Security Doesn’t Stop at the First Alert: Falcon X Threat Intelligence Offers New Context in MITRE ATT&CK Evaluation

April 19, 2022

Kurt Baker - Liviu Arsene - Sanket Karpe Endpoint & Cloud Security

- The CrowdStrike Falcon® platform delivers 100% prevention across all nine steps in the MITRE Engenuity ATT&CK® Enterprise Evaluation
- CrowdStrike extends endpoint and workload protection by fully integrating threat intelligence into the Falcon platform —— CrowdStrike Falcon X™ enables CrowdStrike users to pivot seamlessly from detections to the latest intelligence on today’s adversaries, including their motivation and tradecraft
- Falcon X helps organizations save time by automatically analyzing potential malware with built-in sandbox technology, finding and analyzing related malware samples, and enriching the results with industry-leading threat insights
- Falcon X provided enriched detections throughout eight MITRE Engenuity ATT&CK Evaluation tactics and 18 techniques

CrowdStrike recently demonstrated the power of the Falcon platform and its integrated approach to providing robust protection by exposing all attack tactics used as part of the MITRE Engenuity ATT&CK Enterprise Evaluation released in April 2022. The evaluation focused on emulating two of today’s most sophisticated Russian-based threat groups: WIZARD SPIDER and VOODOO BEAR (Sandworm Team).

Scoring 96% percent visibility of substeps across all 19 steps and 109 substeps, the Falcon platform leveraged the intelligence automation capabilities of Falcon X threat intelligence to deliver additional enriched detections and indicators of compromise on 8 tactics and 18 techniques used by the two persistent adversaries.

Security doesn’t stop at the first alert. Falcon X offers new context on the who, what, why and how behind a security alert. It gives meaning to each alert an analyst works on, helping them prioritize which alerts to handle first and understand detailed insights into the attacker, motivation and methods —— like the two emulated by MITRE Engenuity.

Falcon X helps protect against future attacks by providing context, attribution and information on how to stop the next actor or malware campaign. Falcon X does this by exposing known attack vectors, identifying related malware and malware techniques that have been seen in the past, or predicted for the future, and sharing this information with your security team and across your security devices. All of this investigation and analysis happens without you having to do anything except review the results. You save time, you know your priorities and you can trust your responses to be error-free. Most importantly, you are provided with detailed information on how to protect against future attacks from these adversaries.

Outpace the Adversary with Ready-to-Go Integration and Automation

Throughout the MITRE Engenuity ATT&CK Enterprise Evaluation, the Falcon platform leveraged its native automation capabilities. Typically, when a file-based attack is blocked on the endpoint by CrowdStrike Falcon Prevent™ next-generation antivirus, it is automatically sent to Falcon X for malware analysis and detonated in a safe environment. In this case, since MITRE Engenuity prohibits blocking in the detection portion of the test, we used custom indicator of attack (IOA) detection monitoring that triggered an automated workflow in CrowdStrike Falcon Fusion™, the Falcon platform’s natively integrated security orchestration, automation and response (SOAR) framework.

Figure 1. CrowdStrike Falcon Fusion workflow (Click to enlarge)

Figure 1 shows the Falcon Fusion workflow when custom IOA behavioral detection monitoring events were triggered. This could include, for example, when suspicious files were written to disk by a scripting engine or dropped via remote hands-on desktop sessions. The workflow retrieves and auto-submits the files to the Falcon X malware analysis sandbox to determine the malicious verdict and perform detailed analysis.

Whether using built-in or custom Falcon Fusion automation, the results of the file analysis are available, in context, to the user as a pivot directly from the Falcon detection. The results include the threat score, attribution and an outline of the behavior of the suspicious file, as if it had run in your environment. By automating threat investigations, Falcon X dramatically reduces time spent investigating and alert fatigue, and frees up resources so analysts can focus on other critical and strategic tasks. Falcon X also delivers indicators of compromise (IOCs) generated from the analysis of the file, as well as related files selected from CrowdStrike’s database of over 3.8 billion malware samples.

Falcon X Delivers Key Intelligence to Identify the Attack and Understand Attacker Tactics

Detonating binaries in Falcon X helps uncover the behavior of suspicious files and extract more information than is possible on the endpoint. This enables users to identify additional IOCs and known adversarial tactics, and hunt for secondary payloads, making it difficult for adversaries to bypass detection by changing the file used for initial access.

Figure 2 shows the Falcon X file analysis report for a file used in substep 1.A.2 (part of the WIZARD SPIDER Initial Compromise emulation scenario). The ChristmasCard.docm file is malicious, with a threat score of 100/100. At the same time, Falcon X also detected that the file had macro execution triggered on opening. Along with this information, Falcon X has successfully identified and mapped the dynamic behavior of the file to MITRE tactics, techniques and procedures (TTPs). With this enriched information, analysts can search for processes exhibiting similar technique IDs (TIDs).

Figure 2. CrowdStrike Falcon X report for WIZARD SPIDER malicious payload in the Initial Compromise emulation scenario (Click to enlarge)

In addition to behavioral data, Falcon X also captures memory state during execution and presents extracted strings from the detonated process. As displayed in Figure 3, (from substep 1.A.5 —– part of the same WIZARD SPIDER Initial Compromise emulation scenario), the "Advanced Analysis" helps identify the purpose of the file, which is especially useful in cases where the binary is packed. This data plays a crucial role in helping to analyze the complete behavior of the threat and understand its capabilities.

Figure 3. CrowdStrike Falcon X detonation report highlighting process details and extracted strings (Click to enlarge)

Stop Breaches with the Right Tools and the Right Information at the Right Time

Security analysts are not short on data or tools. Threat intelligence must be integrated directly into their daily workflow and, more importantly, be available when new evidence is discovered. Security teams often use the term "pivot to intelligence," which illustrates this process of understanding the full context of a newly discovered threat alert. Having the latest intelligence such as adversary motivation and known attack methods at your fingertips reduces time and complexity of the remediation effort. Falcon X enriches the events and incidents detected by the Falcon platform, automating intelligence so security operations teams can make better, faster decisions. All security teams, regardless of size or sophistication, can learn from the attacks in their environment, and can apply that knowledge to proactively prevent future attacks. CrowdStrike shuts down attacks before they can start by delivering powerful capabilities like identity-based security, comprehensive indicators of attack (IOAs), machine learning, automated orchestration and Falcon X threat intelligence through a unified, cloud-native platform. This integrated approach provides analysts with the right tools and threat intelligence to understand and defend against future attacks —– and demonstrated excellent value throughout the MITRE Engenuity ATT&CK Enterprise Evaluation.

Additional Resources

- Read more about CrowdStrike's evaluation results in this blog: CrowdStrike Achieves 100% Prevention in Recent MITRE Engenuity ATT&CK Evaluation Emulating Russia-based Threat Groups
- To find out more about how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Threat Intelligence page.
- Download the white paper: Supercharge Your SOC by Extending Endpoint Protection with Threat Intelligence
- Check out the Falcon X demo in our Tech Center.
- Get a full-featured free trial of CrowdStrike Falcon X™ and learn how to get ahead of your attackers next move.

- Tweet
- Share

Related Content