¿Qué es el listado blanco de aplicaciones (Application Whitelisting)?

Introducción

El listado blanco de aplicaciones, en el contexto de Cyber Crucible, consiste en otorgar a una aplicación permiso para realizar alguna acción que de otro modo podría considerarse sospechosa o maliciosa.

La tecnología de listado blanco de aplicaciones se encuentra típicamente en el arte defensivo del análisis de comportamiento, aunque algunos atacantes también la utilizan (no se cubre aquí) en sus operaciones.

Piénselo como en la escuela, donde a los estudiantes normalmente no se les permitía caminar por los pasillos durante la clase. Sin embargo, si una figura de autoridad les daba un “pase de pasillo” de alguna forma, los estudiantes no eran devueltos a su salón de clases ni enviados a la oficina del director.

Tipos de listado blanco de aplicaciones - una descripción no técnica

Si continuamos con la analogía del “pase de pasillo”, puede haber diferentes técnicas que los funcionarios de la administración escolar han aprendido, las cuales ayudaron a formalizar los comportamientos que algunos estudiantes (definitivamente no nuestro CEO Dennis) pudieron haber intentado hacer sin ser descubiertos. Todo esto tiene una correlación directa con las operaciones de seguridad.

El pase de pasillo obvio y engorroso (algo bueno)

21987331.jpg?width=278
¿Recuerda alguna vez haber recibido un pase de pasillo, o una llave de alguna habitación, que era increíblemente grande y evidente?

Había un par de buenas razones para eso:

1. Para que no se perdiera.
2. Para reducir el tiempo y la energía invertidos por parte de una figura de autoridad, en la verificación rápida de las actividades aprobadas del estudiante.

Un buen software no “perderá” una lista blanca, pero el software de listado blanco de aplicaciones debe permitir una validación rápida y eficiente en recursos de que la aplicación ha sido inspeccionada.

El pase de pasillo genérico (probablemente no es algo bueno)

Esto probablemente sea lo menos útil tanto para el monitoreo de aplicaciones como para las escuelas, pero requiere la menor gestión o experiencia.

En este caso, al estudiante se le permite hacer su diligencia en el pasillo. El profesor puede saberlo, por ejemplo, pero no hay validación por parte de los monitores de pasillo sobre lo que el

estudiante está haciendo. Además, si hay un intento de validación, existen dos niveles de inversión considerable de recursos:

1. el nivel de esfuerzo para acercarse al estudiante e interrogarlo sobre sus comportamientos e intenciones
2. el nivel de esfuerzo para asegurarse de que el estudiante está siendo honesto, para validar la explicación del estudiante

Con las aplicaciones, esto se observa con mayor frecuencia cuando un programa se agrega a una lista blanca y no hay más validación de los comportamientos o actividades permitidas. Desafortunadamente, la capacidad de obtener contexto sobre los comportamientos de una aplicación típicamente no está disponible para su adquisición si no es rastreada externamente por algún otro marco de trabajo.

El pase de pasillo genéricamente específico

No confundir con, “¡adelante, Aplicación, haz lo que quieras!”

Volvamos al pase para el baño, porque es muy apropiado aquí. Dada la visibilidad del pase, es relativamente fácil evaluar qué debería estar haciendo el estudiante. Los comportamientos flagrantes fuera de lo esperado con “ir al baño” pueden evaluarse sin mucha dificultad.

El listado blanco de aplicaciones que tiene límites genéricos de actividades es el más común, aunque en muchos casos esos límites equivalen a permitir que un estudiante con un pase para el baño juegue en el patio de recreo.

El pase de pasillo específico-específico

¡No confundir con el pase de pasillo “genéricamente específico”!

22642689.jpg?width=340
Si bien, con el pase de pasillo genéricamente específico, sabemos que el estudiante está usando el baño, en una escuela grande no sabemos
1. Quién le dio permiso al estudiante

2. De dónde acaba de venir.

3. En qué baño pensaba la figura de autoridad cuando dio su aprobación.

4. Cuánto tiempo ha estado el estudiante “fuera y por ahí”.

Esto requirió más trabajo por parte del marco de autoridad de la escuela.

