

4.4.5.8

???????

- تابتكم ةطساوب آقباس دُفُنُت تناك يتي الت فئاطولال نم ءازجال نيصحتال ةدايز ليغشت جمانرب ةطساوب نآالا دُفُنُت تحبصأ ثيح ب Windows، ماظن ب ةصاخال ريفشتال Cyber Crucible. ب صاخال (kernel driver) ةاونال
 - دُغ ب نع سايقلا ي ف ةدايز لىل ةفاضإلاب، ماعال نيصحتال كلذل لمشي (APIs) تاقيبطتال ةجمرب تاهجاوو تابتكم دص ةلمتحم تامجه لىل ريفشت يتيال Windows. ي ف ريفشتالاب ةصاخال

?????????

- تاي لمعال ريراقت ضعب مايق لىل يدؤت تناك ةلكشم حالصإ مت (process reports) ةفيظو نادقف ببسب، "ةقوثوم ريغ" ةجردمال ةداهشال نأ نع حيحص ريغ لكشب غالبلاب Windows. ماظن ب ةصاخال تاداهشال ةبتكم

?????? MD5

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