Agente de Endpoint

- 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 Versões do Agente de Endpoint

- 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

Recursos

- Para grupos com telemetria habilitada, foram adicionados dados do Active Directory à lista de monitoramento de roubo de credenciais

Correções

- Remoção de entradas duplicadas de volumes locais e compartilhamentos de rede em alguns ambientes.
- Comportamento refinado para algumas reconstruções de banco de dados de miniaturas que causavam incidentes
- Corrigido um bug de validação de licença que podia aumentar o tempo de inicialização
- Comportamento refinado para acesso a arquivos em mídias graváveis uma única vez, como CDs e unidades de fita WORM

Status de Validação 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

Funcionalidades

Nenhuma - atualização de manutenção.

Correções

- Corrigido o facto de algumas partilhas de rede ligadas por um utilizador serem inicialmente ignoradas na análise.
- Refinado o comportamento de falso positivo associado a partilhas que aparecem durante sessões de utilizador, seguidas rapidamente por uma caixa de diálogo Guardar Como.

Estado de Validação 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

Funcionalidades

- Suporte expandido para análises de injeção de processos, para aumentar drasticamente a precisão na deteção de intenção maliciosa versus benigna em aplicações.
  - Isto tornou-se especialmente importante devido a um pequeno número (<0.02%) de máquinas na telemetria da Cyber Crucible a alertar sobre comportamentos agressivos de injeção de processos em processos do sistema.
- Aumento da capacidade de monitorização de processos do sistema não assinados.
  - Isto foi, em parte, uma resposta ao facto de os atacantes se focarem fortemente em envolver esses processos durante operações de movimento lateral (num sistema e entre sistemas).

Correções

- Alterado um comportamento de modificação de ficheiros para diminuir os falsos positivos, deixando de ser acionado em certas ações benignas, através de contexto adicional ao nível do kernel sobre os comportamentos de acesso a ficheiros de um processo.

Estado de Validação WHCP/WHQL

Validado.

Hashes MD5

```
service.exe   = 0bab8404900c6a16ac3ad0293c45de5c
assistant.exe = 98f013fd4fdb7325f903d07c87b999ac
CCRRSecMon.sys (Windows10)       = 452719399d9bb98dc6b14fb8787d8415
CCRRSecMon.sys (Windows8)        = a974c7cc46db3759a2da34f37caaa72e
CCRRSecMon.sys (Windows7)        = 6a0f2e55d6a7b66bd9bbe318d5dbbebf
```

4.4.1.1

Funcionalidades

- Processamento analítico aprimorado para relações pai-filho, quando o processo pai termina rapidamente antes que a Cyber Crucible conclua o processamento (milissegundos).
  - O cenário extremamente comum aqui é que os atacantes (e programas legítimos) frequentemente abrem vários programas, às vezes em uma "cadeia" de múltiplas etapas. Isso pode ser proposital, ou devido ao comportamento do Windows ou de outras aplicações "por trás dos panos".
  - Os modelos comportamentais da Cyber Crucible aproveitam variáveis de atividade e estado para todos os processos em uma cadeia de execuções, a fim de alcançar a máxima precisão e contexto.

Correções

- A Cyber Crucible apresentava uma perda na precisão da tomada de decisão do modelo comportamental, devido à perda de telemetria quando múltiplos programas se chamam mutuamente, mas um dos programas terminava em milissegundos.
  - Em uma cadeia em que o Programa A executa o Programa B. O Programa B inicia o Programa C, mas o Programa B termina em milissegundos (geralmente uma falha silenciosa, mas nem sempre). A análise comportamental da Cyber Crucible possuía as variáveis do Programa A e do Programa C, mas não teve tempo de analisar completamente o Programa B, pois esperava que ele estivesse em execução.
  - Isso foi corrigido, resultando em uma tomada de decisão mais precisa pelo mecanismo de decisão hiper-automatizado da Cyber Crucible.

Status de Validação WHCP/WHQL

Validado.

