AhnLab

White Paper

How to Build an Effective Ransomware Defense Strategy

Overview

Ransomware is probably one thing that every business is concerned with regardless of size or industry. It is because ransomware attacks have become quite prevalent in recent years, with new and more advanced ones emerging almost daily.

Ransomware attackers do not discriminate against their targets. Both consumers and businesses can become victims of ransomware. They target various organizations, hospitals, public institutions, manufacturing facilities, financial institutions, and end-users to reap the highest financial gain.

Since the range of targets for ransomware is wide, there is no single, best ransomware defense strategy for all. Thus, businesses are struggling with developing an effective defense strategy that is apt for their business. AhnLab provides a comprehensive guide on implementing the most effective and proactive ransomware response system for each individual business.

Ransomware Attack Methods

Before discussing specific response measures, we will go over some of the most common ransomware attack methods.

The three most common types of ransomware attacks are file, fileless, and BitLocker.

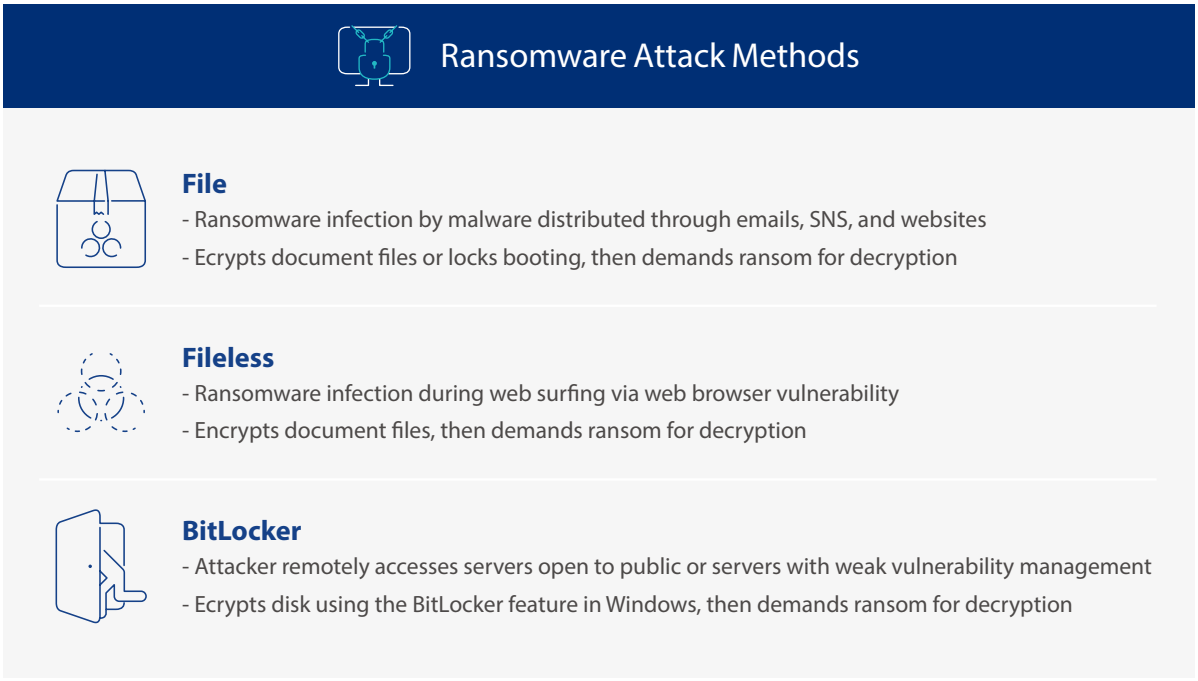

Figure 1. Ransomware Attack Methods

Most ransomware attacks involve files of some sort. The most common way to deliver this file is through phishing emails. The ransomware disguises as a normal file, tricking the user into downloading it. Another popular method to distribute files is using social network services or websites. In most cases, the ransomware encrypts all files existing in the disk upon successful infection in demand for ransom. But recently, cases where the normal startup is blocked and the disk itself is locked from access are becoming increasingly popular.

Fileless is another common attack method. This attack method does not use a malicious file to distribute the ransomware. Instead, it exploits normal running processes in the PC via web browser vulnerability. Although there are cases of ransomware distribution through malicious ad banners, attackers mostly utilize relevant websites to target victims. Instead of targeting consumers, attackers using this method usually target professionals working in the following industries: raw material, automobile, construction, oil refining, and nuclear power. This is because the data saved on these target PC are much more confidential and sensitive, thus a higher chance of ransom being paid for decryption.

