Best Practical Response against Ransomware

AhnLab MDS: Holistic Response on Both Networks and Endpoints

2016. 02. 09

AhnLab

Table of Contents

Copyright (C) AhnLab, Inc. All rights reserved.

Overview

Recent news articles are increasingly reporting hostage situations–these are the new cybercrime, “ransomware”. Indeed, there has been a sharp increase in ransomware and new ransomware and their variants continue to surface, causing damages not only to companies, but also to individual users since attackers who seek financial gain deploy ransomware indiscriminately.

It has only been in the past 1-2 years that ransomware attacks that encrypt important files and demand ransom payment have been reported and made known to the public. In terms of the history of malware, however, Trojan horses that ‘encrypt files’ have steadily persisted for some time. Demanding payment is also a progression from scareware, malicious software that poses as a legitimate antivirus program for financial gain, such as fake antiviruses or as a screen-locking virus. All of these viruses share another common characteristic: they expose their purpose of attack clearly. That is, ransomware is not a totally new malware but malware that has combined with the functions of existing malware. However, seeing as there is no way to restore encrypted files without paying a ransom, ransomware is particularly heinous in that greatly frustrates individual users and organizations.

Today, ransomware is propagating under various names based on attack method and specific actions such as Teslacyrpt, Cryptowall and Teerac. Ransomware is a type of malware that encrypts your important files such as documents and images, making them inaccessible. The attackers then demand a ransom to unlock the files.

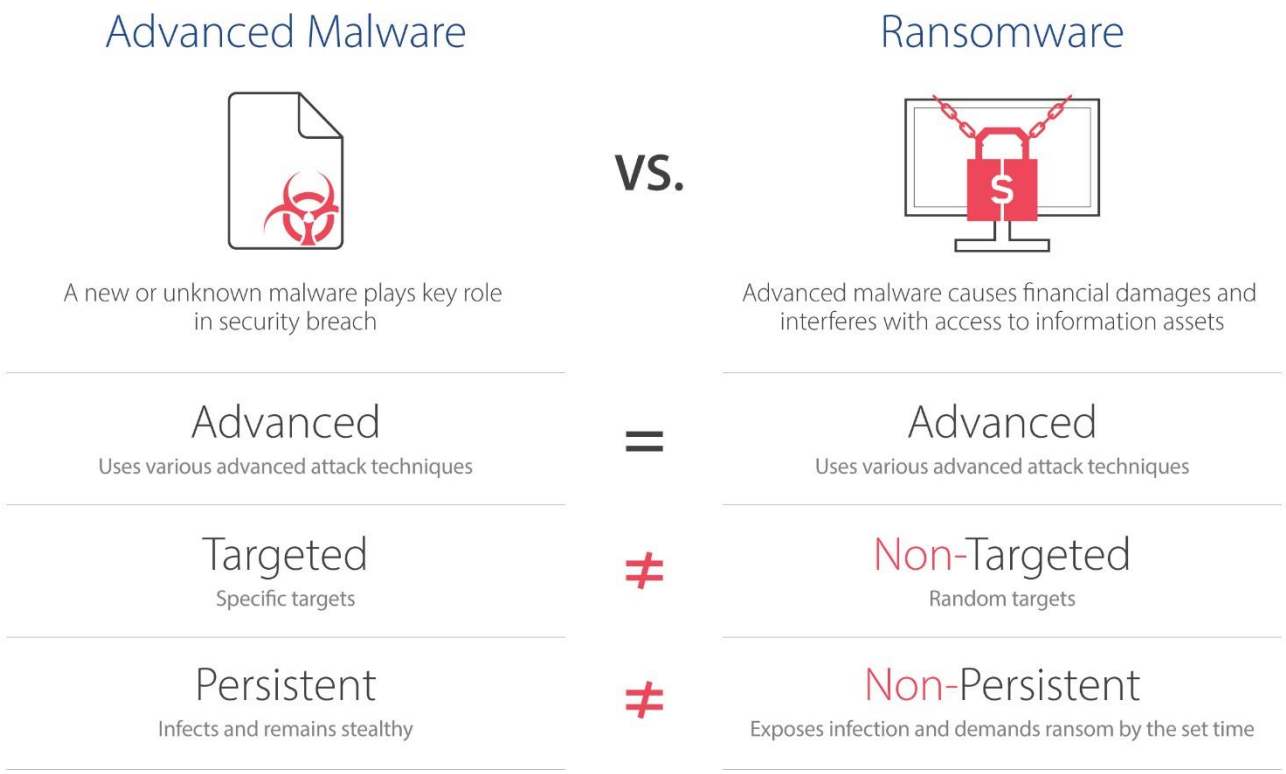
This report presents the latest ransomware trends and best practices for ransomware response using the AhnLab MDS (Malware Defense System).

