

Agente de Endpoint

- [Índice de versiones del agente de endpoint](#)

- [4.4.0.9](#)

- [4.4.0.9.1](#)

- [4.4.1.0](#)

- [4.4.1.1](#)

- [4.4.1.2](#)

- [4.4.1.3](#)

- [4.4.1.4](#)

- [4.4.2.0](#)

- [4.4.2.1](#)

- [4.4.2.2](#)

- [4.4.2.3](#)

- [4.4.2.4](#)

- [4.4.2.5](#)

- [4.4.2.6](#)

- [4.4.2.7](#)

- [4.4.2.8](#)

- [4.4.3.0](#)

- [4.4.3.2](#)

- [4.4.3.1](#)

- [4.4.4.0](#)

- [4.4.4.4](#)

- [4.4.5.1](#)

- [4.4.5.2](#)

- [4.4.5.3](#)

- [4.4.5.9](#)

- [4.4.5.8](#)

- [4.4.5.5](#)
- [4.4.5.6](#)
- [4.4.5.7](#)
- [4.4.5.4](#)
- [4.4.6.0](#)
- [4.4.6.1](#)
- [4.4.6.2](#)
- [4.4.6.3](#)
- [4.4.6.4](#)
- [4.4.7.0](#)
- [4.4.7.1](#)
- [4.4.7.3](#)
- [4.4.8.0](#)
- [4.4.8.1](#)
- [4.4.8.2](#)
- [4.4.9.0](#)
- [4.4.9.1](#)
- [4.4.9.2](#)
- [4.4.9.4](#)
- [4.5.0.0](#)
- [4.5.0.1](#)
- [4.5.0.2](#)
- [4.5.0.3](#)
- [4.5.1.0](#)
- [4.5.1.2](#)
- [4.5.2.1](#)
- [4.5.2.2](#)
- [4.5.3.0](#)
- [4.5.3.1](#)
- [4.5.3.2](#)

Índice de versiones del agente de endpoint

- [4.4.0.9](#)
- [4.4.0.9.1](#)
- [4.4.1.0](#)
- [4.4.1.1](#)
- [4.4.1.2](#)
- [4.4.1.3](#)
- [4.4.1.4](#)
- [4.4.2.0](#)
- [4.4.2.1](#)
- [4.4.2.2](#)
- [4.4.2.3](#)
- [4.4.2.4](#)
- [4.4.2.5](#)
- [4.4.2.6](#)
- [4.4.2.7](#)
- [4.4.2.8](#)
- [4.4.3.0](#)
- [4.4.3.1](#)
- [4.4.3.2](#)
- [4.4.4.0](#)
- [4.4.4.4](#)
- [4.4.5.1](#)
- [4.4.5.2](#)
- [4.4.5.3](#)
- [4.4.5.4](#)
- [4.4.5.5](#)
- [4.4.5.6](#)
- [4.4.5.7](#)

- [4.4.5.8](#)
- [4.4.5.9](#)
- [4.4.6.0](#)
- [4.4.6.1](#)
- [4.4.6.2](#)
- [4.4.6.3](#)
- [4.4.6.4](#)
- [4.4.7.0](#)
- [4.4.7.1](#)
- [4.4.7.3](#)
- [4.4.8.0](#)
- [4.4.8.1](#)
- [4.4.8.2](#)
- [4.4.9.0](#)
- [4.4.9.1](#)
- [4.4.9.2](#)
- [4.4.9.4](#)
- [4.5.0.0](#)
- [4.5.0.1](#)
- [4.5.0.2](#)
- [4.5.0.3](#)
- [4.5.1.0](#)
- [4.5.1.2](#)
- [4.5.2.1](#)
- [4.5.2.2](#)
- [4.5.3.0](#)

4.4.0.9

Funciones

- Para los grupos con telemetría habilitada, se agregaron datos de Active Directory a la lista de vigilancia de robo de credenciales

Correcciones

- Se eliminaron entradas duplicadas de volúmenes locales y recursos compartidos de red en algunos entornos.
- Se refinó el comportamiento para algunas reconstrucciones de bases de datos de miniaturas que causaban incidentes
- Se corrigió un error de validación de licencia que podía aumentar el tiempo de inicio
- Se refinó el comportamiento para el acceso a archivos en medios de escritura única, como CD y unidades de cinta WORM

Estado de validación WHCP/WHQL

Validado

Hashes MD5

```
service.exe    = c32c54381666cbd075fba2b1078b518b
assistant.exe  = 2e4266bf1527f384665f57dc979c4c79
CCRRSecMon.sys (Windows10)      = 35472ab324221af5fb459badb937f899
CCRRSecMon.sys (Windows8)       = 04132be3deb9dff52166f2dd39488874
CCRRSecMon.sys (Windows7)       = fc7f480d417d0bf650bef3e5770f49c2
```

4.4.0.9.1

Funciones

Ninguna - actualización de mantenimiento.

Correcciones

- Se corrigió el problema por el cual algunos recursos compartidos de red conectados por un usuario eran inicialmente ignorados en los análisis.
- Se refinó el comportamiento de falsos positivos asociado con recursos compartidos que aparecen durante las sesiones de usuario, seguidos rápidamente por un cuadro de diálogo Guardar como.

Estado de validación WHCP/WHQL

Validado.

Hashes MD5

```
service.exe    = 52e03ed57dab0fac936364899140af59
assistant.exe  = a90ad6f6544c2c3b2fb44bb57b70180b
CCRRSecMon.sys (Windows10)    = 6201b1a056d85c7576e4357e4ec9494e
CCRRSecMon.sys (Windows8)     = bd86ede6922503890f6d9b69871660e4
CCRRSecMon.sys (Windows7)     = ffcfbdda88faac6743b2de00c2cc4530
```

4.4.1.0

Funciones

- Soporte ampliado para el análisis de inyección de procesos, con el fin de aumentar drásticamente la precisión en la detección de intención maliciosa frente a benigna en aplicaciones.
 - Esto se volvió especialmente importante debido a que un pequeño número (<0.02%) de máquinas en la telemetría de Cyber Crucible generaba alertas por comportamientos agresivos de inyección de procesos en procesos del sistema.
- Mayor capacidad de monitoreo de procesos del sistema sin firmar.
 - Esto fue en parte una respuesta a que los atacantes se enfocan intensamente en involucrar esos procesos durante operaciones de movimiento lateral (dentro de un sistema y entre sistemas).

Correcciones

- Se modificó un comportamiento de modificación de archivos para reducir los falsos positivos, dejando de activarse ante ciertas acciones benignas, mediante contexto adicional a nivel de kernel sobre los comportamientos de acceso a archivos de un proceso.

Estado de validación WHCP/WHQL

Validado.

