

Endpoint Agent

- [Endpoint Agent Versionsindex](#)

- [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](#)

Endpoint Agent Versionsindex

- [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

Funktionen

- Für Gruppen mit aktivierter Telemetrie wurden Active-Directory-Daten zur Überwachungsliste für Anmeldedatendiebstahl hinzugefügt

Fehlerbehebungen

- Doppelte lokale Volumes und Netzwerkfreigabe-Einträge in einigen Umgebungen entfernt.
- Verhalten für einige Miniaturbild-Datenbank-Neuaufbauten, die Vorfälle verursachten, verfeinert
- Fehler bei der Lizenzvalidierung behoben, der die Startzeit verlängern konnte
- Verhalten für den Dateizugriff auf einmalig beschreibbare Medien wie CDs und WORM-Bandlaufwerke verfeinert

WHCP/WHQL-Validierungsstatus

Validiert

MD5-Hashes

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

4.4.0.9.1

Funktionen

Keine – Wartungsupdate.

Fehlerbehebungen

- Ein Problem behoben, bei dem einige von einem Benutzer verbundene Netzwerkfreigaben zunächst in der Analyse ignoriert wurden.
- Das Verhalten bei Falsch-Positiv-Meldungen im Zusammenhang mit Freigaben, die während Benutzersitzungen erscheinen und kurz darauf von einem Speichern-unter-Dialogfeld gefolgt werden, wurde verfeinert.

WHCP/WHQL-Validierungsstatus

Validiert.

MD5-Hashes

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

4.4.1.0

Funktionen

- Erweiterte Unterstützung für Analysen von Prozessinjektionen, um die Genauigkeit der Erkennung von böswilliger vs. gutartiger Absicht bei Anwendungen erheblich zu steigern.
 - Dies wurde besonders wichtig, da eine geringe Anzahl (<0,02 %) der Maschinen in der Cyber-Crucible-Telemetry Warnungen zu aggressivem Prozessinjektionsverhalten von Systemprozessen auslöste.
- Verbesserte Überwachungsfähigkeit für unsignierte Systemprozesse.
 - Dies war teilweise eine Reaktion darauf, dass Angreifer sich stark darauf konzentrieren, diese Prozesse bei seitlichen Bewegungsoperationen (innerhalb eines Systems und zwischen Systemen) einzubeziehen.

Fehlerbehebungen

- Ein Verhalten bei Dateiänderungen wurde geändert, um Fehlalarme zu reduzieren, indem bestimmte gutartige Aktionen nicht mehr ausgelöst werden – durch zusätzlichen Kernel-Level-Kontext zu den Dateizugriffsverhaltensweisen eines Prozesses.

WHCP/WHQL-Validierungsstatus

Validiert.

MD5-Hashes

```
service.exe    = 0bab8404900c6a16ac3ad0293c45de5c
assistant.exe  = 98f013fd4fdb7325f903d07c87b999ac
CCRRSecMon.sys (Windows10)    = 452719399d9bb98dc6b14fb8787d8415
CCRRSecMon.sys (Windows8)     = a974c7cc46db3759a2da34f37caaa72e
CCRRSecMon.sys (Windows7)     = 6a0f2e55d6a7b66bd9bbe318d5dbbebfb
```

4.4.1.1

Funktionen

- Verbesserte analytische Verarbeitung für Eltern-Kind-Beziehungen, wenn der übergeordnete Prozess sehr schnell beendet wird, bevor Cyber Crucible die Verarbeitung abschließen kann (Millisekunden).
 - Ein äußerst häufiges Szenario ist, dass Angreifer (und auch legitime Programme) oft mehrere Programme öffnen, manchmal in einer mehrstufigen „Kettenreaktion“. Dies kann absichtlich geschehen oder auf das Verhalten von Windows oder anderen Anwendungen „im Hintergrund“ zurückzuführen sein.
 - Die Verhaltensmodelle von Cyber Crucible nutzen Aktivitäts- und Zustandsvariablen für alle Prozesse in einer Ausführungskette, um maximale Genauigkeit und Kontext zu erreichen.

Fehlerbehebungen

- Cyber Crucible verzeichnete eine verringerte Genauigkeit bei der Entscheidungsfindung der Verhaltensmodelle, aufgrund des Verlusts von Telemetriedaten, wenn mehrere Programme sich gegenseitig aufrufen, eines der Programme jedoch innerhalb von Millisekunden beendet wurde.
 - In einer Kette, in der Programm A Programm B ausführt. Programm B startet Programm C, wird jedoch innerhalb von Millisekunden beendet (in der Regel ein stiller Absturz, jedoch nicht immer). Die Verhaltensanalyse von Cyber Crucible verfügte über die Variablen von Programm A und Programm C, hatte jedoch keine Zeit, Programm B vollständig zu analysieren, da erwartet wurde, dass es weiterhin ausgeführt wird.
 - Dies wurde korrigiert, was zu einer präziseren Entscheidungsfindung durch die hyperautomatisierte Entscheidungs-Engine von Cyber Crucible führt.