Copyright (C) AhnLab, Inc. All rights reserved.

Ransomware and Advanced Malware: Different, Yet Similar

Security solutions for endpoints such as the latest AV programs respond to ransomware that can cause severe damage based on behavior-based detection or vulnerability exploit protection. However, attackers are also constantly finding ways to bypass the ever-developing security protection technology. As a result, various new ransomware and variants continually engage in cyber robbery, taking 'file encryptions' as hostage. The reason why sophisticated endpoint security solutions fail to respond to the ever-evolving ransomware is because the malware employs various techniques used in advanced threat attacks to bypass various security solutions.

However, unlike other advanced malware, ransomware is sent to unspecified masses in quantities that are as large as possible. 'Advanced malware' hides itself for as long as possible without becoming detected, whereas ransomware exposes itself immediately after encrypting important files to demand a ransom by a set time. To prevent being exposed during the attack and payment process, attackers use a network, such as HTTPS encrypted traffic or Tor, and use bitcoin for ransom payment.



[Figure 1] Advanced Malware vs. Ransomware

Copyright (C) AhnLab, Inc. All rights reserved.

Are Patches and Backups the Only Solutions?

The latest ransomware attacks tend to use new malware and their variants to bypass antivirus programs. Since it is basically impossible to preemptively prevent and block ransomware, we can only establish a passive response strategy to minimize damages. Unfortunately, some security vendors have misled customers into thinking that their security solutions, such as AV programs, can prevent ransomware. However, all security vendors emphasize two basic security measures in order to prevent ransomware attacks: backing up important files and applying the latest security patches.