Hashes MD5

```
service.exe   = db76d0abc8f4bc4b2a093435bc314bde
assistant.exe = a5bac35d839d7a57fcccfceb011083c1
CCRRSecMon.sys (Windows10)       = 935e43368fa95ae740a3f04defcc390d
CCRRSecMon.sys (Windows8)        = ee555ad0f282f36dd11deada8d1ca9c7
CCRRSecMon.sys (Windows7)        = a6a5073c6565361b443651ef29e49490
```

4.4.1.2

Recursos

- Aumento da especificidade disponível para listas brancas, como caminho e argumentos do processo pai.
- Suporte expandido para análises de acesso de identidade a mais bancos de dados de credenciais.
  - O acesso de identidade agora também é monitorado para Slack, Opera, Thunderbird, Discord e Vivaldi.
- Suporte de lista branca expandido para incluir acesso de identidade.

Correções

- Redução da largura de banda utilizada entre os agentes e a API REST.
- Corrigido problema em que algumas edições mais antigas do Windows Server exibiam canários no Explorer.
- Corrigido problema em que alguns logs de acesso de identidade não exibiam indicadores de confiança de certificado.

Status de Validação 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

Funcionalidades

- O Monitoramento de Credenciais/Identidade agora inclui várias VPNs, carteiras de criptomoedas e outras aplicações.
- Numa (isto é comum) cadeia de processos afetados durante um ataque (o atacante move-se do programa em execução A, para B, para C, e D é utilizado para o roubo de dados), o programa “paciente 0” A é suspenso, mas o paciente D é reportado como o processo que executa o comportamento de roubo.
  - O estado da memória é preservado e reportado ao longo de todas as cadeias de processos, para futura análise forense.
- No caso de uma resposta automatizada em que a memória de um processo em execução tenha sido modificada, essa modificação de memória é enviada de forma configurável para a Cyber Crucible para engenharia reversa e análise adicional.
- No caso de um erro de modificação de memória não malicioso numa aplicação, as exceções comportamentais (“listas de permissão”) agora têm a capacidade de sinalizar determinados eventos de corrupção de memória como benignos. Isto não impedirá que o próprio programa falhe ou perca dados devido ao erro, mas a Cyber Crucible saberá ignorar o erro ao procurar por injeção maliciosa de código em processos em execução (injeção de processo/hollowing).

Correções

- Removida vulnerabilidade em que binários podiam ser eliminados por um processo privilegiado enquanto os binários da CC estavam a ser atualizados.
- Removida vulnerabilidade em que chaves de registo podiam ser eliminadas ou alteradas por um processo privilegiado enquanto os binários da CC estavam a ser atualizados.
- Corrigido o rastreamento do estado da memória quando um processo é corrigido (patched) em memória durante a avaliação da memória pela Cyber Crucible.
- Corrigido o rastreamento do estado da memória sob determinadas condições em que a memória é realocada entre páginas de memória.
- Atualizações menores de eficiência de CPU, provavelmente demasiado pequenas para serem registadas no Gestor de Tarefas, uma vez que a utilização é normalmente <1%

Estado de Validação WHCP/WHQL

Validado

Hashes MD5

```
service.exe   = 90a6ca2f5b7a76b847052f3d420f0c9b
assistant.exe = b62ee623f74171f4a3f34ff129188174
CCRRSecMon.sys (Windows10)       = dfdce4016f6920e844615b3d506ec2e2
CCRRSecMon.sys (Windows8)        = 59bbd41c883ca0205fd3adbfdbb5dbb6
CCRRSecMon.sys (Windows7)        = 88e6f047f7fa26e717a24f5fd7b33dc5
```

4.4.1.3.1

Obtida visibilidade sobre alguns processos do sistema que se inicializam antes de o driver da Cyber Crucible ser carregado.

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

Adicionada telemetria adicional para os processos do sistema agora visíveis devido à versão 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

Corrigidos alguns relatórios de incidentes que incluíam dados do processo errado, quando um processo termina a meio de um 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

Otimização dos cálculos de memória, em preparação para a versão 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

Recursos

- Capacidades de correspondência de padrões aprimoradas no modelo comportamental.
  - Isso é especialmente relevante para cobertura adicional de locais de armazenamento de identidade, como locais de carteiras de criptomoedas.
- Funcionalidade de dependência de software aumentada para bibliotecas (Cyber Crucible) em uso para a próxima proteção de acesso à identidade totalmente automatizada.
- Capacidade opcional de executar o agente em modo de segurança

Correções

- Otimização do uso de memória no serviço. Isso só teria sido percebido em servidores muito ocupados com muita análise comportamental ocorrendo (pela Cyber Crucible) simultaneamente.