WHCP/WHQL- Validierungsstatus

Validiert.

MD5-Hashes

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

4.4.1.2

Funktionen

- Erhöhte verfügbare Spezifität für Whitelists, wie z. B. Pfad und Argumente des übergeordneten Prozesses.
- Erweiterte Unterstützung der Identitätszugriffsanalyse auf weitere Anmeldedatenbanken.
 - Der Identitätszugriff wird nun auch für Slack, Opera, Thunderbird, Discord und Vivaldi überwacht.
- Erweiterte Whitelist-Unterstützung um den Identitätszugriff.

Fehlerbehebungen

- Reduzierte die zwischen den Agenten und der REST-API genutzte Bandbreite.
- Behoben: Bei einigen älteren Windows-Server-Editionen wurden Canaries im Explorer angezeigt.
- Behoben: In einigen Identitätszugriffsprotokollen fehlten Zertifikatsvertrauensindikatoren.

WHCP/WHQL-Validierungsstatus

Validiert

MD5-Hashes

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

4.4.1.3

Funktionen

- Die Überwachung von Anmeldeinformationen/Identitäten umfasst nun verschiedene VPN-, Kryptowährungs-Wallet- und andere Anwendungen.
- In einer (häufig vorkommenden) Kette betroffener Prozesse während eines Angriffs (der Angreifer bewegt sich von einem laufenden Programm A zu B, zu C, und D wird für den Datendiebstahl verwendet) wird das „Patient-0“-Programm A angehalten, aber Patient D wird als der Prozess gemeldet, der das Diebstahlverhalten ausführt.
 - Der Speicherzustand wird während der gesamten Prozessketten für zukünftige forensische Analysen erhalten und protokolliert.
- Falls bei einer automatisierten Reaktion der Speicher eines laufenden Prozesses verändert wurde, wird diese Speicheränderung konfigurierbar an Cyber Crucible zur Rückentwicklung und weiteren Analyse hochgeladen.
- Im Falle eines nicht bösartigen Speicherfehlers in einer Anwendung können Verhaltensausnahmen („Whitelists“) nun bestimmte Speicherbeschädigungsereignisse als unbedenklich kennzeichnen. Dies verhindert nicht, dass das Programm selbst aufgrund des Fehlers abstürzt oder Daten verliert, aber Cyber Crucible weiß dann, diesen Fehler bei der Suche nach bösartiger Code-Injektion in laufende Prozesse (Process Injection/Hollowing) zu ignorieren.

Fehlerbehebungen

- Eine Schwachstelle wurde behoben, bei der Binärdateien während der Aktualisierung der CC-Binärdateien von einem privilegierten Prozess gelöscht werden konnten.
- Eine Schwachstelle wurde behoben, bei der Registrierungsschlüssel während der Aktualisierung der CC-Binärdateien von einem privilegierten Prozess gelöscht oder verändert werden konnten.
- Die Nachverfolgung des Speicherzustands wurde korrigiert, wenn ein Prozess während der Speicherbewertung durch Cyber Crucible im Arbeitsspeicher gepatcht wird.
- Die Nachverfolgung des Speicherzustands wurde unter bestimmten Bedingungen korrigiert, bei denen Speicher zwischen Speicherseiten neu zugewiesen wird.
- Kleinere Effizienzverbesserungen bei der CPU-Auslastung, die wahrscheinlich zu gering sind, um im Task-Manager sichtbar zu werden, da die Auslastung normalerweise <1 % beträgt.

WHCP/WHQL-Validierungsstatus

Validiert

MD5-Hashes

```
service.exe    = 90a6ca2f5b7a76b847052f3d420f0c9b
assistant.exe  = b62ee623f74171f4a3f34ff129188174
CCRRSecMon.sys (Windows10)      = dfdce4016f6920e844615b3d506ec2e2
CCRRSecMon.sys (Windows8)       = 59bbd41c883ca0205fd3adbfd5dbb6
CCRRSecMon.sys (Windows7)       = 88e6f047f7fa26e717a24f5fd7b33dc5
```

4.4.1.3.1

Es wurde Einblick in einige Systemprozesse gewonnen, die bereits vor dem Laden des Cyber-Crucible-Treibers initialisiert werden.

MD5-Hashes:

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

4.4.1.3.2

Zusätzliche Telemetriedaten für die durch 4.4.1.3.1 nun sichtbaren Systemprozesse wurden hinzugefügt.

MD5-Hashes:

```
service.exe: 47f408d6102eb06a94f2244cf139a0a5
assistant.exe: 86733da51ee703f93dcda9346231cca6
win7/CCRRSecMon.sys: b01e8933fa9ac9f0a049527b20d9f679
win8/CCRRSecMon.sys: 4467124cf7e8b5ab5652169f9eb41663
win10/CCRRSecMon.sys: 8f06de95303eeac038002ec27c297811
```

4.4.1.3.3

Einige Vorfälle wurden korrigiert, die Daten für den falschen Prozess enthielten, wenn ein Prozess während der Berechnung beendet wird.