[Figure 2] General Ransomware Response Process

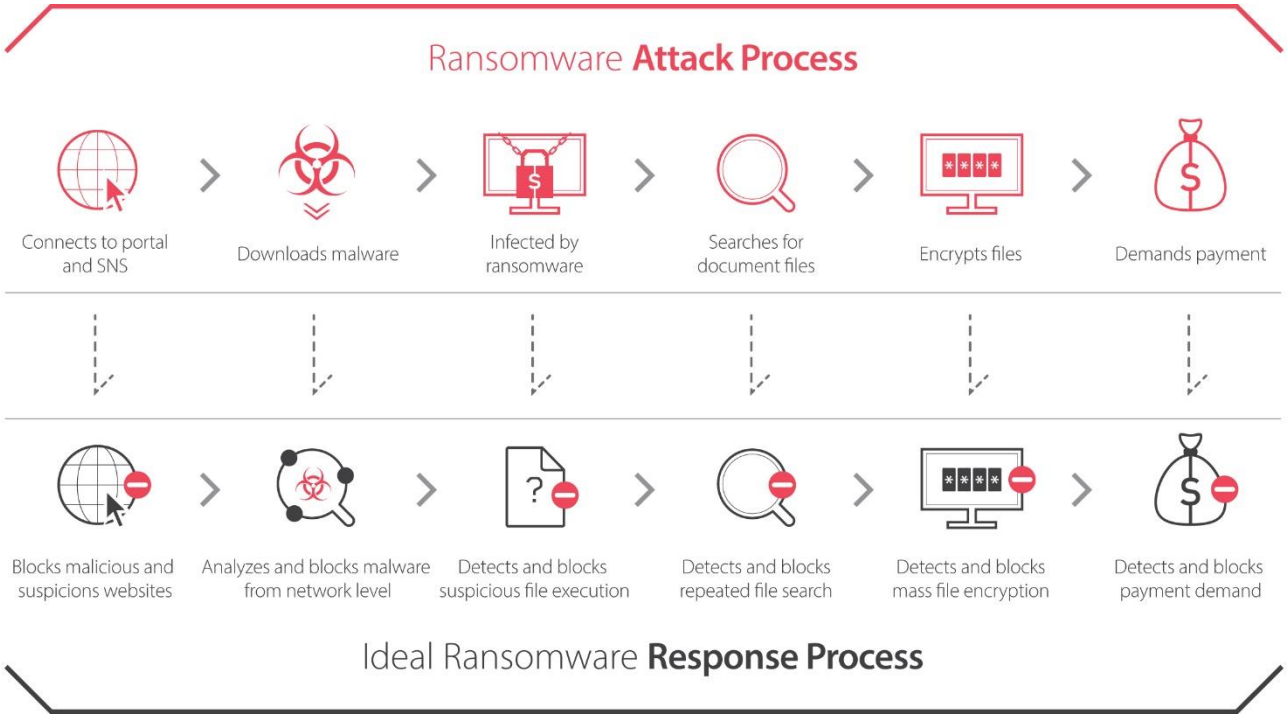
In other words, if you can effectively apply the latest patch on a regular basis, you may at least prevent infection—a pre-response. Even if your computer is infected by ransomware, you can minimize the damages by restoring the backed up file—a post-response. Nevertheless, never be assured that the situation is over just because you restore the encrypted files. Attackers will not just continue to wait for your payment, nor will they simply send the decryption key to victims that make the payment. Once your computer is infected by ransomware, your computer will be recognized as an easy target or as a security hole to infiltrate the entire organization for further attacks.

Copyright (C) AhnLab, Inc. All rights reserved.

Ideal vs. Practical Real-time Ransomware Responses

Apart from making sure people observe security practices such as backups, patches, AV updates and in general just exercising caution, are there no technical means an IT manager can use to control ransomware attacks? Are there any ways to minimize the attacks in terms of real-time response? Let's take a look at whether a real-time response can be a practical approach.

First, let's look into the perfect real-time technical response for ransomware. Ransomware is often spread via email attachments or URL links in email messages, or it can also be deployed by malicious websites that you are redirected to in various ways. At this point, you need technology that blocks suspicious email attachments or suspicious URLs. If not, the malware will break into your network. Now you need technology that uses a sandbox to detect malware at the network level. Then, when the ransomware infects the endpoint system, suspicious behavior occurs at the OS level. A 'perfect' security solution would detect file searching and diagnose behavior, such as mass file encryption, as malicious. It would then automatically detect and block suspicious behavior in real-time.



