AhnLab

eBook

Achieving 95% Detections in MITRE ATT&CK Evaluations Round 6

AhnLab has proven our excellence in cyber threat detection and analysis in the independent 2024 MITRE ATT&CK Evaluations Enterprise Round 6 by achieving 95% detections.

Let's explore how the evaluation played out and what the results mean to real-world defenders.

Understanding MITRE ATT&CK Evaluations

The owner of MITRE ATT&CK Evaluations, MITRE was established to advance national security in new ways and serve the public interest as an independent adviser. Through public-private partnerships and federally funded R&D centers, MITRE works across government and in partnership with industry and academia to tackle challenges. In the cybersecurity industry, MITRE is well-known for creating and developing the MITRE ATT&CK Framework, a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

MITRE ATT&CK Evaluations is built on the backbone of MITRE's objective insight and conflict-free perspective. Cybersecurity vendors participate in the evaluation to improve their offerings and to provide defenders with insights into their product's capabilities and performance. The evaluation enables defenders to make better informed decisions on how to leverage the products that secure their environments.

The evaluation, just completing its sixth round, is recognized worldwide as one of the most trusted security product tests, considering its similarity to real-world threats and completeness of attack scenarios. A total of 19 cybersecurity companies participated in round 6. AhnLab was the only South Korean company to have taken part in the evaluation for four consecutive rounds since round 3.

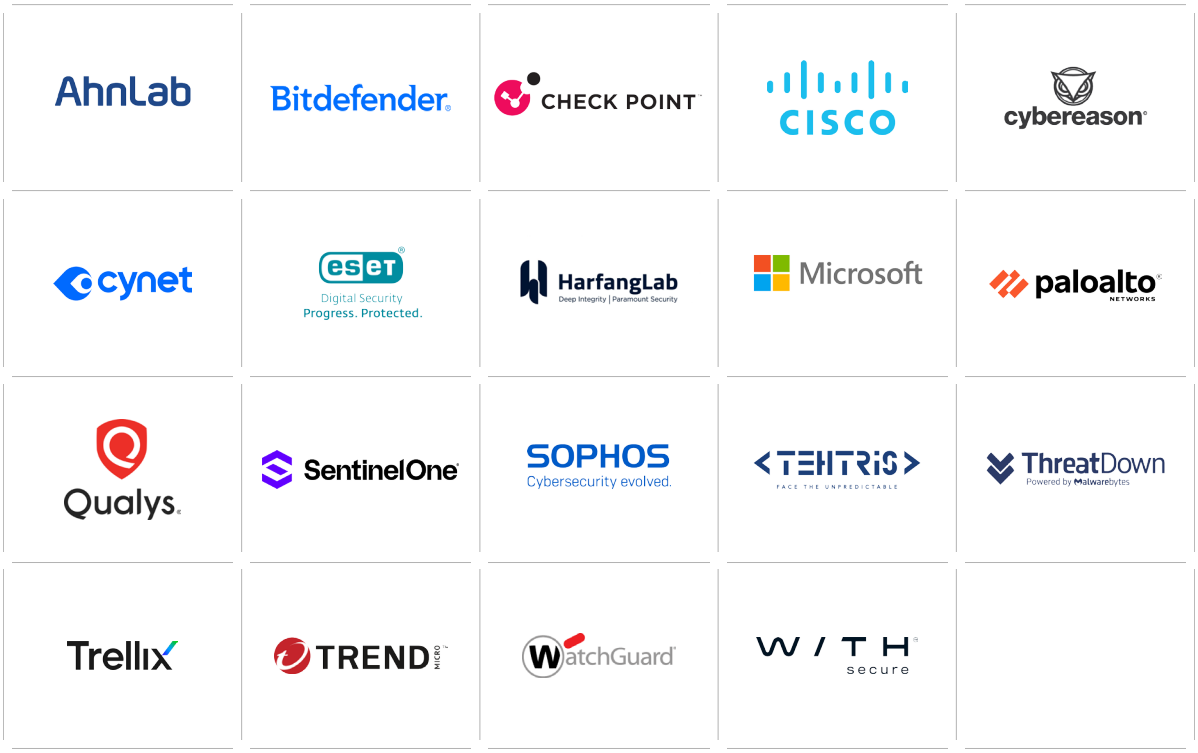

Figure. Participants of MITRE ATT&CK Evaluations Round 6

How the Evaluation Was Designed

MITRE ATT&CK Evaluation consists of cyber threat scenarios, steps that form a scenario, and substeps that make up each step. Based on this structure, MITRE tests participants' defense ability against emulated cyber threats.

