

Ransomware Detection

PLATFORM FEATURE UPDATE

While various ransomware attacks use different methods and techniques, at the core, the attack is carried out by encrypting files across a victim’s network. In doing so, this process triggers a number of file access events: Write/WriteAttribute (Windows Event ID 4663) and Delete (Windows Event ID 4660).

Adlumin’s new **Ransomware Detection Model** monitors the volume of these three events independently of each other per user across the entire network, looking for anomalous spikes in activity during a specific time window using historical data as a benchmark. If the amount of activity (either write or deletion) exceeds a specific threshold relative to the rest of the activity on the network, a detection will be sent for investigation.

In addition to checking the total volume of files accessed, the model also checks the distribution of objects modified across the network. If the majority of activity is focused in a single directory, which could be associated with software installation or updates, the model will not raise a detection. However, if the spike in activity is spread across multiple subdirectories, indicative of system-wide activity, the model will raise a detection.

The screenshot displays the Adlumin Ransomware Detection interface. At the top, it shows the detection ID 'Ransomware Detection - 15587' and the detection time '2021-07-23 09:18:14 UTC'. A callout box labeled 'Aggregate detection information' points to a summary card showing '1725 Total Events' and '1725 Events Surrounding this Detection'. Below this is an 'Event Sample Timeline' showing a 10% sample of file access events as a horizontal line with markers. A callout box labeled '10% Sample timeline of file access events' points to this timeline. The bottom section is a 'Surrounding Events' table with columns for Type, Time (UTC), Host, Object, Process, and View. A callout box labeled 'Table of files accessed during detection time window' points to the table. Another callout box labeled 'Click to view full event information' points to a 'View' button in the table.

Type	Time (UTC)	Host	Object	Process	View
Object Access	2021-07-23 09:17:44 UTC	192.168.1.1	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	View
Object Access	2021-07-23 09:17:44 UTC	192.168.1.1	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	View
Object Access	2021-07-23 09:17:44 UTC	192.168.1.1	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	View
Object Access	2021-07-23 09:17:44 UTC	192.168.1.1	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	View
Object Access	2021-07-23 09:17:44 UTC	192.168.1.1	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	View
Object Access	2021-07-23 09:17:44 UTC	192.168.1.1	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	View
Object Access	2021-07-23 09:17:34 UTC	192.168.1.1	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	View
Object Access	2021-07-23 09:17:34 UTC	192.168.1.1	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	View
Object Access	2021-07-23 09:17:34 UTC	192.168.1.1	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	C:\Program Files\Microsoft\Windows Defender\Windows Defender.exe	View