WannaCry Ransomware

Last Updated: June 8, 2017

INTRODUCTION

A global cyberattack by the "*WannaCry*" ransomware was launched on Friday, May 12, 2017, which targeted the Microsoft Windows operating system and affected hundreds of thousands of computers worldwide.

The following scenario describes an encounter with this previously unknown malware threat in the wild, in which Cisco AMP for Endpoints observed command line argument sequences that allowed us to identify the threats based on indicators of compromise, and detect the infection once it was known to the AMP Cloud. We demonstrate how AMP for Endpoints is used to trace the attack back to the initial infection vector, and to identify the possible malware variant associated with the attack.

The Attack

The WannaCry attack involves a remote compromise through the Windows SMB (Server Message Block) service using the ETERNALBLUE exploit. Upon system compromise, the attacker drops the WannaCry ransomware variant that is initially identified using ransomware indicators of compromise, and later by AMP Cloud signatures.

Detection and Remediation

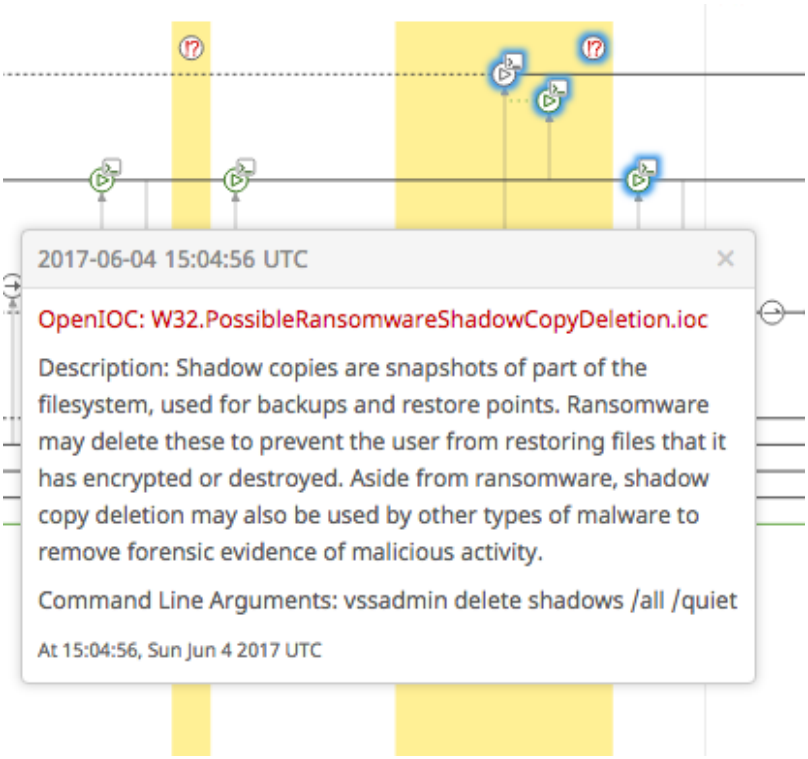
The first page you see after logging into the FireAMP Console is the Dashboard Overview. This page displays recent file and network detection events from your FireAMP Connectors. It's a convenient summary of the major trouble spots in your FireAMP deployment, which allows you to perform triage to determine which computers are in most need of immediate attention.

The **Indications of Compromise** section on the Dashboard Overview helps with triage by listing the computers with multiple events, or with separate events that correlate with certain types of infections.

In our scenario, we see the `Demo_WannaCry_Ransomware` computer with Generic IOC detections.To begin the incident response process, click the information icon next to the computer name in the list, and select **Device Trajectory**.

