

WannaCry Ransomware proactive defense Case Study



In 12th of May 2017, the highest level of Ransomware attack occurred targeting all over the world. The Ransomware used exploit called EternalBlue, a vulnerability operated by the NSA and released to the public by ShadowBrokers. Microsoft has released a security update MS17-010 in March. Unfortunately, not all operating system has patched. This document describes the major characteristics of WannaCry Ransomware, how to prevent infection, and what to do when the infection occurs.

MAJOR CHARACTERISTICS

The ransomware is a worm type and remotely executes code by SMB vulnerability by the network. If a Windows machine doesn't have MS17-010 patch, infection diffuses through the network even when user doesn't take any action.




WannaCry ransomware targets 176 extensions, of which most of the file formats include major Microsoft Office files (.ppt, .pptx, .doc, .docx, .xls, .xlsx) and many image file formats(.tiff, .jpg, .bmp, .png).

MAJOR DETECTION NAMES

Ransom.Wannacry
 Ransom.CryptXXX
 Trojan/Win32.WannaCryptor

WHY IT IS MORE SERIOUS THAN EXISTING RANSOMWARE

Most common infection route of conventional Ransomware was by spreading via phishing e-mail and visiting a website. Ransomware was distributed as a mail to encourage users to click on email attachments or hack into a web server and disguised as an advertisement, so when a user visits the website, the user PC gets infected.

Conventional distribution route		New distribution route
		
Spam Mail	Ad disguise	Network connection

However, WannaCry ransomware has characteristics of a worm, which is distributed autonomously through the network without any user action. Every Windows computer without patch is vulnerable to the infection.

KILLSWITCH ENABLED, IS NOW SAFE?

WannaCry ransomware initially distributed from 12th of May, looks for a specific domain name and stops working when the domain exists. One security expert registered a domain name by mistake, and without intention, this action stopped the WannaCry ransomware from distribution. However, since May 14th, mutation of WannaCry has been distributed without the kill-switch and spread around the globe rapidly.

ENTERPRISE CUSTOMER DEFENSE CASE

One of our enterprise level customer deployed AppCheck to more than a thousand PCs, as the conventional AntiVirus software was unable to provide firm protection against ransomware. Although some of the PCs had an indication of the infection attempt, distribution did not occur. Our customer confirmed that AppCheck detected and blocked the attempted infection, so there was no harm caused by the WannaCry Ransomware.

RansomGuard	File Created by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124b (3).JPG.WNCRYT	Removed
RansomGuard	File Destroyed by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124b (3).JPG	Recovered
RansomGuard	File Created by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124b (4).JPG.WNCRYT	Removed
RansomGuard	File Destroyed by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124b (4).JPG	Recovered
RansomGuard	File Created by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124b (5).JPG.WNCRYT	Removed
RansomGuard	File Destroyed by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124b (5).JPG	Recovered
RansomGuard	File Created by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124b.WNCRYT	Removed
RansomGuard	File Destroyed by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124b.JPG	Recovered
RansomGuard	File Created by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124c (1).JPG.WNCRYT	Removed
RansomGuard	File Destroyed by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124c (1).JPG	Recovered
RansomGuard	File Created by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124c (2).JPG.WNCRYT	Removed
RansomGuard	File Destroyed by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124c (2).JPG	Recovered
RansomGuard	File Created by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124c (3).JPG.WNCRYT	Removed
RansomGuard	File Destroyed by Ransomware	File	C:\Users\ [redacted] \Desktop\ [redacted] \A5df124c (3).JPG	Recovered
RansomGuard	Ransomware Behavior Detected	File	C:\ProgramData\qilspredrpy586\tasksche.exe	Removed

HOW CAN APPCHECK BE SO PROACTIVE?

