THE FUTURE RESPONSE STRATEGY OF RANSOMWARE

DIVERSIFYING RANSOMWARE, BEST DEFENSES?

Every day thousands of new Ransomware are distributed worldwide. This document explores the limitations of existing defense methods against the explosion of Ransomware and how to overcome them.

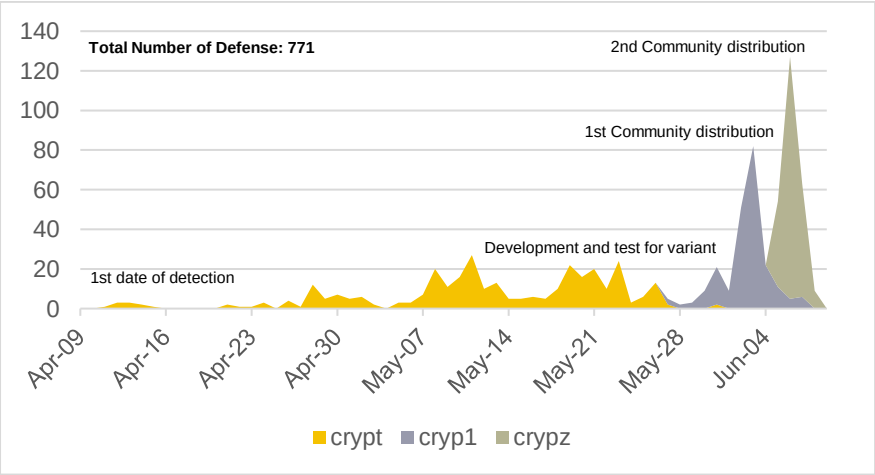
THE FUTURE RESPONSE STRATEGY OF RANSOMWARE

DIVERSIFYING RANSOMWARE, BEST DEFENSES?

THE BEST WAY?

Malicious programs that destroy PCs or data are hidden as normal programs to hide their identity as much as possible. Security software, such as antivirus, analyzes these malicious programs to extract traits and defend against further execution.

However, new and popular malicious programs, such as ransomware attacks, create another variant that looks like a normal program. In fact, in June of 2016, CryptXXX Ransomware was distributed through an advertising server serving large domestic communities. This ransomware has the characteristic of infecting just by visiting a web page, and also spreads the variant every two days and caused damage to a lot of users.



Is it only the best defense method to extract the characteristic when the malicious program emerges such as existing antivirus?

CASE STUDY #1

Large medical center K has 1,500 internal PC's with well known AV products, but reconized more than 10 ransomware attacks per month. More than 70 PCs were reported to defended by AppCheck Pro in the first month of successful deployment.

CHECKMAL

Limitations of existing detection methods:

Information that only can be known by analysis

The most widely used **signature-based** detection method is to list the characteristics of malicious code and judge it. If there is no signature of malicious code to be detected in the list that you have, you can not defend it. Generally, malicious code signatures are updated periodically, so they are more likely to be exposed to new malware until they are updated.

Existing **behavior-based** detection techniques are a method of detecting and signifying actions by "patterning" specific actions, and it is difficult to detect when new actions occur.

A **network-based** detection technique is also difficult to detect when an attacker makes an order through an encrypted network. A **decoy-based** detector method, which is a technique for generating random files and detecting them when ransomware encrypts them, this can simply bypass.

In the case of **exploit-based** detection methods that detect how to execute malicious code using weaknesses of commonly used programs, phishing methods which induce the user to execute them are not detectable, and only the registered normal programs are executed **Access Control List (ACL) -based** defense techniques are less effective in practical work environments because it is difficult to manage newly registered programs and updated normal programs.

In particular, ransomware frequently uses new techniques that are not detected by security products. Indeed, what is the best strategy to defend against Ransomware?

CASE STUDY #2

An Enterprise company held benchmark testing for ransomware defense performance. Only AppCheck performed 100% detection among the well-known Antivirus and Anti-APT solutions within the given environment.

CheckMAL signed a contract with the company to supply 3,000 AppCheck Pro licenses.

CHECKMAL

Next Generation Ransomware Defense Strategy: Context Awareness based Ransomware Behavior Detection Technology

Ransomware, where new variants appear every now and then, is always the same eventually, encrypt the file so that the user can not access it.

