

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

ءاونلا ىوتسم ىلع لىغشتلا ،ينىجل اىعانطصالا ءاكذلا - لخاللا نم Cyber Crucible لمعى فىك ةطقن ىلع تارارقلا ذخت اذاملو ،لىغشتلا ماظن نع ةلالقتسالا ،Rogue Process Prevention ةياهنلا .

- [جماربال قىلعت قىرط نع نوبىجتست اذامل](#)
- [تايلىمعال نقح تايلىمعىم Cyber Crucible نىمى له](#)
- [اها را اىتلاو ةىئاوشع وذب تىتلا ةبىرغال تافلما هذى ه ام](#)
- [Cyber Crucible ب ةصاخلا \(canary files\) ىرانكلا تافلما زىمى ىذلا ام](#)
- [ىرانكلا تافلما دجوت نى ا](#)
- [ةركاذلا تالىلحت Cyber Crucible مدختست فىك](#)
- [Cyber Crucible نم \(Memory Behavioral Analysis\) ةركاذلا ب صاخلا كولسل لىلحت فىلختى فىك](#)
- [ةركاذلا تامجه Cyber Crucible فشتكى امدن ع ثدحى اذامل](#)
- [رىبكلا ةللل جذومن نىب و هنىب قرفلا امو ،\(Genetic AI\) ىنىجل اىعانطصالا ءاكذلا وه ام](#)
- [\(LLM\)؟](#)
- [ةىئات ىللم 200 نم لق اىف ارارق Cyber Crucible ذخت فىك](#)
- [\(Rogue Process Prevention – RPP\) ةقراىملا تايلىمعال ع نم ةزىمى ه ام](#)
- [ةصنملا ربع ةركاذلا تالىلحت هىدؤت ىذلا رودلا ام](#)
- [ءاونلا ىوتسم ىلع Cyber Crucible لمعت اذامل](#)
- [Windows تابتكم نع لقتسم Cyber Crucible ن اىنى اذامل](#)
- [\(air-gapped\) ةكبشلا نع ةلوزعملا تائىبلا فى و ا لاصلالا مدع عضو فى Cyber Crucible لمعت له](#)
- [\(air-gapped\)؟](#)
- [ماظنلا لىغشت فاقى ا نم الدب ةىلمعى قىلعت لال خ نم Cyber Crucible بىجتست اذامل](#)

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

process) تاي لمعل ن قح ل ث م تاي ن ق ت م ا د خ ت س ا ب ، ط ق ف ة ر ك ا ذ ل ا ي ف ل م ع ل ا ن ا ن و م ر ج م ل ا م ل ع ت د ق ل
injection)، ا ي ا ز م ل ا ن م ة ع و ن ت م ة ع و م ج م ر ف و ي :

1. ج م ا ن ر ب ل ا ك ل ذ ب ة ص ا خ ل ا م د خ ت س م ل ا ة ي و ه ي ل ع ا ل ا ي ت س ا ل ا .
2. ة ي و ه ل ا ة ر ا د ا ت ا ص و ح ف ن م ب ر ه ت ل ا .
3. ا ض ا ي ب ل ا م ئ ا و ق ل ل ا و ت ا ق ي ب ط ت ل ا ي ل ع ة م ئ ا ق ل ل ا ة ي ا م ح ل ا ر ا د ج د ع ا و ق ن م ب ر ه ت ل ا .
4. م د ا و خ ل ا ي ل ع ت ا ن ا ي ب ل ا ن ا د ق ف ع ن م ت ا و د ا ن م ب ر ه ت ل ا .
5. ة ي ل م ع ل ا ء ا ه ن ا د ن ع ا ب ي ر ق ت ة ر ك ا ذ ل ا ي ف ة د و ج و م ل ا ة ل د ا ل ا ع ي م ج ف ذ ح .
6. ب و س ا ح ل ا ل ي غ ش ت ة د ا ع ا د ر ج م ب ا ب ي ر ق ت ة ر ك ا ذ ل ا ي ف ة د و ج و م ل ا ة ل د ا ل ا ع ي م ج ف ذ ح .