Attacks exploiting BitLocker are also quite common. BitLocker is an encryption method provided by default in Windows. It is a security support feature that requires a password to access files on the disk. Attackers infiltrate the system to target the main server, then connect via remote desktop to encrypt the disk with BitLocker and demand ransom for the password.

In order to defend against the attacks mentioned above, a multi-layered response measure is required.

Response Measure #1: Conduct an 'Objective Situation Analysis' through Consultation

The first step to ransomware response is conducting an 'objective situation analysis' through security consulting services. Unfortunately, real cases show that many organizations request security consulting after experiencing ransomware attacks for follow-up measures, not prior to the attack.

As security consulting services are very effective in enhancing the overall security level, it is one of the best preventative measure against ransomware attacks for organizations or environments that lack systematic incident response processes.

More specifically, security consulting services examine internal infrastructure from the attacker's point of view to find potential vulnerabilities that could be exploited for internal infiltration. As there are abundant analysis data on security incidents in various fields, looking into best practices to prioritize action plans and optimize response is an effective way to increase ransomware readiness.

Reports provided through security consulting services provide an overall analysis of the data breach status and vulnerability detection information. Scan results across various areas that can be exploited by the attackers — anti-malware program, patch management, account, and shared folder — are also provided.

As the main assets are thoroughly analyzed, the application status of the latest patch, system operation status, as well as detailed statistics data are also provided. Furthermore, a quantified evaluation index for the security level maintained compared to the industry average is also provided. This helps the company to be aware of the areas that lack preparation and helps them to prioritize the areas that need immediate attention.

Security consulting services also provide analysis results for account management. Many organizations make common mistakes, such as using the default administrator account, applying the same password across several servers, and not having a defined policy for the password expiration period. Such cases make it easier for attackers to gain administrator privilege over servers. Consulting services assess the status of how the account of the main server is being managed via account management and provide guidance for an efficient account management system.

The following are the ransomware response features that can be expected from security consulting services.

Firstly, the latest status regarding the IT infrastructure can be provided. During this process, unused servers that are falling behind are scanned and terminated. When an unmanaged server exists internally, attackers can initiate the attack utilizing a known vulnerability code.

The second is an analysis of the internal vulnerability. From email account credentials exposed on public websites to IP/Port that is open for external access, a thorough assessment of various vulnerabilities is carried out from the attacker's point of view.

Lastly, security enhancement strategies are provided via data analytics. It provides an optimized response measure according to the business needs, which is acquired through consulting process.

Response Measure #2: Take an 'Easy and Friendly Approach' to Security Training

The next ransomware response measure is training. Trainings may include training for security operation manager and training for non-technical end-users.

Ransomware attacks are designed to exploit users' curiosity or error. It is not a new technique; it has been one of the most widely used attack techniques from the past. Thus, even with the right solutions in place, ransomware attacks will always be a possibility without proper user education.

Security managers should be up to date with the latest security issues and trends to implement effective security education for internal users.

AhnLab provides various sources in which users can learn about the latest security trends. ASEC Blog —provided by AhnLab's renown security experts — is an optimal platform to acquire intelligence on the latest threats. The blog provides threat information relevant to end-users through regularly updated posts. AhnLab also provides an in-depth analysis of the latest security attacks that threaten global users through its quarterly ASEC Report. Moreover, Security Insight provides various security intelligence regarding the latest trends.

Although improvement of security awareness through education and training may be considered ordinary, it plays a key role in ransomware response. With ransomware attack volumes increasing dramatically every year, it is everyone's job to be well educated and be aware of the issue. In other words, a collaborative effort between security managers and end-users is necessary to defend against ransomware attacks.

To help end-users better understand the topic and be alert for these type of attacks, security managers can share relevant cases where the same industry was attacked and create contents that are easy to understand from the user's perspective. Merely sharing the latest security news may not be enough to grab the user's attention and help them understand why this is a concern to their work and business.

Response Measure #3: Build an "Automated Response System" through Multiple Solutions

The third step is the establishment of an automated response system via multiple security solutions.

Although there are many solutions dedicated to ransomware defense, most of them provide features for a specific area. In other words, the solution does not likely provide a comprehensive defense to thwart elaborately designed, targeted ransomware attacks.

Implementation of various security solutions working closely together can be effective in minimizing the damage from ransomware attacks. Figure 2 shows potential infiltration routes for ransomware attacks.

