???? ???? ????????

- 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

???? ???????? ???? ???? ???????

- 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

???????

- بالنسبة للمجموعات التي تم تمكين القياس عن بُعد (telemetry) فيها، تمت إضافة بيانات Active Directory إلى قائمة مراقبة سرقة بيانات الاعتماد

?????????

- إزالة الإدخالات المكررة للأجهزة المحلية ومشاركات الشبكة في بعض البيئات.
- تحسين السلوك الخاص ببعض عمليات إعادة بناء قاعدة بيانات الصور المصغّرة التي كانت تتسبب في حوادث
- إصلاح خلل في التحقق من الترخيص كان من الممكن أن يزيد من زمن بدء التشغيل
- تحسين السلوك الخاص بالوصول إلى الملفات على وسائط الكتابة لمرة واحدة مثل أقراص CD ومحركات أشرطة WORM

???? ?????? ?? WHCP/WHQL

تم التحقق

??? ????? MD5

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

4.4.0.9.1

???????

ال يوجد - تحديث صيانة.

??????????

- تم إصلاح مشكلة تجاهل بعض مشاركات الشبكة (network shares) المتصلة من قِبل المستخدم في التحليلات في البداية.
- تم تحسين سلوك النتائج الإيجابية الكاذبة المرتبطة بظهور المشاركات أثناء جلسات المستخدم، متبوعة بسرعة بمربع حوار "حفظ باسم" (Save As).

???? ?????? ?? WHCP/WHQL

تم التحقق.

?????? MD5

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

4.4.1.0

???????

- توسيع نطاق الدعم لتحليلات حقن العمليات، لزيادة دقة اكتشاف النواي الخبيثة مقابل الحميدة للتطبيقات بشكل كبير.
  - أصبح هذا الأمر مهمًا بشكل خاص بسبب قيام عدد صغير (أقل من 0.02%) من الأجهزة في بيانات القياس عن بُعد الخاصة بـ Cyber Crucible بإصدار تنبيهات بشأن سلوكيات حقن العمليات العدوانية لعمليات النظام.
- زيادة قدرة المراقبة لعمليات النظام غير الموقّعة.
  - جاء هذا جزئيًا استجابة لتركيز المهاجمين بشكل كبير على استخدام تلك العمليات أثناء عمليات الحركة الجانبية (على النظام، وبين الأنظمة).

??????????

- تم تغيير سلوك تعديل الملفات لتقليل النتائج الإيجابية الكاذبة من خلال عدم إطلاق التنبيهات بعد الآن عند حدوث إجراءات حميدة معينة، وذلك عبر توفير سياق إضافي على مستوى النواة (kernel) لسلوكيات وصول العملية إلى الملفات.

???? ?????? ?? WHCP/WHQL

تم التحقق.

??? ????? MD5

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

4.4.1.1

???????

- تحسين المعالجة التحليلية للعلاقات بين العملية الأصلية والعمليات الفرعية، عندما تنتهي العملية الأصلية بسرعة قبل أن يكمل Cyber Crucible معالجتها (خلال أجزاء من الثانية بالميلي ثانية).
  - السيناريو الشائع جدًا هنا وهو أن المهاجمين (والبرامج الشرعية أيضًا) غالبًا ما يفتحون برامج متعددة، وأحيانًا في "سلسلة متتابعة" متعددة الخطوات. قد يكون هذا مقصودًا، أو نتيجة سلوك ويندوز أو تطبيقات أخرى "خلف الكواليس".
  - تستفيد نماذج Cyber Crucible السلوكية من متغيرات النشاط والحالة لجميع العمليات في سلسلة من عمليات التنفيذ لتحقيق أقصى درجات الدقة والسياق.

?????????

- واجه Cyber Crucible فقدانًا في دقة اتخاذ القرار الخاصة بالنموذج السلوكي، بسبب فقدان بيانات القياس عن بُعد عندما تستدعي برامج متعددة بعضها البعض، لكن أحد هذه البرامج ينتهي خلال أجزاء من الثانية بالميلي ثانية.
  - في سلسلة حيث ينفذ البرنامج A البرنامج B. يبدأ البرنامج B تشغيل البرنامج C، لكن البرنامج B ينتهي خلال أجزاء من الثانية بالميلي ثانية (عادةً ما يكون تعطلًا صامتًا، ولكن ليس دائمًا). يمتلك التحليل السلوكي لـ Cyber Crucible متغيرات البرنامج A والبرنامج C، لكنه لم يحصل على الوقت الكافي لتحليل البرنامج B بشكل كامل، لأنه كان يتوقع استمرار تشغيله.
  - تم تصحيح هذا الأمر، مما أدى إلى اتخاذ قرارات أكثر دقة من قبل محرك اتخاذ القرار فائق الأتمتة الخاص بـ Cyber Crucible.

???? ?????? WHCP/WHQL

تم الاعتماد.

?????? MD5

```
service.exe   = db76d0abc8f4bc4b2a093435bc314bde
assistant.exe = a5bac35d839d7a57fcccfceb011083c1
CCRRSecMon.sys (Windows10)       = 935e43368fa95ae740a3f04defcc390d
```

```
CCRRSecMon.sys (Windows8)        = ee555ad0f282f36dd11deada8d1ca9c7
CCRRSecMon.sys (Windows7)        = a6a5073c6565361b443651ef29e49490
```

4.4.1.2

???????