Hashes MD5

```
service.exe      = 0bab8404900c6a16ac3ad0293c45de5c
assistant.exe    = 98f013fd4fdb7325f903d07c87b999ac
CCRRSecMon.sys (Windows10)      = 452719399d9bb98dc6b14fb8787d8415
CCRRSecMon.sys (Windows8)       = a974c7cc46db3759a2da34f37caaa72e
```

CCRRSecMon.sys (Windows7)

= 6a0f2e55d6a7b66bd9bbe318d5dbbfb

4.4.1.1

Funciones

- Procesamiento analítico mejorado para relaciones padre-hijo, cuando el proceso padre finaliza rápidamente antes de que Cyber Crucible complete el procesamiento (milisegundos).
 - El escenario extremadamente común aquí es que los atacantes (y los programas legítimos) frecuentemente abren múltiples programas, a veces en una “cadena” de varios pasos. Esto puede ser intencional, o debido al comportamiento de Windows u otras aplicaciones “por debajo”.
 - Los modelos de comportamiento de Cyber Crucible aprovechan las variables de actividad y estado para todos los procesos en una cadena de ejecuciones para lograr la máxima precisión y contexto.

Correcciones

- Cyber Crucible tuvo una pérdida en la precisión de la toma de decisiones del modelo de comportamiento, debido a la pérdida de telemetría cuando múltiples programas se llaman entre sí, pero uno de los programas finalizó en milisegundos.
 - En una cadena donde el Programa A ejecuta el Programa B. El Programa B inicia el Programa C, pero el Programa B finaliza en milisegundos (generalmente un fallo silencioso, pero no siempre). El análisis de comportamiento de Cyber Crucible tiene las variables del Programa A y del Programa C, pero no tuvo tiempo de analizar completamente el Programa B, ya que esperaba que estuviera en ejecución.
 - Esto se ha corregido, lo que resulta en una toma de decisiones más precisa por parte del motor de toma de decisiones hiperautomatizado de Cyber Crucible.

Estado de Validación

WHCP/WHQL

Validado.

Hashes MD5

```
service.exe    = db76d0abc8f4bc4b2a093435bc314bde
assistant.exe  = a5bac35d839d7a57fccccfceb011083c1
CCRRSecMon.sys (Windows10)    = 935e43368fa95ae740a3f04defcc390d
CCRRSecMon.sys (Windows8)     = ee555ad0f282f36dd11deada8d1ca9c7
CCRRSecMon.sys (Windows7)     = a6a5073c6565361b443651ef29e49490
```

4.4.1.2

Características

- Mayor especificidad disponible para listas blancas, como la ruta y los argumentos del proceso principal.
- Soporte ampliado para análisis de acceso de identidad a más bases de datos de credenciales.
 - El acceso de identidad ahora también se supervisa para Slack, Opera, Thunderbird, Discord y Vivaldi.
- Soporte de lista blanca ampliado para incluir el acceso de identidad.

Correcciones

- Se redujo el ancho de banda utilizado entre los agentes y la API REST.
- Se corrigió un problema por el cual algunas ediciones más antiguas de Windows Server mostraban señuelos (canaries) en el Explorador.
- Se corrigió un problema por el cual algunos registros de acceso de identidad no incluían indicadores de confianza de certificado.

Estado de validación WHCP/WHQL

Validado

Hashes MD5

```
service.exe      = e289ef44c5a1bca39d57861ff9d05bee
assistant.exe    = d8e83309372b43ffc70feaf2bd538f36
CCRRSecMon.sys (Windows10)      = db736330f5a690a2e828472a357ee6b6
CCRRSecMon.sys (Windows8)       = b9d644930fc52495229dc7f96ffea299
CCRRSecMon.sys (Windows7)       = 7b1ece332986dadfcc6463574fd16616
```

4.4.1.3

Funciones

- El monitoreo de credenciales/identidad ahora incluye varias VPN, billeteras de criptomonedas y otras aplicaciones.
- En una cadena (esto es común) de procesos afectados durante un ataque (el atacante se mueve del programa en ejecución A, a B, a C, y D se utiliza para el robo de datos), el programa "paciente 0" A queda suspendido, pero el paciente D se reporta como el proceso que realiza el comportamiento de robo.
 - El estado de la memoria se preserva y se reporta a lo largo de las cadenas de procesos, para un futuro análisis forense.
- En caso de una respuesta automatizada en la que se haya modificado la memoria de un proceso en ejecución, dicha modificación de memoria se sube de forma configurable a Cyber Crucible para su ingeniería inversa y análisis adicional.
- En caso de un error de modificación de memoria no malicioso en una aplicación, las excepciones de comportamiento ("listas blancas") ahora tienen la capacidad de marcar ciertos eventos de corrupción de memoria como benignos. Esto no evitará que el propio programa se bloquee o pierda datos debido al error, pero Cyber Crucible sabrá ignorar el error mientras busca la inyección maliciosa de código en procesos en ejecución (inyección de procesos/hollowing).

Correcciones

- Se eliminó una vulnerabilidad por la cual los binarios podían ser eliminados por un proceso con privilegios mientras los binarios de CC se estaban actualizando.
- Se eliminó una vulnerabilidad por la cual las claves de registro podían ser eliminadas o alteradas por un proceso con privilegios mientras los binarios de CC se estaban actualizando.
- Se corrigió el seguimiento del estado de la memoria cuando un proceso se parchea en memoria durante la evaluación de la memoria por parte de Cyber Crucible.
- Se corrigió el seguimiento del estado de la memoria en determinadas condiciones en las que la memoria se reasigna entre páginas de memoria.
- Actualizaciones menores de eficiencia de la CPU, probablemente demasiado pequeñas para registrarse en el Administrador de tareas, ya que el uso normalmente es <1%

Estado de validación WHCP/WHQL

Validado

Hashes MD5

```
service.exe    = 90a6ca2f5b7a76b847052f3d420f0c9b
assistant.exe  = b62ee623f74171f4a3f34ff129188174
CCRRSecMon.sys (Windows10)      = dfdce4016f6920e844615b3d506ec2e2
CCRRSecMon.sys (Windows8)       = 59bbd41c883ca0205fd3adbfd5dbb5dbb6
CCRRSecMon.sys (Windows7)       = 88e6f047f7fa26e717a24f5fd7b33dc5
```

4.4.1.3.1

Se obtuvo visibilidad sobre algunos procesos del sistema que se inician antes de que se cargue el controlador de Cyber Crucible.

Hashes MD5:

```
service.exe: a03b91df83f86ffe322f7b16960f503c
assistant.exe: e22641924d3a1811b86a0f4357f74720
win7/CCRRSecMon.sys: b64b63c04f00afd1020a7a43fc0bb67d
win8/CCRRSecMon.sys: c50aacb4aac6ac9f1e95e4ffa749cb2a
win10/CCRRSecMon.sys: 77dd029b8e4b2cf5a2354787402ecc17
```

4.4.1.3.2

Se agregó telemetría adicional para los procesos del sistema ahora visibles debido a 4.4.1.3.1.

Hashes MD5:

```
service.exe: 47f408d6102eb06a94f2244cf139a0a5
assistant.exe: 86733da51ee703f93dcda9346231cca6
```

```
win7/CCRRSecMon.sys: b01e8933fa9ac9f0a049527b20d9f679
win8/CCRRSecMon.sys: 4467124cf7e8b5ab5652169f9eb41663
win10/CCRRSecMon.sys: 8f06de95303eeac038002ec27c297811
```

4.4.1.3.3

Se corrigieron algunos reportes de incidentes que incluían datos del proceso incorrecto, cuando un proceso finaliza a mitad de un cálculo.

