

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

- ةركاذلا تاليلحت
- تاي لمعلل ن قح تاليلحت
- تاي لمعلل ءاشن تاليلحت
- ةياهنلا ىلى ةيادبللا نم لم اش قيقحت - أعم ك لذل ك عيمحت
 - ةلالثملا اذه ضرع ان رتخا اذامل

ام هي بنت يفي قي قححتلا ءانثأ كل ءحاتم لي لحتلل ءيساسأ تانبل ثالث كانه

مادخ تساب ،ماطن لىل ع طشنأل نم ةعونتم ةعومجم ذيفنتب مجاهمل موقى نأ أيلاح حجرمل نم ليغشت نم رثكأ ،(غيرفتلا وأ نقحل) تاي لمعمل فاطت خاوة ركاذل لخاد لمعمل تاينقت نم جي زم .حضاو "hacker.exe" جم انرب

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

ةركاذل تاليلحت عبتتت .اهسفن ثداحل وأ ةباجتسال ءحفص يف ءءوءم ىلولأ ءنبلل
ءلمءءملا زازءبالا تايءولسل رمتسملل صءفلا ءاىأ ءركاذل يف ءيلىمءللا تايءولسل
(رئفشلا وأ ءقرسال) تانىبلل

٤٠. ﺍﻟﻜﺸﻢ ﺩﻭﺟﻮ ﻳﻠﻊ ﺍﻟﻲ ﺩﺩﺓ ﺩﺍﻉ ﻧﻮﻛﺖ ﺍﻫﺐ ﺗﺒﻌﻠﺎ ﻟﺎ ﻣﺘﺤﺎ ﻳﻠﻲ ﺭﻳﺸﺖ ﻳﺘﻠﺎ ﻗﺮﻛﺎﺯﻟﺎ ﻗﻠﺎﺡ

ءاطخأ وأ ؤئئئسل ؤرمربل ؤاسرامم ؤؤؤ نأ نكمئ ؤئئ؁ اءاؤء ؤئ ؤئئءء ؤمءاؤ ؤئسل
لئ؁ ؤئشؤل ؤئق ؤمءنربل ؤرءاؤل ؤلءب ؤللا ؤضئ ؤئءءمربل

63504385.png?width=680

حتف دعب تانايابل زازتبال ةلمتحم تايكولس Adobe Acrobat ةيلمع اهيف رهطت ةلاح ىرن انه Acrobat.exe فلم رثأتي مل .اهل يدعت مت دق Acrobat ةيلمع ةركاذ أن ىرنو ،هل يزنن مت PDF فلم لاكشأل نم لكش أب صرقلا ىلع دوجوملا .

دوچو ډلې ؤلعلعمل Acrobat.exe ؤللمعب ؤطبترملا ؤركاډلل ؤئانجال لئلل رلشې نأ ؤرمرلا نم غلرفل وأ ؤللمع نؤل نؤل مل نأ؁ مالا ؤسالا ؤلل لالغل سا مابر - قلقل الل ؤعءسل ؤلكشم ؤللمع.

دجوت (True)، ةحيص "ةلدعالم ةركاذل" ةمقي اهيف نوكت يتل زازتبالا تاباجتسال ةبسنلاب (Memory Diff) ةركاذل فالتخا فلم ليزنتل يرنجل ببسلال ليلحت دومع يف ليزنت ةنوقيأ ةباجتسالاب صاخلا:

63602693.png?width=680

يف هنقح متامل ةغممالم ةيردصملا ةرفيشلا وه (Memory Diff File) ةركاذل فالتخا فلم للحم موقيل، لالغتسا ةرفيش وأ/و ةثيبح تايجرب يلع يوتحي نأ لمحمل نم. جمانربلا لب، هلمكأب جمانربلا يلع يوتحي ال فلملا اذه نأ طحال. اهصحفب ينمأ للحم وأ ةثيبح تايجرب يلع فرعت. تايلمعل نقح لثم موجه ةينقت وأ لالغتسا لالخنم هليدعت مت يذلا عزجال طقف [ان](#)ه فلملا اذه لوح ديزملا