- زيادة الدقة المتاحة للقوائم البيضاء، مثل مسار العملية الأصلية (parent process path) والوسائط (arguments).
- توسيع دعم تحليلات الوصول إلى الهوية ليشمل المزيد من قواعد بيانات بيانات الاعتماد.
  - يتم الآن أيضًا مراقبة الوصول إلى الهوية لكل من Slack وOpera وThunderbird وDiscord وVivaldi.
- توسيع دعم القوائم البيضاء ليشمل الوصول إلى الهوية.

??????????

- تقليل عرض النطاق الترددي المستخدم بين الوكلاء (agents) وواجهة برمجة التطبيقات REST.
- إصلاح مشكلة ظهور الكناري (canaries) في مستكشف الملفات (Explorer) في بعض إصدارات Windows Server الأقدم.
- إصلاح مشكلة فقدان بعض سجلات الوصول إلى الهوية لمؤشرات ثقة الشهادة.

???? ?????? WHCP/WHQL

تم الاعتماد

?????? MD5

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

4.4.1.3

???????

- أصبحت ميزة مراقبة بيانات الاعتماد/الهوية تشمل الآن العديد من تطبيقات VPN، ومحافظ العملات المشفرة، وتطبيقات أخرى.
- في سلسلة (وهذا أمر شائع) من العمليات المتأثرة أثناء الهجوم (حيث ينتقل المهاجم من تشغيل البرنامج A، إلى B، إلى C، ويُستخدم D لسرقة البيانات)، يتم تعليق البرنامج "المريض 0" A، ولكن يُبلَّغ عن المريض D باعتباره العملية التي تقوم بسلوك السرقة.
  - يتم الحفاظ على حالة الذاكرة والإبلاغ عنها طوال سلاسل العمليات، لأغراض التحليل الجنائي المستقبلي.
- في حالة حدوث استجابة تلقائية تم فيها تعديل ذاكرة عملية قيد التشغيل، يتم رفع تعديل الذاكرة هذا (بشكل قابل للتهيئة) إلى Cyber Crucible لإجراء الهندسة العكسية والمزيد من التحليل.
- في حالة وجود خلل غير ضار في تعديل الذاكرة داخل تطبيق ما، أصبحت الاستثناءات السلوكية ("القوائم البيضاء") الآن قادرة على وضع علامة على أحداث معينة من تلف الذاكرة باعتبارها غير ضارة. لن يمنع هذا البرنامج نفسه من التعطل أو فقدان البيانات بسبب الخلل، ولكن سيعرف Cyber Crucible أن يتجاهل هذا الخلل أثناء البحث عن حقن الشيفرة الضارة في العمليات قيد التشغيل (حقن العمليات/إفراغها).

?????????

- تمت إزالة ثغرة أمنية كان من الممكن من خلالها حذف الملفات الثنائية بواسطة عملية ذات صلاحيات مرتفعة أثناء تحديث الملفات الثنائية الخاصة بـ CC.
- تمت إزالة ثغرة أمنية كان من الممكن من خلالها حذف أو تغيير مفاتيح السجل (registry keys) بواسطة عملية ذات صلاحيات مرتفعة أثناء تحديث الملفات الثنائية الخاصة بـ CC.
- تم تصحيح تتبع حالة الذاكرة عند تصحيح عملية (patched) في الذاكرة أثناء تقييم Cyber Crucible للذاكرة.
- تم تصحيح تتبع حالة الذاكرة في ظل ظروف معينة حيث يُعاد تخصيص الذاكرة بين صفحات الذاكرة.
- تحديثات طفيفة لكفاءة المعالج، من المرجح أنها أصغر من أن تُسجّل في مدير المهام، نظرًا لأن الاستخدام عادةً أقل من 1%

???? ?????? WHCP/WHQL

تم الاعتماد

??? ????? MD5

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

4.4.1.3.1

تم الحصول على رؤية لبعض عمليات النظام التي يتم تهيئتها قبل تحميل برنامج تشغيل (driver) Cyber Crucible.

قيم تجزئة MD5:

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

4.4.1.3.2

تمت إضافة قياس عن بُعد (telemetry) إضافي لعمليات النظام المرئية الآن نتيجة الإصدار 4.4.1.3.1.

قيم تجزئة MD5:

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

4.4.1.3.3

تم إصلاح بعض تقارير الحوادث التي كانت تتضمن بيانات لعملية خاطئة، عندما تتوقف عملية ما أثناء منتصف الحساب.

قيم تجزئة MD5:

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

4.4.1.3.4

تحسين حسابات الذاكرة، تمهيداً للإصدار 4.4.1.4.

قيم تجزئة MD5:

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

4.4.1.4

???????

- تحسين قدرات مطابقة الأنماط في النموذج السلوكي.
  - يُعد هذا الأمر ذا أهمية خاصة لتوسيع التغطية الخاصة بمواقع تخزين الهويات، مثل مواقع محافظ العملات المشفرة.
- زيادة ظائف الاعتماد البرمجي لمكتبات (Cyber Crucible) المستخدمة في الحماية الآلية الكاملة القادمة للوصول إلى الهوية.
- إمكانية الاشتراك الاختياري لتشغيل العميل في الوضع الآمن

??????????

