Detecting PoSeidon Malware on PoS System

EventTracker v7.x

Whitepaper
Publication Date: Mar 23, 2015

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This document provides Information about **Poseidon Malware** recently discovered on **Point-of-Sale (PoS)** systems. This document also provides guidance to the user about detecting this threat using **EventTracker** and blocking any connection attempts made to the known ip address used by this malware.

Scope

The configurations detailed in this guide are consistent with EventTracker 7.x and later**.**

Target Audience

IT administrators or Security administrators who are responsible for maintaining security for the IT infrastructure, especially the **Point-of-Sale (PoS)** systems.

Severity

High

Table of Contents

Introduction

A new and terribly awful breed of Point-of-Sale (POS) malware **Poseidon** has been spotted in the wild by the security researchers at Cisco's Security Intelligence & Research Group. The team says it is more sophisticated and nasty than previously seen Point-of-Sale malwares.

This new malware family is targeting PoS systems, infecting machines to scrape memory for credit card information and exfiltrate that data to servers, also primarily .ru TLD, for harvesting and likely resale. This new malware family that is nicknamed as PoSeidon has a few components to it, as illustrated by the diagram below:

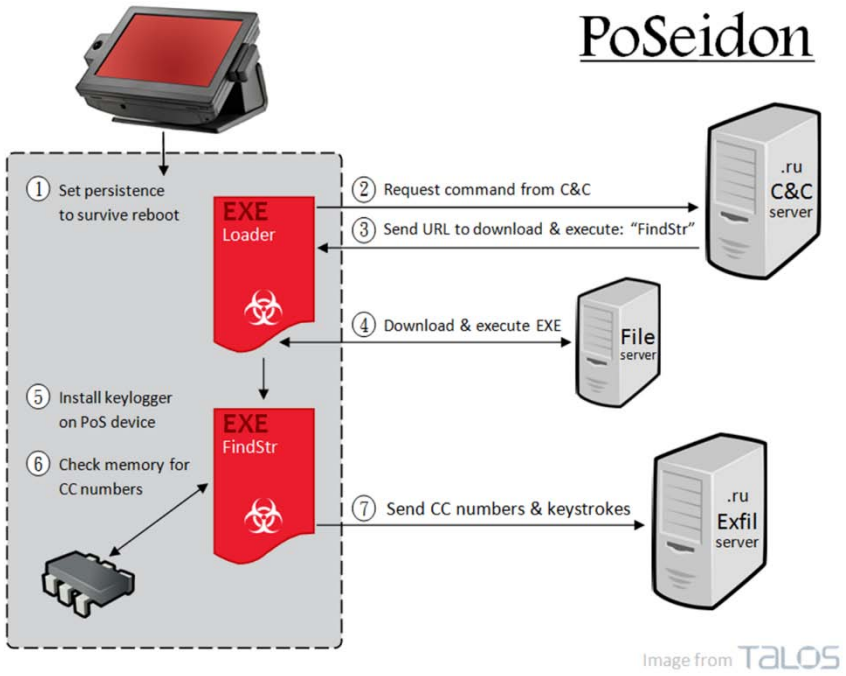

Figure 1

At a high level, it starts with a Loader binary that upon being executed will first try to maintain persistence on the target machine in order to survive a possible system reboot. The Loader then contacts a command and control server, retrieving a URL which contains another binary to download and execute. The downloaded binary, FindStr, installs a keylogger and scans the memory of the PoS device for number sequences that could be credit card numbers. Upon verifying that the numbers are in fact credit card numbers, keystrokes, the credit card numbers are encoded and sent to an exfiltration server.

For more detailed information please visit the link http://blogs.cisco.com/security/talos/poseidon.

Affected systems

- Point-of-Sales (PoS) systems.

Detecting **PoSeidon** malware using EventTracker

Once EventTracker agent is deployed and Process Tracking is enabled on Target systems, and Network connection Monitoring enabled in EventTracker Agent on Target PoS Systems, then the connection made to and from the local system to/from external network is monitored by EventTracker.

EventTracker has released Attack signature pack which contains rules to detect the PoSeidon malware exe and activity detected from or to IP Address exe's and to detect alerts and reports which can be generated for any such activities.