ت ع ق و ي ذ ل ا ت ق و ل ا ي ف ة ل د ا ل ا د ي م ج ت م ت ي ، م ج ا ه م ل ا ة ر ط ي س ل ة ع ض ا خ ل ا ج م ا ر ب ل ا ق ي ل ع ت ل ا ل خ ن م
ه ي ف .

ا ض ا ي ا م ج ا ه م ل ا د ي م ج ت م ت ي ا م ك .

ق ي ق ح ت ل ا ة ي ل م ع ن م ع ز ج ك ي م ق ر ل ا ي ع ر ش ل ا ب ط ل ا ت ا و د ا ل ا ح ا ت م ة ل د ا ل ا ح ب ص ت .

ة د ا ع ا د ر ج م ن ا ف ، ت ق و ل ا ك ل ذ ي ف ي م ق ر ل ا ي ئ ا ن ج ل ا ل ي ل ح ت ل ا ء ا ر ج ا ل ة ز ه ج م ة س س و م ل ا ن ك ت م ل ا ذ ا
ق ل ل م ل ا ج م ا ن ر ب ل ا ء ا ه ن ا ن ا م ك . ة م ي ل س ة ل ا ح ي ل ل ا م ا ط ن ل ا د ي ع ت س م ج ا ه م ل ا ل ب ق ن م ة ط ي س ب ل ي غ ش ت
ا ض ا ي ا ب و ل ط م ل ا ر ث ا ل ا ق ق ح ي ا م ة د ا ع ه ل ي غ ش ت ة د ا ع ا و ا ر س ق .

?? ????? Cyber Crucible ????? ???????? ???? ?????????????

ال!

اهنكل ،تايلمعلال نقح عون نم دُعُتو ةمطنألل ىلع ثدحت يتلا ةطشنألل نم ةعونتم ةعومجم كانه
ةراض ةرورضلاب تسيل

ليحتو تاديدهتلل نع ثحبلل ضارغل ةيئرم هذه تايلمعلال نقح ةطشنألل عيمج Cyber Crucible لعجي
يف ةلثمتلل تانايبلل زازتبا ةطشنألل تادب اذلا ءلا طاشنلل فقوي ال هنكل ،يرذجلل ببسلل
ةيدفلل جمارب ريفشت وأ تانايبلل ةقرس

PC Matic، ب صاخلل ةياهنلل طاقن نامأ جمانرب هب موقوي يذل تايلمعلال نقح ىلع لاثم يلي اميف
ليغشتلل ديقي تايلمعلال صحتل هب نوموقوي أكولس اذه نوكتي نأ حجرمل نم PCPitStop. ىمسمللو

5373968.png?width=680

لصحت Cyber Crucible، ب صاخلل (kernel) ةاونلل ىوتسم ىلع ةيكلولسلل تاليلحتلل لصف
جمارب كلذ ي ف امب) جمانربلل تايحالص ىوتسم نع رظنلل ضغب ،ةطشنألل عيمجل ةلماك ةيؤر ىلع
(ةللالل تايحالصلل تاذ تاسوريفلل ةحفاكم يدروم وأ تفوسوركيام

تايلمعلال ءاشنل ةحفص يفو ،ةحفصلل هذه يف ثحبلل نكمي ،ةيئاقلت ةباجتسا ذيفنت لاج يف
ةعيرس قيقتح جئاتن ىلع لوصللل (Process Creations) ،