For Detections category of this year's evaluation, the vendor and MITRE jointly collected evidence from the vendor's products, and MITRE calibrated evidence based on the five detection types below. In simple terms, detection types in order of None to General, Tactic, and Technique represent more accurate and contextualized threat detection.

Types	Description
N/A	Evaluation for the (sub) step was not completed.
None	The vendor's evidence does not meet the detection criteria, or no evidence is provided.
General	The evidence satisfies the detection criteria but does not provide details on why (tactic) or how (technique) the action was performed.
Tactic	The evidence satisfies the detection criteria for General and provides details on why the action was performed (tactic).
Technique	The evidence satisfies the detection criteria for Tactic and provides details as to how the action was performed (technique).

[Table] Five detection types of MITRE ATT&CK Evaluation

The 2024 Evaluation ruled out "Telemetry" from detection types. The change raised the evaluation standards by only accepting evidence with contextual analysis as valid detections.

Round 6 Scenarios

Through Detections evaluation, MITRE tested participants on their ability to detect the real-world techniques and tactics of two ransomware-as-a-service groups, LockBit and CL0P, and DPRK threat actors. This methodology contrasts with previous rounds, which focused on emulating the adversary behaviors of a single threat group.

Ransomware (CL0P and LockBit)

Enterprise Round 6 focused on LockBit and CL0P to emulate common behaviors prevalent across the ransomware ecosystem. LockBit, which law enforcement agencies have described as the "most deployed ransomware variant across the world," is known for its use of sophisticated tools and dual targeting of Windows and Linux systems. CL0P is a ransomware family associated with the TA505 criminal group and leverages the "steal, encrypt, and leak" strategy across a variety of regions and sectors.

DPRK

North Korea poses a significant cyber threat, targeting the global financial, defense, and technology sectors to fund the advancement of its nuclear capabilities. North Korea has increasingly expanded its targeting of macOS systems, gaining the ability to infiltrate additional high-value systems. The Enterprise Round 6 macOS-focused emulation featured multistage and modular malware that executed operations involving abusing legitimate macOS utilities and collecting and exfiltrating sensitive data.

95% Detections! Highlights of Our Results

In round 6, the detection capability of AhnLab EDR, AhnLab EPP, and AhnLab XDR was rigorously assessed, and our products achieved 95% detections for malicious ransomware behaviors of CL0P and LockBit that the MITRE team emulated.

From the defender's perspective, our round 6 results can be highlighted in terms of:

1. Advanced Detection and Analysis of Real-World Threats

We were able to secure 95% visibility by detecting 56 out of 59 substeps in Ransomware scenarios across Windows and Linux platforms. Our products provided high-quality evidence with comprehensive and contextual analysis into emulated threat behaviors. Also, the chart below indicates that our detection results and capabilities are competent among our industry peers.