Hashes MD5

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

4.4.2.0

Funcionalidades

- Capacidades de monitorização e prevenção melhoradas para proteção automatizada do acesso a identidades.
- Otimização do uso da rede através de taxas de comunicação variáveis, dependentes dos comportamentos do cliente.

Correções

- N/D

Hashes MD5

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

4.4.2.1

Correções

- Otimizado o rastreamento de informações de identidade para aplicativos com um grande número de diretórios profundamente aninhados.

Hashes MD5

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

4.4.2.2

Funcionalidades

- Nenhuma

Correções

- Otimização do tratamento de variáveis para um tipo de comportamento.
  - Causa: Um produto de segurança não especificado gerou um número muito elevado de comportamentos em alguns servidores de grande porte, o que causou um uso excessivo de memória por parte do Cyber Crucible.
  - Sintomas: O uso de memória do Cyber Crucible salta de alguns MB para vários GB. O uso de memória do produto de segurança também aumentou 100 vezes, ultrapassando os 250GB. Se experienciar este comportamento, uma vez que pode ser independente do Cyber Crucible, por favor abra um pedido de suporte para que possamos ajudar. Suspeitamos também que se trate de um problema do produto de segurança, independente da otimização do Cyber Crucible.
  - Correção: O rastreamento desta variável de comportamento foi migrado de um algoritmo que esperava um volume baixo de população para um algoritmo de alto volume, semelhante ao utilizado noutras partes do driver.
  - Quem é afetado? Foi observado apenas um cliente com este problema, e apenas numa pequena parte dos seus servidores de grande porte. Ainda assim, esta atualização é implementada em todos os clientes.

Hashes MD5

```
service.exe   = bbfb0bf47d942d30438a260b497c04cd
assistant.exe = 280d746ed3edea9b7267955a94b97a8e
CCRRSecMon.sys (Windows7)        = cded2aaa7dd0c2fe446694451bd17960
CCRRSecMon.sys (Windows8)        = a06dce5e19627fe1f982cbde632fc313
CCRRSecMon.sys (Windows10)       = 14e0c4e7f86405562701187fac93aea2
```

4.4.2.3

Funcionalidades

- Nenhuma

Correções

- Corrigidos problemas de compatibilidade com o 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

Funcionalidades

- Suporte de proteção de credenciais para Microsoft Teams e Signal Messenger

Correções

- Supressão de registos relacionados com a rede quando em modo de segurança sem rede
- Cópia de segurança de alguns dados do agente na desinstalação para a pasta de armazenamento temporário do 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

Funcionalidades

- Nenhuma

Correções

- Redução da utilização de rede ao enviar grandes quantidades de relatórios de uma só vez
- Correção do tratamento de alguns dados 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

Funcionalidades

- Nenhuma

Correções

- Redução do uso de memória em servidores com muitos certificados de programa exclusivos

Hashes MD5

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

4.4.2.7

Funcionalidades

- Nenhuma

Correções

- Redução do uso de memória durante o tratamento de programas que utilizam comportamento indefinido ao consultar diretórios

Hashes MD5

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

4.4.2.8

Funcionalidades

- Nenhuma

Correções

- Aumento do registo (logging) e da telemetria para estados de máquina defeituosos
- Aumento da estabilidade das proteções de identidade no arranque do sistema

Hashes MD5

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

4.4.3.0

Recursos

- Além das proteções de serviço existentes, o driver em modo kernel reiniciará o serviço caso ele seja encerrado por qualquer motivo.

Correções

- Nenhuma

Hashes MD5

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

4.4.3.2

Funcionalidades

- Nenhuma

Correções

- Redução do uso de CPU durante o início de processos.
- Redução do uso de CPU nas determinações de confiança durante consultas consecutivas de diretórios.

