/4/20 4:10 PM EST**: Added statement from Conduent.

*H/T UnderTheBreach*



---

Source: https://www.bleepingcomputer.com/news/security/business-services-giant-conduent-hit-by-maze-ransomware/