MD5-Hashes:

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

4.4.1.3.4

Optimierung der Speicherberechnungen in Vorbereitung auf 4.4.1.4.

MD5-Hashes:

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

4.4.1.4

Funktionen

- Verbesserte Mustererkennungsfunktionen im Verhaltensmodell.
 - Dies ist besonders relevant für die zusätzliche Abdeckung von Speicherorten für Identitätsdaten, wie z. B. Kryptowährungs-Wallet-Speicherorten.
- Erweiterte Softwareabhängigkeitsfunktionalität für (Cyber Crucible) Bibliotheken, die für den bevorstehenden vollautomatischen Identitätszugriffsschutz verwendet werden.
- Opt-in-Möglichkeit, den Agenten im abgesicherten Modus auszuführen

Fehlerbehebungen

- Optimierung der Speichernutzung im Dienst. Dies wäre nur auf sehr stark ausgelasteten Servern aufgetreten, auf denen gleichzeitig viele Verhaltensanalysen (durch Cyber Crucible) stattfanden.

MD5-Hashes

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

4.4.2.0

Funktionen

- Verbesserte Überwachungs- und Präventionsfunktionen für den automatisierten Schutz des Identitätszugriffs.
- Optimierung der Netzwerknutzung durch variable Kommunikationsraten in Abhängigkeit vom Client-Verhalten.

Fehlerbehebungen

- Nicht zutreffend

MD5-Hashes

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

4.4.2.1

Fehlerbehebungen

- Optimierte Verfolgung von Identitätsinformationen für Anwendungen mit einer großen Anzahl tief verschachtelter Verzeichnisse.

MD5-Hashes

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


4.4.2.2

Funktionen

- Keine

Fehlerbehebungen

- Optimierung der Variablenverarbeitung für eine Art von Verhalten.
 - Ursache: Ein nicht näher bezeichnetes Sicherheitsprodukt erzeugte eine sehr große Anzahl an Verhaltensweisen auf einigen großen Servern, was zu einer übermäßigen Speichernutzung von Cyber Crucible führte.
 - Symptome: Die Speichernutzung von Cyber Crucible springt von wenigen MB auf mehrere GB. Auch die Speichernutzung des Sicherheitsprodukts stieg um das 100-fache an, auf über 250 GB. Sollten Sie dies feststellen, eröffnen Sie bitte ein Support-Ticket, damit wir Ihnen helfen können, da dies möglicherweise unabhängig von Cyber Crucible auftritt. Wir vermuten, dass es sich hierbei ebenfalls um ein Problem des Sicherheitsprodukts handelte, unabhängig von der Optimierung durch Cyber Crucible.
 - Behebung: Diese Verhaltensvariablen-Verfolgung wurde von einem Algorithmus, der für eine geringe Datenmenge ausgelegt war, auf einen Algorithmus für große Datenmengen umgestellt, wie er auch an anderer Stelle im Treiber verwendet wird.
 - Wer ist betroffen? Dieses Problem wurde nur bei einem Kunden beobachtet, und auch dort nur bei einem kleinen Teil seiner großen Server. Unabhängig davon wird dieses Update an alle Kunden ausgeliefert.

MD5-Hashes

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

4.4.2.3

Funktionen

- Keine

Fehlerbehebungen

- Kompatibilitätsprobleme mit Acronis behoben

MD5-Hashes

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

4.4.2.4

Funktionen

- Unterstützung für Anmeldedatenschutz für Microsoft Teams und Signal Messenger

Fehlerbehebungen

- Netzwerkbezogene Protokolle im abgesicherten Modus ohne Netzwerkunterstützung unterdrückt
- Bei der Deinstallation werden einige Agent-Daten im temporären Speicherordner von Windows gesichert

MD5-Hashes

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

4.4.2.5

Funktionen

- Keine

Fehlerbehebungen

- Reduzierte Netzwerknutzung beim gleichzeitigen Versenden großer Mengen an Berichten
- Fehlerbehebung bei der Verarbeitung einiger Zertifikatsdaten

MD5-Hashes

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

4.4.2.6

Funktionen

- Keine

Fehlerbehebungen

- Reduzierter Speicherverbrauch auf Servern mit vielen eindeutigen Programmzertifikaten

MD5-Hashes

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

4.4.2.7

Funktionen

- Keine

Fehlerbehebungen

- Reduzierter Speicherverbrauch bei der Verarbeitung von Programmen, die undefiniertes Verhalten bei der Abfrage von Verzeichnissen verwenden

MD5-Hashes

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

4.4.2.8

Funktionen

- Keine

Fehlerbehebungen

- Erweiterte Protokollierung und Telemetrie für fehlerhafte Systemzustände
- Erhöhte Stabilität der Identitätsschutzfunktionen beim Systemstart

MD5-Hashes

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

4.4.3.0

Funktionen

- Zusätzlich zu den bestehenden Dienstschutzmaßnahmen startet der Kernelmodus-Treiber den Dienst neu, falls dieser aus irgendeinem Grund beendet wird.