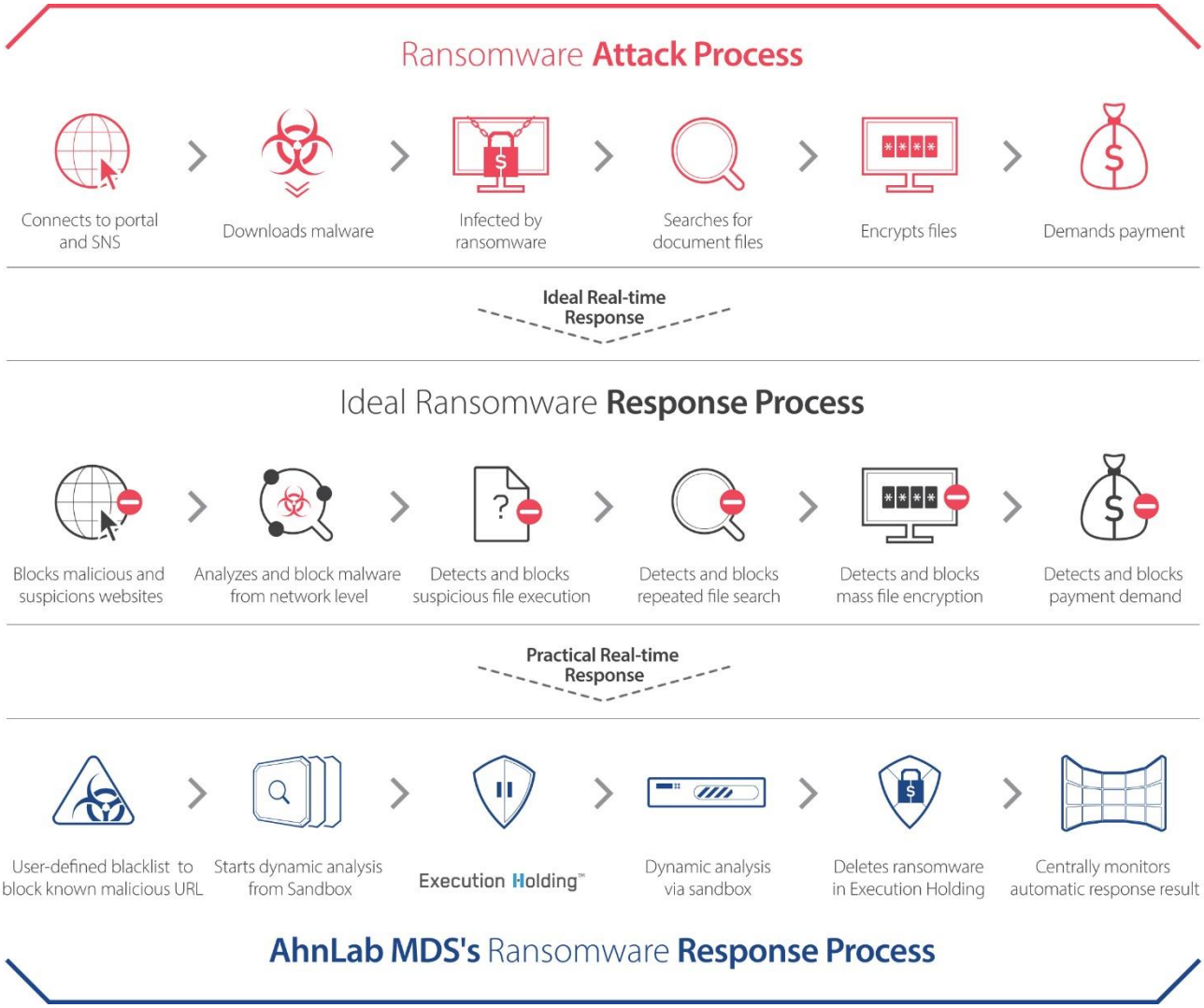
[Figure 3] Perfect Ransomware Prevention Process

Unfortunately, there are still no perfect security solutions that can ideally respond to ransomware in real-time as described above. That is, there are no security solutions that can analyze suspicious URLs or files in real-time and block them at the network level. Also, there are no technological solutions that accurately detect and block suspicious ransomware behavior, such as file searching and encryption at the endpoint level in real-time.

Copyright (C) AhnLab, Inc. All rights reserved.

Even though these technologies are implemented in security products, it may create too many false-positives that are impossible for internal IT security functions to handle.

Though not perfect, if a security solution can block suspicious URLs in real-time, analyze suspicious ransomware files and URLs in a virtual environment before the ransomware file is executed, and let the user decide whether to execute the file according to the results, this would be the best practice for a response process that IT managers could consider to deploy in the organization.