Hashes MD5:

```
service.exe: f2a341ca4856ab3f8a15b7cf725cd0cc
assistant.exe: 5d5d2213e276bc066f4d42ab751c7317
win7/CCRRSecMon.sys: 13da73b66751d12f5f3e65cde0602266
win8/CCRRSecMon.sys: 08fe8cb3391c9215bc37a997ec59b0a2
win10/CCRRSecMon.sys: 4c8a1707839f0d28c386f17ce2dbc8ed
```

4.4.1.3.4

Optimización de los cálculos de memoria, en preparación para la 4.4.1.4.

Hashes MD5:

```
service.exe    = 4a5bd9822ea28c10f399afe437837a2a
assistant.exe  = 7070e61862bc2ede3205c4bfdc6805d2
CCRRSecMon.sys (Windows10)    = 4e9b790522fe61e9206140e15e37b7fe
CCRRSecMon.sys (Windows8)     = 7b477503840f882028ff8bdbbfc72121
CCRRSecMon.sys (Windows7)     = 65e95b4dd58cb1c9a5dab398155e2113
```

4.4.1.4

Funciones

- Capacidades de coincidencia de patrones mejoradas en el modelo de comportamiento.
 - Esto es especialmente relevante para la cobertura adicional de ubicaciones de almacenes de identidad, como las ubicaciones de billeteras de criptomonedas.
- Funcionalidad de dependencia de software incrementada para las bibliotecas (de Cyber Crucible) en uso para la próxima protección de acceso a identidades totalmente automatizada.
- Capacidad opcional para ejecutar el agente en modo seguro

Correcciones

- Se optimizó el uso de memoria en el servicio. Esto solo se habría experimentado en servidores muy ocupados con mucho análisis de comportamiento en curso (por parte de Cyber Crucible) simultáneamente.

Hashes MD5

```
service.exe    = 1cb8e19fc9ed2788189684f23693087a
assistant.exe  = c60e851d9836955b078474270e04d0c1
CCRRSecMon.sys (Windows7)      = 3b7656b24a0e2387389f0ce9db375379
CCRRSecMon.sys (Windows8)      = 204689e666bb704621ebbd5d606a1274
CCRRSecMon.sys (Windows10)     = f9839b8b2437a3a7b6a099d2598dc639
```

4.4.2.0

Características

- Capacidades de monitoreo y prevención mejoradas para la protección automatizada del acceso a identidades.
- Optimización del uso de la red mediante tasas de comunicación variables según el comportamiento del cliente.

Correcciones

- N/A

Hashes MD5

```
service.exe    = 408d8ae9e35ee65c8e208cfa76c67df6
assistant.exe  = 8ba7fa2a201ae92f595e85e4cf52b804
CCRRSecMon.sys (Windows7)      = 359ff6e23107798fd01a3afb33716f78
CCRRSecMon.sys (Windows8)      = 2bd4267eeea697a137447d91a8b38e1c
CCRRSecMon.sys (Windows10)     = fcf979529c13eba5f93bf6c6d0096d6f
```


4.4.2.1

Correcciones

- Se optimizó el seguimiento de información de identidad para aplicaciones con un gran número de directorios profundamente anidados.

Hashes MD5

```
service.exe    = 9c6474e44959e8eba54876c46e13fb25
assistant.exe  = 03d671ffa567ac8dc783ce905d624351
CCRRSecMon.sys (Windows7)      = 5fbd3b4a9066299c9ce3d619dc6fca17
CCRRSecMon.sys (Windows8)      = 0ee960548846da463d4c66381dea0841
CCRRSecMon.sys (Windows10)     = bda977682effcd61e6d478da750c966b
```

4.4.2.2

Funciones

- Ninguna

Correcciones

- Optimización del manejo de variables para un tipo de comportamiento.
 - Causa: Un producto de seguridad no especificado generó una cantidad muy grande de comportamientos en un par de servidores grandes, lo que provocó un uso excesivo de memoria por parte de Cyber Crucible.
 - Síntomas: El uso de memoria de Cyber Crucible aumenta de unos pocos MB a GB. El uso de memoria del producto de seguridad también aumentó 100 veces, hasta superar los 250 GB. Si experimenta esto, dado que podría ser independiente de Cyber Crucible, por favor abra un ticket de soporte para que podamos ayudarlo. Sospechamos que esto también fue un problema del producto de seguridad, independiente de la optimización de Cyber Crucible.
 - Corrección: Este seguimiento de la variable de comportamiento se migró de un algoritmo que esperaba una población de bajo volumen a un algoritmo de alto volumen, similar al utilizado en otras partes del controlador.
 - ¿Quién se ve afectado? Solo se observó este problema en un cliente, y únicamente en una pequeña parte de sus servidores grandes. De todos modos, esta actualización se implementa para todos los clientes.

Hashes MD5

```
service.exe    = bbf0bf47d942d30438a260b497c04cd
assistant.exe  = 280d746ed3edea9b7267955a94b97a8e
CCRRSecMon.sys (Windows7)      = cded2aaa7dd0c2fe446694451bd17960
CCRRSecMon.sys (Windows8)      = a06dce5e19627fe1f982cbde632fc313
CCRRSecMon.sys (Windows10)     = 14e0c4e7f86405562701187fac93aea2
```

4.4.2.3

Funciones

- Ninguna

Correcciones

- Se corrigieron problemas de compatibilidad con Acronis

Hashes MD5

```
service.exe    = 4747ae6372a0f3a410c145e64314123c
assistant.exe  = f7c0ac0044a3b186d2f6db2a8a1989f0
CCRRSecMon.sys (Windows10)      = f69661a61bb9364d6f25f5f4b410729c
CCRRSecMon.sys (Windows8)       = 25b496529282e6c973b53a14a94a3480
CCRRSecMon.sys (Windows7)       = ca9ee3cde474ea3b6b5b61b8bc26f170
```

4.4.2.4

Características

- Compatibilidad de protección de credenciales para Microsoft Teams y Signal Messenger

Correcciones

- Se suprimieron los registros relacionados con la red cuando se está en modo seguro sin redes
- Se realiza una copia de seguridad de algunos datos del agente al desinstalar, en la carpeta de almacenamiento temporal de Windows

Hashes MD5

```
service.exe    = 23735f3ca870b1d70017c433d5e24d17
assistant.exe  = 57d8742b1bbc27b73dd134fb3ac6ebc2
CCRRSecMon.sys (Windows8)      = 99262ee4a93e4751adb8b4b1ef2102ce
CCRRSecMon.sys (Windows10)     = 0f2809c32a22af2eda0fe606c361d6d2
CCRRSecMon.sys (Windows7)     = 0d73a497bebfad7b85441ae981ed4be1
```

4.4.2.5

Características

- Ninguna

Correcciones

- Reducción del uso de red al enviar grandes cantidades de informes a la vez
- Corrección en el manejo de algunos datos de certificados

Hashes MD5

```
service.exe    = a54087913a6ddd451853ffce64112e21
assistant.exe  = 14859d6c32192a073c0518b0d3e957ee
CCRRSecMon.sys (Windows8)      = 99262ee4a93e4751adb8b4b1ef2102ce
CCRRSecMon.sys (Windows10)     = 0f2809c32a22af2eda0fe606c361d6d2
CCRRSecMon.sys (Windows7)      = 0d73a497bebfad7b85441ae981ed4be1
```

