Best Use Case

AhnLab

Detecting Cross-Network File Transfer via Extension Tampering

Industry
Advanced Manufacturing

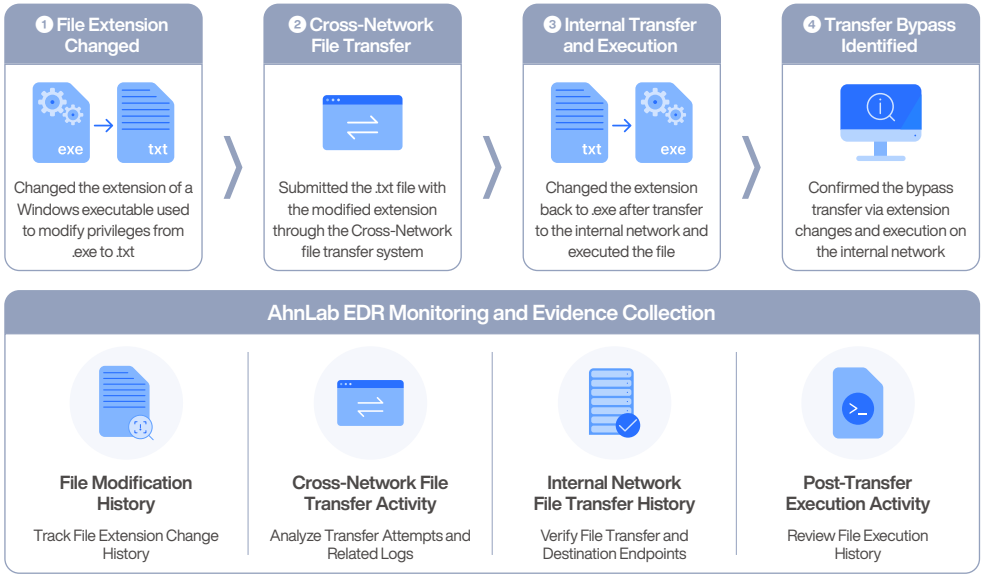
Company Size
Enterprise

Solutions
AhnLab EDR

Company C identified a case in which an executable file was transferred into its internal network through a cross-network file transfer system after its extension was changed to bypass file transfer controls, and was subsequently executed.
AhnLab EDR correlated file modification, cross-network file transfer, and internal execution activity to identify the associated user and endpoint. The findings were used to support on-site verification and follow-up actions in accordance with internal policies.

How Was the Executable Transferred into the Internal Network?

Company C operated a cross-network file transfer system to move files between its external and internal networks. However, files were screened primarily by extension rather than by actual file type or executability, allowing executable files to potentially bypass transfer restrictions through extension changes.
An executable used to modify Windows privileges had its extension changed from .exe to .txt, was transferred into the internal network through the cross-network file transfer system, then had its extension changed back to .exe and was executed.
Because file modification, cross-network file transfer, and execution on the internal network were logged as separate events, individual logs alone could not provide a complete view of the activity. AhnLab EDR correlated these events chronologically to reconstruct the full sequence—from the extension change on the external network to transfer into the internal network and subsequent execution.



[Figure 1] Bypassing Cros-Network File Transfer Controls via File Extension Modification and Collecting Investigative Evidence with AhnLab EDR

Results

File Transfer Flow Visibility

Trace the full flow from file extension changes to execution on the internal network

