
**EG-CERT**

Egyptian Computer
Readiness Team

# Alert: Suspected ransomware spreading through TeamViewer

| | |
|---|---|
| **Date** | 17-July-2019 |
| **Created By** | EG-CERT<br>Malware analysis team |

**Summary:**

- EG-CERT malware team encountered multiple incidents where the victims were infected with Dalle Ransomware (a variant from the Djvu family) , All the victims were running TeamViewer on Windows 7.
- It's not new for ransomware to abuse TeamViewer to gain access to vulnerable machines , in 2016 , a ransomware named "surprise" spread widely by using weak TeamViewer credentials to gain access to victims machines.
- These new ransomware variants use Salsa20 encryption algorithm to encrypt personal files and documents on the system ; the victim is then presented a note that asks for ransom money to send you an application that will decrypt the files.
- Salsa20 is almost as strong as AES but 2-3x faster and thus cannot be brute forced to decrypt the files without needing to pay the ransom.
- If the ransomware failed to connect to the C&C server , It will encrypt the files using a hard coded key which can be retrieved and used to decrypt the files , this is the only case where the files could be recovered .

**Advisory**:

- Use strong and unique TeamViewer credentials and Enable two-factor authentication (More details).
- Download and use TeamViewer only through their official website teamviewer.com .
- Update TeamViewer regularly to patch any vulnerabilities.
- Apply windows updates regularly and use strong RDP credentials or disable them if not needed.
- Backup your critical files regularly on an external storage.