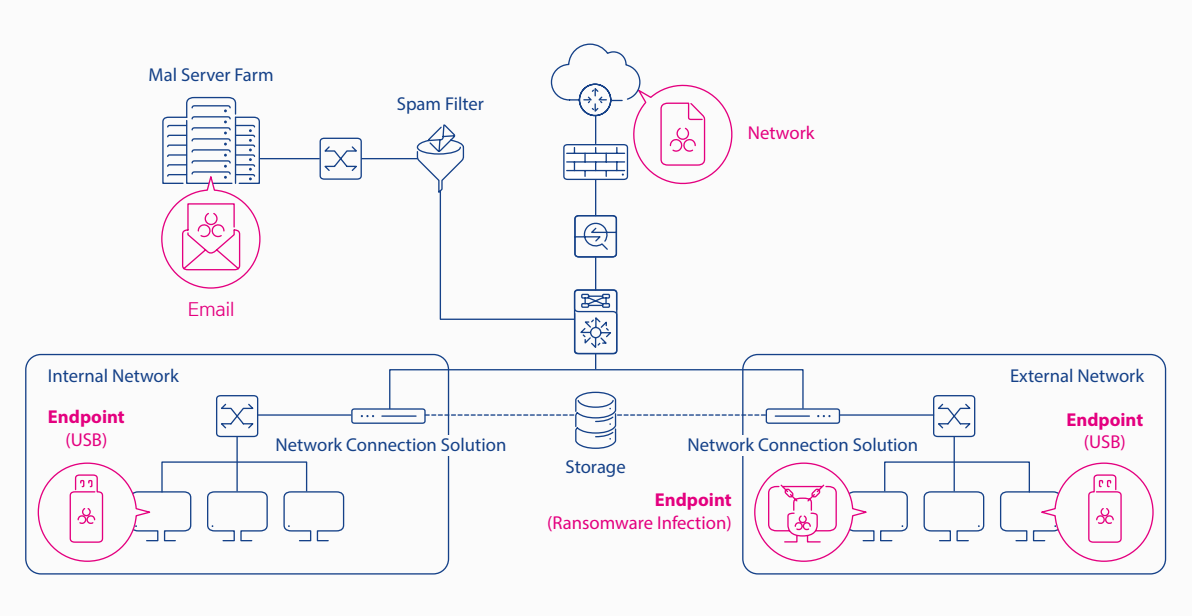

Figure 2. Potential Infiltration Routes of Ransomware Attacks

As ransomware attacks can occur through various routes, such as the network, email, and endpoint, response measures across each area would be ideal.

Let's take a closer look at each section.

Network: Integration of Firewall, IPS/IDS, and APT Response Solutions

It is common for a firewall to exist in the network by default. The firewall blocks IP or websites with a high risk of ransomware infection in real-time. It also blocks external IP and port access to important internal assets.

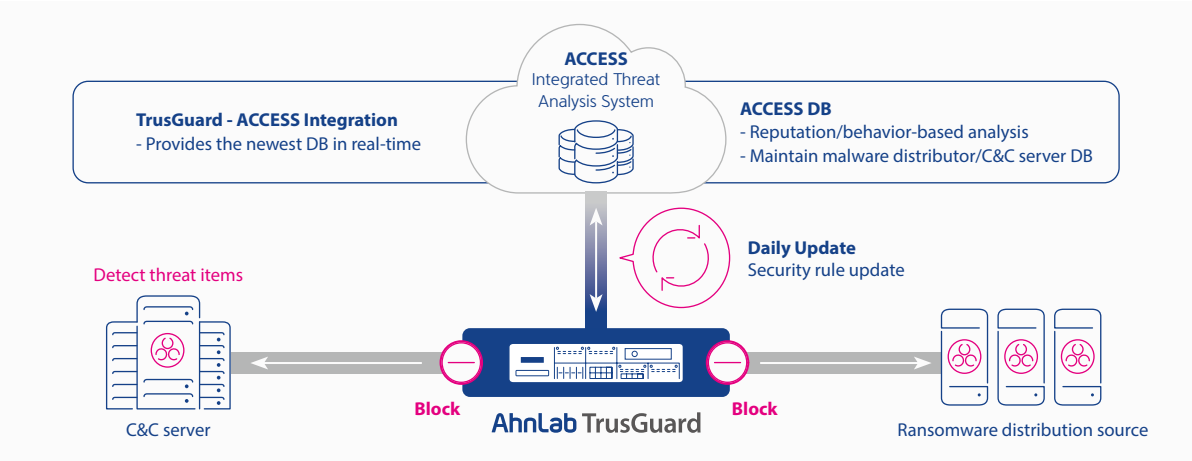

Figure 3. Ransomware Response via AhnLab TrusGuard Firewall

The administrator should always maintain the latest blocklist C&C IP and manage the block and allow rules for IP and ports. The administrator should also check firewall policies regularly for any external access allowed policies that are not managed.

IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) solutions detect attempts for port scan attacks and defend against attacks that attempt to spread to the main server via network vulnerability attacks. IPS and IDS solutions can also identify PC information suspected of infection.

APT solution identifies and analyzes ransomware among all files moving through the network via the web, file server, and FTP. It also detects new, unknown ransomware and variants via signature, reputation, and sandbox engine. If the network areas consisting of the Internet backbone and the main server are also monitored, threats through various protocols can also be detected and blocked in real-time.

Email: Utilizing APT Response Solution

Scanning attachments and URLs in the email body is necessary to defend against ransomware that comes in through emails.

Due to the rise in ransomware attacks, many put restrictions on email attachments. An example

of these restrictions include application of policies that filter executables attached in the email or script extensions used in attacks. In response to this, attackers are using advanced method of inserting an external URL within the email body to download the ransomware or disguising the ransomware as a normal document file download, instead of attaching the ransomware directly.

To effectively defend against such ransomware attacks, it is critical to collect and analyze the files distributed via email body and file attachments in sandbox environment using APT solutions.

Endpoint: Response via Integration of Security Platforms

AhnLab has consistently emphasized the importance of flexible integration and security platforms. Anti-malware, patch management, and EDR must be flexibly integrated to effectively respond to threats in the endpoint while actively carrying out their main functions.

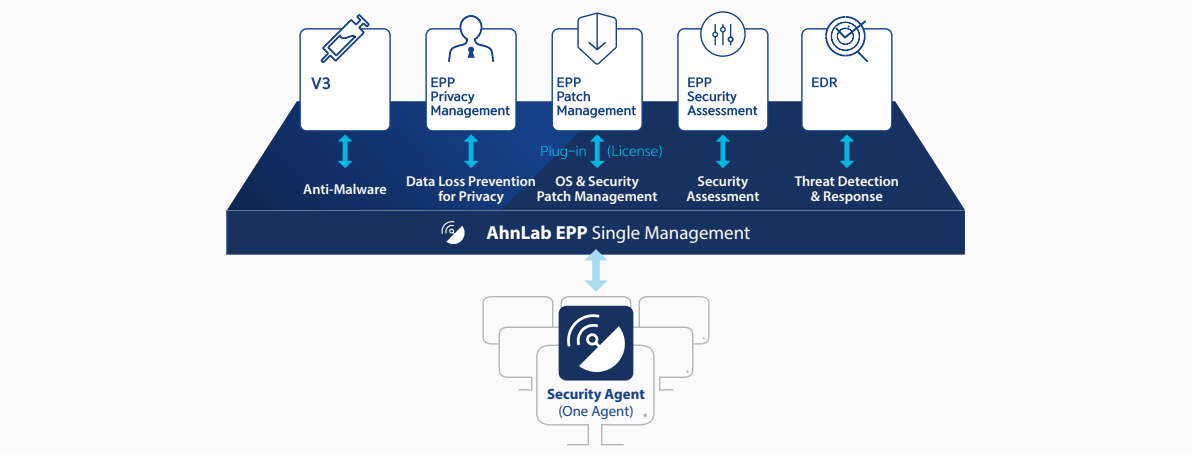

Figure 4. AhnLab EPP Structure

In detail, AhnLab's anti-malware solution, V3 blocks known ransomware at the endpoint during the point of infiltration in Windows, Unix, Linux, macOS, and VDI environments based on signature and behavior analysis. Registering folders with sensitive information as ransomware protection targets can prevent encryption even upon ransomware infection.

Although anti-malware is one of the most basic solutions at the endpoint, it is often the case that only some of its features are used, putting most of its other good features to waste. Thus, it is recommended to enable all the features built for ransomware response while maintaining the engine to the latest version.

Let's now talk about patch management solution. Some may question the relation between patch management and ransomware. However, many ransomware attacks attempt to steal PC administrator privilege by exploiting vulnerabilities in the OS or application. Some ransomware attacks attempts to move laterally to other PCs in the network after infecting one PC. When an OS

vulnerability is exploited, ransomware infections may spread to hundreds and thousands of PCs. A good example of that is WannaCry ransomware.
The application of the latest security patch is very important in terms of vulnerability management, and it can drastically lower the chances of ransomware infection and minimize the proliferation.