Tracing the Attack

Upon opening the Device Trajectory for the `W32.PossibleRansomwareShadowCopyDeletion` Generic IOC Detection, we see an Indicator of Compromise due to command line arguments being provided to the execution of `vssadmin` to delete shadow copies:

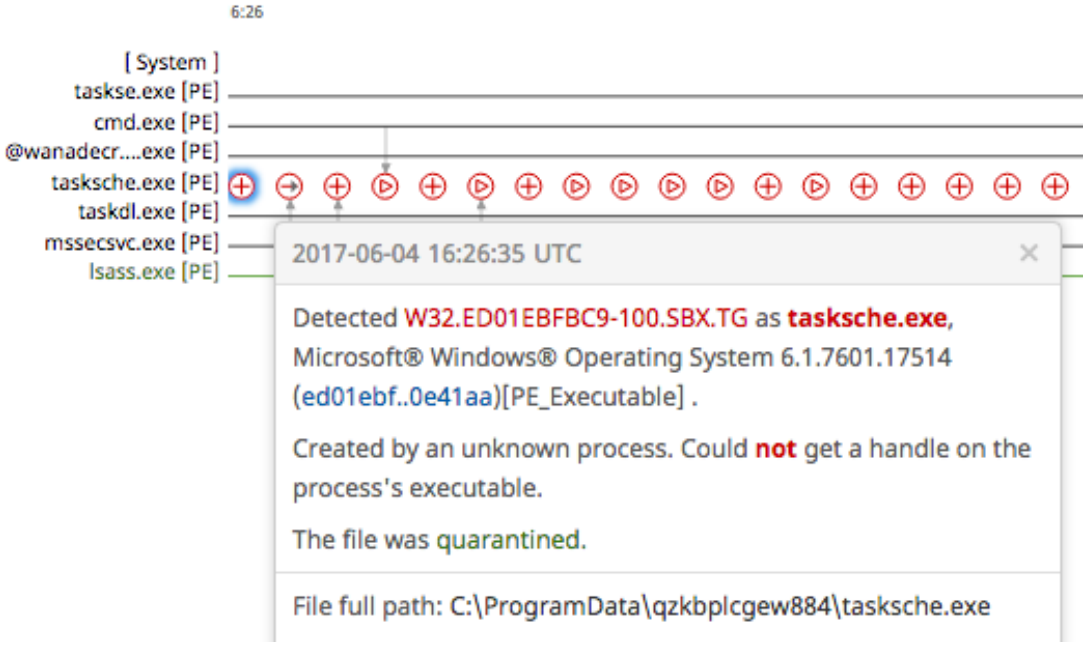


The execution event can be selected to provide further details about the pattern that triggered the detection event:

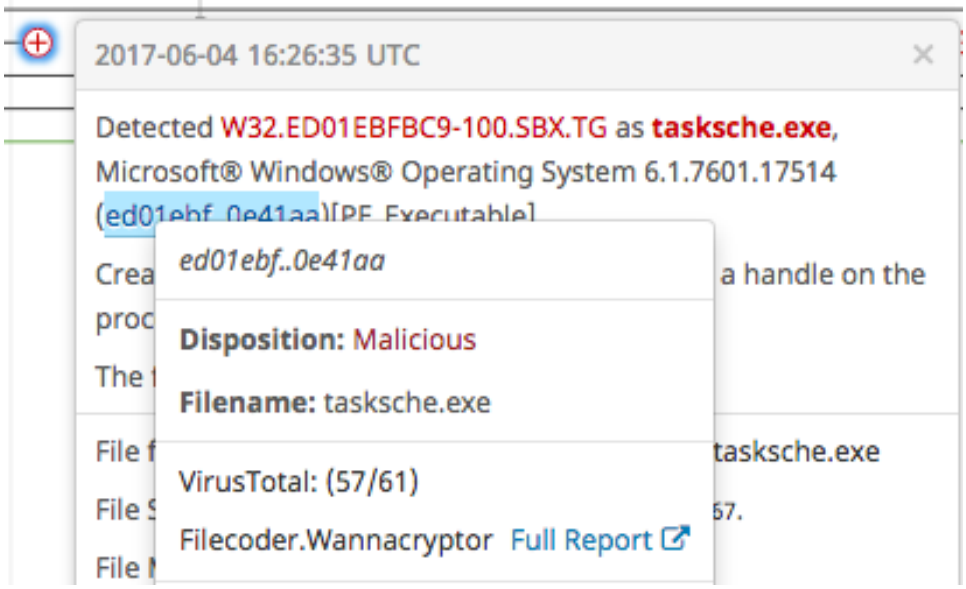
This is a common technique used by ransomware variants to prevent possible recovery of system files using shadow copy backups.