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

طويخلا" دومع وه ةيئاقلت ةباجتساب ةلص يذ ةيلمع نقح ثدح دوجو لامتحا يلع لوألا رشؤملا نأ لىل اذه ريشي. ةباجتسال/ثداحلاب صاخلا (Untrusted Remote Threads) "ةقوئوملا ريغ ةديعبل عم قوئوم ريغ ديغب طيخ ةطحالم نع فشك (kernel) ةاونلا يوتسم يلع يكولسلال ليلحتلا ةيدفل جاماربب هيبش كولس وأ تانايب ةقرس كولسب موقت ةيلمع

63471635.png?width=680

دومع يف (True) "حيص" ةارق دغت. تايلمعل نقح ةحفص يف قيقحتلا نم ديزملا ءارج نكمي. كانه لىل هجوتلا يغبني ناك اذا ام يلع آديج ارشؤم ةقوئوملا ريغ ةديعبل طويخلا

نقحلا ةحفص لىل ائاقلت كهيجوت ةداعل ةنوقيأ يلع اضيأ يرنجل ببسلال ليلحت دومع يوتحي طقف ةباجتسالاب ةلصل تاذ نقحلا تايلمع ضرعل

63602703.png?width=680

تايلمع طقف ىرتس شيح تايلمعل نقح ةحفص لىل كللقن متيس، نقحلا ةنوقيأ يلع رقلن دعب ةباجتسالاب ةلصل تاذ نقحلا:

63569930.png?width=680

راسمو، ةمدختسملا تالماعملاو نقاحلا ةيلمع راسم ىرن، تايلمعل نقح ثادحأ ةحفص يف انه تاليلحت يف آدج أمهم أرو تالماعملا بعلت أم ةداع. ةمدختسملا تالماعملاو ةنوقحملا ةيلمعل رفوت امك. اهليغشت بجي يتلا PowerShell رمأو لىل، لاثملا لىبس يلع، ريشت وأ، ةركاذل ءانثأ مت يتلا ةرركتملا نقحلا تايلمع عبتت يف ةدعاسم لل (Process IDs) تايلمعل تافرعءاشن ةحفص يف يرنجل ببسلال ليلحت نع ثحبلل وأ، رخأ لىل ةيلمع نم مجاهملا لاقتنا تايلمعل.

63438879.png?width=680

ةءارقلل عبات؟ تاسوري ةحفاكم جمانرب عئاب ةقيقحتلا يف ناك rundll32.exe نأ انفرع فيك

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

يتل تاودأل نأ ىتح ملعي ال دق .هـموجه ءانثأ طقف ةدحاو ةيلمع مجاهملا مدختسي نأ آدج ردانل نم
باصملا ماظنلا ىلع ةعونتم ةيرادإ تاودأ مدختستو ،ةديج تايلمع ؤلوت اهمدختسي

،(ةيلمعل سفن وأ) ىرخأ تايلمع حتفت يتلا تايلمعل عي مج تايلمعل ءاشنإ ءحفص عبتت
،ةهجوو ردصم لكل (Pids) تايلمعل تافّرعمو ،ةمدختسملا تالماعملاو

ءيش انتوفي ال هـنأ ينعي امم ،(kernel) ةاونلا ىوتسم ىلع كلذ ذيفنت متي

نكلو ،تانايبل هذه ضعب ىلع Microsoft نم (telemetry) دُعُب نع سايقلا تانايبل يوتحت :ةطحال
دق اذه دُعُب نع سايقلا ردصم نأ انطحال انأل ،اذه تانايبل ردصم مادختسا مدع انرتخا .اهلك سيل
موجهل ءانثأ ني مجاهملا لبق نم هـفاقيا مت وأ ،تالاحل ضعب يف ةمهم اثادحأ توف

؟انتيفر ةدوج ىدم ام

????? - ?????
???? ???? ?????????? ???????????

