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
```

Revision #1
Created 2026-07-24 02:30:36 UTC by Dennis Underwood
Updated 2026-07-24 02:30:36 UTC by Dennis Underwood