Rapid Identification of Investigation Targets

Identify associated users, endpoints, files, and timestamps

Evidence for On-Site Response

Establish evidence to support on-site verification and follow-up actions

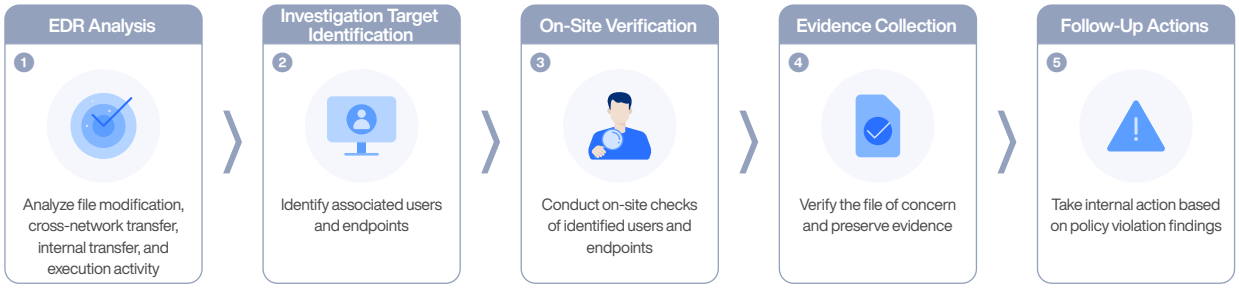
Establishing Investigative Evidence Through Activity Correlation

Effective security operations require more than detecting suspicious events. Security teams must also determine who performed the activity, on which endpoint, and when it occurred. When relevant records are scattered across multiple systems and points in time, identifying the responsible user and determining whether internal policies were violated can be difficult.

AhnLab EDR correlates file modification and execution activity with user and endpoint data. Using this information, Company C identified the users and endpoints associated with the file, along with key timestamps related to its modification and use.

This enabled the security team to narrow the scope of the investigation and clearly define the users, endpoints, and files that required priority verification during the on-site investigation.

> "Previously, we had to manually collect and analyze records scattered across multiple systems, which made investigations time-consuming. With AhnLab EDR, we can view related activity as a single sequence, reducing the time required for initial analysis and investigation scoping."
> - Information Security Manager, Company C



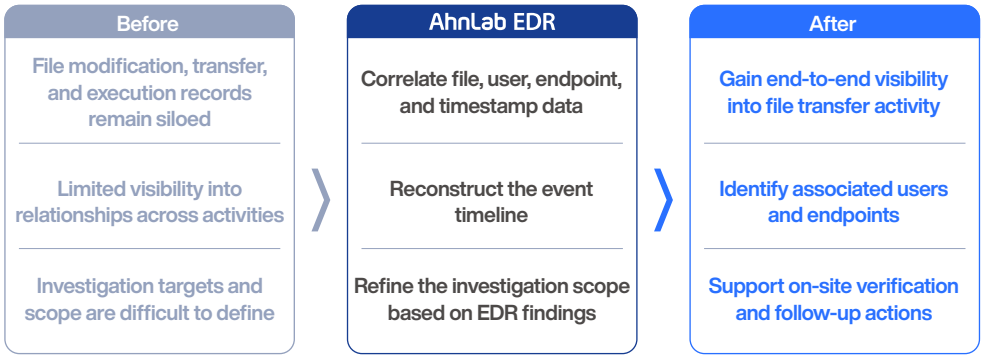
[Figure 2] On-Site Verification and Follow-Up Actions Based on AhnLab EDR Analysis

Supporting On-Site Response and Follow-Up Through Precise Target Identification

Once AhnLab EDR analysis narrowed the investigation scope, the security team conducted on-site checks focused on the identified users and endpoints. During the investigation, the team verified the presence and use of the Windows privilege-modification tool transferred into the internal network and collected and preserved relevant evidence.

The team then correlated AhnLab EDR analysis records with evidence collected on site to determine whether internal policies had been violated and carried out follow-up actions in accordance with the company's security policies.

> "By correlating the analysis results with evidence collected on site, we were able to establish the facts based on evidence rather than circumstantial indicators. Having clearly defined investigation targets and verification points also made our on-site checks and follow-up actions much more systematic"
> - Security Operations Manager, Company C



[Figure 3] On-Site Response Benefits with AhnLab EDR

Tracing Hidden Bypass Paths and Establishing Evidence for Response

AhnLab EDR correlated previously fragmented file modification, transfer, and execution records into a single activity timeline, providing visibility into the file transfer bypass path.

This enabled Company C to quickly identify the users, endpoints, files, and timestamps involved and establish objective evidence to support on-site verification and subsequent actions.