- تحسين استخدام الذاكرة في الخدمة. لم يكن من الممكن ملاحظة هذا الأمر إلا على الخوادم شديدة الانشغال التي يجري فيها قدر كبير من التحليل السلوكي (بواسطة Cyber Crucible) في آن واحد.

?????? MD5

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

4.4.2.0

???????

- تحسين قدرات المراقبة والوقاية لحماية الوصول إلى الهوية بشكل آلي.
- تحسين استخدام الشبكة من خلال معدلات اتصال متغيرة تعتمد على سلوكيات العميل.

??????????

- لا يوجد

?????? MD5

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

4.4.2.1

??????????

- تحسين تتبع معلومات الهوية للتطبيقات ذات العدد الكبير من الأدلة المتداخلة بعمق.

?????? MD5

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

4.4.2.2

???????

- دجوي ال

??????????

- تحسين معالجة المتغيرات لنوع واحد من السلوك.
  - السبب: أنتج أحد منتجات الألمان غير المحدد عددًا كبيرًا جدًا من السلوكيات على عدد قليل من الخوادم الكبيرة، مما تسبب في استخدام مفرط للذاكرة من قبل Cyber Crucible.
  - الأعراض: يقفز استخدام الذاكرة لدى Cyber Crucible من بضعة ميغابايت إلى غيغابايتات. كما قفز استخدام الذاكرة لدى منتج الألمان بمقدار 100 ضعف أيضًا، ليتجاوز 250 غيغابايت. إذا واجهت هذه المشكلة، والتي قد تكون مستقلة عن Cyber Crucible، يرجى فتح تذكرة دعم حتى نتمكن من مساعدتك. نشتبه أن هذه كانت مشكلة في منتج الألمان أيضًا، بشكل مستقل عن تحسينات Cyber Crucible.
  - الإصلاح: تم نقل تتبع متغير السلوك هذا من خوارزمية كانت تتوقع كثافة منخفضة إلى خوارزمية عالية الكثافة، على غرار ما هو مستخدم في أماكن أخرى من برنامج التشغيل (driver).
  - من هو المتأثر؟ لوحظت هذه المشكلة لدى عميل واحد فقط، وفقط في جزء صغير من خوادمه الكبيرة. بغض النظر عن ذلك - يتم نشر هذا التحديث لجميع العملاء.

??? ????? MD5

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

4.4.2.3

???????

- دجوي ال

??????????

- تم إصلاح مشكلات التوافق مع Acronis

?????? MD5

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

4.4.2.4

???????

- دعم حماية بيانات الاعتماد لتطبيق Microsoft Teams وتطبيق Signal Messenger

?????????

- تم إخفاء السجلات المتعلقة بالشبكة عند العمل في الوضع الآمن بدون شبكات
- نسخ احتياطي لبعض بيانات الوكيل عند إلغاء التثبيت إلى مجلد التخزين المؤقت في Windows

??? ????? MD5

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

4.4.2.5

???????

- ال يوجد

?????????

- تقليل استخدام الشبكة عند إرسال كميات كبيرة من التقارير دفعة واحدة
- إصلاح معالجة بعض بيانات الشهادات

?????? MD5

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

4.4.2.6

???????

- ال يوجد

?????????

- تقليل استخدام الذاكرة في الخوادم التي تحتوي علي عدد كبير من شهادات البرامج الفريدة

?????? MD5

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

4.4.2.7

???????

- ال يوجد

??????????

- تقليل استخدام الذاكرة أثناء التعامل مع البرامج التي تستخدم سلوكًا غير محدد عند الاستعلام عن الألدلة (directories)

?????? MD5

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

4.4.2.8

???????

- ال يوجد

??????????

- زيادة التسجيل والقياس عن بُعد لحالات الجهاز غير السليمة
- زيادة الاستقرار لحمايات الهوية أثناء الإقلاع

?????? MD5

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

4.4.3.0

???????

- بالإضافة إلى الحمايات الحالية للخدمة، سيقوم برنامج تشغيل وضع النواة (kernel mode driver) بإعادة تشغيل الخدمة إذا توقفت لأي سبب.

??????????

- لا يوجد

?????? MD5

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

4.4.3.2

???????

- ال يوجد

??????????

- تقليل استخدام وحدة المعالجة المركزية (CPU) أثناء بدء تشغيل العمليات.
- تقليل استخدام وحدة المعالجة المركزية (CPU) في تحديد الثقة أثناء الاستعلامات المتتالية عن الدلائل.

?????? MD5

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

4.4.3.1

???????

- دجوي ال

??????????

- تم إصالح مشكلة ظهور الكناري (canaries) بشكل مرئي في مستكشف الملفات (Explorer) على بعض الأجهزة التي تحتوي على خصائص تثبيت غير اعتيادية لنظام Windows.

????? MD5

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

4.4.4.0

???????

- يتم تخزين تقارير الحوادث والقياس عن بُعد (telemetry) على القرص لسيناريوهات العمل دون اتصال.
  - نظرًا لمحاولات العبث التي لوحظت ضد العديد من مخازن تسجيل EDR/XDR، قامت Cyber Crucible بتفعيل الحماية على مستوى النواة (kernel) للبيانات المخزنة على القرص قبل نشر هذه الإمكانية.
- زيادة حماية عملية الخدمة (service process) المستخدمة للاتصال الخلفي والتحديثات، كجزء من التحصين الاستباقي القائم على مبدأ انعدام الثقة (zero-trust).
  - لم يكن هذا استجابة لتهديد قائم، بل إجراءً استباقيًا لتهديد يتوقع الفريق ظهوره مستقبلًا.

