Ransomware shuts down 600+ employees of a Swiss franchise business
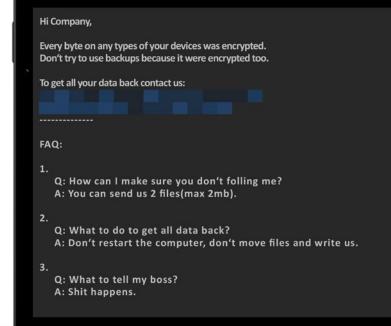
A recent attack shows how Ransomware can grind any business to a halt in a second: A sizeable Swiss franchise business with more than 190 branches, 126 servers, and 600+ employees were hit overnight on a Saturday morning. The message was plain and simple …

As more than 20 TB of critical files were encrypted and entire systems shut down, a task force was put together: Swiss IT Security AG assembled the next day and performed a thorough analysis of all impacted systems, immediately beginning recovery steps. Within a few days, all systems were restored and even backups were searched for traces of the Ransomware. The company was able to resume operations within a few days, while Swiss IT Security AG established new security solutions and network segmentation within the first week to help shield from any future malicious attempts.

Hi Company,

Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:

FAQ:

1.
    Q: How can I make sure you don't folling me?
    A: You can send us 2 files(max 2mb).

2.
    Q: What to do to get all data back?
    A: Don't restart the computer, don't move files and write us.

3.
    Q: What to tell my boss?
    A: Shit happens.

If you need further assistance or have any questions related to the offer, please do not hesitate to contact our team of experts.

Timeline of Events

**Saturday
11 am**

The attack begins
**First service outages
and unrest among
employees begins**

**Saturday
4 pm**

Discovery of attack
**More infected
devices were discovered
over time**

**Saturday evening
and Sunday**

Taskforce
**Assembly of multiple
experts and forensics**

Analysis
**Taskforce analyzes
infected devices and
the severity of the attack**

Monday

Police involvement
Filing a police report

**Subsequent
two weeks**

Restoring backup
**Scanning the backup
for infected files**

Following year

**Establishing new
security guidelines**
**Establishing and evaluating
new security solutions
and expand on
network segmentation**

If you need further assistance or
have any questions related to the
offer, please do not hesitate to
contact our team of experts.