Hashes MD5

```
service.exe   = a1e5c45b87f914343c772c05e18b153e
CCRRSecMon.sys (Windows7)        = c995f7efeb88ef42425cf54b0b210dc7
CCRRSecMon.sys (Windows8)        = 3135a7787076286f3e8d82ca384582e9
CCRRSecMon.sys (Windows10)       = 0f6be8ec8806d4acabb8d03904c1b148
```

4.4.3.1

Recursos

- Nenhum

Correções

- Corrigido problema em algumas máquinas com características incomuns de instalação do Windows que apresentavam canários visíveis no Explorer.

Hashes MD5

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

4.4.4.0

Recursos

- Relatórios de incidentes e telemetria são armazenados em disco para cenários offline.
  - Devido a tentativas de adulteração observadas contra múltiplos armazenamentos de registros de EDR/XDR, a Cyber Crucible habilitou proteção em nível de kernel para os dados armazenados em disco antes de implantar esse recurso.
- Aumento da proteção do processo de serviço utilizado para comunicação de backend e atualizações, como parte do endurecimento de zero-trust com visão prospectiva.
  - Isso não foi uma resposta a uma ameaça existente, mas sim uma medida proativa para uma ameaça que a Equipe prevê estar por vir.

Correções

- Corrigido o problema de processos carregados na inicialização não estarem disponíveis no painel em criações de processo.
- Impedida a execução simultânea de dois instaladores, o que registraria a mesma máquina duas vezes.

Hashes MD5

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

4.4.4.4

Funcionalidades

- Nenhuma

Correções

- Desempenho aprimorado para a análise de dados de certificados na inicialização do sistema.

Hashes MD5

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

4.4.5.1

Funcionalidades

- Redução do uso de largura de banda:
  - Uso de compressão para dados de telemetria maiores e respostas de servidor maiores
  - Uso de HTTP/2 para cabeçalhos comprimidos e maior eficiência de sockets
- Maior visibilidade sobre as operações de certificados.

Correções

- Codificação de metadados de certificados na telemetria bruta quando existem rótulos não compatíveis com RFC. A infraestrutura de segurança de rede estava corrompendo ou eliminando as cargas úteis, fazendo com que o agente retransmitisse até obter êxito.

Hashes MD5

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

4.4.5.2

Recursos

- Nova telemetria de acesso em nível de kernel para comportamentos baseados em rede, para melhor identificar possíveis bugs de rede no lado do cliente, ou oportunidades de otimização
- A telemetria de saída agora é agrupada e enviada em conjunto, assim como as configurações de entrada
  - Transmitida com uma variação de tempo de 25%, para que nem todas as máquinas enviem pacotes simultaneamente em uma rede de clientes
- O HTTP/2 agora é totalmente utilizado de ponta a ponta

Correções

- Redução do número mínimo de threads em uso no espaço do usuário
- Redução do uso de CPU pelo serviço em espaço do usuário
- A autenticação Agente-Servidor agora é realizada de forma mais eficiente
- Substituído o algoritmo anterior de suspensão/reinício do serviço quando as licenças não estavam disponíveis.
  - O algoritmo anterior causava um "serviço encerrado inesperadamente" no gerenciador de eventos a cada 15 minutos.
  - Permitir que o Sistema Operacional instrua o serviço a desligar (algo explorado indevidamente por criminosos e outras ferramentas de segurança) teria permitido um reinício "limpo" do serviço sem registros no gerenciador de eventos. Em vez de criar essa vulnerabilidade, o serviço da Cyber Crucible se reiniciou sozinho sem o envolvimento do Windows, gerando o registro de evento.

Hashes MD5

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

4.4.5.3

Funcionalidades

- Adicionado um segundo domínio para comunicação com o servidor (consulte a lista de domínios aqui).
  - Se houver problemas de comunicação com um domínio, o agente mudará automaticamente para o outro.

Correções

- Alteradas algumas cadeias de caracteres antigas que faziam referência a “Ransomware Rewind” para agora fazerem referência a “Cyber Crucible”.