Behebungen

- Keine

MD5-Hashes

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


4.4.3.2

Funktionen

- Keine

Fehlerbehebungen

- Reduzierte CPU-Auslastung beim Start von Prozessen.
- Reduzierte CPU-Auslastung bei Vertrauensbestimmungen während aufeinanderfolgender Verzeichnisabfragen.

MD5-Hashes

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

4.4.3.1

Funktionen

- Keine

Fehlerbehebungen

- Ein Problem behoben, bei dem auf einigen Rechnern mit ungewöhnlichen Windows-Installationsmerkmalen Canaries im Explorer sichtbar waren.

MD5-Hashes

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

4.4.4.0

Funktionen

- Berichte zu Vorfällen und Telemetriedaten werden für Offline-Szenarien auf der Festplatte gespeichert.
 - Aufgrund beobachteter Manipulationsversuche gegen mehrere EDR-/XDR-Protokollierungsspeicher hat Cyber Crucible vor der Bereitstellung dieser Funktion einen Schutz auf Kernel-Ebene für die auf der Festplatte gespeicherten Daten aktiviert.
- Erhöhter Schutz des Serviceprozesses, der für die Backend-Kommunikation und Updates verwendet wird, im Rahmen der vorausschauenden Zero-Trust-Härtung.
 - Dies erfolgte nicht als Reaktion auf eine bestehende Bedrohung, sondern proaktiv im Hinblick auf eine Bedrohung, die das Team kommen sieht.

Fehlerbehebungen

- Behoben: Prozesse, die beim Systemstart geladen werden, waren im Dashboard unter „Prozesserstellungen“ nicht verfügbar.
- Verhindert, dass zwei Installationsprogramme gleichzeitig ausgeführt werden, was dazu führen würde, dass dieselbe Maschine zweimal registriert wird.

MD5-Hashes

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

4.4.4.4

Funktionen

- Keine

Fehlerbehebungen

- Verbesserte Leistung beim Parsen von Zertifikatsdaten beim Systemstart.

MD5-Hashes

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

4.4.5.1

Funktionen

- Reduzierte Bandbreitennutzung:
 - Verwendung von Komprimierung für größere Telemetriedaten und größere Serverantworten
 - Verwendung von HTTP/2 für komprimierte Header und höhere Socket-Effizienz
- Erweiterte Einblicke in Zertifikatsvorgänge.

Fehlerbehebungen

- Kodierung der Zertifikatsmetadaten in Rohmetriedaten, wenn nicht RFC-konforme Labels vorhanden sind. Netzwerksicherheitsinfrastruktur beschädigte oder löschte die Nutzdaten, wodurch der Agent so lange erneut übertrug, bis die Übertragung erfolgreich war.

MD5-Hashes

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

4.4.5.2

Funktionen

- Neue Telemetrie auf Kernel-Ebene für netzwerkbasierende Verhaltensweisen, um mögliche clientseitige Netzwerkfehler besser zu identifizieren oder Optimierungsmöglichkeiten zu erkennen
- Ausgehende Telemetrie wird nun gebündelt und gemeinsam gesendet, genau wie die eingehenden Einstellungen
 - Übertragung mit einer zeitlichen Abweichung von 25 %, sodass nicht alle Geräte gleichzeitig Pakete über ein Client-Netzwerk senden
- HTTP/2 wird nun durchgängig vollständig genutzt

Fehlerbehebungen

- Reduzierte minimale Anzahl an genutzten Threads im Userspace
- Reduzierte CPU-Auslastung für den Userspace-Dienst
- Die Authentifizierung zwischen Agent und Server wird nun effizienter durchgeführt
- Der bisherige Algorithmus für Dienst-Ruhezustand <> Neustart wurde ersetzt, wenn keine Lizenzen verfügbar waren.
 - Der bisherige Algorithmus verursachte alle 15 Minuten einen Eintrag „Dienst wurde unerwartet beendet“ im Ereignis-Manager.
 - Es dem Betriebssystem zu erlauben, den Dienst abzuschalten (was von Kriminellen und anderen Sicherheitstools missbraucht wird), hätte einen „sauberen“ Dienst-Neustart ohne Einträge im Ereignis-Manager ermöglicht. Anstatt diese Schwachstelle zu schaffen, startete sich der Dienst von Cyber Crucible selbst neu, ohne Einbindung von Windows, was zu dem Ereigniseintrag führte.

MD5-Hashes

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

4.4.5.3

Funktionen

- Eine zweite Domain für die Serverkommunikation wurde hinzugefügt ([Domainliste hier ansehen](#)).
 - Bei Kommunikationsproblemen mit einer Domain wechselt der Agent automatisch zur anderen.

Fehlerbehebungen

- Einige alte Legacy-Zeichenfolgen, die sich auf „Ransomware Rewind“ bezogen, wurden geändert und verweisen nun auf „Cyber Crucible“.