Process to use the ASIG pack in EventTracker

Import Category

1. Download the update.
2. Extract the zip file.
3. To import the category file into EventTracker using Export Import Utility. Please follow the steps given below.
   a. Launch **EventTracker Control Panel**.
   b. Double click **Import Export Utility**, and then click the **Import** tab.
   c. To import Category, click **Category** option, and then click the **browse**  button.
   d. Locate the file **Threat-PoSeidon malware detection.iscat** and then click the **Open** button.
   e. Click the **Import** button to import the categories.

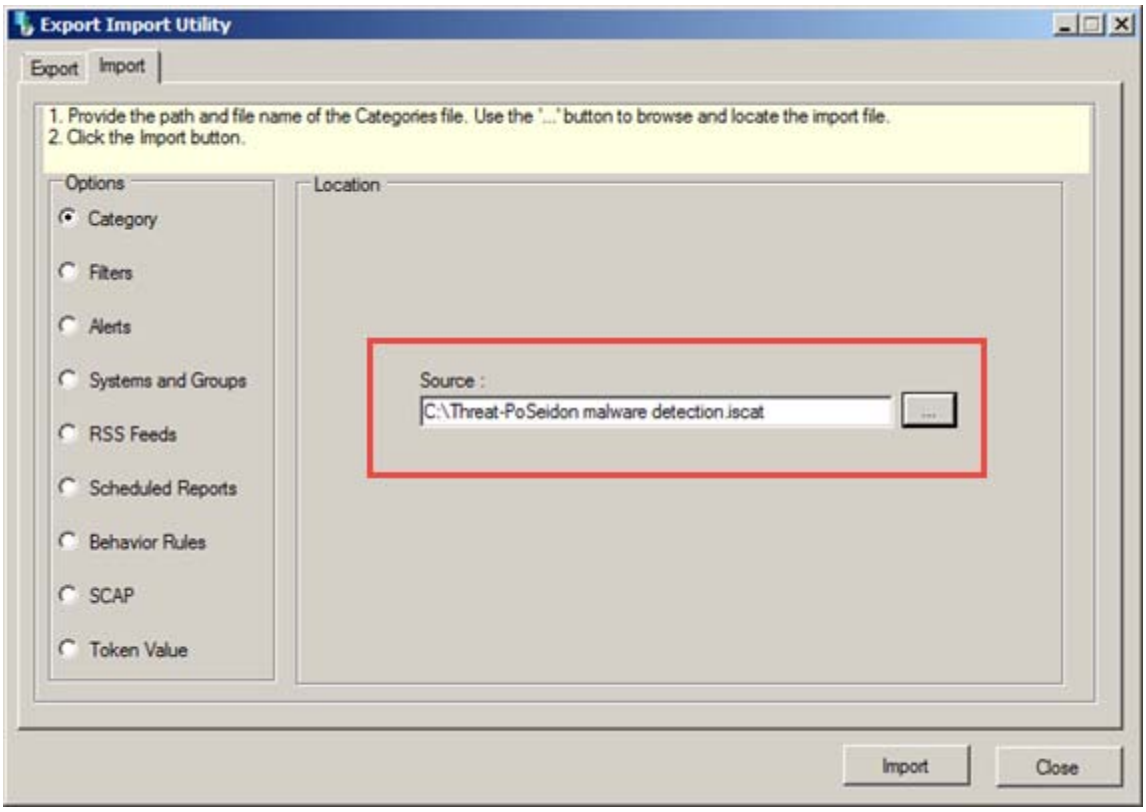

Figure 2

The categories are imported successfully.

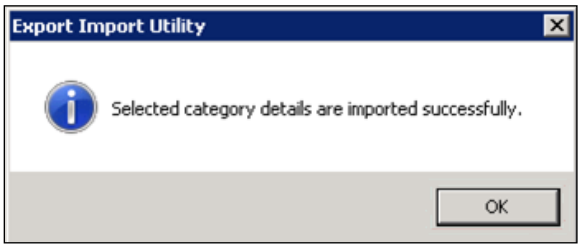

Figure 3

a. To view the categories imported, click the **Admin** menu and then click **Category**.

b. Expand **Threat Intelligence** node.

The relevant categories are displayed.