Hashes MD5

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

4.4.5.9

Recursos

- Aumento do endurecimento de partes da funcionalidade anteriormente realizada pelas bibliotecas de criptografia do Windows, agora realizadas pelo driver de kernel do Cyber Crucible.
  - Trata-se tanto de um endurecimento geral quanto de um aumento na telemetria que indica possíveis ataques contra as bibliotecas e APIs de criptografia do Windows.
- Este é um lançamento de marco (milestone) em relação aos lançamentos incrementais encontrados nas versões 4.4.5.4 a 4.4.5.8, todos alinhados com a funcionalidade anterior de endurecimento de análise de criptografia.
  - A telemetria inicial indica que as falhas nas bibliotecas de certificados e criptografia do Windows foram respondidas de forma legítima pelo Cyber Crucible.
  - No momento, não se sabe qual percentual dos problemas se deveu a exploração de vulnerabilidades versus um bug na biblioteca principal do Windows. Entre em contato com seu representante da Cyber Crucible para discutir mais detalhes, conforme necessário.

Correções

- Corrigido um problema em que alguns relatórios de processos reportavam incorretamente o certificado listado como “não confiável”, devido à perda de funcionalidade da biblioteca de certificados do Windows.

Hashes MD5

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

4.4.5.8

Recursos

- Aumento do hardening de partes da funcionalidade anteriormente realizada pelas bibliotecas de criptografia do Windows, agora conduzida pelo driver de kernel da Cyber Crucible.
  - Trata-se tanto de um hardening geral quanto de um aumento na telemetria que indica possíveis ataques contra as bibliotecas e APIs de criptografia do Windows.

Correções

- Corrigido um problema em que alguns relatórios de processo reportavam incorretamente o certificado listado como “não confiável”, devido à perda de funcionalidade da biblioteca de certificados do Windows.

Hashes MD5

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

4.4.5.5

Funcionalidades

- Foi reforçado o endurecimento (hardening) de partes da funcionalidade anteriormente realizadas pelas bibliotecas de criptografia do Windows, passando a ser realizadas pelo driver de kernel da Cyber Crucible.
  - Trata-se tanto de um reforço geral, como de um aumento na telemetria que indica possíveis ataques contra as bibliotecas e APIs de criptografia do Windows.

Correções

- Corrigido um problema em que alguns relatórios de processos indicavam incorretamente o certificado listado como “não confiável”, devido à perda de funcionalidade da biblioteca de certificados do Windows.

Hashes MD5

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

4.4.5.6

Funcionalidades

- Aumento do endurecimento (hardening) de partes da funcionalidade anteriormente realizadas pelas bibliotecas de criptografia do Windows, agora realizadas pelo driver de kernel da Cyber Crucible.
  - Trata-se tanto de um endurecimento geral, quanto de um aumento na telemetria que indica possíveis ataques contra as bibliotecas e APIs de criptografia do Windows.

Correções

- Corrigido um problema em que alguns relatórios de processos indicavam incorretamente o certificado listado como “não confiável”, devido à perda de funcionalidade da biblioteca de certificados do Windows.

Hashes MD5

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

4.4.5.7

Funcionalidades

- Reforço aumentado de partes da funcionalidade anteriormente realizadas pelas bibliotecas de criptografia do Windows, agora realizadas pelo driver de kernel da Cyber Crucible.
  - Trata-se tanto de um reforço geral quanto de um aumento na telemetria que indica possíveis ataques contra as bibliotecas e APIs de criptografia do Windows.

Correções

- Corrigido um problema em que alguns relatórios de processo reportavam incorretamente o certificado listado como “não confiável”, devido à perda de funcionalidade da biblioteca de certificados do Windows.

Hashes MD5

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

4.4.5.4

Funcionalidades

- Aumento do endurecimento de partes da funcionalidade anteriormente realizadas pelas bibliotecas de criptografia do Windows, agora realizadas pelo driver de kernel da Cyber Crucible.
  - Trata-se tanto de um endurecimento geral quanto de um aumento na telemetria que indica possíveis ataques contra as bibliotecas e APIs de criptografia do Windows.

Correções

- Corrigido problema em que alguns relatórios de processos indicavam incorretamente o certificado listado como “não confiável”, devido à perda de funcionalidade da biblioteca de certificados do Windows.