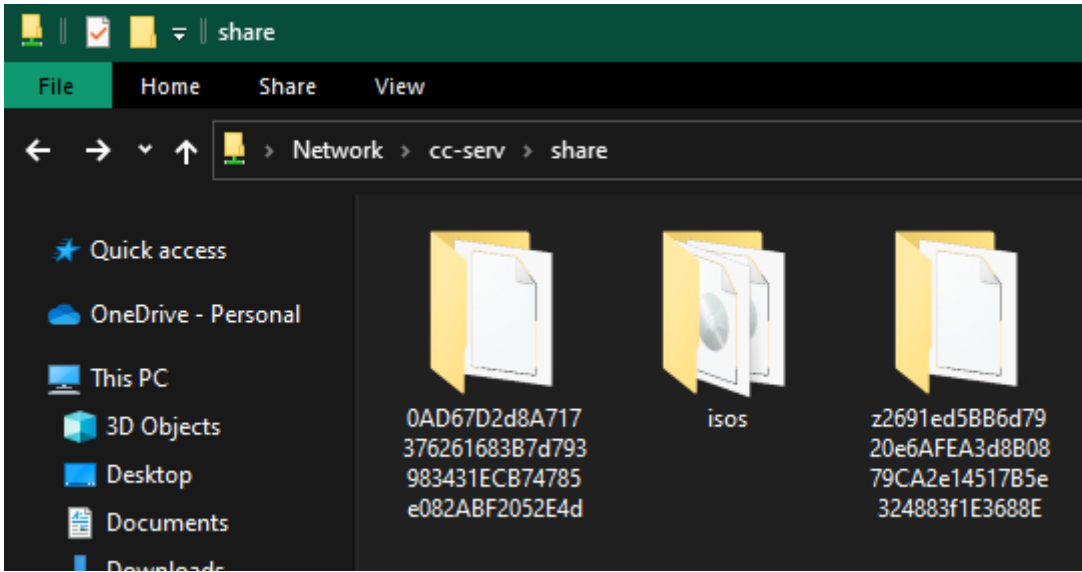
تاقببطلل ةجمرب ةهجاو نم ةدافتسالل تاديدهتلل نع ثحبلل قرفل نكمي ،كلذل ءلا ةفاضللاب
ةركاذلل لخاد ةلثمتحم ةراض بيللاسأ دوجو تارشؤم نع مالعئسللل REST API

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

رارق داخا لبق تاكرحم ةدع نم ةيكلولس تارشؤم انيدل تانايبلا زازتبا عنم جمانرب ىقلتي
تافل مديتسي، تافلما ةبقارم كرحم وهو، تاكرحملا هذه دحأ راج موجه كانه ناك اذا ام نأشب يروف
عقاوم ةدع يف ةصاخ.

ىلع ادامتعا Cyber Crucible لعل ةدوجوم، رخأ انايحا اهارت الو، انايحا اهارت يتلا تافلما كلت
مدختسي جمانرب، لاثملا ليبس ىلع. كل رهطت دق، تافلما جاردإ ام قيبطت مايقة يف
نآلا كل اهرهطيس، ااحتف وأ اهظحل تافلما جاردإ (File Explorer) تافلما فشكتسم.

([wiki](#)) "محفل مجنم يف يرانكل" ةرابع رارغ ىلع، "canaries" مسا تافلما كلت ىلع قلطن



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

(canary files) ??????? ?? Cyber Crucible?

دحاً لبق نم أموي اهتقرس لاجي ف ،اهلخاد ةيفخم ةصاخ تانايب ىلع يرانكل تافلم يوتحت
يصلأال هكلام ىلإ هتداعإو فلملا عبتت Cyber Crucible -ل نكمي .نيمجاهملا

نم لعت ةقيرطب (ةفئازلا ةيئوشعلا بفرغت) ةيئوشع هبش تافلملا ءامسأ نوكت
ةلداعم مادختساب ءامسألا ءاشنإ متي .اهبجت واهيلى لفرعتلا نيمجاهملا ىلع ليحتسملا
ولى تح ،يرانك فلمك فلملا ىلع فرعتلا انجمانربل حيتت Cyber Crucible، نم ةصاخ ةيضاي
رخآ ىلإ فلم نم وأ رخآ ىلإ زاهج نم ءامسألا تفلتخا .

فلم يوس مزلي ال هنأ اضيأ ينعت تافلملا هذه ىلع فرعتلا ىلع Cyber Crucible جمانرب ةردق نإ
مداخلا كلذ مدختست لمعل تاطحم فالآ تناك ولى تح ،مداخ لكل دحاو يرانك

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

كيدل تافلملل ماطن لخاد ةددعتم نكامأ يف يرانكلل تافللم دجوت

Cyber موقى ،لمتحم مدختسم يأ نم ،كماطن ىلع تافلملل ديدج ردصم هيف رهظي تقويأ يف
تاكرحم كلذل لمشي و .لعفلاب تعضو دق يرانكلل تافللم تناك اذا امم ققحتلاب أيئاقلت Crucible
يباحسلل نيزختلاو ،ةيكبشلل تافلملل رداصمو ،USB يصع لثم ةلازالل ةلباقلا صارقألا
تافلملل .