??????????

- تم إصلاح مشكلة عدم ظهور العمليات التي يتم تحميلها عند الإقلاع في لوحة التحكم ضمن قسم إنشاء العمليات.
- تم منع تشغيل برنامجي تثبيت في نفس الوقت، وهو ما كان سيؤدي إلى تسجيل نفس الجهاز مرتين.

????? MD5

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

4.4.4.4

???????

- ال يوجد

?????????

- تحسين الأداء الخاص بتحليل بيانات الشهادات عند بدء تشغيل النظام.

?????? MD5

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

4.4.5.1

???????

- تقليل استخدام النطاق الترددي:
  - استخدام الضغط لبيانات القياس عن بُعد الأكبر حجمًا واستجابات الخادم الأكبر حجمًا
  - استخدام HTTP/2 للتوريسات المضغوطة وزيادة كفاءة المقابس (sockets)
- زيادة الرؤية في عمليات الشهادات.

??????????

- ترميز بيانات وصفية للشهادة (metadata) ضمن بيانات القياس عن بُعد الخام عند وجود تسميات غير متوافقة مع RFC. كانت البنية التحتية لأمن الشبكات تُفسد أو تحذف الحمولات (payloads)، مما يتسبب في إعادة إرسال العميل حتى النجاح.

????? MD5

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

4.4.5.2

???????

- قياس عن بُعد جديد على مستوى النواة (kernel) للوصول إلى السلوكيات المستندة إلى الشبكة، لتحديد الأخطاء المحتملة في الشبكة على جانب العميل بشكل أفضل، وأ فرص التحسين
- يتم الآن تجميع القياس عن بُعد الصادر وإرساله معًا، تمامًا مثل الإعدادات الواردة
  - يتم الإرسال بتفاوت زمني نسبته 25%، بحيث لا ترسل جميع الأجهزة الحزم في وقت واحد عبر شبكة العميل
- أصبح الآن يتم استخدام HTTP/2 بالكامل من طرف إلى طرف

?????????

- تم تقليل الحد الأدنى لعدد مسارات التنفيذ (threads) المستخدمة في مساحة المستخدم
- تم تقليل استخدام وحدة المعالجة المركزية (CPU) لخدمة مساحة المستخدم
- يتم الآن تنفيذ عملية المصادقة بين الوكيل (Agent) والخادم (Server) بكفاءة أكبر
- تم استبدال خوارزمية السكون <> إعادة التشغيل السابقة للخدمة عند عدم توفر التراخيص.
  - كانت الخوارزمية السابقة تتسبب في ظهور رسالة "الخدمة توقفت بشكل غير متوقع" (service exited unexpectedly) في مدير الأحداث كل 15 دقيقة.
  - السماح لنظام التشغيل بإخبار الخدمة بالتوقف (وهو أمر يُساء استخدامه من قبل المجرمين وأدوات الأمان الأخرى) كان سيسمح بإعادة تشغيل "نظيفة" للخدمة دون تسجيل أي أحداث في مدير الأحداث. وبدلًا من إنشاء هذه الثغرة الأمنية، قامت خدمة Cyber Crucible بإعادة تشغيل نفسها دون تدخل من Windows، مما تسبب في تسجيل الحدث في السجل.

?????? MD5 (MD5 Hashes)

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

4.4.5.3

???????

- تمت إضافة نطاق ثانٍ للاتصال بالخادم (راجع قائمة النطاقات هنا).
  - في حال حدوث مشكلات في الاتصال بأحد النطاقين، سيقوم العميل تلقائيًا بالتبديل إلى النطاق الآخر.

?????????

- تم تغيير بعض النصوص القديمة التي كانت تشير إلى "Ransomware Rewind" لتشير الآن إلى "Cyber Crucible".

?????? MD5

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

4.4.5.9

???????

- زيادة تحصين أجزاء من الوظائف التي كانت تُنفّذ سابقاً بواسطة مكتبات التشفير الخاصة بـ Windows، حيث أصبحت تُنفّذ الآن بواسطة برنامج تشغيل النواة (kernel driver) الخاص بـ Cyber Crucible.
  - يشمل ذلك تحصيناً عاماً، بالإضافة إلى زيادة في بيانات القياس عن بُعد (telemetry) التي تشير إلى احتمال وجود هجمات ضد مكتبات وواجهات برمجة تطبيقات (APIs) التشفير الخاصة بـ Windows.
- هذا إصدار محوري (milestone) يأتي بعد سلسلة الإصدارات التدريجية الموجودة في الإصدارات من 4.4.5.4 إلى 4.4.5.8، وجميعها تتماشى مع وظيفة تحصين تحليل التشفير السابقة.
  - تشير بيانات القياس عن بُعد المبكرة إلى أن حالات الفشل في مكتبات الشهادات والتشفير الخاصة بـ Windows قد تمت الاستجابة لها بشكل صحيح من قبل Cyber Crucible.
  - من غير المعروف في الوقت الحالي ما هي نسبة المشكلات التي كانت ناتجة عن الاستغلال مقابل خلل في مكتبة أساسية لنظام Windows. يُرجى التواصل مع ممثل Cyber Crucible الخاص بكم لمناقشة الأمر بمزيد من التفصيل حسب الحاجة.