MD5-Hashes

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

4.4.5.9

Funktionen

- Erhöhte Härtung von Teilen der Funktionalität, die zuvor von den Windows-Kryptografiebibliotheken übernommen wurde, wird nun vom Cyber Crucible-Kerneltreiber durchgeführt.
 - Dies umfasst sowohl eine generelle Härtung als auch eine Erhöhung der Telemetrie, die auf mögliche Angriffe gegen Windows-Kryptografiebibliotheken und -APIs hinweist.
- Dies ist ein Meilenstein-Release, das auf den inkrementellen Releases von 4.4.5.4 bis 4.4.5.8 aufbaut, die alle auf der bisherigen Härtungsfunktionalität zur Kryptografieanalyse basieren.
 - Erste Telemetriedaten deuten darauf hin, dass die Fehler in den Windows-Zertifikats- und Kryptografiebibliotheken von Cyber Crucible ordnungsgemäß behandelt wurden.
 - Es ist derzeit nicht bekannt, welcher Prozentsatz der Probleme auf Ausnutzung versus einen Fehler in einer Windows-Kernbibliothek zurückzuführen ist. Bitte wenden Sie sich bei Bedarf an Ihren Cyber Crucible-Ansprechpartner, um dies weiter zu besprechen.

Fehlerbehebungen

- Behoben: Einige Prozessberichte meldeten das aufgeführte Zertifikat fälschlicherweise als „nicht vertrauenswürdig“, was auf einen Funktionsverlust der Windows-Zertifikatsbibliothek zurückzuführen war.

MD5-Hashes

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


4.4.5.8

Funktionen

- Verstärkte Härtung von Teilen der Funktionalität, die zuvor von den Windows-Kryptografiebibliotheken durchgeführt wurde, wird nun vom Cyber Crucible-Kerneltreiber übernommen.
 - Dies umfasst sowohl eine allgemeine Härtung als auch eine verbesserte Telemetrie, die auf mögliche Angriffe gegen Windows-Kryptografiebibliotheken und -APIs hinweist.

Fehlerbehebungen

- Behoben: Einige Prozessberichte meldeten das aufgeführte Zertifikat fälschlicherweise als „nicht vertrauenswürdig“, aufgrund eines Funktionsverlusts der Windows-Zertifikatsbibliothek.

MD5-Hashes

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

4.4.5.5

Funktionen

- Erhöhte Härtung von Teilen der Funktionalität, die zuvor von den Windows-Kryptografiebibliotheken durchgeführt wurden, werden nun vom Cyber Crucible-Kerneltreiber durchgeführt.
 - Dies ist sowohl eine allgemeine Härtung als auch eine Erhöhung der Telemetrie, die auf mögliche Angriffe gegen Windows-Kryptografiebibliotheken und -APIs hinweist.

Fehlerbehebungen

- Behoben: Einige Prozessberichte meldeten das aufgeführte Zertifikat aufgrund eines Funktionsverlusts der Windows-Zertifikatsbibliothek fälschlicherweise als „nicht vertrauenswürdig“.

MD5-Hashes

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

4.4.5.6

Funktionen

- Erhöhte Härtung von Teilen der Funktionalität, die zuvor von den Windows-Kryptografiebibliotheken durchgeführt wurde, wird nun vom Cyber Crucible-Kerneltreiber durchgeführt.
 - Dies umfasst sowohl eine allgemeine Härtung als auch eine erhöhte Telemetrie, die auf mögliche Angriffe gegen Windows-Kryptografiebibliotheken und -APIs hinweist.

Fehlerbehebungen

- Behebung eines Fehlers, bei dem einige Prozessberichte das aufgeführte Zertifikat aufgrund eines Funktionsverlusts der Windows-Zertifikatsbibliothek fälschlicherweise als „nicht vertrauenswürdig“ meldeten.

MD5-Hashes

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

4.4.5.7

Funktionen

- Erhöhte Härtung von Teilen der Funktionalität, die zuvor von den Windows-Kryptografiebibliotheken durchgeführt wurde, wird nun vom Cyber Crucible-Kernel-Treiber übernommen.
 - Dies umfasst sowohl eine allgemeine Härtung als auch eine erhöhte Telemetrie, die auf mögliche Angriffe gegen Windows-Kryptografiebibliotheken und -APIs hinweist.

Behebungen

- Behoben: Einige Prozessberichte meldeten das aufgeführte Zertifikat aufgrund eines Funktionsverlusts der Windows-Zertifikatsbibliothek fälschlicherweise als „nicht vertrauenswürdig“.

MD5-Hashes

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

4.4.5.4

Funktionen

- Erhöhte Härtung von Teilen der Funktionalität, die zuvor von den Windows-Kryptografiebibliotheken durchgeführt wurde, werden nun vom Cyber Crucible Kernel-Treiber übernommen.
 - Dies umfasst sowohl allgemeine Härtung als auch eine erhöhte Telemetrie, die auf mögliche Angriffe gegen Windows-Kryptografiebibliotheken und APIs hinweist.

Fehlerbehebungen

- Ein Fehler wurde behoben, bei dem einige Prozessberichte das aufgeführte Zertifikat aufgrund eines Funktionsverlusts der Windows-Zertifikatsbibliothek fälschlicherweise als „nicht vertrauenswürdig“ meldeten.