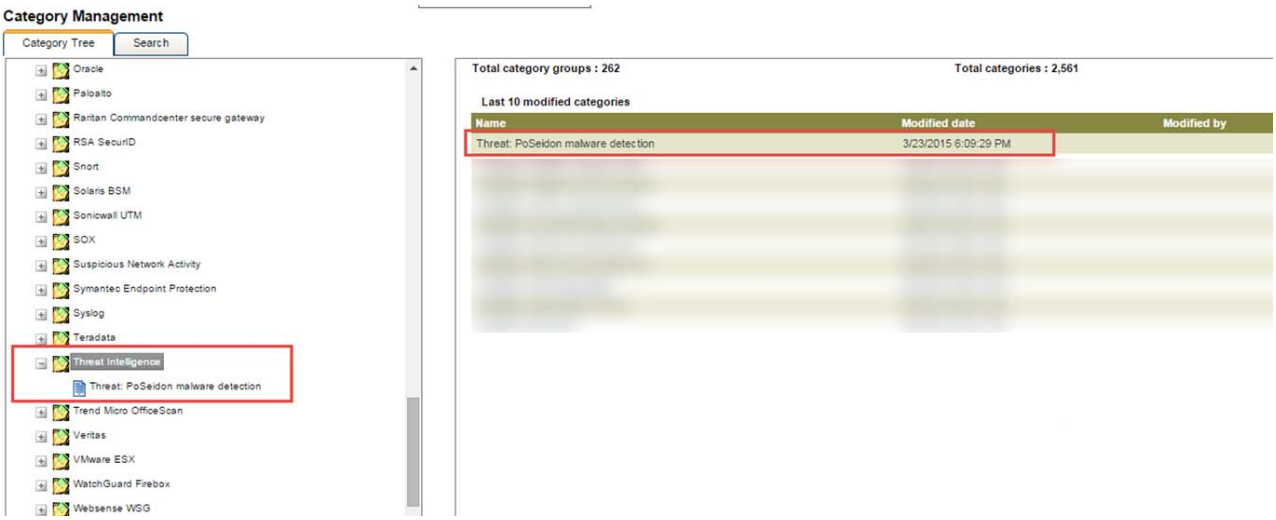

Figure 4

4. You can do a Log Search to detect PoSeidon Malware threats.

   a. To do a Log Search, click the **Search** menu**.**

      Log search window displays.

   b. Expand **all categories** node, expand **Threat Intelligence** node and then select the relevant category**.**

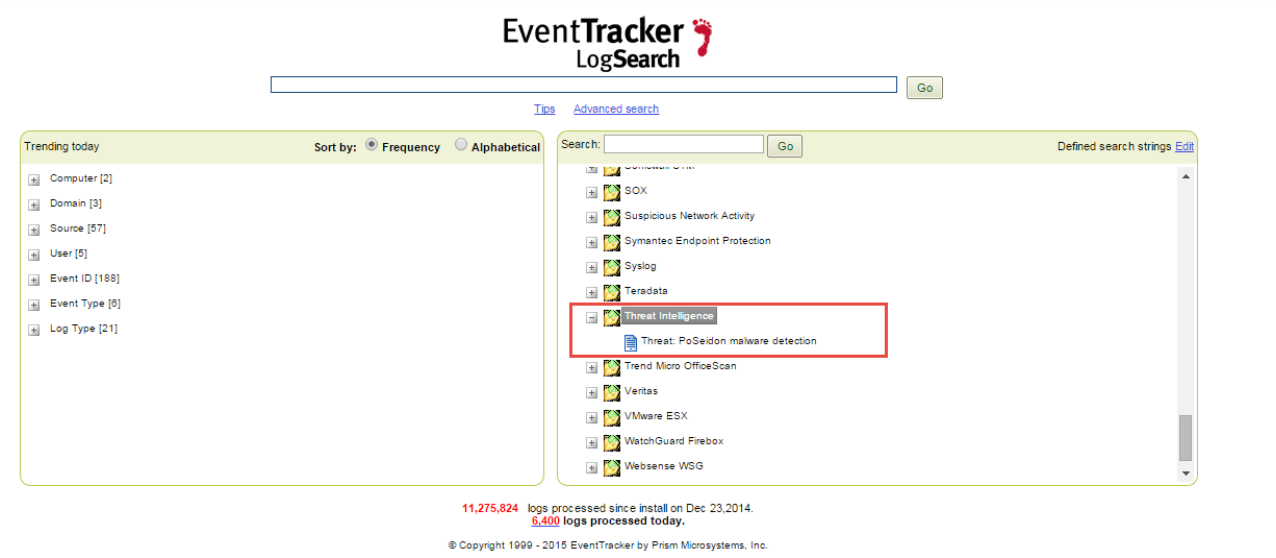

Figure 5

   c. Click the **Go** button**.**

5. You can add category in Security Dashboard to Threat-PoSeidon malware.

   a. Logon to EventTracker Enterprise.

   b. Select the **Dashboard** menu and then select **Security**.

   c. To configure Security Dashboard, select **Security** drop down, and then select **Configure**.