To the left of this initial IOC we see another corresponding to the BCDEdit command that was used to disable system recovery options on Windows boot:

In order to acquire more context about the compromise we look at the surrounding activity and detection events. Scrolling to the right we see detection events associated with a number of file events:

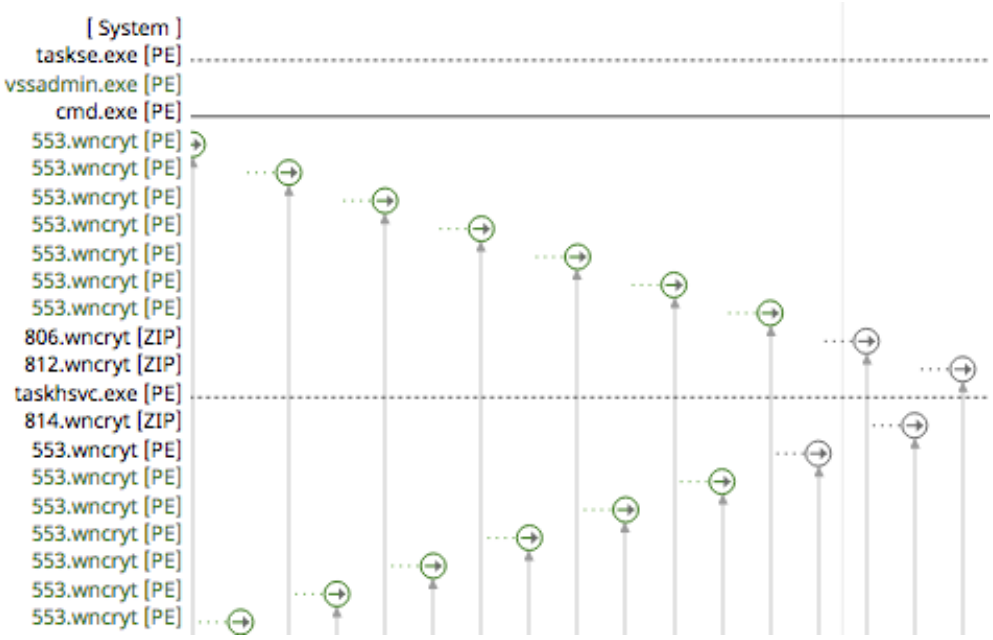


Right clicking on the SHA256 for this detection event we can acquire further information from our third party anti-virus service:

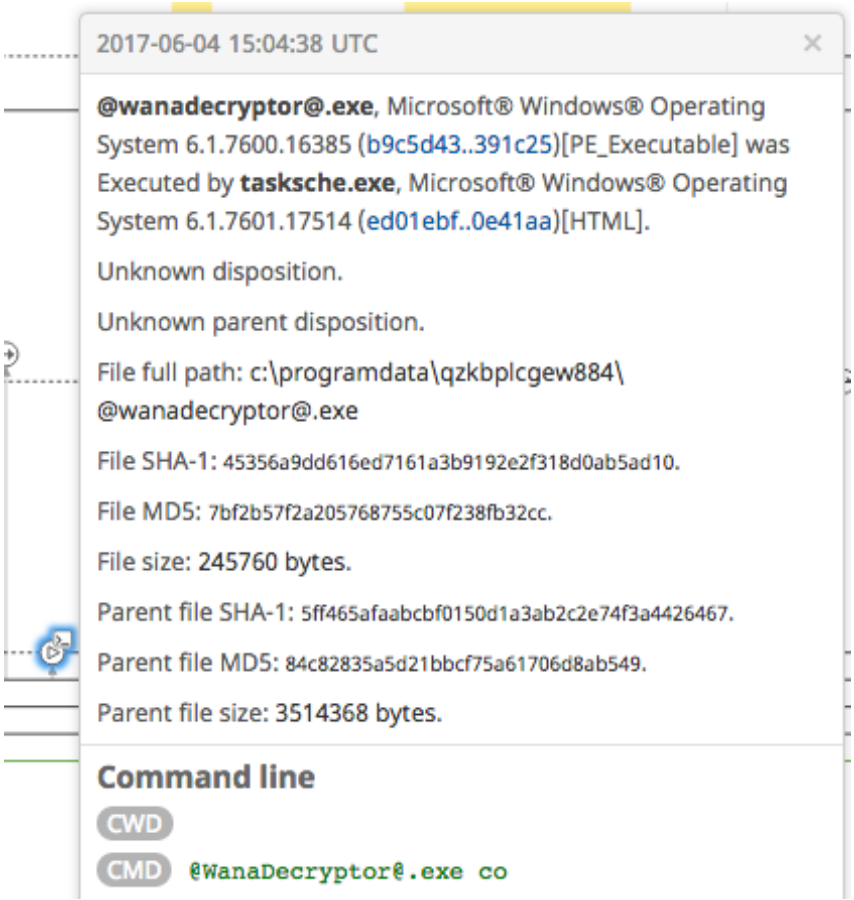


The service has an associated detection name of `Filecode.Wannacryptor`, which indicates that we are likely dealing with a WannaCry ransomware infection.

Scrolling to the left of our initially reviewed indicators of compromise we can see a number of file move events with filenames ending in the `.wncryt` extension by `taskhsvc.exe` which is the extension appended to encrypted files by WannaCry:

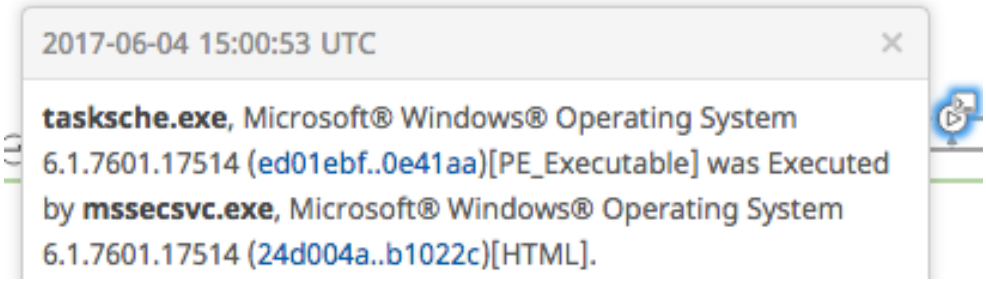


Scrolling down from this section we see our initially observed malicious process executing the `@wannadecryptor@.exe` binary:

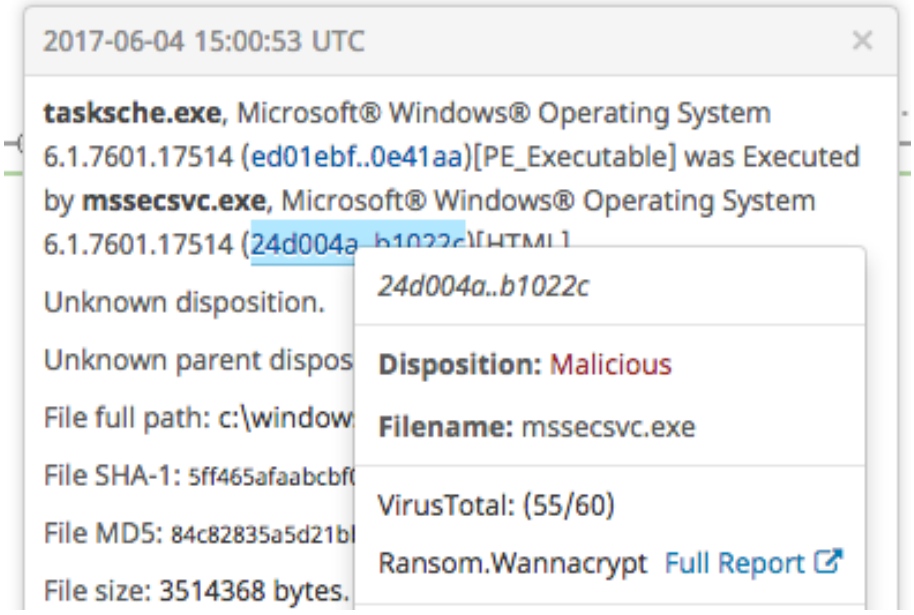


All of these events further enforce our theory that we're dealing with a WannaCry Ransomware infection.

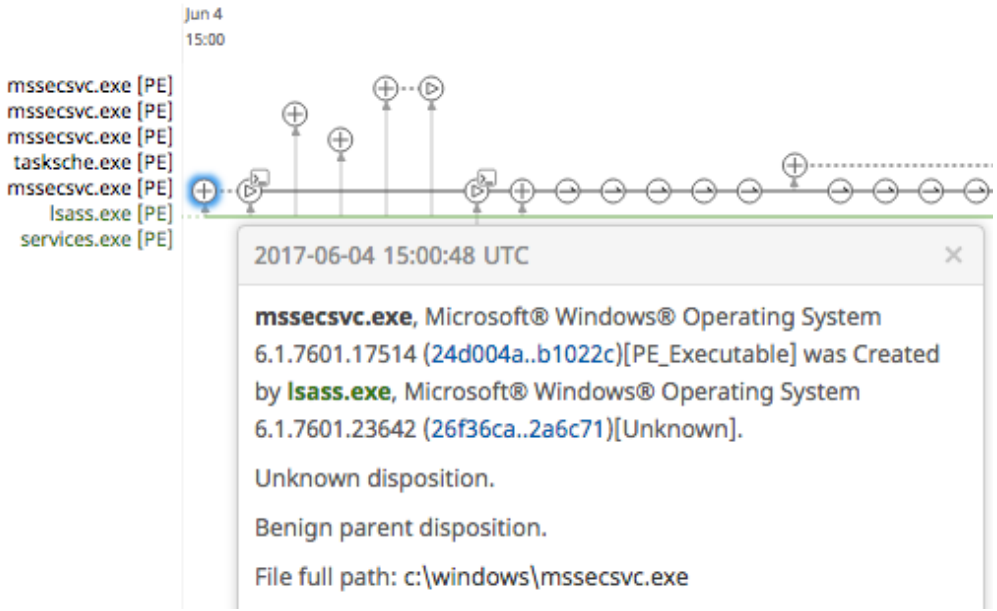
Tracing the execution of this malicious process we can see that this was executed by the `mssecsvc.exe` process:



This executable is attempting to emulate the Microsoft Security Center process, however, right clicking on the SHA256 shows us that this is yet another WannaCry Ransomware binary:



Scrolling back further we can see that this binary was dropped and executed by the `lsass.exe` process:



The exploited system driver `srv2.sys` by `ETERNALBLUE` will inject a launcher DLL into this process upon successful exploitation, which explains why we are only seeing activity from `lsass.exe` in this instance.

Summary

This scenario highlights the power of AMP for Endpoint's command line argument capture functionality, third party Virus Total integration, rapid detection capabilities of an ongoing infection, and being able to rapidly distinguish the malware family through visibility into file activity. Even though the initial detection of WannaCry was not caught, AMP for Endpoints was able to detect generic ransomware activity, and provide detection of the threat once it was known to the AMP Cloud.