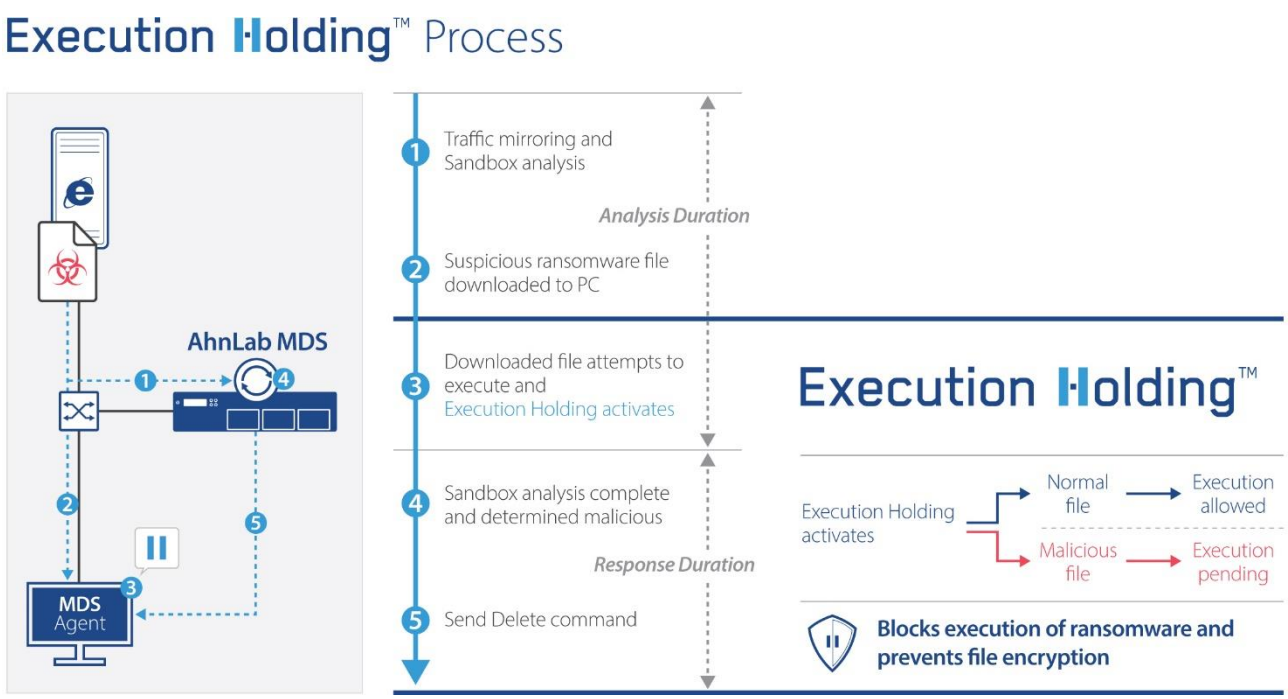


[Figure 4] Perfect vs. Practical Response

Copyright (C) AhnLab, Inc. All rights reserved.

Applicable to all Advanced Threat Response Solutions?

