Detecting Known Bad and Unknown Process
How to – Detect Known Bad and Unknown Process

About this Guide:

In the recent times we have seen increase in Malware or Trojan getting installed and executed on windows systems and it infects the local system as well as spreads to other systems in network depending on the logged in user permissions or access level required to execute it on remote machines. Users’ visit various websites and sometime they unknowingly click on the popups or advertisements displayed on the web page. Sometimes these ads and popups contain links to Trojans, Malwares or harmful scripts which gets downloaded and installed when user clicks on these links.

This guide will help the EventTracker Administrators configure unknown process execution using EventTracker. This configuration will check existent of new process detected by EventTracker against windows known exe’s list database. EventTracker will alert when any unknown exe’s detected in the network.

Scope:

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and later and Windows Operating systems.

Audience:

IT/Security or network administrators, who are responsible for monitoring and maintaining the security of the network.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. © 2015 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents:

About this Guide: ......................................................................................................................................... 1
Scope: ............................................................................................................................................................ 1
Audience: ...................................................................................................................................................... 1
Introduction ................................................................................................................................................. 3
Pre-requisite ................................................................................................................................................ 4
Setting up windows process lookup .......................................................................................................... 6
  Preparing Scripts for use as per your environment ............................................................................. 6
  Import Category ....................................................................................................................................... 6
  Import Alert .............................................................................................................................................. 9
  Import Scheduled Reports: ................................................................................................................... 11
  Import Knowledge Object ..................................................................................................................... 13
  Import KnownExeWhitelist into EventTracker ................................................................................... 15
Configuring Remedial Action for Alerts ............................................................................................... 17
  Configure Scheduled Reports ............................................................................................................... 23
Verify Alerts and Reports ......................................................................................................................... 28
Tuning Alerts and Reports ........................................................................................................................ 30
How to – Detect Known Bad and Unknown Process

Introduction

In the recent times we have seen increase in Malware or Trojan getting installed and executed on windows systems and it infects the local system as well as spreads to other systems in network, depending on the logged in user permissions or access level required to execute it on remote machines. Users’ visit various websites and sometime they unknowingly click on the popups or advertisements displayed on the web page. Sometimes these ads and popups contain links to Trojans, Malwares or harmful scripts which gets downloaded and installed when user clicks on these links.

EventTracker alerts IT/Security administrators whenever any new process is executed on windows systems in the network which is not a part of known exe list in the database. It provides detailed information about Process such as Process name, File path, User name, Domain name, Logon ID, Process ID and System name, where new process is executed.

Example uses:

- Track any new exe’s launched which is a part of list of exe’s known to be Trojan, Virus or Malware which can cause damage to the system or network.

- Get alerted, when any new exe is launched and it is not a part of the authorized exe list.

EventTracker alerts and provides report if any such activity is detected in network so that the administrators can act on that immediately and take proper action.
How to – Detect Known Bad and Unknown Process

Pre-requisite

- EventTracker v7.x should be installed and List Management feature should be present.
- Windows PowerShell 4.0 and later must be installed.
  To check the PowerShell version:
  ▪ Launch Windows PowerShell as Administrator.
  ▪ Run command $PSVersionTable.PSVersion
- Script Execution policy must be set to Unrestricted.
  To change PowerShell execution policy,
  ▪ Launch Windows PowerShell as Administrator.
  ▪ Run command ‘Set-Execution Policy Unrestricted’.
  ▪ Make sure you do this for both x86 and x64 versions.
- Process tracking audit setting on windows monitored systems must be enabled.
- EventTracker Agent should be configured to send event ID 592 and 4688 in real time.
How it works?

The list Management option in EventTracker, allows users to maintain the list of whitelist and blacklist exe’s. EventTracker provides list of known executable’s from windows server operating systems for AD, DNS, IIS and SQL server installed.

Whenever any process is launched on monitored systems, event id 592 and 4688 is generated, EventTracker Agent sends this event to Manager in real time and an alert is raised. It launches remedial action script by passing the process name as parameter. Script checks the exe name against the list of exe and if launched exe is not part of that list then it generates another event ID 9999.

**NOTE**: Event description containing user name with $ sign will not be considered for list lookup.
How to – Detect Known Bad and Unknown Process

Setting up windows process lookup

Preparing Scripts for use as per your environment

- Contact support@eventtracker.com to obtain the ProcessListlookupScript pack.
- Save ProcessListLookupScript.zip (saved to D:\ProcessListLookupScript\ folder in the example below).
- Extract all files to D:\ProcessListLookupScript\.
- Make sure all the checklists mentioned in the prerequisite section has been installed and configured.
- Files in the package are shown below.

