# Israeli IRS themed ransomware attack

## General information

| | |
|---|---|
| **UUID** | 5d8129c9-8fb8-4aff-8cfa-72b60a000082 |
| 2019-09-17 | **Date** |
| **Owner org** | No value specified. |
| **Threat level** | No threat level specified. |
| **Analysis** | Initial (0) |
| **Info** | Israeli IRS themed ransomware attack |
| **Event date** | 2019-09-17 19:03:35 |
| **Published** | **Yes** (2019-09-17 19:03:57) |
| **Creator Org** | Profero |
| **# Attributes** | 9 |
| **Tags** | **Ransomware**<br>**tlp:white**<br>**misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1192"**<br>**misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1059"**<br>**misp-galaxy:mitre-attack-pattern="Execution through API - T1106"**<br>**misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047"**<br>**misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1158"**<br>**misp-galaxy:mitre-attack-pattern="New Service - T1050"**<br>**misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1060"**<br>**misp-galaxy:mitre-attack-pattern="File Deletion - T1107"**<br>**misp-galaxy:mitre-attack-pattern="Modify Registry - T1112"**<br>**misp-galaxy:mitre-attack-pattern="Query Registry - T1012"** |

# Attributes

### *Attribute #1*

| | |
|---|---|
| **UUID** | 5d812ad9-bde4-4b00-abdb-73a30a000082 |
| **Category** | External analysis |
| **Type** | link |
| **Value** | https://www.eset.co.il/eset-blog/law-enforcement-and-collection-ransomware |

### *Attribute #2*

| | |
|---|---|
| **UUID** | 5d812b20-4b60-4db0-950c-7c3f0a000082 |
| **Category** | External analysis |
| **Type** | link |
| **Value** | https://app.any.run/tasks/ca6e6576-07a4-4ebc-b5b4-b59b39d4d8e7/ |

### *Attribute #3*

| | |
|---|---|
| **UUID** | 5d812b3f-2674-448d-b427-7c320a000082 |
| **Category** | External analysis |
| **Type** | link |
| **Value** | https://www.virustotal.com/gui/file/71327d7ca505fe4fae8fb285b634c9150c3a3253188879fcea2e3bf68196a766/detection?fbclid=IwAR3OFOe0O7zOiAnft8leT_XetK4AdnTYyjxpkNOGIl9TqYpyzhECAf-MtCk |

### *Attribute #4*

| | |
|---|---|
| **UUID** | 5d812b97-a230-4439-81f5-7c320a000082 |
| **Category** | Payload delivery |
| **Type** | sha256 |
| **Value** | 71327d7ca505fe4fae8fb285b634c9150c3a3253188879fcea2e3bf68196a766 |

### *Attribute #5*

| | |
|---|---|
| **UUID** | 5d812bc7-40d4-4591-b7d9-72b60a000082 |
| **Category** | Network activity |
| **Type** | domain |
| **Value** | aurmus.is |

### *Attribute #6*

| | |
|---|---|
| **UUID** | 5d812bf5-7774-46a6-b31d-7c330a000082 |
| **Category** | Other |
| **Type** | comment |
| **Value** | Ransom emails: BhatMaker@protonmail.com,BhatMaker@tutanota.com |

### *Attribute #7*

| | |
|---|---|
| **UUID** | 5d812c12-e870-4a6a-a2d9-72b40a000082 |
| **Category** | Network activity |
| **Type** | url |
| **Value** | http://iplogger.ru/1OnzW.jpg |

### *Attribute #8*

| | |
|---|---|
| **UUID** | 5d812c69-472c-4163-8244-72b50a000082 |
| **Category** | Artifacts dropped |
| **Type** | sha256 |
| **Value** | 029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7 |

### *Attribute #9*

| | |
|---|---|
| **UUID** | 5d812c80-e2b4-4df4-bc9f-73a30a000082 |
| **Category** | External analysis |
| **Type** | link |
| **Value** | https://analyze.intezer.com/#/files/029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7 |

# Objects

### *No object*