4.4.2.6

Características

- Ninguna

Correcciones

- Reducción del uso de memoria en servidores con muchos certificados de programa únicos

Hashes MD5

```
service.exe    = c7afcb665f6849d39430df2271703cd6
assistant.exe  = d6ed1b6f2d6d914e9bb08396a3d03a57
CCRRSecMon.sys (Windows8)      = 1a399a22cecdca9b5ffefe69a211fc66
CCRRSecMon.sys (Windows7)      = 57363998c02e1334f6fda931c6c194ba
CCRRSecMon.sys (Windows10)     = d15ddd4035830b80a67e9057456560c2
```

4.4.2.7

Características

- Ninguna

Correcciones

- Se redujo el uso de memoria durante el manejo de programas que utilizan un comportamiento indefinido al consultar directorios

Hashes MD5

```
service.exe    = 7bf08deada69a09e2c0362337554c124
assistant.exe  = ced782e4c6793e4b8a2ec2d4580b90f8
CCRRSecMon.sys (Windows10)    = 1eea1da529c0251a5438a0169ace53b7
CCRRSecMon.sys (Windows7)     = f82d5fbe2b22b70158dbbfb57949e948
CCRRSecMon.sys (Windows8)     = 9ff7406c41c583337357163a8dd8aeb2
```

4.4.2.8

Características

- Ninguna

Correcciones

- Aumento del registro y la telemetría para estados de máquina defectuosos
- Aumento de la estabilidad de las protecciones de identidad en el momento del arranque

Hashes MD5

```
service.exe    = 5f33211e1c36f31439a9d5efb8e7b029
assistant.exe  = ced782e4c6793e4b8a2ec2d4580b90f8
CCRRSecMon.sys (Windows10) = 49c474f127041672509d31f013653259
CCRRSecMon.sys (Windows7)  = 411f80c24854874d81b80a7d7af03ac9
CCRRSecMon.sys (Windows8)  = fac1a12c4d1bbebd1e7ed1c21bf9fc2f
```


4.4.3.0

Características

- Además de las protecciones de servicio existentes, el controlador en modo kernel reiniciará el servicio si este se detiene por cualquier motivo.

Correcciones

- Ninguna

Hashes MD5

```
service.exe    = 65c8d59a22f376a8918347166def50a3
assistant.exe  = ced782e4c6793e4b8a2ec2d4580b90f8
CCRRSecMon.sys (Windows7)      = 3a336be46b11c5875dda0e94340eb62a
CCRRSecMon.sys (Windows8)      = 8ddef1c798f94931ef8131674ad9ebf6
CCRRSecMon.sys (Windows10)     = 9fb3336a3c1990be3a1c4c3fdd8c53e2
```

4.4.3.2

Características

- Ninguna

Correcciones

- Se redujo el uso de CPU durante el inicio de procesos.
- Se redujo el uso de CPU en las determinaciones de confianza durante consultas consecutivas de directorios.

Hashes MD5

```
service.exe    = ale5c45b87f914343c772c05e18b153e
CCRRSecMon.sys (Windows7)      = c995f7efeb88ef42425cf54b0b210dc7
CCRRSecMon.sys (Windows8)      = 3135a7787076286f3e8d82ca384582e9
CCRRSecMon.sys (Windows10)     = 0f6be8ec8806d4acabb8d03904c1b148
```

4.4.3.1

Características

- Ninguna

Correcciones

- Se corrigió un problema en algunas máquinas con características de instalación de Windows inusuales que presentaban canarios visibles en el Explorador.

Hashes MD5

```
service.exe      = b2a62cc2285afe01a28f4859afc03511
CCRRSecMon.sys (Windows7)      = 16b9d8946189feb7d620351a4d9c6a9f
CCRRSecMon.sys (Windows8)      = 24f55af4414447ec46f450eeca35c92e
CCRRSecMon.sys (Windows10)     = 2305ebd13864355ef384099dae1bee57
```

4.4.4.0

Funciones

- Los informes de incidentes y telemetría se almacenan en disco para escenarios sin conexión.
 - Debido a los intentos de manipulación observados contra múltiples almacenes de registro de EDR/XDR, Cyber Crucible habilitó la protección a nivel de kernel para los datos almacenados en disco antes de implementar esta capacidad.
- Mayor protección del proceso de servicio utilizado para la comunicación y las actualizaciones de backend, como parte del endurecimiento de confianza cero anticipatorio.
 - Esto no fue en respuesta a una amenaza existente, sino de forma proactiva ante una que el Equipo prevé próximamente.

Correcciones

- Se corrigieron los procesos que se cargan al arrancar y que no estaban disponibles en el panel bajo creaciones de procesos.
- Se impidió que dos instaladores se ejecutaran al mismo tiempo, lo cual registraría el mismo equipo dos veces.

Hashes MD5

service.exe	= 116dab615aab07d804667b13ecfe821a
CCRRSecMon.sys (Windows7)	= db358b3d6e784d11827ff899722e3070
CCRRSecMon.sys (Windows8)	= a95dd87d2ea9944e8643de787f11d71c
CCRRSecMon.sys (Windows10)	= 6eb017a5cb3a9dd45bc065b466fb4789

4.4.4.4

Características

- Ninguna

Correcciones

- Rendimiento mejorado para el análisis de datos de certificados durante el inicio del sistema.

Hashes MD5

```
service.exe      = 69395e14240c91bc4df73168615927d9
CCRRSecMon.sys (Windows7)      = 2dd89c52e5a2914289371d4c3fd80ef8
CCRRSecMon.sys (Windows8)      = 41f25ea44e1f1a6ba11c7e7181554467
CCRRSecMon.sys (Windows10)     = ecc7f1f0a1d63f801a3a84f7b52b850c
```

4.4.5.1

Características

- Reducción del uso de ancho de banda:
 - Uso de compresión para datos de telemetría más grandes y respuestas del servidor más grandes
 - Uso de HTTP/2 para encabezados comprimidos y mayor eficiencia de sockets
- Mayor visibilidad de las operaciones de certificados.

Correcciones

- Codificación de los metadatos del certificado en la telemetría sin procesar cuando existen etiquetas no conformes con RFC. La infraestructura de seguridad de red estaba corrompiendo o eliminando las cargas útiles, lo que provocaba que el agente retransmitiera hasta lograr el éxito.