MD5-Hashes

```
service.exe = fd2157d8deed07ec45406a1d323359c
CCRRSecMon.sys (Windows7) = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8) = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10) = 0d1fc32fba2cb878ce8cb0f549b8d167
```

4.4.6.0

Funktionen

- CPU-Leistungsverbesserung für einige Anwendungen, die im Rahmen ihres Anwendungsverhaltens eine große Anzahl automatisierter und gleichzeitiger Verzeichnisdurchläufe auslösen.

Fehlerbehebungen

.

MD5-Hashes

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

4.4.6.1

Funktionen

- Weitere Migration vom Produktnamen „Ransomware Rewind“ zu „Cyber Crucible“.
 - Der bisherige Dienstname "Ransomware Rewind" wird zu "CyberCrucibleAgent" migriert. Der Prozessname bleibt unverändert.
 - Der Registrierungsschlüssel in HKLM\SOFTWARE wird vom bisherigen RansomwareRewind zum aktuellen CyberCrucibleAgent migriert.

Fehlerbehebungen

- Ein Fehler wurde behoben, bei dem einige 32-Bit-Prozesse fälschlicherweise als „geänderter Speicher“ ausgelöst wurden, wenn das Prozessabbild die maximal zulässige Größe eines 32-Bit-Prozesses erreicht.

MD5-Hashes

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

4.4.6.2

Funktionen

- Optionale „Zugriffstyp“-Kennzeichnungen hinzugefügt, die Endbenutzern für eine detailliertere Verhaltenszugriffssteuerung zur Verfügung gestellt werden.

Fehlerbehebungen

- Keine.

MD5-Hashwerte

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


4.4.6.3

Funktionen

- Optionale SOCKS5-Proxy-Unterstützung hinzugefügt, um die Agenten-Bereitstellung zu erleichtern.

Fehlerbehebungen

- Neuinstallationen von älteren Agenten, die eine falsche Installations-ID verwendeten, wurden behoben.
- Bestehende Installationen älterer Installationsprogramme mit einem nicht in Anführungszeichen gesetzten Dienstpfad wurden behoben.

MD5-Hashes

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

4.4.6.4

Funktionen

- Informationen zum Speicher des übergeordneten Prozesses sind für Prozessberichte verfügbar, wenn Änderungen erkannt wurden.

Verbesserungen

- Einige Serverkommunikationsfrequenzen geändert, sodass für die Anpassung kein Neustart mehr erforderlich ist.

Fehlerbehebungen

Keine in dieser Version.

MD5-Hashes

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

4.4.7.0

Funktionen

- Beginn der Einführung von JWE-basierter HTTPS-Kommunikation.
 - Verschlüsselungsschlüssel sind für jeden Agenten eindeutig.
 - Alle Nutzdaten werden unter HTTPS verschlüsselt. Während der anfänglichen Einführung standardmäßig deaktiviert.
 - Möglichkeit, optional von JWE-verschlüsseltem HTTPS zu unverschlüsseltem HTTPS zurückzukehren, falls JWE-formatierte Nutzdaten nicht erfolgreich übertragen werden.

MD5-Hashes

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

4.4.7.1

Funktionen

- Mehr Telemetriedaten für Prozesserstellungen und Vorfälle
 - Benutzer-SID
 - Benutzer-Anmeldename im Down-Level-Format
 - Ob der Prozess mit erhöhten Rechten ausgeführt wird (Als Administrator ausführen)
- Vorfälle melden nun, wo iterativer Datenzugriff stattgefunden hat

Fehlerbehebungen

- Reduzierter Speicherverbrauch bei Serververbindungsproblemen und gleichzeitig hohem Telemetrieaufkommen
- Reduzierter Speicherverbrauch bei der Vorfallsmeldung

MD5-Hashes

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

4.4.7.3

Funktionen

- DMZ-Modus
 - Optionale Konfiguration zur Verwendung eines signierten CA-Bundles für die TLS-Kommunikation mit Authentifizierungs- und Telemetrieservern. Diese CA-Bundles werden anschließend durch die proprietären Anti-Tampering-Funktionen von Cyber Crucible vor Manipulation oder Löschung geschützt.
 - OSCP- und CRL-Prüfungen sind deaktiviert, um die Liste der Domains zu reduzieren, die durch eine Firewall zugelassen werden müssen.

Fehlerbehebungen

- Reduzierter Speicherverbrauch und geringere CPU-Zeit für die Übermittlung von Speicher-Diffs, insbesondere nach längeren Offline-Zeiträumen.

MD5-Hashes

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

4.4.8.0

Funktionen

- Authenticode-Telemetrie im Kernel-Modus
 - Für höhere Geschwindigkeit und Zuverlässigkeit werden Zertifikatsdaten für Prozesserstellungen und Vorfälle künftig ausschließlich vom Treiber erfasst.
 - Dieses Update entfernt keine Abhängigkeiten von den Windows-Kryptografiebibliotheken, führt jedoch kryptografische Berechnungen parallel durch. Langfristig kann die Abhängigkeit von Windows möglicherweise vollständig entfallen.