The next is EDR, which has been receiving lots of attention in recent years. EDR solution scans and tracks all behaviors of the PC and detects any suspicious activities. Specifically, it detects encryption and backup deletion while collecting information regarding the infection, such as the attack flow. Therefore, system administrators can check the information, including the attack routes, C&C IP, and URL, through the EDR and block it accordingly.

APT solutions also provides ransomware response features. After the execution holding of files, executed through network, email, and USB, it analyzes them in a sandbox environment. Encryption of documents in the PC can be easily detected using sandbox behavior analysis. The detected ransomware is then blocked and deleted from the execution holding status. Thus, all responses can be completed automatically before infection.

APT solutions can also effectively respond to fileless attacks. It prevents malicious behaviors from executing by monitoring web browser vulnerability attacks and force-terminating the process inserted with vulnerability code at the time of discovery.

Figure 5 shows the response order of each solution upon ransomware attack at the endpoint.

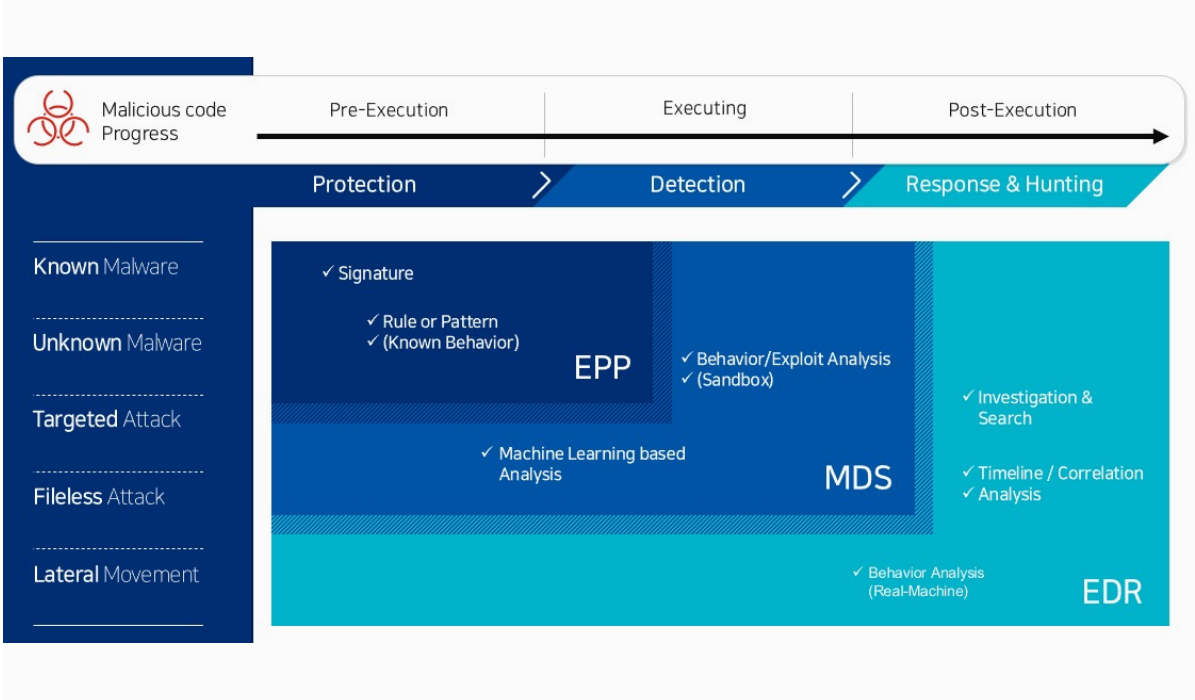

Figure 5. Ransomware Response Process by Each Endpoint Solution

Conclusion: Ransomware Response Requires Cooperation between Human and Technology

In this whitepaper, three types of ransomware response measures were discussed. Although the adoption of a new security solution seems like the quickest and easiest way to prepare a ransomware response plan, this would not be appropriate for businesses that have not yet undergone a detailed analysis of their internal IT infrastructure. Thus, a more reasonable way would be to remove all externally exposed threats via security consulting services.

Having an extensive amount of experience dealing with various businesses and organizations, AhnLab believes that an organization with optimized security solutions and end-users that have a high-level security awareness is critical in building an efficient ransomware response strategy.

All end-users need to be notified of ransomware attacks via email or notices, with each of them knowing how to report emails or files suspected of ransomware. Also, they must be capable of quickly responding to the attack to prevent lateral movement by following the guidelines established by the security team.

Ransomware can be effectively prevented by the cooperation of human and technology. Instead of fearing for ransomware, businesses should constantly assess their ransomware response plan and improve their strategy to build an even more solid defense system.

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com / global.sales@ahnlab.com