      Configure Dashlets window displays.

   d. Enter **Title** of the Dashlets.

   e. Select **Category** tab and **Search for** the category **Threat-PoSeidon malware detection**.

   f. Click the **Configure** button.

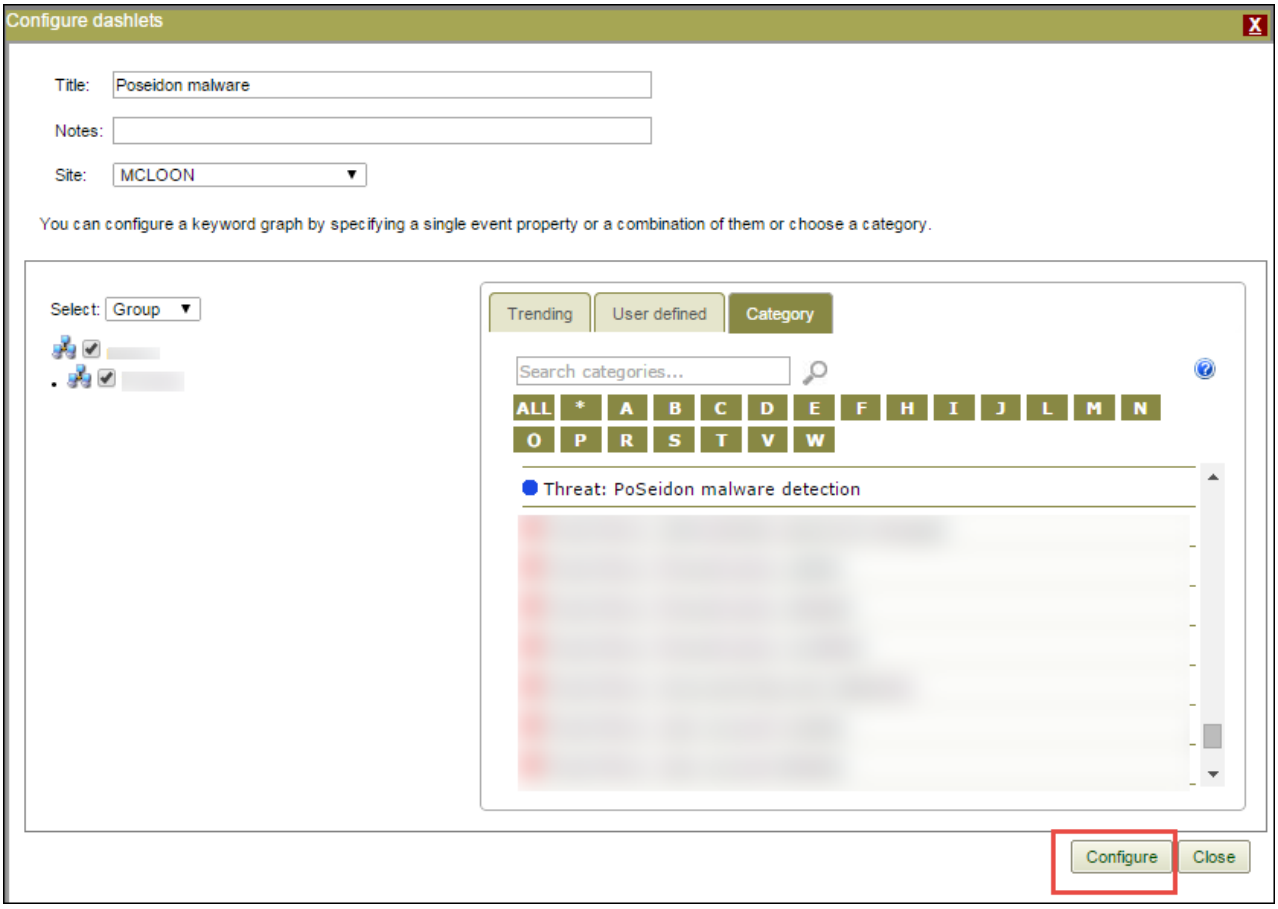

Figure 6

   g. Select **Security** drop down and then select **Customize**.