Fehlerbehebungen

- Reduzierter Speicherverbrauch und verringerte CPU-Zeit bei versuchter Ereignisübermittlung im Offline-Zustand, während der die Telemetrie sicher gespeichert wird, bis das Gerät die Verbindung zu den Cyber Crucible-Servern wiederherstellt.
- Einige Nvidia-Treiberinstallationsprogramme gingen fälschlicherweise davon aus, keine Berechtigung zur Installation zu haben, da eine interne Microsoft-Kernelfunktion verwendet wurde, um auf von Cyber Crucible installierte Dateien zuzugreifen.
- Inkompatibilität mit dem JWE-Modus und dem DMZ-Modus behoben

MD5-Hashes

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

4.4.8.1

Funktionen

- Ausführbare Metadaten wie Produktversion, Firmenname usw. für Prozesse im Arbeitsspeicher werden vom Treiber über Kernel-Sichtbarkeit gemeldet. Normale Funktionalität ist die Verwendung von Windows-API-Aufrufen im User-Space. Diese Umstellung auf das Parsen im Kernel entfernt die (beobachtete) Möglichkeit für Angreifer, die Prozessinformationen zu manipulieren.
- Authentifizierungsinformationen des Agenten werden an anderer Stelle im System repliziert, um sie wiederherzustellen, falls die Registrierung durch einen böartigen Treiber beschädigt wird.

Verbesserungen

- Serververbindungsfehler werden vom Agenten nur minimal protokolliert, wodurch die Protokollgröße auf der Festplatte reduziert wird.

Fehlerbehebungen

- Entfällt

MD5-Hashes

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

4.4.8.2

Funktionen

- Unterstützung für ein optionales Symbol im Systembereich (Tray) hinzugefügt. Diese Funktion ist standardmäßig deaktiviert.

Fehlerbehebungen

- Workaround für ein Problem bei Kernel-Windows-API-Hashing-Anfragen hinzugefügt. Der Workaround kann zu einem späteren Zeitpunkt entfernt werden, falls das Windows-Problem behoben wird, möglicherweise beim nächsten Kernel-Update.

MD5-Hashes

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


4.4.9.0

Funktionen

- Kernelmodus-DLL-Telemetrie
 - Zertifikatanalyse und Vertrauensberechnung für alle im Treiber geladenen DLLs.

Fehlerbehebungen

- Keine.

MD5-Hashes

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

4.4.9.1

Funktionen

- Keine.

Fehlerbehebungen

- Erhöhte Menge an Telemetriedaten, die vom Dienst gleichzeitig für Erstellungs- und Injektionsdaten verarbeitet werden.
- Angepasste Reihenfolge der Canaries für Programme, die ungewöhnliche Dateiiterationsmethoden verwenden.
- Angepasste ACL bei einigen Canaries, um besser zu realen Dateisystemen zu passen.

MD5-Hashes

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

4.4.9.2

Funktionen

- Speicheränderungsverfolgung für geladene DLLs.
- Erstellung von Speicher-Diffs für geänderte DLLs.

Fehlerbehebungen

- Behebung eines Problems, bei dem einige nicht konforme DLLs zu falschen Authenticode-Hash-Ergebnissen führten.

MD5-Hashes

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

4.4.9.4

Fehlerbehebungen

- Service-Dump-Dateien sind jetzt auf 10 pro Kombination aus Version und Thread begrenzt.

MD5-Hashes

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

4.5.0.0

Funktionen

- KI-Kernel-Firewall
- Beschleunigung der Authenticode-Hash-Berechnung
- Deutlich reduzierter Speicherverbrauch für DLL-Telemetrie
- Erhöhte Sichtbarkeit von Speicheränderungen in DLLs

Fehlerbehebungen

- Behebung der Kompatibilität der Dienstwiederherstellung mit 24H2

MD5-Hashes

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

4.5.0.1

Funktionen

- Option zur Migration auf die gehostete OAuth-Authentifizierungsserver-Domain
- Task zur dynamischen Konfiguration von REST- und OAuth-Server-URLs

Fehlerbehebungen

- Keine.

MD5-Hashes

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

4.5.0.2

Funktionen

- Keine.

Fehlerbehebungen

- Reduzierter Speicherverbrauch für die AI Kernel Firewall.
- Schnellere Nutzung der neuen Authentifizierungs-Endpunkte.
- Aufrufe von icanhazip.com entfernt, zuvor optional, aber nicht mehr erforderlich.

MD5-Hashes

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

4.5.0.3

Funktionen

- Die Statusanzeige im Infobereich zeigt nun bei Neuinstallationen den Status der Selbstkonfiguration an.

MD5-Hashes

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


4.5.1.0

Funktionen

- OpenSSL wird nun für die TLS-Kommunikation verwendet.
 - Dies sollte Probleme auf älteren Betriebssystemversionen umgehen, die nicht mehr für neuere TLS-Anforderungen gepatcht werden.

Fehlerbehebungen

- Verbesserte Parsing-Unterstützung für nicht konforme Authenticode-Signaturen.

