Alert, report and respond to new ransomware attacks in under 10 minutes with LepideAuditor™

While there is no simple way of addressing ransomware entirely, there are number of measures that all organisations can take to help spot and mitigate the risk and spread of such an attack. LepideAuditor offers probably the easiest, fastest (and most cost effective) means of spotting and reacting to potential ransomware attacks on your Windows File Servers or NetApp Filers. While there are many preventative ways Lepide can help with ransomware, this document takes a focus on the detection and response of such a threat.

Detect and alert on potential ransomware threats

Our threshold alerting capability enables organisations to detect and alert on bulk changes made to files and folders. For example, we enable you to create alerts based on trends that could indicate the start of a ransomware attack. Essentially, we use three criteria to define our alerts:

1. Number of instances of the event 2. Event Type 3. Time Lapsed

In the context of ransomware this would enable us to track and alert on file modification, or failed modification attempts. For example we would send you an alert if we spot X number of Y events over Z period of time.

All our alerts are real time and are delivered either to a LiveFeed to the Lepide Dashboard, via email or directly to any Apple or Android enabled mobile device.

Dealing with the threat

Our threshold alerting also offers you the option to automatically run a script triggered by the conditions specified within the alert. It supports all common scripting languages and enables you to automate anything you specify. For example, in the context of ransomware you may want a script to execute the following actions:

- Disable a user account
- Change firewall configuration settings
- Stop a specific process
- Shut the server down

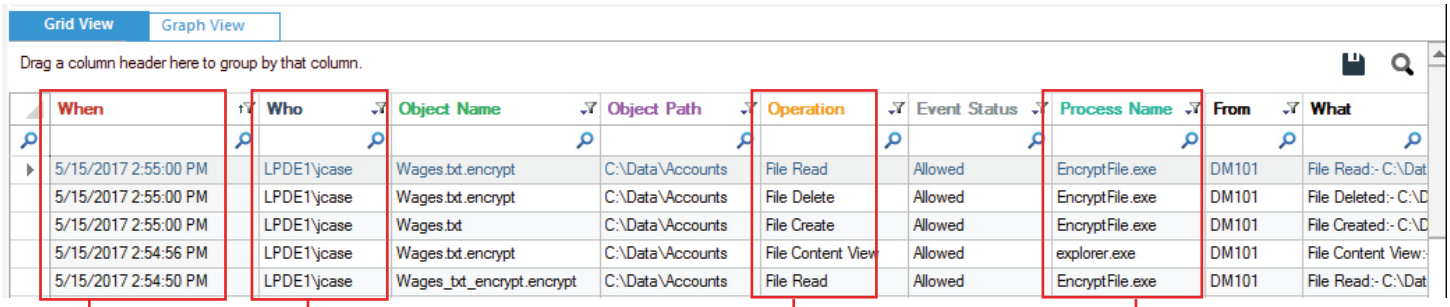
How we do it

LepideAuditor, in the specific context of detecting ransomware, is designed for Windows File Servers and NetApp filers within your organisation. It requires a small, unobtrusive agent to be installed on the server itself and typically installs in under 10 minutes. It will require an instance of SQL Server to be in place to run. Immediately upon installation, specify the alerts and reports you need and then everything is set.

What to do next

If you'd like to know more contact us via the details below – we can take you through a demo to show you how it works in action. Alertatively, more information is available at www.lepide.com

How to spot and react to ransomware attacks using LepideAuditor™

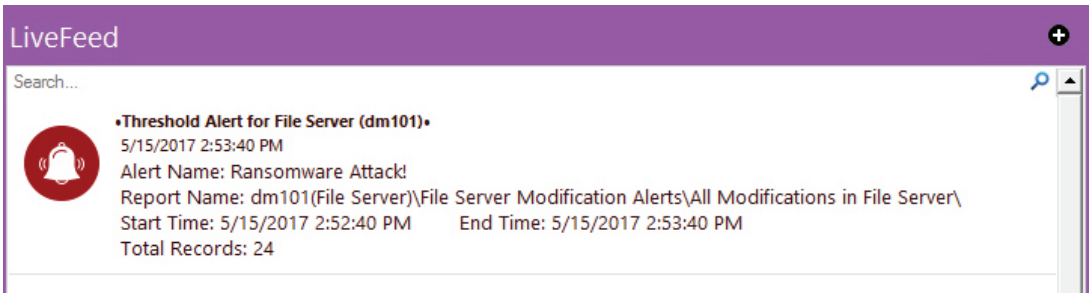


Determine the user account from which the event originated (to establish the source of the attack)

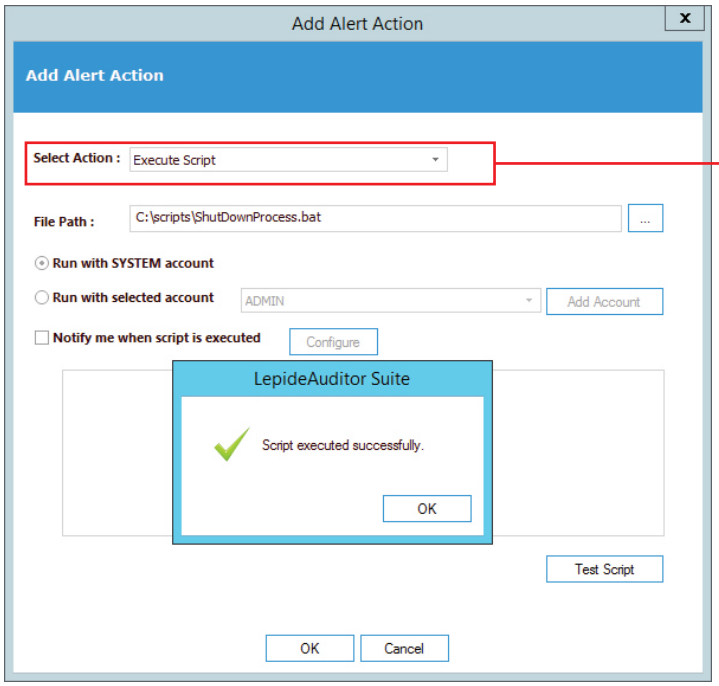
The operation field shows you which files and folders are being modified

The process name shows you the application or process that instigated the actual event

LepideAuditor shows when the event took place, to help you keep track of the spread



Shows a LiveFeed alert within the main LepideAuditor dashboard configured using threshold based conditions. These alerts can show the potential signs of a ransomware attack.



Shows the execution of an automated script to stop the spread of ransomware.