Safeguard your devices against ransomware with **Log360**

ManageEngine
Log360

Safeguard your devices against ransomware with Log360

Network attack mechanisms continue to evolve on a daily basis. Of the network attacks that aim to steal or compromise data in some way, ransomware attacks have gained significance in recent times. An attacker uses ransomware to take your data "hostage" by encrypting it, then demands payment as ransom for the return of your data. A breakdown of the typical ransomware process is illustrated below:

Attacker emails malware attachment to intended victims

Victim clicks on the attachment

Malware launches, encrypts all files on victim's computer

Attacker controls system, delivers ransom note

Malware spreads to other computers on the network

The role of SIEM in ransomware attacks

In order to properly implement and utilize security information and event management (SIEM) as a defense against ransomware, you must first understand how ransomware operates. Ransomware attacks advance through several steps as they're executed, including:

- Installing services
- Creating processes
- Modifying registry keys
- Creating or renaming files

On their own, each of these steps is a basic system action, which means that they're recorded in system logs. Since it is nearly impossible to manually audit all of your system logs, automating the process with a SIEM tool is ideal. When it comes to auditing logs for threat detection and instantly notifying you of threats, Log360 is the perfect choice for the job. You can use some of its powerful features to do the following:

- Centrally audit all your systems, and view an array of predefined reports on the tell-tale signs of ransomware mentioned above.
- Receive notifications instantly when a potential ransomware indicator has been identified.
- Audit vulnerability scanner logs and generate reports on all the exploitable weak points in your network.
- Trace the starting point of a ransomware attack with the log forensics module.
- Launch automatic remediation scripts to prevent the spread of a ransomware attack.
- Track the status of all raised incidents in the incident management module.

SIEM in action: Fighting WannaCry

In May 2017, the WannaCry attack shook the world with it's unprecedented assault on global Windows systems. WannaCry is self-propagating ransomware, which spreads using the EternalBlue vulnerability found on unpatched Windows operating systems, including Windows 7, Windows Server 2008, and older systems running Windows XP. Using a few key features, Log360 can help organizations prevent, identify, and contain any ransomware attack, even a widespread, sophisticated attack like WannaCry.

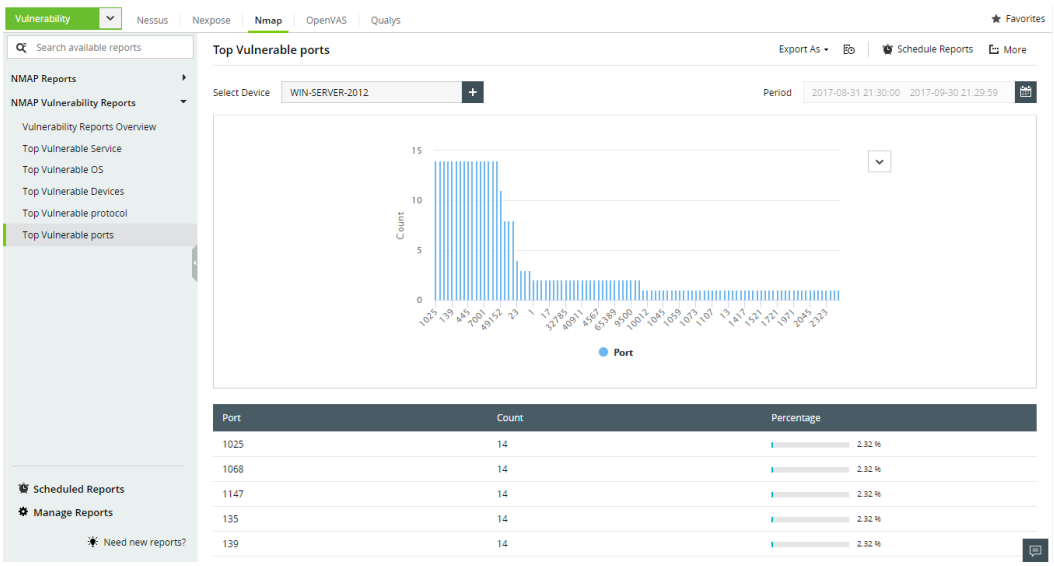
Using Log360 to handle Wannacry

At the time of writing, some of the facts known about the WannaCry ransomware are that it:

- Installs a service named **mssecsvc2.0.**
- Creates a registry key named **HKLM\SOFTWARE\WanaCrypt0r\\wd.**
- Creates some files named **tasksche.exe.**
- Creates a randomly named service which uses a background process called **tasksche.exe.**
- Renames files with the **.wncry** extension.