Hashes MD5

```
service.exe      = 686e91ca0f1bab7a0f3b09d2052d7e4c
CCRRSecMon.sys (Windows7)      = 25c194ee5f3c4ef25ef86124303aec82
CCRRSecMon.sys (Windows8)      = 6b4b8b6cc960a718464fd3ebb89b1fe8
CCRRSecMon.sys (Windows10)     = 8c668fe57652530d77d323b8563d3f4e
```

4.4.5.2

Características

- Nueva telemetría de acceso a nivel de kernel para comportamientos basados en red, con el fin de identificar mejor posibles errores de red del lado del cliente, u oportunidades de optimización
- La telemetría saliente ahora se agrupa y se envía en conjunto, al igual que la configuración entrante
 - Transmitida con una variación de tiempo del 25%, para que no todas las máquinas envíen paquetes simultáneamente a través de una red de clientes
- HTTP/2 ahora se utiliza completamente de extremo a extremo

Correcciones

- Se redujo el número mínimo de subprocesos en uso en el espacio de usuario
- Se redujo el uso de CPU para el servicio de espacio de usuario
- La autenticación Agente-Servidor ahora se realiza de manera más eficiente
- Se reemplazó el algoritmo anterior de suspensión <> reinicio del servicio cuando las licencias no estaban disponibles.
 - El algoritmo anterior causaba un "el servicio finalizó inesperadamente" en el administrador de eventos cada 15 minutos.
 - Permitir que el sistema operativo indique al servicio que se apague (algo que ha sido explotado por delincuentes y otras herramientas de seguridad) habría permitido un reinicio "limpio" del servicio sin registros en el administrador de eventos. En lugar de crear esa vulnerabilidad, el servicio de Cyber Crucible se reinició por sí mismo sin la intervención de Windows, provocando el registro de eventos.

Hashes MD5

```
service.exe = b17a2a528a4424771fdeca8559b9f56b
CCRRSecMon.sys (Windows7) = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8) = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10) = 0d1fc32fba2cb878ce8cb0f549b8d167
```

4.4.5.3

Características

- Se agregó un segundo dominio para la comunicación con el servidor ([vea la lista de dominios aquí](#)).
 - Si hay problemas de comunicación con un dominio, el agente cambiará automáticamente al otro.

Correcciones

- Se cambiaron algunas cadenas antiguas heredadas que hacían referencia a “Ransomware Rewind” para que ahora hagan referencia a “Cyber Crucible”.

Hashes MD5

```
service.exe = 8cf710b96d15ec9ff0b88bba12dcd142
CCRRSecMon.sys (Windows7) = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8) = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10) = 0d1fc32fba2cb878ce8cb0f549b8d167
```


4.4.5.9

Funciones

- Se ha aumentado el endurecimiento de partes de la funcionalidad previamente realizada por las bibliotecas de criptografía de Windows, las cuales ahora son gestionadas por el controlador del kernel de Cyber Crucible.
 - Esto incluye tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.
- Este es un lanzamiento importante (milestone) respecto a los lanzamientos incrementales encontrados en 4.4.5.4 - 4.4.5.8, todos alineados con la funcionalidad de endurecimiento de análisis criptográfico anterior.
 - La telemetría inicial indica que los fallos en las bibliotecas de certificados y criptografía de Windows fueron respondidos legítimamente por Cyber Crucible.
 - En este momento se desconoce qué porcentaje de los problemas se debió a explotación frente a un error en la biblioteca central de Windows. Póngase en contacto con su representante de Cyber Crucible para conversar más al respecto según sea necesario.

Correcciones

- Se corrigieron algunos informes de procesos que indicaban incorrectamente el certificado listado como “no confiable”, debido a una pérdida de funcionalidad en la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe = 79650eea0a93b8f480b4247d57ddd03b
CCRRSecMon.sys (Windows7) = 06a647c897f9f385416482a4e899e204
CCRRSecMon.sys (Windows8) = 72c1b462e3e8e3fa4dcf6344ce3b0acd
CCRRSecMon.sys (Windows10) = 02b1c53268059ae38427fe43152d593c
```

4.4.5.8

Funciones

- Se incrementó el endurecimiento (hardening) de partes de la funcionalidad previamente realizada por las bibliotecas de criptografía de Windows, las cuales ahora son realizadas por el controlador (driver) de kernel de Cyber Crucible.
 - Esto incluye tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió un problema por el cual algunos informes de procesos indicaban incorrectamente que el certificado listado no era “de confianza”, debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe = d8187cf4468cba634470772fe8e7ba8b
CCRRSecMon.sys (Windows7) = b97b6bc79529be5ccd88807892e16153
CCRRSecMon.sys (Windows8) = 6a6b5801b5a4552a4be8477d74706198
CCRRSecMon.sys (Windows10) = 4f3e54c2a9d348b0279767bc03420c99
```

4.4.5.5

Funcionalidades

- Mayor fortalecimiento de partes de la funcionalidad previamente realizadas por las bibliotecas de criptografía de Windows, ahora realizadas por el controlador del kernel de Cyber Crucible.
 - Esto constituye tanto un fortalecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió el hecho de que algunos informes de procesos indicaban incorrectamente que el certificado listado era “no confiable”, debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe = 90525bbf61ae57bd5e61f79198ae031f
CCRRSecMon.sys (Windows7) = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8) = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10) = 0d1fc32fba2cb878ce8cb0f549b8d167
```

4.4.5.6

Funciones

- Se ha aumentado el endurecimiento de partes de la funcionalidad previamente realizadas por las bibliotecas de criptografía de Windows, las cuales ahora son realizadas por el controlador del kernel de Cyber Crucible.
 - Esto incluye tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió un problema por el cual algunos informes de procesos indicaban incorrectamente que el certificado listado era “no confiable”, debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe = 60c0b7b7d00dc14415334ddef590f593
CCRRSecMon.sys (Windows7) = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8) = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10) = 0d1fc32fba2cb878ce8cb0f549b8d167
```

4.4.5.7

Funcionalidades

- Se ha incrementado el endurecimiento de partes de la funcionalidad anteriormente realizada por las bibliotecas de criptografía de Windows, las cuales ahora son gestionadas por el controlador del núcleo de Cyber Crucible.
 - Esto representa tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió un problema por el cual algunos informes de procesos indicaban incorrectamente que el certificado listado no era de confianza (“not trusted”), debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe = c97ce96b69c0be846af70c2359671e22
CCRRSecMon.sys (Windows7) = 475915b1881add45c6af260f82bd43b9
CCRRSecMon.sys (Windows8) = dfc09e7504b4aa73ecfb15e62f8cde86
CCRRSecMon.sys (Windows10) = 5581c7c11aa52488a1858fa728cfaf46
```

4.4.5.4

Características

- Se ha aumentado el endurecimiento de partes de la funcionalidad anteriormente realizada por las bibliotecas de criptografía de Windows, las cuales ahora son realizadas por el controlador del kernel de Cyber Crucible.
 - Esto incluye tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió un problema por el cual algunos informes de procesos indicaban incorrectamente que el certificado listado no era de confianza (“not trusted”), debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe = fd2157d8dee1d07ec45406a1d323359c
CCRRSecMon.sys (Windows7) = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8) = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10) = 0d1fc32fba2cb878ce8cb0f549b8d167
```

4.4.6.0

Funciones

- Mejora del rendimiento de la CPU para algunas aplicaciones que generan grandes cantidades de recorridos de directorios automatizados y simultáneos como parte del comportamiento de sus aplicaciones.

Correcciones

.

Hashes MD5

```
service.exe = 3e443b55efdf1c1fd10a2b2931aa1bfd  
CCRRSecMon.sys (Windows7) = eb992a496b88874e59d71f8ad83ba917  
CCRRSecMon.sys (Windows8) = 2e9786c84a55911e1b94aec38b4a90ff  
CCRRSecMon.sys (Windows10) = c68c4d4ba3f2e42953e6550b5e7c0b47
```

4.4.6.1

Funcionalidades

- Continuación de la migración del nombre de producto “Ransomware Rewind” a “Cyber Crucible”.
 - El nombre del servicio heredado "Ransomware Rewind" migrará a "CyberCrucibleAgent". El nombre del proceso permanece igual.
 - La clave de registro en HKLM\SOFTWARE migrará de la heredada RansomwareRewind a la actual CyberCrucibleAgent.