Hashes MD5

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

4.4.6.0

Funcionalidades

- Melhoria de desempenho de CPU para algumas aplicações que geram um grande número de travessias de diretório automatizadas e simultâneas como parte do comportamento da aplicação.

Correções

-

Hashes MD5

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

4.4.6.1

Recursos

- Continuação da migração do nome de produto “Ransomware Rewind” para “Cyber Crucible”.
  - O nome de serviço legado `"Ransomware Rewind"` será migrado para `"CyberCrucibleAgent"`. O nome do processo permanece o mesmo.
  - A chave de registro em `HKLM\SOFTWARE` será migrada do `RansomwareRewind` legado para o atual `CyberCrucibleAgent.`

Correções

- Corrigido um problema em que alguns processos de 32 bits eram sinalizados como tendo “memória modificada” quando a imagem do processo estava no tamanho máximo permitido para um processo de 32 bits.

Hashes MD5

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

4.4.6.2

Recursos

- Adicionados sinalizadores opcionais de “tipo de acesso” expostos aos usuários finais para especificidade de acesso comportamental.

Correções

- Nenhuma.

Hashes MD5

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

4.4.6.3

Recursos

- Adicionado suporte opcional a proxy SOCKS5 para auxiliar na implantação do agente.

Correções

- Corrigidas reinstalações a partir de agentes mais antigos que usavam o ID de instalação incorreto.
- Corrigido o caminho de serviço sem aspas em instalações existentes provenientes de instaladores mais antigos.

Hashes MD5

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

4.4.6.4

Recursos

- As informações de memória do processo pai estão disponíveis para relatórios de processo quando modificações forem detectadas.

Melhorias

- Alteradas algumas frequências de comunicação com o servidor para que não seja mais necessário reiniciar o sistema para ajustá-las.

Correções

Nenhuma nesta versão.

Hashes MD5

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

4.4.7.0

Funcionalidades

- Início da implementação de comunicações HTTPS baseadas em JWE.
  - As chaves de encriptação são exclusivas para cada agente.
  - Todos os payloads encriptados sob o HTTPS. Desativado por predefinição durante a implementação inicial.
  - Possibilidade de reverter opcionalmente de HTTPS encriptado com JWE para HTTPS não encriptado, caso os payloads no formato JWE não sejam transmitidos com sucesso.

Hashes MD5

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

4.4.7.1

Funcionalidades

- Mais telemetria para criações de processos e incidentes
  - SID do usuário
  - Nome de logon down-level do usuário
  - Se o processo está ou não elevado (Executar como Administrador)
- Os incidentes agora informam onde ocorreu o acesso iterativo aos dados

Correções

- Redução do uso de memória durante períodos de problemas de conectividade com o servidor e alta telemetria ocorrendo simultaneamente
- Redução do uso de memória durante o relatório de incidentes

Hashes MD5

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

4.4.7.3

Funcionalidades

- Modo DMZ
  - Configuração opcional para utilizar um pacote de CA assinado para comunicação TLS com os servidores de autenticação e telemetria. Estes pacotes de CA são então protegidos contra adulteração ou eliminação pelas capacidades proprietárias de anti-adulteração da Cyber Crucible.
  - As verificações OCSP e CRL são desativadas para reduzir a lista de domínios a permitir através de uma firewall.

Correções

- Redução da utilização de memória e do tempo de CPU gasto no envio de diferenças de memória, especialmente após longos períodos offline.

Hashes MD5

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

4.4.8.0

Funcionalidades

- Telemetria Authenticode em modo kernel
  - Para maior velocidade e fiabilidade, os dados de certificado para criações de processos e incidentes serão registados apenas pelo driver.
  - Esta atualização não remove as dependências das bibliotecas de criptografia do Windows, mas realiza os cálculos criptográficos em paralelo. Eventualmente, a dependência do Windows poderá ser totalmente removida.