??? ????? Cyber Crucible ???????? ?????????

ءدب نم ،لماك لاب هتايح ةرود لاوط جامانربلا ةركاذ ةلاح Cyber Crucible ةاون تاليلحت عبتتت
ىرخأل جاماربال عم ةركاذلا لخاد تالعاتلا ةلاح عبتتت امك .هئاهتنا ىلإ جامانربلا ليغشت
ةرغث ثودح كلذ ينعي دقو .جامانربلا ةركاذ يف ةنمآلا ريغت تالاحلا ةيكولسللا ةبقارملا بقارت
("تافلما لب تامجهلا"-ب أضيأ فرغت) ةركاذلا لخاد متت ةفورعم تامجه وأ ،يجرمب أطخ وأ ،لالغتسا
تايلمع رثأت مدع نامضل ،ةءافكلا ةيلاع ةقيرطب جاماربال ىلع يحي لكشب ةبقارملا هذه دُفُت
Cyber Crucible. ليحلحتب ليملعلاو ماظنلا

نيمضت متي ،زازتبالا وأ تانايبلا وأ ةيوهلا ةقرس فدهتسي مجاهم كولس دوجو لامتحا ةطقن دنع
،اهعمج متي يتلا ىرخأل دُعُب نع سايقلا تانايب نمض ةركاذلل ةيكولسللا ليحلحتلاو عبتتلا اذه
ال مأ جامانربلا قيلعت يغبني ناك اذا ام ديدحتل

???? ?????? ?????? ?????? ??????
?????????? (Memory Behavioral
Analysis) ?? Cyber Crucible ??
???? ???????????

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

م اطنل ا ي ف فلتخم عقوم ىل ا اءسن متي ام ءءاو ، ءركاذل نم ءلتك ذء ءسرامم وه ءركاذل صءف
ل. لىلءلتل صاءءل اءصءف مء ، لىلءلتل صءرءل

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

هناك ورم ال ا ي ف ركف . ءمانربلل ءىنمز ءطق ل وه لب ، هلمء ءانءا ءمانربلل اءىء اصءف سىل اءه
ىل ءظءل نم اءربك اءالءءا ءمانربلل ءلءء ءق . رءشابم ءبب ءنراقم ءىف اءوءوء ءروء
ءئىب ءىف ءءاف لقا وهو . ءرطىسلل ءءضاء ءئىب ءىف ءئانء ءىرمتك ءءاف رءكأل وهف اءل ، ىءءا
هب موءى ام ءاءزا وأ ، زاءءل ءىلوءءشم ءءاءزا ام لكف . لىمءل ءئىب لءم ، ءرطىسلل ءءضاء رىء
ءمانربلل ءىلءل ءلءل ءقء ءروء ىلء لوءءل ءبوءص ءءاءزا ، ءمانربلل

ءالءل "رءصلا" نم رىءكك لاءلءل ءلواءم ، ءركاذل صءفل فءكك مءءءءساب Cyber Crucible ءءب
، ءركاذل ءالءل ذء ءءرس ىءمب ءلءءء ءءءءم ءاقانءءا انءءاو ، انءءرس ءاءىءزا ءمو . ءمانربلل ءركاذ
، ءءءءم ءمانرب ربءو .

????? ?????????? ?????? ?????? ???????????
?????????? (CPU) ?? ?????? ???????
?????????? (GPU)

ءقءولا صءب ءرءءسى ءقو ، رىبك لكءشب ءراوملل اكلاءءسم اءه ءركاذل صءف نوكل نأ نكل مى
نم الءب ، ءركاذل صءف مءءءءسء Cyber Crucible ءناك امءنء . ءرىبكك لءمانربلل ءبسنلاب

هـيـلـمـعـل (CPU core) هـلـمـاـك هـجـلـاـعـم هـاـوـن صـيـصـخـت مـتـي نـاـك ،هـكـاـذـلـل هـيـكـذـلـا هـيـكـوـلـسـلـا هـبـقـاـرـمـلـا صـحـفـلـا .