![Image of file structure]

Import Category

To import the category,

- Go to EventTracker Control Panel.
- Select the Export Import Utility feature as displayed in the figure below:
• In the Import Tab, select Category and browse the Category name i.e. EventTracker: Unknown process launched.

• Select the category file and click on Open, as shown below:
Click the **Import** button, and the category file **EventTracker: Unknown process launched** gets imported.
Import Alert

For importing the alert EventTracker: New exe launched-process lookup, select the Alerts Option.

- Provide the path name and file name of the Alert file.
- For this, click the icon and browse the Alert File i.e. EventTracker: New exe launched-process lookup from your system and click Open.
Now, click the Import button.
The success message box of ‘Selected alert configurations are imported’ will be displayed.

![Image of Export Import Utility window with success message]

Figure 6

- Click OK.

Thus, the two alerts, namely, _EventTracker: New exe launched-process lookup_ and _EventTracker: Unknown process launched_, gets successfully imported.

**Import Scheduled Reports:**

To Import Scheduled Reports,

- Select _Scheduled Report_ from the Export Import Utility Window.

![Image of Export Import Utility window showing Scheduled Reports]

Figure: 7
How to – Detect Known Bad and Unknown Process

- Provide the path and file name of the scheduled report file i.e. **Eventtracker-Unknown process launched-defined**, by browsing the Report file from your system.

![Figure: 8]

- Open the Report file and click the **Import** button.

![Figure: 9]

The report file **Eventtracker-Unknown process launched-defined** will be successfully imported.
How to – Detect Known Bad and Unknown Process

Import Knowledge Object

For importing Knowledge Object,

- Go to EventTracker Web Console.
- Click Admin drop down and select Knowledge Objects from the list.
- Click the Import Icon for importing the Knowledge Object file, as highlighted in the below figure:

![Figure: 10](image)

- Choose the Knowledge Object file, i.e. WindowsProcessLookup.

![Figure: 11](image)

- Click On Upload.
- Now, select the check box and click on Merge, as shown in the figure below:

![Figure: 12](image)

- The success message box will be displayed. Click OK.

![Figure: 13](image)

The Knowledge Object gets successfully imported.
Import KnownExeWhitelist into EventTracker

- Login to EventTracker Enterprise Web Console.
- Click Admin dropdown and click List Management.
- Click + icon to add Process List group as highlighted in the figure below:

![Figure: 14](image1.png)

- Select Processes from the drop down menu.
- Enter Name as KnownExeWhitelist.

![Figure: 15](image2.png)

- Click Save.
• You will see KnownExeWhiteList group under Processes in List Management page.
• Click KnownExeWhiteList under Processes group in left pane again and click the icon available in right pane for importing it, as shown in above figure.
• Enter the details with File Type as CSV, Field Separator as ‘,’ (comma), Row Terminator as \n, Data Index as 1 and Skip Header Row as 1.
• Also browse the KnownExeWhiteList file as shown in below figure and click Import.
• One process list is imported successfully and you will see list of processes shown in List Management page.

![List Management](image18)

Figure: 18

Configuring Remedial Action for Alerts

• Login to EventTracker Enterprise Web Console.
• Click Admin dropdown and click Alerts.

EventTracker displays the Alert Management page.

![Alert Management](image19)

Figure: 19
How to – Detect Known Bad and Unknown Process

- Enter the Alert Name EventTracker: New exe launched-process lookup in the Search box.
- Click the Go button.

The Alert Name with specified details will be displayed.

Figure: 20

- Click on the alert EventTracker: New exe launched-process lookup hyperlink to make changes in the Alert Configuration.

Figure: 21
How to – Detect Known Bad and Unknown Process

- Click the **System** hyperlink to choose the EventTracker Manager system as shown in the figure below:
- Here the local system MCLOON is selected.

![Figure: 22](image)

For assigning Remedial Action based on a particular Alert,

- Click the **Action** hyperlink and then click the **Console Remedial Action**.