Correções

- Redução do uso de memória e do tempo de CPU gasto em tentativas de envio de eventos quando offline, período durante o qual a telemetria é armazenada de forma segura até que a máquina recupere a conectividade com os servidores da Cyber Crucible.
- Alguns instaladores de drivers Nvidia acreditavam que não tinham privilégio para instalar devido ao uso de uma função interna do kernel da Microsoft para tentar aceder aos ficheiros instalados da Cyber Crucible.
- Corrigida a incompatibilidade com o modo JWE e o modo DMZ

Hashes MD5

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

4.4.8.1

Funcionalidades

- Os metadados do executável, como versão do produto, nome da empresa, etc., para processos em memória, são reportados pelo driver através da visibilidade do kernel. A funcionalidade normal é utilizar chamadas da API do Windows em espaço de utilizador. Esta alteração para a análise no kernel elimina a oportunidade (observada) para os atacantes adulterarem a informação do processo.
- A informação de autenticação do agente é replicada noutro local do sistema para restauro no caso de o registo ser corrompido por um driver malicioso.

Melhorias

- Os erros de ligação ao servidor são registados de forma mínima pelo agente, reduzindo o tamanho do registo em disco.

Correções

- N/A

Hashes MD5

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

4.4.8.2

Funcionalidades

- Adicionado suporte para um ícone opcional na bandeja do sistema. Este recurso está desativado por padrão.

Correções

- Adicionada solução alternativa para problema relacionado a solicitações de hashing da API do kernel do Windows. A solução alternativa poderá ser removida no futuro, caso o problema do Windows seja corrigido, possivelmente na próxima atualização do kernel.

Hashes MD5

```
service.exe  = 6e21b0a7c41b156f2001c93bbcd142de
CCRRSecMon.sys (Windows7)        = 43cce21323465eac015fc7c90b88ac87
CCRRSecMon.sys (Windows8)        = c7b2d8d130f8c3e768891ad0b20931a5
CCRRSecMon.sys (Windows10)       = d95d162bc7f87f3eaef46d58eb543364
```

4.4.9.0

Recursos

- Telemetria de DLL em modo kernel
  - Análise de certificados e cálculo de confiança para todas as DLLs carregadas no driver.

Correções

- Nenhuma.

Hashes MD5

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

4.4.9.1

Recursos

- Nenhum.

Correções

- Aumento da quantidade de telemetria processada de uma só vez pelo serviço para dados de criação e injeção.
- Ajuste na ordenação de canários para programas que utilizam métodos incomuns de iteração de arquivos.
- Ajuste na ACL de alguns canários para melhor adequação a sistemas de arquivos reais.

Hashes MD5

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

4.4.9.2

Funcionalidades

- Rastreamento de modificação de memória para DLLs carregadas.
- Geração de diff de memória para DLLs modificadas.

Correções

- Tratamento de algumas DLLs não conformes que geravam resultados incorretos de hash authenticode.

Hashes MD5

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

4.4.9.4

Correções

- Os arquivos de dump do serviço agora são limitados a 10 por combinação de versão+thread.

Hashes MD5

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

4.5.0.0

Funcionalidades

- AI Kernel Firewall
- Melhorias de velocidade no cálculo de hash Authenticode
- Redução significativa do uso de memória para telemetria de DLL
- Maior visibilidade para modificações de memória em DLLs

Correções

- Correção da compatibilidade da recuperação do serviço com o 24H2

Hashes MD5

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

4.5.0.1

Recursos

- Opção para migrar para o domínio do servidor de autenticação OAuth hospedado
- Tarefa para configurar dinamicamente as URLs dos servidores REST e OAuth

Correções

- Nenhuma.

Hashes MD5

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

4.5.0.2

Funcionalidades

- Nenhuma.

Correções

- Redução da memória utilizada pelo AI Kernel Firewall.
- Utilização mais rápida dos novos endpoints de autenticação.
- Removidas as chamadas a icanhazip.com, anteriormente opcionais mas já não necessárias.

Hashes MD5

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

4.5.0.3

Funcionalidades

- O indicador da bandeja de status agora exibe o status de autoconfiguração para novas instalações.

Hashes MD5

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

4.5.1.0

Funcionalidades

- O OpenSSL agora é utilizado para comunicação TLS.
  - Isto deverá contornar problemas em versões mais antigas do SO que já não recebem correções para os requisitos mais recentes do TLS.