يـلـع هـمـئـاـق هـدـدـم تـاـيـرـاـمـعـم يـلـع هـرـفـوـتـم يـهـو ،[Intel TDT AMS](#) يـعـذـت هـرـكـتـبـم هـيـنـقـت Intel كـلـتـمـت مـ Intel نـم هـجـمـدم (GPU) تـاـمـوـسـر هـجـلـاـعـم هـدـحـوب هـدـوزـم Intel تـاـجـلـاـعـم .

هـجـلـاـعـم هـدـحـو هـمـدـخـتـسـم ،هـرـم لـوـأـل هـلـيـغـشـت هـدـب دـنـع جـمـاـنـرـبـلـا هـرـكـاـذ صـحـفـب هـيـنـقـتـلـا هـذـه مـوـقـت هـجـلـاـعـم هـدـحـو نـأ اـمـك . (CPU) هـيـزـكـرـمـلـا هـجـلـاـعـمـلـا هـدـحـو لـاـقـثـا مـدـع يـلـع هـدـعـاـسـمـلـل (GPU) تـاـمـوـسـرـلـا (أـقـحـاـل كـلـذ لـوـح دـيـزـمـلـا) هـذـيـفـنـت مـتـي يـذـلـا صـحـفـلـا هـوـن اـدـأ يـف هـاـفـك رـثـكـأ تـاـمـوـسـرـلـا .

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

يـه هـذـه نـوـكـت اـم اـبـلـاـغـو .هـدـدـم (strings) "هـيـصـن لـسـاـلـس" وـأ دـاـوـكـأ نـع ثـحـبـلـل هـرـكـاـذـلـا صـحـف اـرـجـا مـتـي لـمـتـخـي يـتـلـا تـاـفـلـمـلـا يـف EDR/تـاـسـوـرـيـفـلـا هـجـفـاـكـم تـاـوـدـأ اـهـنـع ثـحـبـت يـتـلـا تـاـنـاـيـبـلـا اـزـجـا سـفـن هـرـاـض نـوـكـت نـأ .

اـهـؤـاـرـجـا نـكـمـي يـتـلـا هـدـقـعـمـلـا ثـحـبـلـا تـاـيـلـمـع ضـعـب نـم هـيـدـوـدـم رـثـكـأ دـيـدـحـتـلـا هـجـو يـلـع هـرـكـاـذـلـا صـحـف فـلـم يـلـع .

هـثـيـبـخـلـا تـاـيـجـمـرـبـلـا لـثـم ،أـقـبـسـم هـفـوـرـعـم رـصـاـنـع نـع يـضـاـرـتـفـا لـكـشـب صـحـفـلـا ثـحـبـي ،كـلـذـل كـلـذـب مـاـيـقـلـا يـلـع هـتـرـدـق يـف دـوـدـم هـنـكـل ،هـمـيـدـقـلـا .

تـبـثـأ كـلـذ نـكـل ،هـيـرـيـفـشـت دـاـوـم نـع اـثـحـب هـرـكـاـذـلـا اـزـجـا صـحـفـب اـقـبـاـس مـوـقـت Cyber Crucible تـنـاـك هـبـقـاـرـمـلـا هـفـلـتـخـم هـقـيـرـطـا نـرـكـتـبـا فـ ،هـثـيـدـحـلـا تـاـيـيـبـلـل هـبـسـنـلـاـب هـدـيـدـشـلـا هـتـيـدـوـدـم (kernel-based logic) هـاـوـنـلـا يـلـع مـئـاـق قـطـنـم مـاـدـخـتـسـا بـ ،تـاـيـكـوـلـسـلـا .

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

هـدـعـل كـوـلـسـلـا يـلـع هـمـئـاـق هـيـجـهـنـم يـلـا صـحـفـلـا يـلـع هـمـئـاـق هـيـجـهـنـم نـم Cyber Crucible تـلـقـتـنـا بـاـبـسـأ .