MD5-Hashes

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

4.5.1.2

Funktionen

- Veraltete Zertifikatsvalidierung entfernt, die auf integrierten, langsamen Windows-Bibliotheken beruhte.
- Möglichkeit hinzugefügt, Protokolle bei der Deinstallation zu behalten.

MD5-Hashes

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

4.5.2.1

Funktionen

- Breite Veröffentlichung von Berichten für den Fortress AI-Zugriff

Fehlerbehebungen

- Optimierung der Cyber Crucible-Kernel-Operationen, die keine Windows-APIs verwenden, um der erhöhten Latenz in einigen Windows-Umgebungen um etwa 20 % entgegenzuwirken.

MD5-Hashes

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

4.5.2.2

Fehlerbehebungen

- Optimierung der Cyber Crucible-Kernel-Vorgänge durch Vermeidung problematischer Windows-Ereignis- und Datenbus-Kernfunktionen des Betriebssystems.

MD5-Hashes

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

4.5.3.0

Funktionen

- FortressAI
 - Benachrichtigungen hinzugefügt, wenn ein Richtlinienverstoß gemeldet wird
 - Integration mit dem Windows-Benachrichtigungscenter
 - GUI zur Anzeige des Verlaufs von Richtlinienbenachrichtigungen hinzugefügt
 - Simulationsmodus hinzugefügt
- Cyber Crucible Core
 - Konfigurierbare asynchrone DLL-Analysen für Maschinen mit minimalen Hardware-Ressourcen
 - Analysen und Telemetrie zur Prozesserstellung
 - verwendet jetzt Festplattenpersistenz
 - Abhängigkeiten von Windows MiniFilter entfernt
 - Analysen und Telemetrie zu Prozessinjektionen
 - verwendet jetzt Festplattenpersistenz
 - Abhängigkeiten von Windows MiniFilter entfernt
 - Zusätzliche Abhängigkeiten von Windows-Kernel-Ressourcen entfernt

Fehlerbehebungen

- Optimierung der Telemetrieberichterstattung für eine noch schnellere Meldung
- Deadlock behoben, der durch exklusiven versus gemeinsamen Kernel-Ressourcenzugriff für eine bestimmte Kernel-Ressource entstand, die von Microsoft Defender benötigt wird, wenn Defender den Treiber-Debugmodus aktiviert

MD5-Hashes

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

4.5.3.1

Funktionen

- FortressAI
 - Erkennt Versuche, Richtlinienkontrollen durch die Verwendung von Screenshots zu umgehen.
- Cyber Crucible Core
 - Unterstützt die Neuinitialisierung der Identität eines Agenten, ohne dass eine vollständige Neubereitstellung erforderlich ist.
 - Dies behebt Situationen, in denen ein Rechner mit installiertem Cyber Crucible geklont wird und dadurch die Lizenz- und Agenten-Kennungen ebenfalls geklont werden. Genau wie bei IP-Adressen, MAC-Adressen, Rechnernamen und anderen eindeutigen Kennungen erkennt Cyber Crucible einen geklonten Agenten und weist die CC-Administratoren auf die Möglichkeit hin, neue CC-Kennungen zu generieren.

MD5-Hashes

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

4.5.3.2

Funktionen

- FortressAI
 - Keine
- Cyber Crucible Core
 - Verbesserung des Kernel-Puffer-Betriebs
 - Der Treiber nutzt Puffer, um Telemetriedaten vorübergehend zu speichern, die letztendlich an das Kundendashboard gesendet werden. Diese Aktivität ist getrennt von der Befüllung oder dem Betrieb des Verhaltensmodells zu betrachten.
 - Wenn ein Kernel-Puffer überlastet wird, steigt die System-CPU-Auslastung.
 - Dies würde nur aufgrund eines großen Betriebssystemfehlers oder eines Angriffs auf die Systeme auftreten.
 - Eine automatisierte Kundenbenachrichtigung bei sehr hoher Pufferauslastung ist ab 1. Juni 2026 verfügbar.
 - Fast alle Kernel-Pufferoperationen für CC betreffen drei primäre Puffer.
 - Der Auslastungsprozentsatz aller drei primären Puffer wird nun an die CC-Infrastruktur übermittelt, um Metriken zu erfassen und die Pufferauslastung pro Agent zu identifizieren.
 - Alle drei primären Puffer können in ihrer Größe remote angepasst werden, und ihr Status kann von den Nutzern verfolgt werden.

Fehlerbehebungen

- Ein kürzliches Update mit DotNet- und MSVC-Redistributable-Bibliotheken überlastete die Cyber Crucible-Puffer mit anhaltend sehr hohen (500 %+) Prozess- und DLL-Betriebsereignissen, was einige Kunden betraf. Obwohl die Pufferauslastung wieder auf das normale Niveau von 1-5 % zurückgekehrt ist, einschließlich bei den betroffenen Kunden, wurden alle Puffer in ihrer Größe verdoppelt, um zukünftige Probleme zu vermeiden. Dies ergänzt die oben aufgeführten Konfigurationsmöglichkeiten.

Sha-256-Hashes

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

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