Correcciones

- Se corrigió que algunos procesos de 32 bits se activaran como si tuvieran “memoria modificada” cuando la imagen del proceso alcanza el tamaño máximo permitido para un proceso de 32 bits.

Hashes MD5

```
service.exe = 51ff73ab3caac8d269d1fad823de9f60
CCRRSecMon.sys (Windows7) = 6014b3fa07cec7e39753f7eaea4d1ea7
CCRRSecMon.sys (Windows8) = 26756d6394a70482952519c104730676
CCRRSecMon.sys (Windows10) = 8665c9f7b99b385acaecc11d42fda468
```


4.4.6.2

Funciones

- Se agregaron indicadores opcionales de “tipo de acceso” expuestos a los usuarios finales para mayor especificidad de acceso conductual.

Correcciones

- Ninguna.

Hashes MD5

```
service.exe = 07a709d672f38ea466de675b8c8f1b76
CCRRSecMon.sys (Windows7) = 4d9195aeda4ae5dafb6f27405b541d9a
CCRRSecMon.sys (Windows8) = 12deea5a512128e62aba173c2f786387
CCRRSecMon.sys (Windows10) = 39daf75dd7678ae2b83a5f79aeab3b68
```

4.4.6.3

Características

- Se agregó compatibilidad opcional con proxy SOCKS5 para ayudar en la implementación del agente.

Correcciones

- Se corrigieron las reinstalaciones desde agentes anteriores que utilizaban un ID de instalación incorrecto.
- Se corrigió que las instalaciones existentes provenientes de instaladores anteriores tuvieran una ruta de servicio sin comillas.

Hashes MD5

```
service.exe = 610b75a1a4fc7460138f545751cc7606
CCRRSecMon.sys (Windows7) = 4d9195aeda4ae5dafb6f27405b541d9a
CCRRSecMon.sys (Windows8) = 12deea5a512128e62aba173c2f786387
CCRRSecMon.sys (Windows10) = 39daf75dd7678ae2b83a5f79aeab3b68
```

4.4.6.4

Características

- La información de memoria del proceso principal está disponible para los informes de procesos cuando se detectaron modificaciones.

Mejoras

- Se modificaron algunas frecuencias de comunicación con el servidor para que ya no requieran reinicio para su ajuste.

Correcciones

Ninguna en esta versión.

Hashes MD5

```
service.exe = 608ab69e92f5592a3da66801edaafd0e
CCRRSecMon.sys (Windows7) = 090b0b8decd4634797de4acf3aef05ae
CCRRSecMon.sys (Windows8) = d993e733702bc810de9139965850e210
CCRRSecMon.sys (Windows10) = 65a48c062156b4723894783fa9115204
```

4.4.7.0

Características

- Inicio de la implementación de comunicaciones HTTPS basadas en JWE.
 - Las claves de cifrado son únicas para cada agente.
 - Todas las cargas útiles cifradas bajo el HTTPS. Deshabilitado de forma predeterminada durante la implementación inicial.
 - Capacidad de revertir opcionalmente de HTTPS cifrado con JWE a HTTPS no cifrado si las cargas útiles con formato JWE no se transmiten correctamente.

Hashes MD5

```
service.exe = 581a528318644c55d9dc6d552fb295c0
CCRRSecMon.sys (Windows7) = 629e77591a672915021842a9f5271157
CCRRSecMon.sys (Windows8) = 3f499538502e0b7c4fe956eb7b4bd0ab
CCRRSecMon.sys (Windows10) = 0f7db98f84a6f67aac02dd4eb2dbd547
```

4.4.7.1

Características

- Más telemetría para creaciones de procesos e incidentes
 - SID de usuario
 - Nombre de inicio de sesión de nivel inferior del usuario
 - Si el proceso está elevado o no (Ejecutar como administrador)
- Los incidentes ahora informan dónde ocurrió el acceso iterativo a datos

Correcciones

- Reducción del uso de memoria durante períodos de problemas de conectividad con el servidor y de gran volumen de telemetría simultánea
- Reducción del uso de memoria durante la generación de informes de incidentes

Hashes MD5

```
service.exe = 0df0b7d76abd0978734ac961cd4cddaf
CCRRSecMon.sys (Windows7) = dced5933e7b3e720a72160eb32cd83cb
CCRRSecMon.sys (Windows8) = e14aa1324a9a42958cd955b9fffd4f79
CCRRSecMon.sys (Windows10) = 9d2edcf2288e7563892dac6300517102
```

4.4.7.3

Características

- Modo DMZ
 - Configuración opcional para utilizar un paquete de CA firmado para la comunicación TLS con los servidores de autenticación y telemetría. Estos paquetes de CA quedan protegidos contra manipulación o eliminación mediante las capacidades antimanipulación propietarias de Cyber Crucible.
 - Las comprobaciones OCSP y CRL están deshabilitadas para reducir la lista de dominios que deben permitirse a través de un firewall.

Correcciones

- Se redujo el uso de memoria y el tiempo de CPU dedicado al envío de diferencias de memoria (memory diff), especialmente después de períodos prolongados sin conexión.

Hashes MD5

```
service.exe = 536adc06bd5ac3d4caca53dd5b780759
CCRRSecMon.sys (Windows7) = dc446d663e8c865b039de0eb585de1fb
CCRRSecMon.sys (Windows8) = ea96fdf4b097ac9afb646e6a766431aa
CCRRSecMon.sys (Windows10) = 434c9061390804e4e61f5299158aaa00
```

4.4.8.0

Características

- Telemetría de Authenticode en modo kernel
 - Para aumentar la velocidad y la fiabilidad, los datos de certificados para las creaciones de procesos e incidentes serán registrados únicamente por el controlador.
 - Esta actualización no elimina las dependencias de las bibliotecas de criptografía de Windows, pero realiza los cálculos criptográficos en paralelo. Eventualmente, la dependencia de Windows podría eliminarse por completo.

Correcciones

- Reducción del uso de memoria y del tiempo de CPU dedicado a los intentos de envío de eventos cuando se está sin conexión, durante los cuales la telemetría se almacena de forma segura hasta que el equipo recupera la conectividad con los servidores de Cyber Crucible.
- Algunos instaladores de controladores de Nvidia consideraban que no tenían privilegios para instalarse debido al uso de una función interna del kernel de Microsoft para intentar acceder a los archivos instalados de Cyber Crucible.
- Se corrigió una incompatibilidad entre el modo JWE y el modo DMZ

Hashes MD5

```
service.exe = 5189fe49a1bfade50766fce2a1980eef
CCRRSecMon.sys (Windows7) = 342dd1bbe5f5dfcffe7752b74b34a9e8
CCRRSecMon.sys (Windows8) = a20c9cca59be651db7ae69f9f1f64cf2
CCRRSecMon.sys (Windows10) = a3cf6860d3f059a1ab38ee7b2d82b097
```

4.4.8.1

Características

- Los metadatos ejecutables, como la versión del producto, el nombre de la empresa, etc., para los procesos en memoria son informados por el controlador mediante visibilidad a nivel de kernel. La funcionalidad normal es utilizar llamadas a la API de Windows en espacio de usuario. Este cambio hacia el análisis en el kernel elimina la oportunidad (observada) de que los atacantes manipulen la información del proceso.
- La información de autenticación del agente se replica en otra parte del sistema para poder restaurarla en caso de que el registro sea corrompido por un controlador malicioso.