?????????

- تم إصلاح مشكلة كانت تتسبب في قيام بعض تقارير العمليات بالإبلاغ بشكل غير صحيح عن الشهادة المدرجة على أنها "غير موثوقة"، وذلك بسبب فقدان وظيفة مكتبة الشهادات الخاصة بـ Windows.

????? MD5

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

4.4.5.8

???????

- زيادة التحصين لأجزاء من الوظائف التي كانت تُنفّذ سابقًا بواسطة مكتبات التشفير الخاصة بنظام Windows، بحيث أصبحت تُنفّذ الآن بواسطة برنامج تشغيل النواة (kernel driver) الخاص بـ Cyber Crucible.
  - يشمل ذلك التحصين العام، بالإضافة إلى زيادة في القياس عن بُعد (telemetry) التي تشير إلى هجمات محتملة ضد مكتبات ووجهات برمجة التطبيقات (APIs) الخاصة بالتشفير في Windows.

?????????

- تم إصلاح مشكلة كانت تؤدي إلى قيام بعض تقارير العمليات (process reports) بالإبلاغ بشكل غير صحيح عن أن الشهادة المدرجة "غير موثوقة"، بسبب فقدان وظيفة مكتبة الشهادات الخاصة بنظام Windows.

?????? MD5

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

4.4.5.5

???????

- زيادة تحصين أجزاء من الوظائف التي كانت تُنفّذ سابقاً بواسطة مكتبات التشفير الخاصة بـ Windows، بحيث أصبحت تُنفّذ الآن بواسطة برنامج تشغيل النواة (kernel driver) الخاص بـ Cyber Crucible.
  - يشمل ذلك تحصيناً عاماً، بالإضافة إلى زيادة في القياس عن بُعد (telemetry) الذي يشير إلى هجمات محتملة ضد مكتبات وواجهات برمجة تطبيقات (APIs) التشفير الخاصة بـ Windows.

?????????

- تم إصلاح مشكلة كانت تتسبب في أن تُبلِّغ بعض تقارير العمليات بشكل غير صحيح عن الشهادة المدرجة على أنها "غير موثوقة"، بسبب فقدان وظيفة مكتبة الشهادات الخاصة بـ Windows.

?????? MD5

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

4.4.5.6

???????

- زيادة تحصين أجزاء من الوظائف التي كانت تُنفّذ سابقاً بواسطة مكتبات التشفير الخاصة بـ Windows، لتصبح الآن مُنفّذة بواسطة مُشغّل Cyber Crucible للنواة (kernel driver).
  - يشمل ذلك تحصيناً عاماً، بالإضافة إلى زيادة في القياس عن بُعد (telemetry) التي تشير إلى احتمال وقوع هجمات ضد مكتبات وواجهات برمجة تطبيقات (APIs) التشفير الخاصة بـ Windows.

??????????

- تم إصلاح مشكلة في بعض تقارير العمليات التي كانت تُبلِّغ بشكل غير صحيح عن أن الشهادة المدرجة "غير موثوقة"، بسبب فقدان وظيفة مكتبة الشهادات الخاصة بـ Windows.

????? MD5

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

4.4.5.7

???????

- زيادة التحصين لأجزاء من الوظائف التي كانت تُنفّذ سابقاً بواسطة مكتبات التشفير الخاصة بـ Windows، بحيث تُنفّذ الآن بواسطة برنامج تشغيل النواة (kernel driver) الخاص بـ Cyber Crucible.
  - يشمل ذلك تحصيناً عاماً، بالإضافة إلى زيادة في بيانات التتبع (telemetry) التي تشير إلى هجمات محتملة تستهدف مكتبات وواجهات برمجة التطبيقات (APIs) الخاصة بالتشفير في Windows.

?????????

- تم إصلاح بعض تقارير العمليات التي كانت تُظهر بشكل غير صحيح الشهادة المدرجة على أنها "غير موثوقة"، بسبب فقدان وظيفة مكتبة الشهادات الخاصة بـ Windows.

??? ????? MD5

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

4.4.5.4

???????

- زيادة تحصين أجزاء من الوظائف التي كانت تُنفذ سابقاً بواسطة مكتبات التشفير الخاصة بـ Windows، حيث أصبحت الآن تُنفذ بواسطة برنامج تشغيل النواة (kernel driver) الخاص بـ Cyber Crucible.
  - يشمل ذلك تحصيناً عاماً، وزيادة في القياس عن بُعد (telemetry) الذي يشير إلى احتمال وجود هجمات ضد مكتبات وواجهات برمجة تطبيقات التشفير الخاصة بـ Windows.

??????????

- تم إصلاح بعض تقارير العمليات التي كانت تُبلّغ بشكل غير صحيح عن الشهادة المدرجة على أنها "غير موثوقة"، بسبب فقدان وظيفة مكتبة الشهادات الخاصة بـ Windows.

?????? MD5 (MD5 Hashes)

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

4.4.6.0

???????

- تحسين أداء المعالج (CPU) لبعض التطبيقات التي تنفّذ عمليات تصفح دلائل تلقائية ومتزامنة بأعداد كبيرة كجزء من سلوكيات تطبيقها.

??????????

-

????? MD5

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

4.4.6.1

???????