Volviendo al listado blanco de aplicaciones, el análisis de comportamiento es más preciso cuantas más variables se agreguen a cualquier capacidad de toma de decisiones.

Además, al investigar un pase de pasillo que ha sido emitido, normalmente no es necesario rastrear una cadena de 5 profesores para llegar a la fuente. También casi siempre se puede confiar en que el profesor no era algún tipo de “mal profesor” que les dice a los estudiantes que se comporten de manera inapropiada. El listado blanco de aplicaciones, en un ejemplo de lista blanca específica-específica, requiere trabajar hacia atrás, para examinar cada aplicación padre o ancestro que abrió la siguiente aplicación. Por ejemplo, una pieza de malware puede haber abierto una utilidad legítima de Windows.

Las siguientes preguntas son aproximadamente equivalentes al “pase de pasillo estudiantil” mencionado anteriormente:

1. ¿Para qué se inició la aplicación, o qué se le indicó que hiciera? Necesitamos conocer el comportamiento previsto.
2. ¿Quién inició la aplicación? Esto típicamente es otro programa.
3. ¿Qué programas “padre” o “ancestro” resultaron en la apertura de este programa? ¿Qué estaba haciendo cada uno de ellos, o qué pretendía hacer?

La aplicación comprometida

Recuerde en varias obras de ciencia ficción, o literatura y películas de terror, cuando un impostor de alguna manera ha tomado

22413315.jpg?width=226
el control del comportamiento de un personaje? En las escuelas, no hay muchas posibilidades de que un instructor sea poseído por alienígenas.

La toma de control de aplicaciones es una técnica favorita de los atacantes porque, al igual que en las películas, la mayoría de los observadores no notan nada extraño hasta que es demasiado tarde.

En este caso, un atacante toma un programa en ejecución, que actualmente está cargado en memoria. Así, el programa completamente intacto en el sistema de archivos es ignorado. El programa en memoria se edita para agregar el código del atacante. Muy parecido a un alienígena dentro del cuerpo de un humano. El atacante realiza sus comportamientos delictivos, y cuando el programa termina de ejecutarse, la mayor parte de la evidencia desaparece. Cuando el programa legítimo se ejecuta nuevamente, si el atacante no edita el código otra vez, es tal como los codificadores legítimos originales lo pretendían. ¿Tal vez una mejor analogía, en ese caso, sería un hombre lobo?

Un listado blanco de aplicaciones, entonces, necesita trabajo adicional para garantizar que el programa, y cualquier ancestro o programa padre, estén intactos sin que un hacker edite los programas mientras se están ejecutando.

En resumen - Preguntas que hacer al investigar una capacidad de listado blanco de aplicaciones

Asegúrese de comprender los límites que permite una lista blanca al discutir el listado blanco de aplicaciones con su equipo de tecnología o proveedor.

1. ¿Esta capacidad examina y rastrea lo que se supone que un programa debe hacer, y compara los comportamientos esperados frente a los observados?
2. ¿Cuánto detalle captura la capacidad de listado blanco en su toma de decisiones? ¿Más o menos que un pase de pasillo estudiantil detallado?
3. ¿La capacidad de listado blanco rastrea e investiga los programas padre y ancestro en busca de comportamiento malicioso? (El Programa A abre B, abre C, abre D – muy común)
4. ¿La capacidad de listado blanco valida que el programa en ejecución no haya sido manipulado?

Lectura profunda del Instituto Nacional de Estándares y Tecnología (NIST)

Una publicación autorizada que no es para una lectura casual, pero que es muy descriptiva.

Aunque no cubre todos los escenarios, y los detalles no se actualizan con la frecuencia suficiente para mantenerse al día con cada escenario, las descripciones son lo suficientemente estratégicas como para ser valiosas en la mayoría de las circunstancias.

El equipo de Cyber Crucible siempre valora las ideas de las publicaciones del NIST, y dedica tiempo en consecuencia.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf

---

Revision #1
Created 2026-07-24 01:40:43 UTC by Dennis Underwood
Updated 2026-07-24 01:40:43 UTC by Dennis Underwood