Travelex Ransomware Attack

SODINOKIBI

- First appeared April 2019
- June 2019 Breached 3 MSPs to attack customer systems
- Aug 2019 Attacked 22 local and state entities in Texas
- Jan 2020 published stolen data for the first time

31 Dec 2019 — Attack

Travelex systems impacted by malware.

A number of major retail banks all impacted and unable to issue foreign currency online.

2 Jan 2020 — Reported

Metropolitan Police Service Cyber Unit informed of attack.

3 Jan 2020 — Impact

Travelex website down with 'Planned Maintenance' message.

Parent company share price -12%

7 Jan 2020 — Ransom

BBC report contact with attackers who claim they have exfiltrated 5GB personal data and are demanding a £4m ransom.

8 Jan 2020 — Statements

Travelex admits it has been attacked with Sodinokibi ransomware but claims no evidence of data theft.

ICO says that Travelex made no formal notification of a data breach.

13 Jan 2020 — Recovery

Travelex says that it has started to return some systems online.

They do not confirm whether any ransom was paid to the attackers.

21 Jan 2020 — New Victim

GEDIA Automotive Group attacked by SODINOKIBI with threats to release 50GB of stolen data unless the ransom is paid

24 Jan 2020 — Data Leak

SODINOKIBI attackers release portion of data including details of internal infrastructure, backup plans, network and software with threats to publish in full if the ransom isn't paid.

Ransomware Trends

The theft of sensitive data prior to encryption, and threats to release this data unless a ransom is paid, is a new tactic which has been seen not only with SODINOKIBI, but also MAZE and NEMTY ransomware groups. Given the already significant costs associated with recovering from a ransomware attack, the potential reputational and financial impact of sensitive company and employee information also being released may prove to be an effective method to ensure victims pay the ransom quickly and discreetly. It is likely that this is a trend which will become more common in future ransomware attacks.

Ransomware Mitigation Advice

1. Ensure backups are secure
2. Protect the perimeter
3. Ensure common methods that ransomware use to spread are reduced
4. Implement application whitelisting
5. Enable Credential Guard in Windows 10, and don't allow users to have local admin access
6. Control highly privileged accounts
7. Patch IT infrastructure
8. Decommission end-of-life hardware/software

BAE SYSTEMS

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

learn@baesystems.com baesystems.com/threatintel twitter.com/baesystems_ai