- مزيد من الانتقال من اسم المنتج "Ransomware Rewind" إلى "Cyber Crucible".
  - سيتم نقل اسم الخدمة القديم `"Ransomware Rewind"` إلى `"CyberCrucibleAgent"`. يبقى اسم العملية كما هو.
  - سيتم نقل مفاتح التسجيل الموجود في `HKLM\SOFTWARE` من الاسم القديم `RansomwareRewind` إلى الاسم الحالي `CyberCrucibleAgent.`

?????????

- تم إصلاح مشكلة تشغيل بعض العمليات ذات 32 بت بشكل خاطئ كـ "ذاكرة معدّلة" عندما تكون صورة العملية بالحجم الأقصى المسموح به لعملية 32 بت.

?????? MD5

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

4.4.6.2

???????

- تمت إضافة علامات "نوع الوصول" الاختيارية المتاحة للمستخدمين النهائيين لتحديد خصوصية الوصول السلوكي.

??????????

- لا يوجد.

?????? MD5

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

4.4.6.3

???????

- تمت إضافة دعم اختياري لبروكسي SOCKS5 للمساعدة في نشر العميل (agent).

??????????

- تم إصلاح مشكلة إعادة التثبيت من العملاء (agents) القديمة التي كانت تستخدم معرّف تثبيت (installation ID) غير صحيح.
- تم إصلاح مشكلة وجود مسار خدمة (service path) غير محاط بعلامات اقتباس في التثبيتات الحالية من برامج التثبيت القديمة.

????? MD5

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

4.4.6.4

???????

- باتت معلومات ذاكرة العملية الأصل (parent process) متوفرة في تقارير العمليات عند اكتشاف تعديلات.

??????????

- تم تغيير بعض ترددات الاتصال بالخادم بحيث لم تعد تتطلب إعادة تشغيل الجهاز عند تعديلها.

??????????

لا توجد إصلاحات في هذا الإصدار.

????? MD5

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

4.4.7.0

???????

- بدء طرح اتصالات HTTPS القائمة على JWE.
  - مفاتيح التشفير فريدة لكل عميل (agent).
  - يتم تشفير جميع الحمولات (payloads) ضمن HTTPS. مع طلّقة افتراضيًا خلال الطرح الأولي.
  - إمكانية العودة اختياريًا من HTTPS المشفّر بـ JWE إلى HTTPS غير المشفّر في حال عدم نجاح إرسال الحمولات المنسّقة بصيغة JWE.

?????? MD5

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

4.4.7.1

???????

- مزيد من القياس عن بُعد (Telemetry) لعمليات إنشاء العمليات والحوادث
  - معرّف أمان المستخدم (SID)
  - اسم تسجيل الدخول للمستخدم بالصيغة القديمة (down-level logon name)
  - ما إذا كانت العملية ممتازة الصلاحيات (تشغيل كمسؤول) أم لا
- تُبلِّغ الحوادث الآن عن الموضع الذي حدث فيه الوصول التكراري إلى البيانات

?????????

- تقليل استهلاك الذاكرة خلال فترات مشاكل الاتصال بالخادم وحدوث قياس عن بُعد كثيف في وقت واحد
- تقليل استهلاك الذاكرة أثناء الإبلاغ عن الحوادث

?????? MD5

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

4.4.7.3

???????

- وضع DMZ
  - تهيئة اختيارية لاستخدام حزمة CA موقعة للاتصال عبر TLS مع خوادم المصادقة والقياس عن بُعد. تُحمى حزم CA هذه بعد ذلك من العبث أو الحذف بواسطة قدرات مكافحة العبث الخاصة بشركة Cyber Crucible.
  - يتم تعطيل فحوصات OCSP وCRL لتقليل قائمة النطاقات المطلوب السماح بها عبر جدار الحماية.

??????????

- تقليل استخدام الذاكرة ووقت المعالج المُستهلك في إرسال فروقات الذاكرة (memory diff)، خاصة بعد فترات طويلة من عدم الاتصال.

??? ????? MD5

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

4.4.8.0

???????

- بيانات تتبع Authenticode في وضع النواة (Kernel-mode)
  - لزيادة السرعة والموثوقية، سيتم تسجيل بيانات الشهادات الخاصة بعمليات إنشاء العمليات (process creations) والحوادث بواسطة المُشغّل (driver) وحده.
  - لا يزيل هذا التحديث الاعتماد على مكتبات التشفير الخاصة بـ Windows، ولكنه يجري عمليات الحساب التشفيري بالتوازي معها. وقد يتم إزالة الاعتماد على Windows بالكامل في نهاية المطاف.

?????????

- تقليل استخدام الذاكرة ووقت المعالج (CPU) المُستهلك أثناء محاولة إرسال الأحداث في حالة عدم الاتصال، حيث يتم تخزين بيانات التتبع بشكل آمن حتى تستعيد الجهاز الاتصال بخوادم Cyber Crucible.
- اعتقدت بعض برامج تثبيت مُشغّلات Nvidia أنها لا تملك الصلاحية للتثبيت بسبب استخدام دالة داخلية من نواة Microsoft لمحاولة الوصول إلى الملفات المُثبّتة الخاصة بـ Cyber Crucible.
- تم إصلاح عدم التوافق مع وضع JWE ووضع DMZ

????? MD5

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

4.4.8.1

???????