Context Awareness based Ransomware Behavior detection technology is a technique to detect the encryption of a user's file to prevent it from being used. It does not focus the ransomware characteristics like existing security products, but comprehensively judges the situation of modifying the actual user's files. This also enables accurate detection without any signature updates for the new behavior of ransomware.

- Signature and Behavior-based Detection. In the case of ransomware detouring the detection, the context-awareness detection technique is able to defend with pure behavior without signatures since it continuously monitors before and after the file is changed.

- Ransomware bypassing Network-based detection are also detected because it detects actual behavior at the end-point.

- In case of bypassing decoy-based detection technique and even ransomware is accidentally executed by mistake, it can detect the file tampering action by monitoring files in real-time.

If the blocking fails, an alternative to restore the user's files should be presented.

In other words, if Ransomware's ultimate goal of "file corruption" can be thoroughly monitored, both efficiency and effectiveness of the system can be improved

CASE STUDY #3

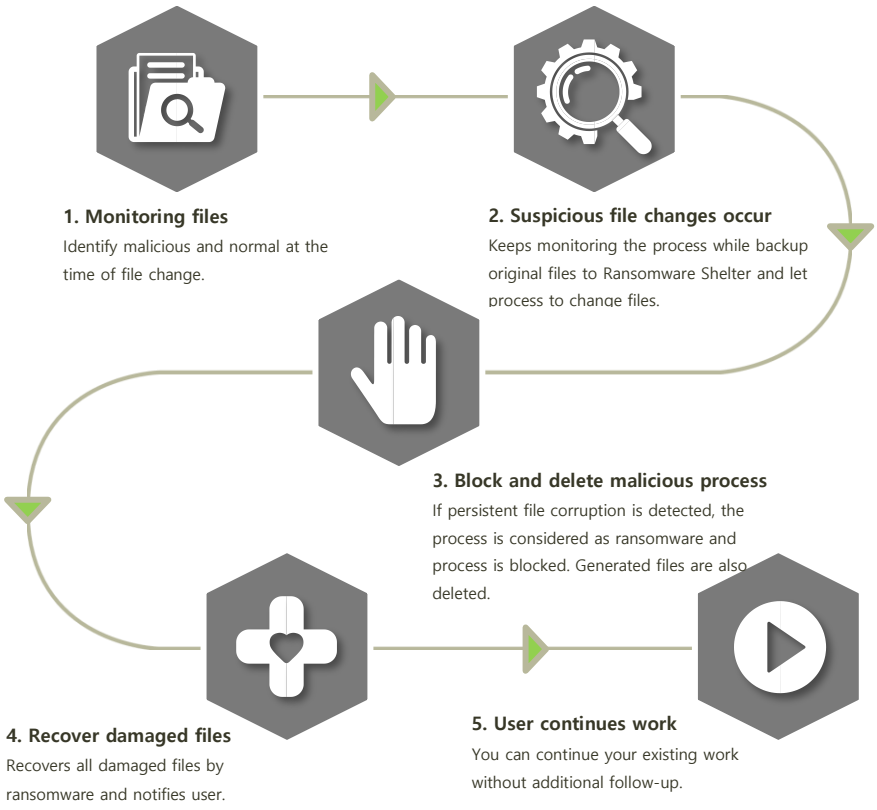
Recently, a public agency have introduced more than 500 Context-awareness based anti-ransomware, AppCheck Pro, in order to defend ransomware occurs frequently in Korea.

CHECKMAL

Ransomware compliant solution: AppCheck Pro

CheckMAL's AppCheck Pro is a faithful product to defend ransomware that monitors and defends mainly the last action of ransomware through its own context awareness algorithm.

The CARB engine, developed by CheckMAL, is a key technology for judging the situation at the time of file modification without any signature or pattern. By monitoring the change of the file in real-time, accurate detection and recovery are possible.



This unique feature differentiates from conventional security software, that is not affected by the detection rate even in an environment where the Internet is unavailable. Since it can judge the damage of the file by itself, this puts unique position while most other analysis system is replying to cloud assisted method.

CHOICE OF 15 MILLION USERS

Context awareness based engine running in a kernel environment must ensure speed, stability, and compatibility.

With more than 150,000 users, AppCheck Pro is a proven solution for ransomware detection in a variety of user environments.

CHECKMAL