Mejoras

- Los errores de conexión al servidor son registrados de forma mínima por el agente, reduciendo el tamaño del registro en disco.

Correcciones

- N/A

Hashes MD5

```
service.exe = 8c1f6999ccd176193e493686216f14c6
CCRRSecMon.sys (Windows7) = 3b032d0e43674509126c6cb1c9efd688
CCRRSecMon.sys (Windows8) = d3131131c83c2cf833ebc2157149c364
CCRRSecMon.sys (Windows10) = eac8a8b38a8743a13dd7130509de9907
```


4.4.8.2

Funciones

- Se agregó soporte para un icono opcional en la bandeja del sistema. Esta función está deshabilitada de forma predeterminada.

Correcciones

- Se agregó una solución alternativa para un problema relacionado con las solicitudes de hashing de la API de Windows del kernel. Esta solución alternativa podría eliminarse en algún momento en el futuro si se corrige el problema de Windows, posiblemente en la próxima actualización del kernel.

Hashes MD5

```
service.exe = 6e21b0a7c41b156f2001c93bbcd142de
CCRRSecMon.sys (Windows7) = 43cce21323465eac015fc7c90b88ac87
CCRRSecMon.sys (Windows8) = c7b2d8d130f8c3e768891ad0b20931a5
CCRRSecMon.sys (Windows10) = d95d162bc7f87f3eaeef46d58eb543364
```

4.4.9.0

Características

- Telemetría de DLL en modo kernel
 - Análisis de certificados y cálculo de confianza para todas las DLL cargadas en el controlador.

Correcciones

- Ninguna.

Hashes MD5

```
service.exe = f4e017fab1f1117859bcfcd4733cc439
CCRRSecMon.sys (Windows7) = 976f8826ebd5bacb1803fcf6d274a6d0
CCRRSecMon.sys (Windows8) = 90f02751eca65f6286b3676ea8b2bb2c
CCRRSecMon.sys (Windows10) = af9c0469fb05a0104579d8fb1694719e
```

4.4.9.1

Funciones

- Ninguna.

Correcciones

- Se aumentó la cantidad de telemetría gestionada a la vez por el servicio para los datos de creación e inyección.
- Se ajustó el orden de los canarios para programas que utilizan métodos inusuales de iteración de archivos.
- Se ajustó la ACL en algunos canarios para adaptarse mejor a los sistemas de archivos reales.

Hashes MD5

```
service.exe = 5728b771c4b89d47942043fece634be9
CCRRSecMon.sys (Windows7) = fd1b9163edfcfa66370a0510286de6bf
CCRRSecMon.sys (Windows8) = c7bf417fdd2f2f0fdec9a9011913b672
CCRRSecMon.sys (Windows10) = 22066d3fcf90b3a0e672a41d8fe787d8
```

4.4.9.2

Funciones

- Seguimiento de modificaciones de memoria para DLL cargadas.
- Generación de diferencias de memoria (memory diff) para DLL modificadas.

Correcciones

- Se solucionó un problema por el cual algunas DLL no conformes generaban resultados incorrectos de hash de authenticode.

Hashes MD5

```
service.exe = 7b76a84809347d1caa4f46217d7c02ad
CCRRSecMon.sys (Windows7) = 27cc77a22706f1f007f0c8f433910efd
CCRRSecMon.sys (Windows8) = d94978e73452be5869b194fe234fc125
CCRRSecMon.sys (Windows10) = c321cf4abafbd8f2b6d3ef1917904d57
```

4.4.9.4

Correcciones

- Los archivos de volcado del servicio ahora están limitados a 10 por combinación de versión + subproceso.

Hashes MD5

service.exe	=	TBD
CCRRSecMon.sys (Windows7)	=	27cc77a22706f1f007f0c8f433910efd
CCRRSecMon.sys (Windows8)	=	d94978e73452be5869b194fe234fc125
CCRRSecMon.sys (Windows10)	=	c321cf4abafbd8f2b6d3ef1917904d57

4.5.0.0

Características

- Firewall de Kernel con IA
- Mejoras de velocidad en el cálculo de hash Authenticode
- Uso de memoria significativamente reducido para la telemetría de DLL
- Mayor visibilidad de las modificaciones de memoria en las DLL

Correcciones

- Corrección de la compatibilidad de recuperación del servicio con 24H2

Hashes MD5

service.exe	=	2a01dc8267e6bbae3c42c0f0d873286f
CCRRSecMon.sys (Windows7)	=	502b85e17a7103a35d5b6eb50ce0eea7
CCRRSecMon.sys (Windows8)	=	65c315313330c83f602d19e031d99f67
CCRRSecMon.sys (Windows10)	=	d17ba3cde6c2051d85dea395891caff9

4.5.0.1

Características

- Opción para migrar al dominio del servidor de autenticación OAuth alojado
- Tarea para configurar dinámicamente las URL de los servidores REST y OAuth

Correcciones

- Ninguna.

Hashes MD5

```
service.exe = 171e15eb5bf2a8c2d5f13ef6711d09d0
CCRRSecMon.sys (Windows7) = 502b85e17a7103a35d5b6eb50ce0eea7
CCRRSecMon.sys (Windows8) = 65c315313330c83f602d19e031d99f67
CCRRSecMon.sys (Windows10) = d17ba3cde6c2051d85dea395891caff9
```

4.5.0.2

Funciones

- Ninguna.

Correcciones

- Se redujo la memoria utilizada para el Kernel Firewall.
- Uso más rápido de los nuevos puntos de conexión de autenticación.
- Se eliminaron las llamadas a icanhazip.com, previamente opcionales pero ya no necesarias.

Hashes MD5

```
service.exe = 716d0a77b44e612342007d64cb1b54aa
CCRRSecMon.sys (Windows7) = 754908e2775c1e88e2ca693e8fc4f71b
CCRRSecMon.sys (Windows8) = 50c180de6862f4741fa6569736b61c97
CCRRSecMon.sys (Windows10) = b3a32b9d639f481aa14a36bfe2f37092
```


4.5.0.3

Funciones

- El indicador de la bandeja de estado ahora muestra el estado de autoconfiguración para nuevas instalaciones.

Hashes MD5

```
service.exe = 517b27279ea728223d6dd32ecb90f2e5
CCRRSecMon.sys (Windows7) = 754908e2775c1e88e2ca693e8fc4f71b
CCRRSecMon.sys (Windows8) = 50c180de6862f4741fa6569736b61c97
CCRRSecMon.sys (Windows10) = b3a32b9d639f481aa14a36bfe2f37092
```

4.5.1.0

Características

- Ahora se utiliza OpenSSL para la comunicación TLS.
 - Esto debería evitar problemas en versiones de sistemas operativos más antiguos que ya no reciben parches para los nuevos requisitos de TLS.