- يتم الإبلاغ عن البيانات الوصفية للملفات التنفيذية مثل إصدار المنتج، واسم الشركة، وما إلى ذلك، للعمليات الموجودة في الذاكرة من قبل التعريف (driver) عبر الرؤية على مستوى النواة (kernel). تتمثل الوظيفة الطبيعية في استخدام استدعاءات واجهة برمجة تطبيقات Windows في مساحة المستخدم. يؤدي هذا الانتقال إلى التحليل في النواة إلى إزالة الفرصة (التي تم رصدها) للمهاجمين للتلاعب بمعلومات العملية.
- يتم نسخ معلومات مصادقة العميل (Agent) في مكان آخر من النظام لاستعادتها في حال تلف السجل (registry) بسبب تعريف ضار.

??????????

- يتم تسجيل أخطاء الاتصال بالخادم بشكل محدود من قبل العميل (Agent)، مما يقلل من حجم السجلات على القرص.

??????????

- لا ينطبق

????? MD5

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

4.4.8.2

???????

- تمت إضافة دعم لأيقونة اختيارية في شريط النظام (system tray). هذه المميزة معطّلة بشكل افتراضي.

??????????

- تمت إضافة حل مؤقت (workaround) لمشكلة تتعلق بطلبات تجزئة (hashing) واجهة برمجة تطبيقات Windows على مستوى النواة. قد يتم إزالة هذا الحل المؤقت في المستقبل في حال تصحيح مشكلة Windows، وربما مع تحديث النواة القادم.

?????? MD5

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

4.4.9.0

???????

- بيانات القياس عن بُعد لملفات DLL في وضع النواة (Kernel-mode)
  - تحليل الشهادات وحساب الثقة لجميع ملفات DLL المُحمّلة في المُشغّل (driver).

??????????

- لا يوجد.

????? MD5

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

4.4.9.1

???????

- ال يوجد.

?????????

- زيادة كمية القياس عن بُعد (telemetry) التي تتم معالجتها دفعة واحدة بواسطة الخدمة لبيانات الإنشاء والحقن.
- تعديل ترتيب الكناري (canaries) للبرامج التي تستخدم أساليب غير معتادة لتكرار الملفات.
- تعديل قائمة التحكم بالوصول (ACL) على بعض الكناري لتتناسب بشكل أفضل مع أنظمة الملفات الحقيقية.

?????? MD5

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

4.4.9.2

???????

- تتبّع تعديلات الذاكرة لملفات DLL المُحمّلة.
- توليد الفروقات (diff) الخاصة بالذاكرة لملفات DLL المُعدّلة.

??????????

- معالجة بعض ملفات DLL غير المتوافقة التي كانت تؤدي إلى نتائج غير صحيحة لتجزئة Authenticode.

?????? MD5

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

4.4.9.4

??????????

- أصبحت ملفات تفريغ الخدمة (dump files) الآن مقتصرة على 10 ملفات لكل مجموعة من الإصدار والخيط (thread).

?????? MD5

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

4.5.0.0

???????

- جدار حماية النواة بالذكاء الاصطناعي (AI Kernel Firewall)
- تسريعات في حساب تجزئة Authenticode
- تقليل ملحوظ في استخدام الذاكرة لبيانات القياس عن بُعد الخاصة بملفات DLL
- زيادة الرؤية للتعديلات في الذاكرة الخاصة بملفات DLL

??????????

- إصلاح توافق استعادة الخدمة مع 24H2

??? ????? MD5

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

4.5.0.1

???????

- خيار الانتقال إلى نطاق خادم مصادقة OAuth المستضاف
- مهمة لتهيئة عناوين URL لخوادم REST وOAuth ديناميكياً

??????????

- لا شيء.

?????? MD5

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

4.5.0.2

???????

- ال شيء.

?????????

- تقليل الذاكرة المستخدمة لجدار حماية AI Kernel Firewall.
- استخدام أسرع لنقاط النهاية الجديدة للمصادقة.
- إزالة استدعاءات icanhazip.com، والتي كانت اختيارية سابقاً ولكنها لم تعد ضرورية.

?????? MD5

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

4.5.0.3

???????

- يعرض الآن مؤشر شريط الحالة حالة التهيئة الذاتية للتثبيتات الجديدة.

?????? MD5

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

4.5.1.0

???????

- يتم الآن استخدام OpenSSL للاتصال عبر TLS.
  - من المفترض أن يتجاوز هذا المشكلات على إصدارات أنظمة التشغيل القديمة التي لم تعد تتلقى تحديثات لمتطلبات TLS الأحدث.

??????????

- تحسين دعم تحليل توقيعات Authenticode غير المتوافقة.

????? MD5

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

4.5.1.2

???????

- إزالة التحقق من صحة الشهادات القديم الذي كان يعتمد على مكتبات Windows المدمجة والبطيئة.
- إضافة إمكانية الاحتفاظ بالسجلات عند إلغاء التثبيت.

?????? MD5

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

4.5.2.1

???????

- إصدار واسع للتقارير الخاصة بالوصول إلى Fortress AI

??????????

- تحسين عمليات نواة Cyber Crucible التي لا تستخدم واجهات برمجة تطبيقات Windows (Windows APIs) للتصدي لزيادة زمن الاستجابة في بعض بيئات Windows بنسبة تقارب 20%.

?????? MD5

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

4.5.2.2

??????????