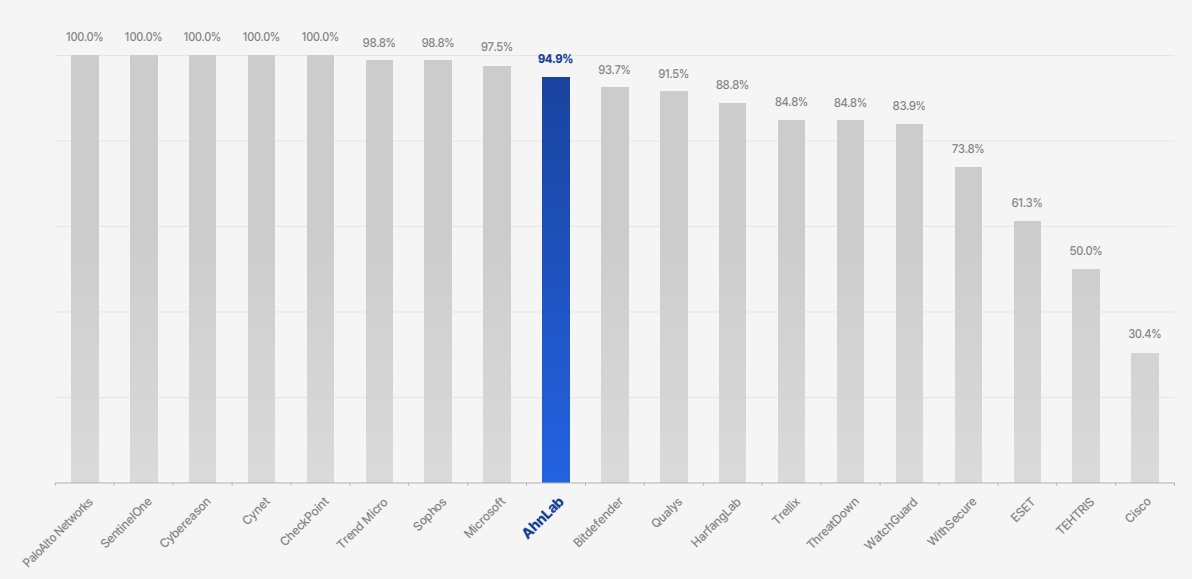

Figure. The "Detections" results of participants in Round 6

**The results in the figure were analyzed by AhnLab. MITRE does not rank its participants.*

On top of that, our products delivered 49 "Techniques" among 56 substeps detected. This demonstrates that our customers can thoroughly understand the underlying context (how and why) of malicious behaviors and make informed decisions by referring to the evidence of our solutions. The result is even more meaningful as context-aware detection is key to triggering an optimal response, especially when we have to deal with sophisticated and ever-evolving modern cyber threats.

2. Relentless Development of Our Solutions

Our results (95%) in this round represent a significant improvement from the previous round, in which we secured 82% detections. Given that the MITRE team raised the bar of evaluation by removing "Telemetry" from the detection category, our recent performance has greater implications beyond just numbers.

We want to stress that the objective of MITRE ATT&CK Evaluations is to help cybersecurity vendors improve their offerings, and this is exactly why we have been participating in this evaluation. Our experience in three previous rounds played a massive part in identifying what and how to enhance our solutions to reach the current state. In line with our progress, we will make relentless efforts to bring our offerings to the next level by reinforcing their accuracy, efficiency, and usability.

How We Specifically Detected Threat Behaviors

Now, let's sift through how we uncovered emulated threat behaviors of ransomware cybercriminals. Here, we have a series of examples across substep 11.01, 12.01, and 12.03 of the LockBit scenario.

1. Substep 11.01 – Enabling Automatic Login

The goal of MITRE Red Team for step 11 was to maintain persistence on quirrell (10.111.9.202) by modifying the subkey to enable automatic login.

In substep 11.01, as part of step 11, the red team played the role of the user "GORNUK" to modify the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon subkey to attain their aims, initiation of automatic login.