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

هـبـعـص هـيـنـمـزـلـا تـاـطـقـلـلـا تـنـاـك .جـمـاـرـبـلـا عـيـمـج رـبـع هـيـح هـرـوـص مـاـدـخـتـسـا هـرـوـض هـو لـوـأـل اـبـبـسـلـا طـاـشـن نـم رـيـثـكـلـا نـاـك .يـرـخـأ هـطـقـلـلـا يـلـا هـجـاـح كـاـنـه نـوـكـت نـأ لـبـق ،دـوـدـم لـيـلـحـت يـتـح لـاـمـكـاـلـا هـيـاـغـلـل رـمـأـلـا اـذـه مـقـاـفـت دـقـو .أـدـج ضـفـخـنـم تـاـرـاـطـا لـدـعـمـب لـمـعـت وـيـدـيـف اـرـيـمـاـك لـثـم اـمـاـمـت ،تـوـفـي جـمـاـنـرـبـلـا يـتـلـا و ،هـمـحـزـمـلـا لـمـعـلـا تـاـطـحـم وـأ مـدـاـوـخـلـا .هـسـفـن تـقـوـلـا يـف جـمـاـرـبـلـا عـيـمـج هـبـقـاـرـم يـلـا هـجـاـحـلـا عـم

نم ةبسنن لقأب رمألا اهب ىهتنا ،ةيمهأ رثكألاو ةبقارم لل ةجاح رثكألا ةزهجألا اهنإ لوقلا نكمي ريغو ةحضاو ةينقتلا دويقلا تناك ،جنتنملا وأ ةكرشلا نع رظنلا ضغبو .ةيلعفل ةبقارملا ةيلمع .

نع ثحبلا يضارثفا لكشب بلطتي ،دراوملا كالهتسا نع آديعب ،صحفلا نأ وه يئانثلا ببسلا ،كلذك .(signature-based) تاعيقوتلا ىلع أمئاق ةركاذلا صحف نوكي نأ بجي ،اذل .**فورعم ءيش** ألامتكا رثكألا تاعيقوتلا صحف نم ةدودحم ةيعرف ةعومجم اذه تاعيقوتلا صحف نوكي نأ بجي نم لعفلاب نومجاهملا نكمت دقل .تافللملا ىلع مئاقلا تاسوريفلا ةحفاكم صحف يف دوجوملا آج ةلئض ةصرف كانهو ؛تاونسلا تافللملا ىلع ةمئاقلا تاعيقوتلا تاعافد نم برهتلا .ةردق لقأ تاعيقوتلا ىلع مئاق ماظن ةطساوب نيجمجاهملا فاشتكال

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

ىلإ لوصولا نم ديفتستو ،تاعيقوت Cyber Crucible نم ةركاذلل ةيكولسل ةبقارملا بلطتتال لصفن انوعد .هسفن تقولا يف جماربلا عيمج تايكولس عبتتل (kernel memory) ةاونلا ةركاذ كلذ .

يتلا كلت وأ ،ةديجلل ةثبخلل تايجمربلا فاشتكا نكمي هنأ ةيكولسل ةبقارملا يئعت ،ألاو ىلع مئاقلا صحفل دمتعي .يلعفل تقولا يفو ةلوهسب ،ةديج وذبتل نومجاهملا اهلدع تايجمربلا نم ةددحلا ةعطقلا كلت ةيؤر قبس ىلع ،تافللملا وأ ةركاذلل ءاوس ،تاعيقوتلا ،تاونسلا تاعيقوتلا ىلع ةمئاقلا تاعافدلا نم نوبرهتي نومجاهملا لظ دقل .لبق نم ةثبخلل ةحاتملا صحفل تايئقت امأ .تافللملا دض صحفل تايئقت نم ةلماك ةعومجم دوجو نم مغرلا ىلع .ةيلعفل لقأ يهو ،كلذ نم ةيعرف ةعومجم يهف ةركاذلا دض