- تحسين عمليات نواة Cyber Crucible من خلال تجنب أحداث ويندوز الإشكالية وقدرات نقل البيانات الأساسية لنظام التشغيل.

?????? MD5

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

4.5.3.0

???????

- FortressAI
  - تمت إضافة إشعارات عند الإبلاغ عن انتهاك للسياسة
    - التكامل مع مركز إشعارات Windows
  - تمت إضافة واجهة مستخدم رسومية لعرض سجل إشعارات السياسة
  - تمت إضافة وضع المحاكاة (simulate mode)
- Cyber Crucible Core
  - تحليلات DLL غير متزامنة وقابلة للتهيئة للأجهزة ذات الموارد المادية المحدودة
  - تحليلات وقياسات إنشاء العمليات (telemetry)
    - تستخدم الآن الاستمرارية على القرص (disk persistence)
    - تمت إزالة الاعتماديات على Windows MiniFilter
  - تحليلات وقياسات حقن العمليات (process injections)
    - تستخدم الآن الاستمرارية على القرص (disk persistence)
    - تمت إزالة الاعتماديات على Windows MiniFilter
  - تمت إزالة اعتماديات إضافية على موارد نواة Windows (kernel)

?????????

- تحسين آلية إعداد تقارير القياسات (telemetry) لتحقيق إعداد تقارير أسرع
- إزالة حالة الجمود (deadlock) الناتجة عن الوصول الحصري مقابل المشترك لمورد معين من موارد النواة (kernel) يطلبه Microsoft Defender عند تفعيله وضع تصحيح أخطاء برنامج التشغيل (driver debug mode)

??? ????? MD5

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

4.5.3.1

???????

- FortressAI
  - يكتشف محاولات تجاوز ضوابط السياسات من خلال استخدام لقطات الشاشة.
- Cyber Crucible Core
  - يدعم إعادة تهيئة هوية العميل (agent) دون الحاجة إلى إعادة نشر كاملة.
    - يعالج هذه الحالات التي يتم فيها استنساخ جهاز مثبت عليه Cyber Crucible، مما يؤدي إلى استنساخ الترخيص ومعرّفات العميل. تمامًا كما هو الحال مع عناوين IP، وعناوين MAC، أو أسماء الأجهزة، والمعرّفات الفريدة الأخرى، يقوم Cyber Crucible بتحديد العميل المستنسخ وتنبيه مسؤولي CC إلى فرصة إنشاء معرّفات CC جديدة.

?????? MD5

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

4.5.3.2

???????

- FortressAI
  - ال شيء
- Cyber Crucible Core
  - تحسين عملية المخزن المؤقت للنواة (Kernel Buffer)
    - يستخدم برنامج التشغيل المخازن المؤقتة لتخزين بيانات القياس عن بُعد مؤقتاً قبل إرسالها في النهاية إلى لوحة معلومات العميل. يختلف هذا النشاط عن تعبئة النموذج السلوكي أو عملياته.
    - إذا حدث تحميل زائد على المخزن المؤقت للنواة، يزداد حمل وحدة المعالجة المركزية (CPU) للنظام.
      - ال يحدث ذلك إال نتيجة خلل كبير في نظام التشغيل أو هجوم على الأنظمة.
      - سيتوفر الإشعار التلقائي للعميل عند استخدام مرتفع جداً للمخزن المؤقت اعتباراً من 1 يونيو 2026.
    - تتم جميع عمليات المخزن المؤقت للنواة الخاصة بـ CC تقريباً عبر ثلاثة مخازن مؤقتة رئيسية.
    - يتم الآن إرسال نسبة استخدام المخازن المؤقتة الرئيسية الثلاثة جميعها إلى بنية CC التحتية لجمع المقاييس وتحديد استخدام المخزن المؤقت على أساس كل عميل (agent) على حدة.
    - يمكن الآن تعديل حجم المخازن المؤقتة الرئيسية الثلاثة عن بُعد، ويمكن للمستخدمين تتبع حالتها.

?????????

- تسبب تحديث حديث يتعلق بمكتبات DotNet وMSVC Redistributable في إغراق مخازن Cyber Crucible المؤقتة بأحداث مستمرة ومرتفعة جداً (أكثر من 500%) لعمليات وأحداث مكتبات DLL، مما أثر على بعض العمالء. وعلى الرغم من عودة استخدام المخزن المؤقت إلى المعدل الطبيعي البالغ 1-5%، بما في ذلك لدى العمالء المتأثرين، فقد تم مضاعفة حجم جميع المخازن المؤقتة لمراعاة أي مشكلات مستقبلية. ويأتي هذا بالإضافة إلى إمكانيات التهيئة المذكورة أعاله.

????? Sha-256

```
service.exe  = 2f46657af8809339d16546f1e6f2b58975bbf4d5c10fde3510363d628b129492
fai-alert.exe  = 890ccca7e0ce14a0e2ff7f90bae75a7ef12ad6c8cd43ffb52093c8431e65770b
CCRRSecMon.sys   = d0e941bc25d31e38cbebbe9ce3918f82d0b9c7b433efed318cb34e36a50acf94
CCRRSecMon.inf   = db54d8077afdfef81286868f7bda1e8df17dbd812178ddac989127550a904a8c
ccrrsecmon.cat   = a01c31db7231fed3852c9e559eb2c3f7496a016982207c102b88d8b36dcb0486
```