Customer Care Giant TTEC Hit By Ransomware

Published: 2021-09-24 · Archived: 2026-04-05 16:35:23 UTC

TTEC, [NASDAQ: TTEC], a company used by some of the world's largest brands to help manage customer support and sales online and over the phone, is dealing with disruptions from a network security incident resulting from a ransomware attack, KrebsOnSecurity has learned.

While many companies have been laying off or furloughing workers in response to the Coronavirus pandemic, TTEC has been massively hiring. Formerly TeleTech Holdings Inc., Englewood, Co.-based TTEC now has nearly 60,000 employees, most of whom work from home and answer customer support calls on behalf of a large number of name-brand companies, like **Bank of America**, **Best Buy**, **Credit Karma**, **Dish Network**, **Kaiser Permanente**, **USAA** and **Verizon**.

On Sept. 14, KrebsOnSecurity heard from a reader who passed on an internal message apparently sent by TTEC to certain employees regarding the status of a widespread system outage that began on Sunday, Sept. 12.

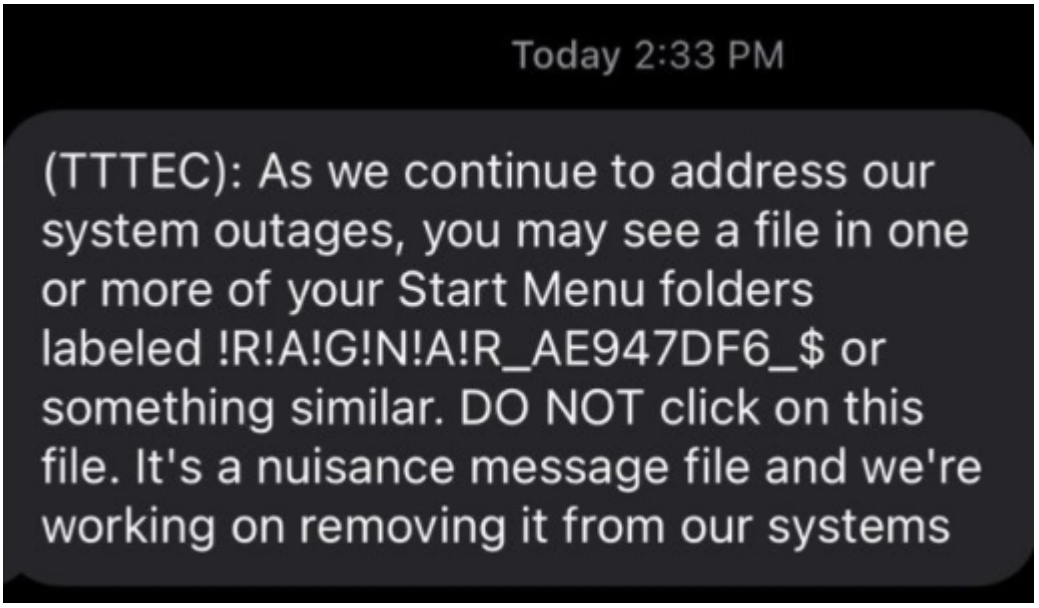
"We're continuing to address the system outage impacting access to the network, applications and customer support," reads an internal message sent by TTEC to certain employees.

TTEC has not responded to requests for comment. A phone call placed to the media contact number listed on an August 2021 TTEC earnings release produced a message saying it was a non-working number.

[**Update, 6:20 p.m. ET:** TTEC confirmed a ransomware attack. See the update at the end of this piece for their statement]

TTEC's own message to employees suggests the company's network may have been hit by the ransomware group "Ragnar Locker," (or else by a rival ransomware gang pretending to be Ragnar). The message urged employees to avoid clicking on a file that suddenly may have appeared in their Windows start menu called "!RA!G!N!A!R!"

"DO NOT click on this file," the notice read. "It's a nuisance message file and we're working on removing it from our systems."



Ragnar Locker is an aggressive ransomware group that typically demands millions of dollars worth of cryptocurrency in ransom payments. In an announcement published on the group's darknet leak site this week, the group threatened to publish the full data of victims who seek help from law enforcement and investigative agencies following a ransomware attack.

One of the messages texted to TTEC employees included a link to a **Zoom** videoconference line at **ttec.zoom.us**. Clicking that link opened a Zoom session in which multiple TTEC employees who were sharing their screens took turns using the company's Global Service Desk, an internal TTEC system for tracking customer support tickets.

The TTEC employees appear to be using the Zoom conference line to report the status of various customer support teams, most of which are reporting "unable to work" at the moment.

For example, TTEC's Service Desk reports that hundreds of TTEC employees assigned to work with Bank of America's prepaid services are unable to work because they can't remotely connect to TTEC's customer service tools. More than 1,000 TTEC employees are currently unable to do their normal customer support work for Verizon, according to the Service Desk data. Hundreds of employees assigned to handle calls for Kaiser Permanente also are unable to work.

"They've been radio silent all week except to notify employees to take another day off," said the source who passed on the TTEC messages, who spoke to KrebsOnSecurity on condition of anonymity. "As far as I know, all low-level employees have another day off today."

The extent and severity of the incident at TTEC remains unknown. It is common for companies to disconnect critical systems in the event of a network intrusion, as part of a larger effort to stop the badness from spreading

elsewhere. Sometimes disconnecting everything actually does help, or at least helps to keep the attack from spreading to partner networks. But it is those same connections to partner companies that raises concern in the case of TTEC's ongoing outage.

In the meantime, if you're unlucky enough to need to make a customer service call today, there's a better-than-even chance you will experience….wait for it…longer-than-usual hold times.

This is a developing story. Further details or updates will be noted here with a date and time stamp.

Update, 5:37 p.m. ET: TTEC responded with the following statement:

> TTEC is committed to cyber security, and to protecting the integrity of our clients' systems and data. We recently became aware of a cybersecurity incident that has affected certain TTEC systems. Although as a result of the incident, some of our data was encrypted and business activities at several facilities have been temporarily disrupted, the company continuous to serve its global clients. TTEC immediately activated its information security incident response business continuity protocols, isolated the systems involved, and took other appropriate measures to contain the incident. We are now in the process of carefully and deliberately restoring the systems that have been involved.
>
> We also launched an investigation, typical under the circumstances, to determine the potential impacts. In serving our clients TTEC, generally, does not maintain our clients' data, and the investigation to date has not identified compromise to clients' data. That investigation is on-going and we will take additional action, as appropriate, based on the investigation's results. This is all the information we have to share until our investigation is complete.