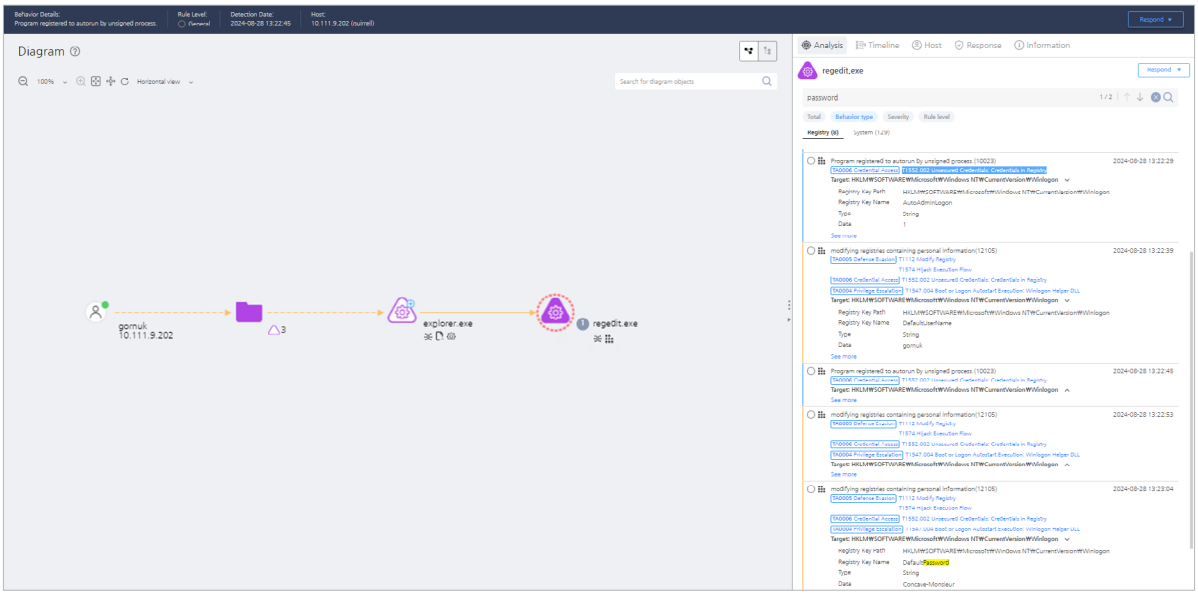

Figure. Our evidence for substep 11.01

AhnLab EDR graphically visualized the behavioral flow of the GORNUK registering program for autorun by using unsigned processes. The solution precisely provided the registry key name and path along with concise descriptions and corresponding TIDs (TA0006 Credential Access & T1552.002 Unsecured Credentials: Credentials in Registry). The evidence delivered complete context for defenders to perceive that the adversary attempted to modify the subkey to activate auto-login as part of its operations.

2. Substep 12.01 – Password Dumping via Software Deployment Tools

In step 12, the red team attempted to ingress the FireFox password dumper using Chocolatey (choco) and dump passwords from FireFox. Then, they tried to recover the domain admin credentials to ultimately access the Linux KVM server.

As part of their operations, substep 12.01, the operator made cmd.exe execute choco and install FoxAdminPro.

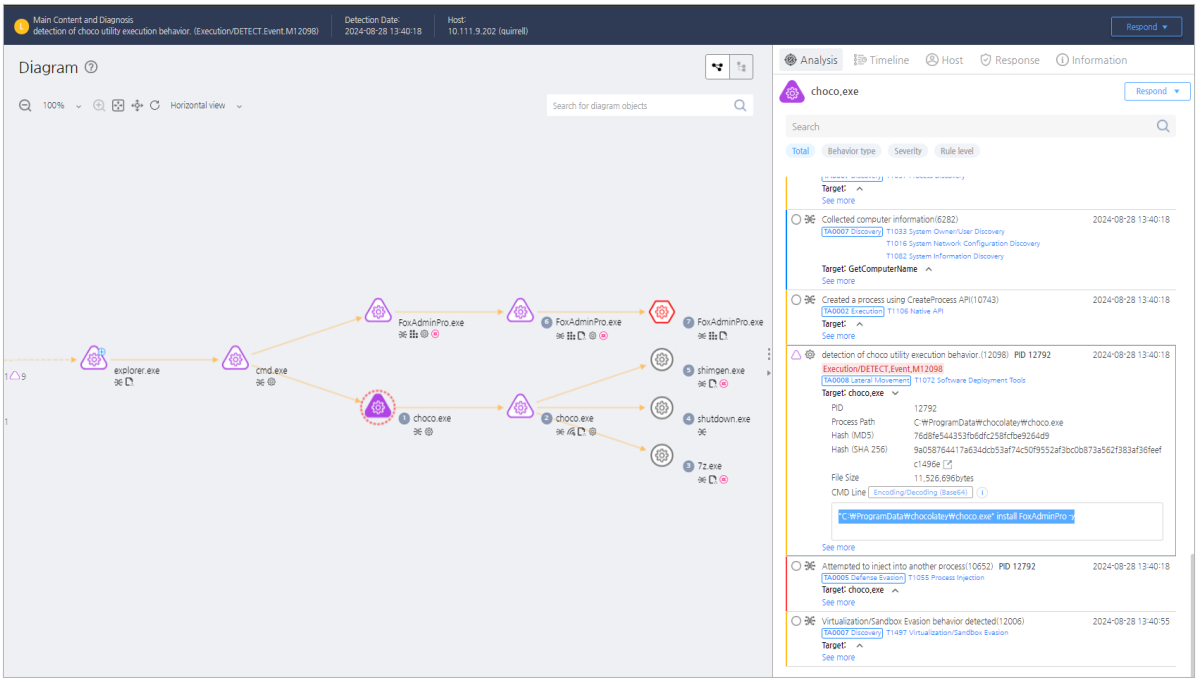

Figure. Our evidence for substep 12.01

AhnLab EDR successfully uncovered adversary behaviors in different ways. First, the diagram vividly illustrating the entire process of cmd.exe installing FoxAdminPro assisted defenders in learning about the context. In addition, the details, including the choco execution path and TID (T1072 Software Deployment Tools), supercharged investigators with adequate insight into malicious events.