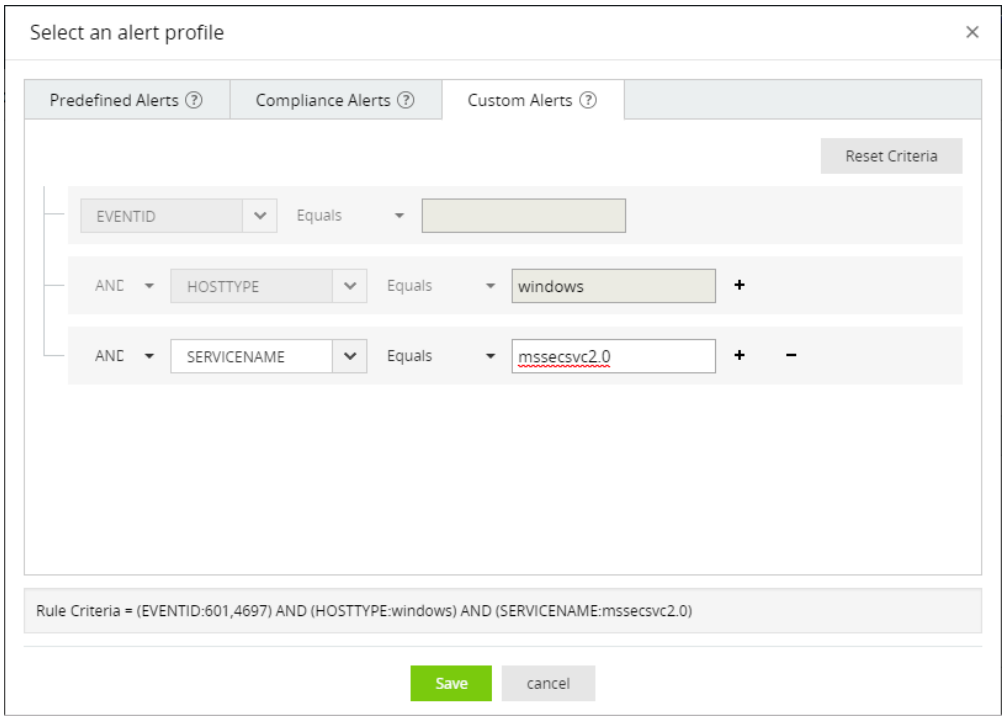
Log360 provides several avenues of approach that allow you to handle the WannaCry attack at every stage:

1. Prevention



Log360 reports and alerts on items detected by your vulnerability scanners, helping you identify your network's weak points and take steps to correct them immediately.

2. Detection



Log360's predefined and custom alerts, once established, keep you notified about various attack conditions:

Service installation alert: Configure this predefined alert with an additional criteria "Service name equals mssecsvc2.0"

.

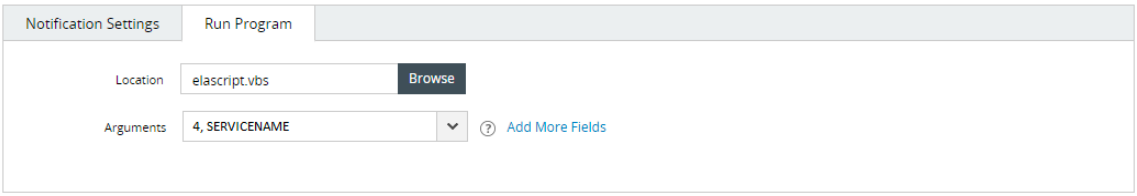
Registry key creation alert: Set up a custom alert with the following criteria: "Event ID equals 4656" and "Object Type equals key" and "Object Name equals *WanaCrypt0r*".

File creation alert: Configure this predefined alert with an additional criteria "Filename equals tasksche.exe".

Process creation alert: Set up a custom alert with the following criteria: "Event ID equals 4688" and "Process name equals tasksche.exe". You can also set up a custom alert to be notified of any activity involving this process, by providing the following criteria: "Accesses equals *" and "Process name equals tasksche.exe".

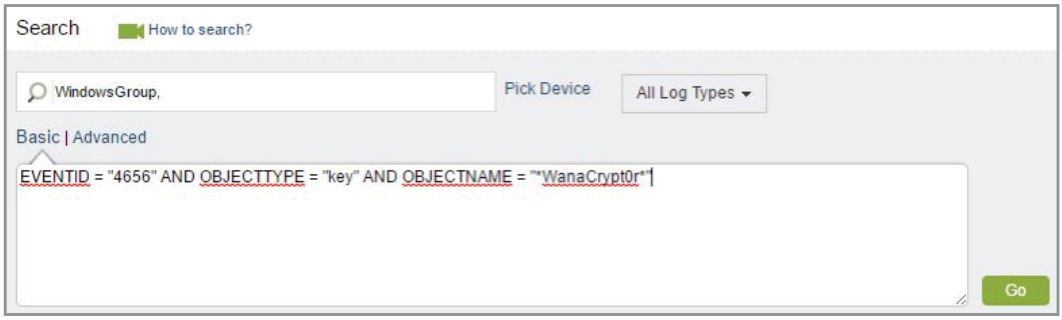
File rename alert: Configure this predefined alert with an additional criteria "Filename contains .wncry".

3. Automatic remediation



Log360 allows you to invoke custom scripts automatically whenever an alert is triggered. You can also use the built-in scripts to perform certain common tasks, including controlling when a service starts or stops. For example, when you create an alert to notify you when the "mssecsvc2.0" service is installed, use the "Run Program" option under the notification settings for the alert profile. Then, specify the location as "<Log360_Home>/tools/elascript.vbs". Pass the arguments "4" (to invoke the stop service task) and "service name" (which would be "mssecsvc2.0" in this case).

4. Forensics and incident management



If any of your systems are compromised despite these safety measures, you can always conduct an investigation into the incident by using the log forensics module, and searching the log trail to trace the root cause of the attack. To ensure accuracy, you can also review all the predefined reports pertaining to the various indicators mentioned. Furthermore, you can keep track of all forensic investigations and assign tickets for raised alerts using Log360's incident management module.

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-timeservices and support. Worldwide, more than 60,000 established and emerging enterprise-including more than 60 percent of the Fortune 500-rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.

Log360 offers the capability to correlate different events across the network to recreate and detect known attack patterns.

Log360 is a champion in Software Reviews' Customer Experience Diamond for SIEM 2019

The Customer Experience Diamond, which assesses solutions based on feature satisfaction and vendor experience, ranks Log360 ahead of all other solutions in the SIEM market.

Get the full report

Email:
log360-support@manageengine.com.

Or

Dial Toll Free:

+1 925 924 9500 (Toll Free)

+1 408 916 9393 (Direct)

Or

Visit www.manageengine.com/log360 for in-depth information about the solution and all its features.