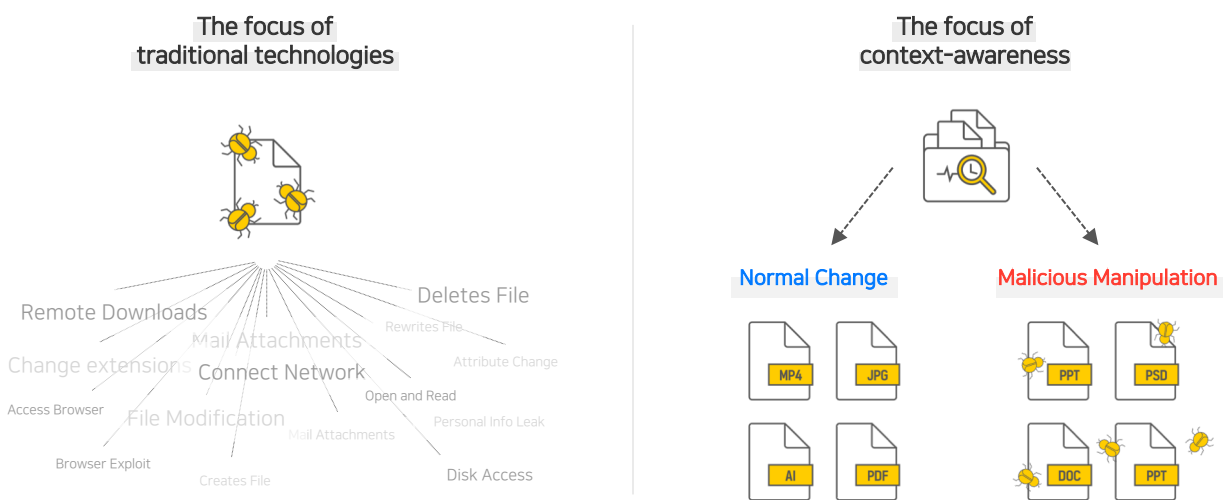
As you can see in the above log, release date of WannaCry Ransomware was 13th May in KST. First detection log was reported to CheckMAL Center at 19:48 on 12th, and this is earlier than VirusTotal's collection time for the corresponding ransomware. AppCheck was able to defend against the new distribution method of a new ransomware without conducting any update to "Context Awareness Ransomware Behavior" engine, the unique engine developed by CheckMAL.

WHY IS THE DAMAGE SUSTAINING DESPITE THE USE OF ANTIVIRUS?

It took only two days for the kill-switch removed WannaCry to be redistributed as a new format. The mutation has grown to more than 280 by the time of this writing. As shown in this case, the new mutation appears in a very short timeframe. Conventional detection method requires a sample and time for its analysis and time to update signatures for blocking ransomware. In most of the cases, ransomware developer tests the sample against the well-known antivirus software before the distribution, which makes very hard for immediate response before the actual incident. Conventional antivirus includes behavior detection methods as well. One of them is decoy type method. This method creates specific files inside the disk and detects any altering process. However, it is far insufficient when a ransomware avoids the decoy from its encryption target. Exploit detection mechanism is ineffective when ransomware is executed by the user, most likely from links generated through phishing email or website.

CONTEXT AWARENESS RANSOMWARE BEHAVIOR ENGINE?