3. Substep 12.03 – Credentials from Web Browsers

The next step for the read team was to make cmd.exe execute FoxAdminPro in the following path: C:\Users\gornuk\AppData\Roaming\Mozilla\Firefox\Profiles\ohbrdd1o.default-release\. The emulator made this move to access the password store and obtain credentials from the web browser.

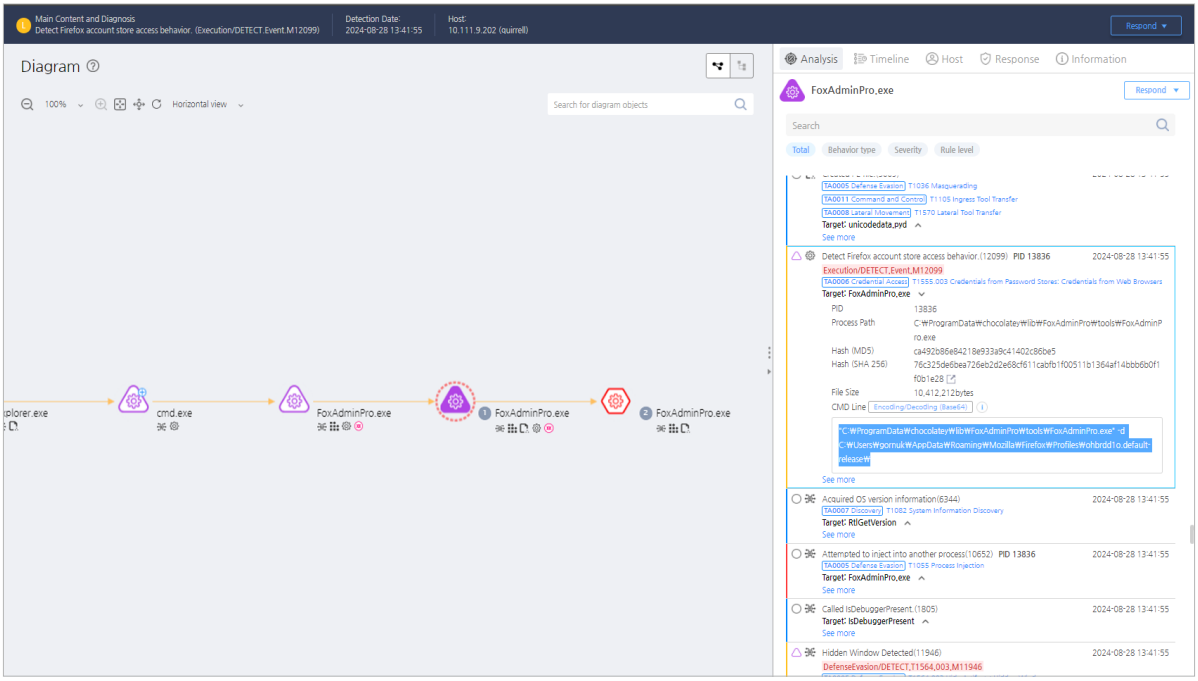

Figure. Our evidence for substep 12.03 (1)

AhnLab EDR disclosed ill-willed activities as if we peeled back the onion. The solution made it transparent that there was access to the FireFox credential stores by providing a behavioral diagram, TIDs (TA0006 Credential Access & T1555.000 Credentials from Web Browsers), execution command line, and associated details.