Correções

- Suporte de análise melhorado para assinaturas Authenticode não conformes.

Hashes MD5

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

4.5.1.2

Recursos

- Removida a validação de certificado legada que dependia de bibliotecas nativas e lentas do Windows.
- Adicionada a capacidade de manter os logs na desinstalação.

Hashes MD5

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

4.5.2.1

Funcionalidades

- Lançamento amplo de relatórios para acesso ao Fortress AI

Correções

- Otimização das operações do kernel do Cyber Crucible que não utilizam APIs do Windows, de forma a compensar o aumento de latência em alguns ambientes Windows em aproximadamente 20%.

Hashes MD5

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

4.5.2.2

Correções

- Otimização das operações do kernel do Cyber Crucible por meio da prevenção de capacidades problemáticas do sistema operacional relacionadas a eventos do Windows e ao barramento de dados principal.

Hashes MD5

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

4.5.3.0

Funcionalidades

- FortressAI
  - Adicionadas notificações quando uma violação de política é reportada
    - Integração com o Windows Notification Center
  - Adicionada uma interface gráfica para visualizar o histórico de notificações de políticas
  - Adicionado o modo de simulação
- Cyber Crucible Core
  - Análise assíncrona configurável de DLL para máquinas com recursos de hardware mínimos
  - Análise e telemetria de criação de processos
    - agora utiliza persistência em disco
    - removidas as dependências do Windows MiniFilter
  - Análise e telemetria de injeções de processos
    - agora utiliza persistência em disco
    - removidas as dependências do Windows MiniFilter
  - Removidas dependências adicionais de recursos do kernel do Windows

Correções

- Otimização do relatório de telemetria para relatórios ainda mais rápidos
- Removido impasse (deadlock) causado pelo acesso exclusivo versus compartilhado a um recurso específico do kernel exigido pelo Microsoft Defender quando o Defender ativa o modo de depuração de driver

Hashes MD5

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

4.5.3.1

Recursos

- FortressAI
  - Detecta tentativas de contornar controles de política através do uso de capturas de tela.
- Cyber Crucible Core
  - Suporta a reinicialização da identidade de um agente sem exigir uma reimplantação completa.
    - Isso corrige situações em que uma máquina com o Cyber Crucible instalado é clonada, clonando assim a licença e os identificadores do agente. Assim como com endereços IP, endereços MAC, nomes de máquina e outros identificadores exclusivos, o Cyber Crucible identifica um agente clonado e alerta os administradores do CC sobre a oportunidade de gerar novos identificadores do CC.

Hashes MD5

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

4.5.3.2

Funcionalidades

- FortressAI
  - Nenhuma
- Cyber Crucible Core
  - Melhoria da Operação de Buffer do Kernel
    - O driver utiliza buffers para armazenar temporariamente a telemetria que, em última análise, é enviada ao painel do cliente. Esta atividade é distinta da população ou das operações do modelo comportamental.
    - Se um buffer do kernel sofrer sobrecarga, a carga de CPU do sistema aumenta.
      - Isso só ocorreria devido a um grande bug do sistema operacional ou a um ataque aos sistemas.
      - Notificação automática ao cliente sobre uso muito elevado de buffer disponível em 1 JUN 2026.
    - Quase todas as operações de buffer do kernel para o CC ocorrem em três buffers principais.
    - A percentagem de utilização dos três buffers principais é agora transmitida à infraestrutura do CC para recolha de métricas e identificação do uso de buffer por agente.
    - Os três buffers principais podem ser ajustados remotamente em tamanho, e o seu estado pode ser acompanhado pelos utilizadores.

Correções

- Uma atualização recente envolvendo as bibliotecas redistribuíveis DotNet e MSVC sobrecarregou os buffers do Cyber Crucible com eventos sustentados de operações de processos e DLLs em níveis muito elevados (500%+), afetando alguns clientes. Embora o uso do buffer tenha voltado ao normal de 1-5%, incluindo para os clientes afetados, todos os buffers tiveram o seu tamanho duplicado para prevenir quaisquer problemas futuros. Isto é adicional às capacidades de configuração listadas acima.

Hashes Sha-256

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

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