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
```

Revision #1
Created 2026-07-24 02:37:33 UTC by Dennis Underwood
Updated 2026-07-24 02:37:33 UTC by Dennis Underwood