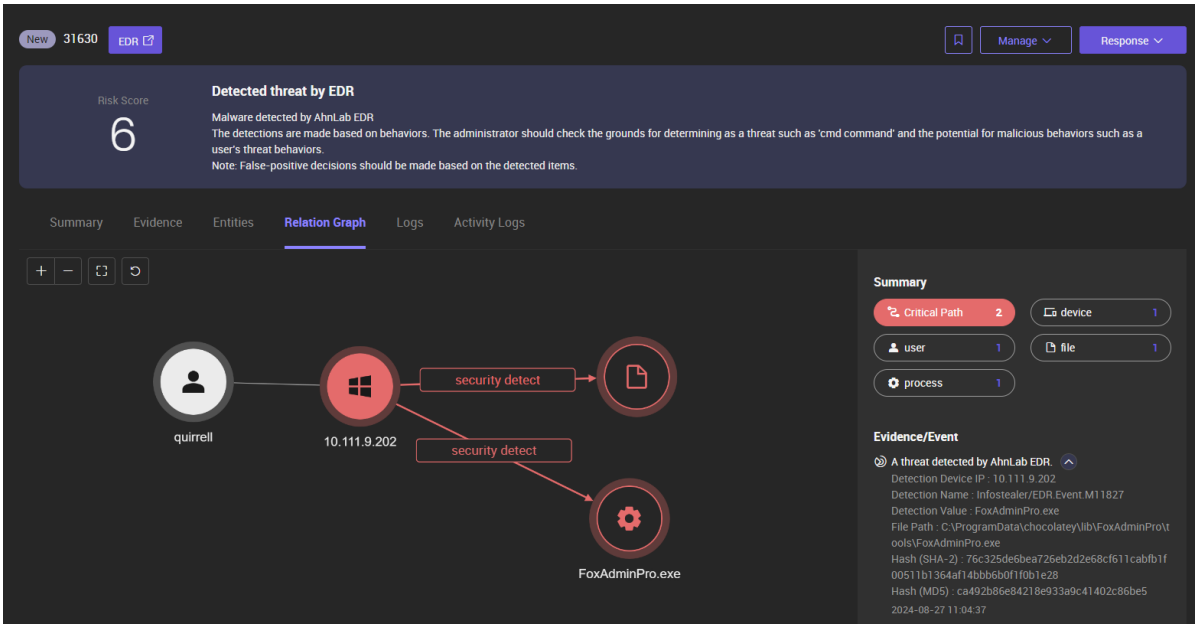

Figure. Our evidence for substep 12.03 (2)

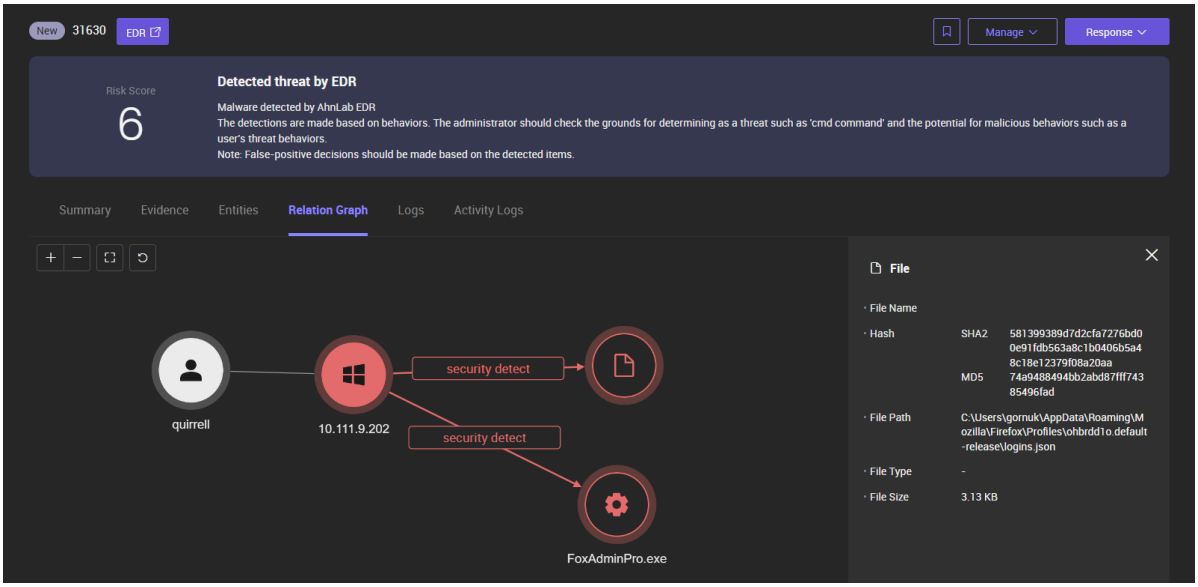

Figure. Our evidence for substep 12.03 (3)

Furthermore, AhnLab XDR enriched our detection by providing a diagram, file information, and other details to help defenders achieve greater situational awareness.

After all, we had three substeps above calibrated as Technique. The result is particularly meaningful as it manifests how our solutions can fuel our customers to truly comprehend the sequence and context of real-world techniques ranging from auto-login enablement and password dumping to credential store access. It is also solid proof of the fact that our customers can stay response-ready against actual cyber threats by leveraging the precise detection and robust analysis capabilities of our security offerings.

Visit the MITRE ATT&CK Evaluation website to find the results of Round 6. Also, learn more about our products assessed in MITRE ATT&CK Evaluations Enterprise Round 6.

▶ AhnLab EDR
▶ AhnLab XDR
▶ AhnLab EPP

AhnLab

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