Available Dashlets window displays.

h. Select **PoSeidon Malware** option and then select the **Add** button.

The respective details display in Security Dashlets.

Import Alert

1. To import the alert file into EventTracker using Export Import Utility. Please follow the steps given below.

   a. Launch **EventTracker Control Panel**.

   b. Double click **Import Export Utility**, and then click the **Import** tab.

   c. To import Alert, click **Alert** option, and then click the **browse** ... button.

   d. Locate the file **Threat-PoSeidon malware detection.isalt** and then click the **Open** button.

   e. Click the **Import** button to import the alerts.

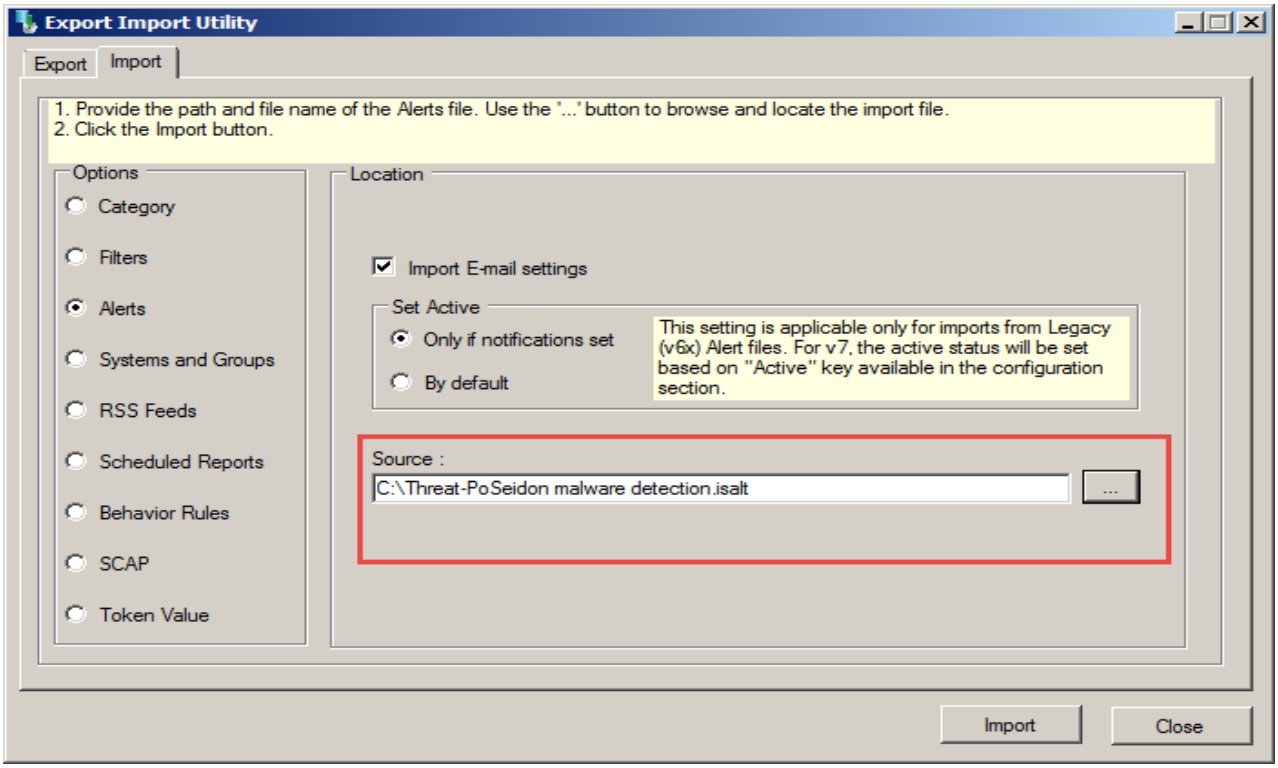

Figure 7

The alerts are imported successfully.