**NOTE:** The user must select the **Console Remedial Action**, to assign an action for this alert.

- Enter the file name with the mentioned path as shown below:

```
"C:\Windows\SysWoW64\WindowsPowerShell\v1.0\powershell.exe" -File "D:\ProcessListLookupScript\ProcessListLookupScript.ps1"
```

**NOTE:** In case if you have stored script in different path, replace d:\ProcessListLookupScript\ with the path where you have stored the script.
How to – Detect Known Bad and Unknown Process

• Click the Finish button.
• Now click the Activate Now button after confirming all the changes made and activate the Alert EventTracker: New exe launched-process lookup.

Similarly, for configuring the alert EventTracker: Unknown process launched,

• Enter the alert name EventTracker: Unknown process launched in the Search box and click the Go button.
• Click on the **EventTracker: Unknown process launched** hyperlink.

The Alert Configuration dialog box displays.

• Select the EventTracker Manager system by clicking the hyperlink **Systems**.
The local system MCLOON is selected here.

For assigning Remedial actions,

- Click **Actions** hyperlink and select the option **E-mail Configuration** to generate an e-mail for this alert.

- Click **Finish**.
• Now, Click the **Activate Now** button to activate the alert.

![Figure: 29](image)

**Configure Scheduled Reports**

To assign remedial action to Scheduled Reports,

• Go to EventTracker.
• Click on **Reports** and select the **Configuration** option from the dropdown box.
• Select the **Defined** option.

The Report file **Eventtracker-Unknown process launched-defined** is displayed.
• For scheduling the report file, click the icon.

• From the drop down box select Systems and click on your EventTracker Manager System name. Here, MCLOON is selected.

• Click on Next to continue the steps.
• Add time range and click on the **Next** option to continue.

• Click **Next**.
How to – Detect Known Bad and Unknown Process

- Add specific details, if you want to narrow down your criteria and click Next.
- Enter Title and Description and click Next.
  Here, the title is changed to Eventtracker-Unknown process launched.

- Review the cost details, configure the publishing options and click Next.
The Completing report configuration wizard is displayed.

- Click on the **Scheduled** button.

The process of configuring report is successfully completed.
Verify Alerts and Reports

- Login to EventTracker web.
- Go to **Incidents** menu and select **Graphical View** from the drop down box.

![Graphical View Example]

To view the Alerts in a tabular format, you can click the **Tabular** option.
For viewing the reports,

- Go to Report and select Dashboard.

### Summary:

<table>
<thead>
<tr>
<th>Image File Name</th>
<th>Total Event Occurred</th>
<th>Event Id (Total Count)</th>
</tr>
</thead>
<tbody>
<tr>
<td>D:\Shared Files\Accounting Password\Trojan.exe</td>
<td>2</td>
<td>9999(2)</td>
</tr>
<tr>
<td>C:\Shared Files\Password Safe\Trojan.exe</td>
<td>1</td>
<td>9999(1)</td>
</tr>
<tr>
<td>Process Name</td>
<td>Total Event Occurred</td>
<td>Event Id (Total Count)</td>
</tr>
<tr>
<td>KeePass.exe</td>
<td>2</td>
<td>9999(2)</td>
</tr>
<tr>
<td>pwsafe.exe</td>
<td>1</td>
<td>9999(1)</td>
</tr>
<tr>
<td>System Name</td>
<td>Total Event Occurred</td>
<td>Event Id (Total Count)</td>
</tr>
<tr>
<td>Contoso-ITDC1</td>
<td>3</td>
<td>9999(3)</td>
</tr>
<tr>
<td>User Name</td>
<td>Total Event Occurred</td>
<td>Event Id (Total Count)</td>
</tr>
<tr>
<td>Karon</td>
<td>2</td>
<td>9999(2)</td>
</tr>
<tr>
<td>Kate</td>
<td>1</td>
<td>9999(1)</td>
</tr>
</tbody>
</table>
Tuning Alerts and Reports

Once process lookup is configured and you receive alerts and reports for few days. You might feel that many exe’s which is observed in this reports are known and safe. In that case you will have to add that process names into the KnownEXEWhilelist group in List Management page. Or if you don’t want to see the alert if it is observed on a specific server.

All this can be done easily by adding filter in Process lookup alerts or reports.

Sample description generated for Process lookup is shown below. You can filter out by adding Filter exception rule by any of the columns listed below.

Unknown Process trojan.exe launched on contoso-appsvr1

Process Details:-
Process Name: Trojan.exe
Image File Name: c:\users\contosoadmin\temp\trojan.exe
User Name: contosoadmin
Domain Name: Contoso
Logon ID: 0x1CC5D8C4
New Process ID: 0x294
Caller Process ID: 0x470
System Name: contoso-appsvr1