ثيح - لاثملا اذه ىلع علّطا ؟يرذجل ببسلال ليحلحتل كذيفنت ةعرس ىدم امو ،انتيفر ةدوج ىدم ام
تايجالصلال ىلعأ نم آضعب كلتمي هـنأب ةيوق ءجحب عتمتي ،تاسوري ءحفاكم جمانرب نأ طحول
ضرب كلذ نوكي نأ لم أن .انب صاخلا Cyber Crucible جمانرب يف ءرفيش نقح لواحي ،ماظنلا ىلع
ضفري فكلذ ببست ،يلالابو) ةيتاذلا ةيامحل عضو يف لخدن كذل عم اننكل ،انجمانرب صحف
ءيجراخل فارطألل حمست ةيفلخ بابوأ دجوت ال ...تاسوريفل ءحفاكم جمانرب ثبعل انجمانرب
(.همادختسا وأ انجمانرب ليذعتل لوصولاب

:ةيئاقلت ءباجتسا عم ،انه نم أدبنل ،نذا

63569937.png?width=680

طبخ كولس نمضتت ةيلمع نقح ءلواحم انه ىرن .ةيدف جمانرب سيل Cyber Crucible نأ حضاولا نم
،تانايبل زازتباب ةهيبش تايلكولس بناج ىلإ ،آهوبشم ديعب

نـاوث 5 دعب .نقحلا ءنوقيأ ىلع رقنلاب تايلمعل نقح ثادحأ يف يرجي ام ىلع ءرطنق لنل - أنسح
- انتباج ىلع انلصح -

63471644.png?width=56463438879.png?width=680

ضعبب مقنل hacker.exe جمانرب سيل ،ديكأتلاب ؟آقرتخم كلذ سيلأ rundll - الهم نكلو
،انه ءشاش ءطقل انيدل رفوتت ال .تايلمعل ءاشنإ ءحفص يف انتباج ىلع لوصحلل ،ةيفصللا
،تاباجتسال ءحفص ىلإ دغل .نقحلا تايلمعو تاباجتسال عي مجل ءحاتم تايلمعل تافّرعم نكل
ءكبشلل ةيفصلتو تايلمعل ءاشنإ ءحفص ىلإ انلقنتل تايلمعل ءاشنإ ءنوقيأ ىلع رقننو
،ءباجتسال هـذهب ءصللا تاذ ءاشنإل تايلمع ضرعل آيئاقلت

63537184.png63438886.png?width=680

ةحفاكم جمارب عئاب وهو WebRoot، ناك (ةيروتلا دصق نودب) "رذجلال" نأ نآلا ىرن، ةلوهسو ةعرسب
(DLL)، ةيكيما ني دل WebRoot تابتكم ىدحإ لي محت ل rundll32.exe ةيلمع قلطأ دق، تاسوريف
ربع رورملا ىلع هرابجإل Cyber Crucible، جمانرب عم مائقلا كلذ دعب تلواح يتل او
تانايبلال ةقرس ةادأ لثم تافلما

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

بناج نم ةءافكلال نم ةتوافتم تايوتسمب، ني مجاهملا بيلاسأ ىلع ةريفو ةلثمأ انيدل
ب لطي ماطنلا ىلع تايحالصلال نم ىوتسم ىلع تاسوريفلا ةحفاكم جمارب لصحت. ني مجاهملا
Cyber Crucible فاشتكا نإ. ني مجاهملا لبق نم ريضحتلاو ةينقتلاو ةراهملا نم آدج آيلاع ىوتسم
نم أضعب رهطي، آيئاقلت اهفاقيإ مث، ةئاس ةينمأ ةادأ نم "ني قرتخم لاب ةهيبش" تايكولسل
تاي لمع لي صافت يفايضلال نود، انبناج نم ي نم ألالا ىسدنهلل زيملتال تايوتسم ىلع
ني مجاهملا بيلاسأ وأ ةيدرفلا لالغتسالا