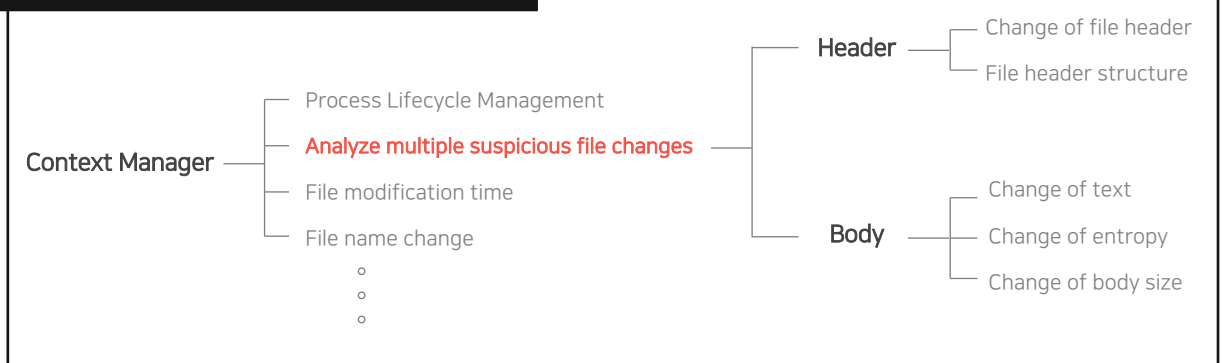
Context awareness based ransomware detection technology differentiates itself by monitoring malicious file modification behavior of the process. Conventional detection method relies on ransomware itself, such as its file properties, specific patterns to define the ransomware its uniqueness. This method requires ransomware sample to analyze and define the unique identifier, which requires updates on users PC. CARB Engine doesn't require a single signature update, completely independent from it, but focus on file changes.



Many information can be obtained at the moment of file modification, and file modification can be determined either normal or malicious by carefully monitoring them. For example, if the editor application modifies a picture file, the header should not be changed but only contents. In the case of ransomware encryption, all contents are overwritten with encrypted string. Including the case, AppCheck can determine file's modification is either malicious tampering or normally changed by the user, by monitoring the file's modification behavior.

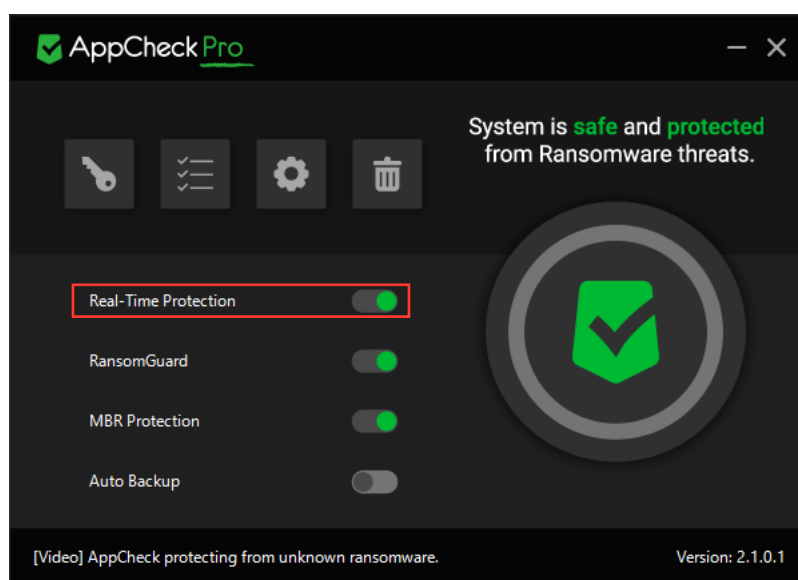
Main Concept of CARB Engine

Context Awareness Ransomware Behavior detection engine



HOW TO PREVENT RANSOMWARE?

1. Go to homepage URL and download and install AppCheck. <https://www.checkmal.com>
2. Check AppCheck version: Newest release of AppCheck is 2.0.1.8 on May 22, 2017, at the time of this writing.
3. Make sure Real-Time Protection is enabled.



4. Go to Microsoft Windows Update to update your Windows Operating system. WannaCry uses the EternalBlue exploit, and the specific patch is available at the following URL.
5. Please contact our sales through the link below to purchase for company or business use.
<https://www.checkmal.com/page/shop/distributor/index.php?lang=en>

References

APPCHECK PROTECTING WANNACRY RANSOMWARE:

<https://www.checkmal.com/page/resource/video/?detail=read&idx=416&p=1&pc=20>

NOTICE FOR WANNACRY

<https://www.checkmal.com/page/support/notice/?detail=read&idx=418&lang=en>