# StealthDEFEND Threat Analytics

## Ransomware

If files are renamed to known ransomware extensions, a threat is created for each rename action.

| Ransomware | |
|---|---|
| **Definition** | The Ransomware threat creates a threat for any file activity that involves a file with a known ransomware extension or a file with a name that resembles common ransom notes. |
| **Example** | A user created a ".locky" file, which is a known ransomware extension. |
| **Trigger** | Using a pre-defined library of known ransomware extensions, StealthDEFEND alerts on file create/rename activity with known extensions. |

## Abnormal Behavior

A baseline of 14 days is established on a per user basis. If the user deviates from the baseline, a threat is created.

| Abnormal Behavior | |
|---|---|
| **Definition** | The Abnormal Behavior threat detects user behaviors that deviate from the user's normal behavioral profile. |
| **Example** | **Sensitive Data Example:** A user suddenly accesses far more files containing sensitive content than they normally do.<br>**Ransomware Example:** New ransomware variants not represented in StealthDEFEND's pre-defined library will still exhibit abnormal behavior with regard to file access operations, including large volumes of updates, renames and writes.<br>**Lateral Movement Example:** If a user is accessing an abnormal number of hosts and is performing file activity on a large number of resources, this could be an indicator of suspicious lateral movement. |

| | |
|---|---|
| | **Delete Example:** Upon termination, disgruntled employees sometimes delete large volumes of files to cause the organization harm. |
| **Trigger** | StealthDEFEND analyzes the following aspects of each user’s behavior and creates a threat when abnormalities are detected based on a given user's normal level of activity.<br>→ Number of Reads<br>→ Number of Updates<br>→ Number of Deletes<br>→ Number of Renames<br>→ Number of Permission Changes<br>→ Number of Writes<br>→ Number of Denied Events<br>→ Number of Hosts Accessed<br>→ Number of Resources<br>→ Number of Files with Sensitive Data<br>Outliers are detected through unsupervised clustering of a user's historical activity. |

## First Time Host Access

If a user accesses a host for the first time, a threat is created.

| First Time Host Access | |
|---|---|
| **Definition** | The First Time Host Access threat detects when a user performs file activity on a new host they haven’t accessed previously. |
| **Example** | Most users only interact with a few file servers based on their geographic location, the department they are in, etc. Over a learning period (e.g. 30 days), StealthDEFEND profiles which hosts a user commonly accesses data on. After the learning period, StealthDEFEND will create a threat if a new host is accessed for the first time. |
| **Trigger** | A user accessed an open share on a new host for the first time. |

## First Time Client Access

If a user accesses a share using a new client, a threat is created.

| First Time Client Access | |
|---|---|
| **Definition** | The First Time Client Access threat detects when a user accesses file share data from a client they have never used to access data previously. |
| **Example** | A user normally uses his own workstation to access file shares. On a given day, the user accesses files from a different workstation, indicating the user's account may be compromised. |
| **Trigger** | StealthDEFEND analyzes user behavior over a learning period (e.g. 30 days) to profile which clients a user normally leverages. Once a new client is used to perform file system activity for the first time for a particular user, StealthDEFEND creates a threat. |

## Unusual Processes

If a user runs a process on a monitored server for the first time, a threat is created.

| Unusual Processes | |
|---|---|
| **Definition** | The Unusual Processes threat detects of previously unseen processes are launched on critical file servers. |
| **Example** | A user launches a "python.exe" process that has never been launched by anyone else in the environment. |
| **Trigger** | StealthDEFEND records the name of the processes associated with file access activities. Over a learning period (e.g. 30 days), StealthDEFEND profiles which processes are normal by aggregating data across all file servers. After that, if a new process is identified that has not been seen on any other file servers, a threat will be created.<br>**NOTE:** This threat is only applicable on Windows file servers when the activity is performed locally. |