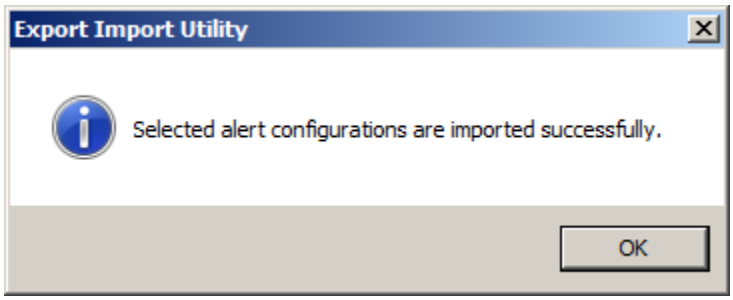

Figure 8

c. To configure the alerts imported, click the **Admin** menu and then click **Alerts**.

d. Type **Threat-PoSeidon malware detection.isalt** on the search space.

e. Click on **Go**.

The relevant Alerts are displayed.

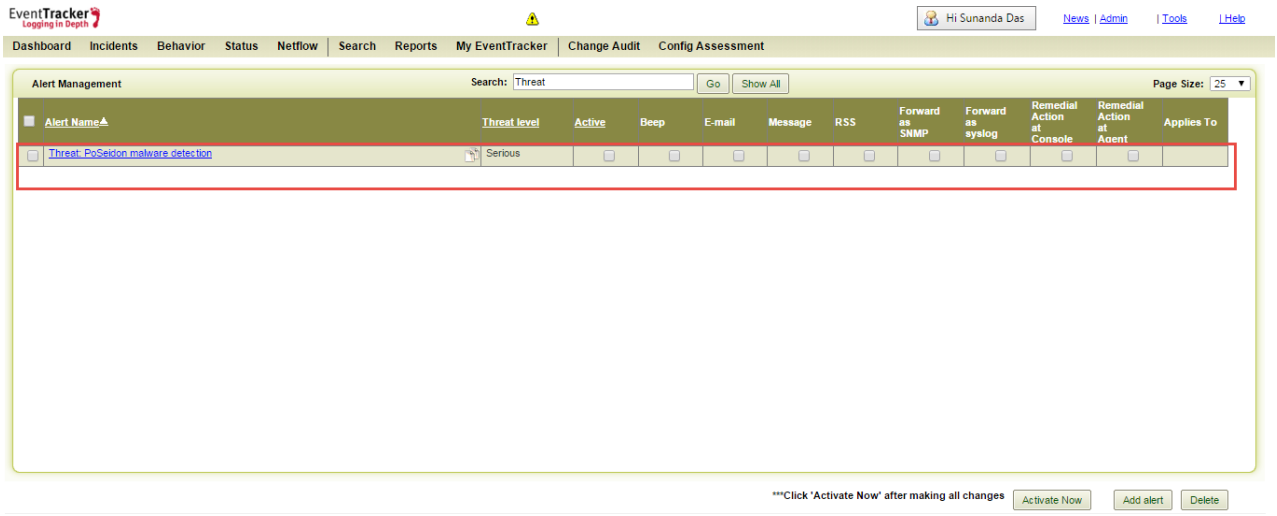

Figure 9

2. Select the **Active** check box and click the **Activate Now** button.
3. If any log matches the **Threat-PoSeidon malware detection.isalt** rule**,** it will be displayed in the Incident Dashboard.

Preventing connections to external servers IP addresses used by PoSeidon malware

As it is known that once PoS systems are infected by PoSeidon malware it tries to connect to linturefa.com,xablopefgr.com,tabidzuwek.com,lacdileftre.ru,tabidzuwek.com,xablopefgr.com,lacdileftre.ru,weksrubaz.ru,linturefa.ru,mifastubiv.ru,xablopefgr.ru,tabidzuwek.ru domains or 151.236.11.167,185.13.32.132,185.13.32.48,31.184.192.196,91.220.131.116,91.220.131.87 IP Addresses.

IT Security or Network Administrators can block connections to above ip addresses in central Gateway firewall or router, if used.

Support

Customers in the USA and Canada can receive support by calling Prism Microsystems at 877-333-1433.

International customers can receive support by calling at +1-410-953-6776.

All customers can get updates at http://www.eventtracker.com or contact Technical Support via e-mail at support@eventtracker.com.