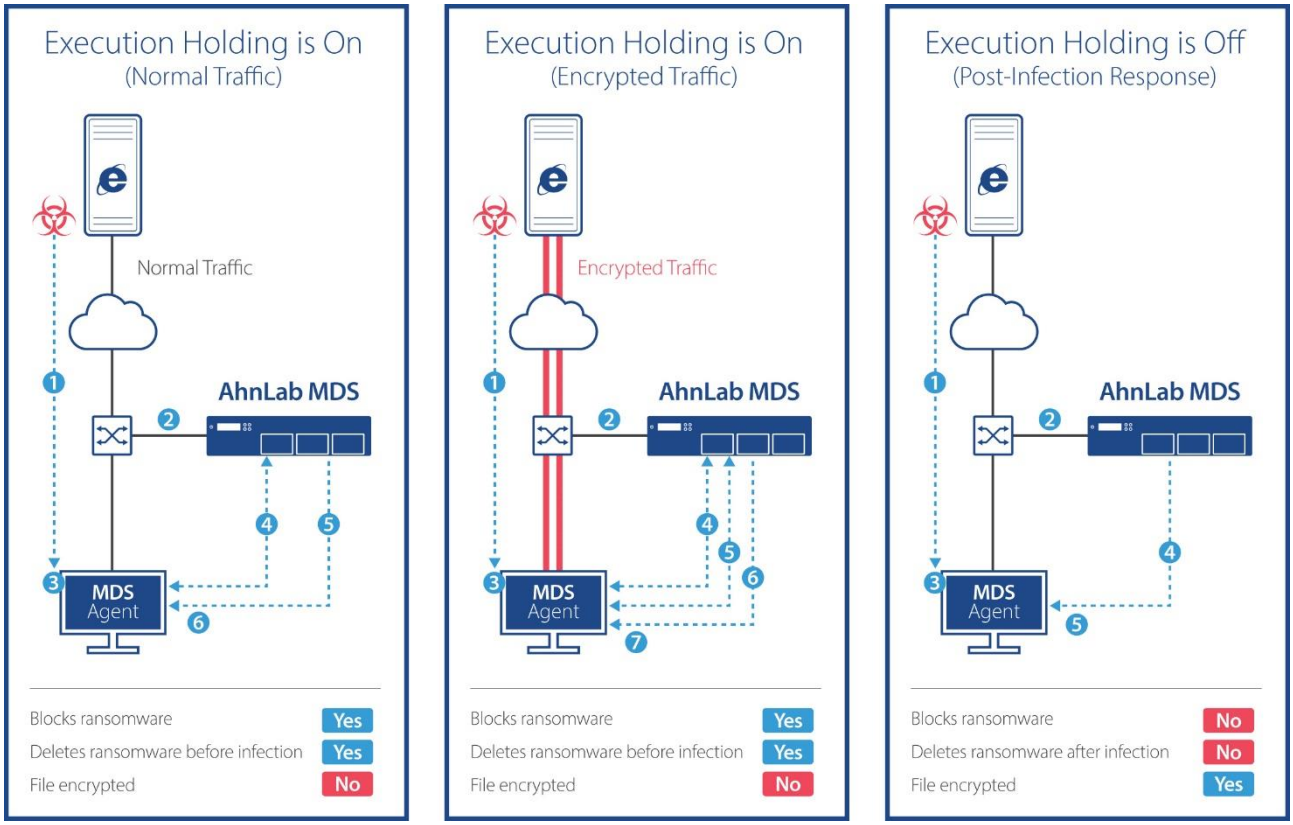
It is a fallacy to think that the practical real-time response process mentioned above can be implemented in all advanced threat protection solutions that use a sandbox. AhnLab MDS has provided the first-ever agent among the sandbox-based advanced threat protection solutions, which was designed at the very initial product planning stage, recognizing the necessity of real-time action at the endpoint level. Furthermore, since 2013, the Execution Holding feature has been provided through an MDS agent to not only detect unknown threats, but to also automatically block these threats, reflecting APT response cases and the evolving security threat trend.



[Figure 5] AhnLab MDS Execution Holding Feature

The sophisticated ransomware malware functions are subdivided and modularized to bypass sandbox-based security products at the network level, and encrypted communication is also used to bypass network security solutions. Expensive security solutions, such as SSL proxy or decryption devices, can be additionally deployed to existing security products. However, if a non-standard encrypted protocol that does not follow the standard SLL certification is used, encrypted traffic cannot be decrypted. AhnLab MDS Execution Holding feature works when traffic has been decrypted and files have been recombined at the endpoint level, so it works effectively in the encrypted traffic environment without restrictions.

Copyright (C) AhnLab, Inc. All rights reserved.



[Figure 6] AhnLab MDS Execution Holding Process for Encrypted Traffic

Conclusion: Finding the Broken Window

Sandbox-based advanced threat protection solutions are not security solutions planned and developed to detect, analyze and respond to specific malware, such as ransomware. In other words, it cannot respond 100 percent effectively to evolving ransomware, and this would be the same even for other solutions developed with new concepts.

If the victim of ransomware is not an individual user, but an organization, the organization may be deemed to be poor in managing patches and vulnerabilities or actualizing Internet/email security policies. There is a high possibility of the organization being targeted again. The Broken Window Theory can be applied to cyber crime – if a window is broken and left unrepaired, people will think no one cares and no one is in charge; thus, the crime rate in the neighborhood will be higher. Victims of ransomware attacks may be targeted with more sophisticated attacks. What is important now is to carefully consider and select the best way to provide a maximum security effect from within the currently feasible technological boundaries.

Copyright (C) AhnLab, Inc. All rights reserved.

AhnLab

AhnLab Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do,463-400, Korea
www.ahnlab.com
©2014 AhnLab,Inc. All rights reserved.