Correcciones

- Se mejoró la compatibilidad de análisis para firmas Authenticode no conformes.

Hashes MD5

```
service.exe = b19823fcc66eef583fa4dc3e2f16a6d6
CCRRSecMon.sys (Windows10) = 0f27455b5ca7c7e028e1a4ce6a7d7f68
CCRRSecMon.sys (Windows8) = 0ac88365a3585ae79928a337900ae16b
CCRRSecMon.sys (Windows7) = 041f03d5e37154f183deb5af7b89bc6b
```

4.5.1.2

Características

- Se eliminó la validación de certificados heredada que dependía de bibliotecas de Windows integradas y lentas.
- Se agregó la capacidad de conservar los registros al desinstalar.

Hashes MD5

```
service.exe = fe8a70286926dba3b6277a9cdf446c38
CCRRSecMon.sys (Windows10) = d4e458f3960a7b1c4b6d06ce4d062f1e
CCRRSecMon.sys (Windows8) = 1f090bc190b80c9c08b03a1017381e6c
CCRRSecMon.sys (Windows7) = 592020ee1f145357c3b77c681ebb3bac
```

4.5.2.1

Funcionalidades

- Lanzamiento amplio de informes para el acceso a Fortress AI

Correcciones

- Optimización de las operaciones del núcleo de Cyber Crucible que no utilizan las API de Windows para contrarrestar el aumento de latencia en algunos entornos Windows en aproximadamente un 20%.

Hashes MD5

```
service.exe = 6ddad1f20f43e8ba799b562235363ceb
CCRRSecMon.sys (Windows10) = d9c81609fafd99957063b2b6574b4a3c
CCRRSecMon.sys (Windows8) = 429dd8f9e39fe8e3bad6b5592dea91f9
CCRRSecMon.sys (Windows7) = 1f6aa2cf085e710c01a0347d6f4489d2
```

4.5.2.2

Correcciones

- Optimización de las operaciones del kernel de Cyber Crucible mediante la evitación de capacidades problemáticas del núcleo del sistema operativo relacionadas con eventos de Windows y el bus de datos.

Hashes MD5

```
service.exe = a4bfeca13496d47c8b91121a5da2b3b8
CCRRSecMon.sys (Windows10) = 042d39305b91caff229605c3a043a24b
CCRRSecMon.sys (Windows8) = 429dd8f9e39fe8e3bad6b5592dea91f9
CCRRSecMon.sys (Windows7) = 1f6aa2cf085e710c01a0347d6f4489d2
```

4.5.3.0

Funciones

- FortressAI
 - Se agregaron notificaciones cuando se informa una infracción de política
 - Integración con el Centro de notificaciones de Windows
 - Se agregó una interfaz gráfica para ver el historial de notificaciones de políticas
 - Se agregó el modo de simulación
- Cyber Crucible Core
 - Análisis asíncrono configurable de DLL para equipos con recursos de hardware mínimos
 - Análisis y telemetría de creación de procesos
 - ahora utiliza persistencia en disco
 - se eliminaron las dependencias de Windows MiniFilter
 - Análisis y telemetría de inyecciones de procesos
 - ahora utiliza persistencia en disco
 - se eliminaron las dependencias de Windows MiniFilter
 - Se eliminaron dependencias adicionales de recursos del kernel de Windows

Correcciones

- Optimización de los informes de telemetría para lograr informes aún más rápidos
- Se eliminó un bloqueo mutuo (deadlock) debido al acceso exclusivo frente al acceso compartido a un recurso específico del kernel requerido por Microsoft Defender cuando Defender habilita el modo de depuración del controlador

Hashes MD5

```
service.exe = 37ba9005bb7dc8a8e5b86670dd02f5dd
CCRRSecMon.sys (Windows10) = aabc6d7299e2c5da21784f12b8836647
CCRRSecMon.sys (Windows8) = 678bb0459a74030dcaab19646141fde7
CCRRSecMon.sys (Windows7) = 07d4c04a12da5979dd8f2d7347669887
```

4.5.3.1

Funciones

- FortressAI
 - Detecta intentos de eludir los controles de política mediante el uso de capturas de pantalla.
- Cyber Crucible Core
 - Admite la reinicialización de la identidad de un agente sin necesidad de una reimplementación completa.
 - Esto soluciona situaciones en las que una máquina con Cyber Crucible instalado se clona, clonando así la licencia y los identificadores del agente. Al igual que con las direcciones IP, las direcciones MAC, los nombres de máquina y otros identificadores únicos, Cyber Crucible identifica un agente clonado y alerta a los administradores de CC sobre la posibilidad de generar nuevos identificadores de CC.

Hashes MD5

```
service.exe = 5db5b2dfe65b9908c93d04a136123c98
CCRRSecMon.sys (Windows10) = e4a27842cc4352cffaea780116e5ae00
CCRRSecMon.sys (Windows8) = 060170a2cfff082c2092dc99a8330717
CCRRSecMon.sys (Windows7) = 63a39eb153298766a3ff7034eaafa5af
```

4.5.3.2

Características

- FortressAI
 - Ninguna
- Cyber Crucible Core
 - Mejora de la operación del búfer del kernel
 - El controlador utiliza búferes para almacenar temporalmente la telemetría que finalmente se envía al panel del cliente. Esta actividad es distinta de la población o las operaciones del modelo de comportamiento.
 - Si un búfer del kernel se sobrecarga, la carga de CPU del sistema aumenta.
 - Esto solo ocurriría debido a un gran error del sistema operativo o a un ataque a los sistemas.
 - La notificación automática al cliente sobre un uso de búfer muy alto estará disponible el 1 de junio de 2026.
 - Casi todas las operaciones del búfer del kernel de CC corresponden a tres búferes principales.
 - El porcentaje de uso de los tres búferes principales ahora se transmite a la infraestructura de CC para la recopilación de métricas y la identificación del uso de búfer por agente.
 - Los tres búferes principales pueden ajustarse en tamaño de forma remota, y los usuarios pueden hacer seguimiento de su estado.

Correcciones

- Una actualización reciente relacionada con las bibliotecas redistribuibles de DotNet y MSVC saturó los búferes de Cyber Crucible con eventos sostenidos y muy altos (500%+) de operaciones de procesos y DLL, lo que afectó a algunos clientes. Aunque el uso del búfer ha vuelto al nivel normal del 1-5%, incluidos los clientes afectados, se duplicó el tamaño de todos los búferes para prevenir posibles problemas futuros. Esto se suma a las capacidades de configuración mencionadas anteriormente.

Hashes Sha-256

```
service.exe = 2f46657af8809339d16546f1e6f2b58975bbf4d5c10fde3510363d628b129492
fai-alert.exe = 890ccca7e0ce14a0e2ff7f90bae75a7ef12ad6c8cd43ffb52093c8431e65770b
```


CCRRSecMon.sys	=	d0e941bc25d31e38cbebbe9ce3918f82d0b9c7b433efed318cb34e36a50acf94
CCRRSecMon.inf	=	db54d8077afdfef81286868f7bda1e8df17dbd812178ddac989127550a904a8c
ccrrsecmon.cat	=	a01c31db7231fed3852c9e559eb2c3f7496a016982207c102b88d8b36dcb0486