تقولا يف ءاقبل نم Cyber Crucible نم ةركاذلل ةركتبملا ةيكولسل ةبقارملا نكمتت ،آيئانث نم ةركاذلا صحف يئاعي .لمالكلا بجماربلا ذيفنت ةدم لاوط ،دحاو نأ يف جماربلا عيمج ربع يلعلل نومجاهملا موقي ام ةداع .جماربلا نم ديزملا ليغشت عم آءوس دادزت دراوملا يف ةديش تاقانثا ةركاذلا صحف ليحلت قنخي امم ،دحاو تقو يف ةثبخلل تايجمربلا تانيي نم تارشعل ليغشتب ةيجمرب تناك اذإ امع رظنلا ضغب ،دحاو نأ يف اهصحف بجي يتلا جماربلا ددعو ةعرسلال خ نم ةيميدق وأ (zero day) ةديج ةثبخل

???? ???? ?????? ?????? Cyber Crucible ?????? ??????????

ةفלתخم بابسأ ةدعل ثدحت ةركاذلا تاليدعت نأ ةطحالمّ ادج مهملا نم ،الوأ

- 1. ةركاذلا لخاد تامجهلا
- 2. جماربلا نيب لعافتلا
- 3. تايجمربلا ءاطخأ
- 4. ةلغتسملا تارغثلا

ةرورضلاب سيل ،جماربلا نيب ىتح ،ةركاذلا ليدعت وأ تاليلمعل نوقح ةينقت مادختسا إف ،كلذل
أراضاً الممع

يف اطروتم ناكو (هالغأ 4 وأ 1 مقرر دنبل اي) راض هنأ حجّري ةركاذ ثدحل ضّرعت دق جماربلا دحأ ناك اذا
ةيئاقلت تانايب عمج ةيلمع ثدحت ،Cyber Crucible لبق نم ةيئاقلت ةباجتسا

ليدعتلا "لبق" ةلاحلا إلى ةفاضلاب ،جمانربلا يف هليدعت مت يذلا ةركاذلا نم عزجلا ظفح متي
ccdiffe .يمسّي Cyber Crucible ـب صاخ مّطنم قيسنت يف

Cyber ةبابوب نم ليزننتلل احاتم نوكيو ،ةركاذلا نم لّدعمل وأ نوقحمل عزجلا كلذ ظفح متي
Crucible ةينورتكللا

????? ?? ???? ?????? ??? ?????????? ??? Virustotal (??? ??????) ??????????

ةديرف تاريغتم ىلع موجهلا يف ةمدختسملا ةراضلا ةرفيشلا يوتحي ،فورظلا ضعب يف
ةيحصلل ةبسنلاب اديدحتو ،موجهلل ةبسنلاب

هيف بوغرم ريغّ احاصفإ لثم ي Virustotal لثم ماع ليلحت كرحم ىلى ةراضلا ةرفيشلا هذه لاسرإ نإ
نمألا عمتجم امامأ ةيحصلا فّرعت تامولعم نع

????? ?? ???? ?????? ??? ?????????? ?????????? ??? Virustotal (??? ??????)

???????

تاتياب وأةيصن لسالس ن ع تاعيقوتلا ىل ع ةدمتعملا EDR و تاسوري فلا ةحفاكم تاودأ ثحبت
نم تدهوش دق ةثيبلال ةيجمربلال هذه نكت مل ول ىتح . ةقباس تامجه يف تدهوش ةرفيشلا نم
نأ ىلإ هذه صحفا لا تاودأ جاتحت الةءاع . نملال عم تجم ىدل ةفورعم ةرتف دعب حبصت دق ، لبق
ةثيبلال تايجمربلل نم ةفورعم ةعطقب اهطبرت يكل حيحص يئانث قيسنن تب ةرفيشلا نوكت

تاكبش ىل ع رفصلا موي تامجه نم ديدعلا Cyber Crucible تفقو اذق — سايق لل ةلباق جئاتنلا اهل ةباجتسالا واهنع رخا دروم اى غالبا نم اموى 90 ىلا لصى ام لباق لاءملا

??? Cyber Crucible

?????? ?? ??? ?? 200 ????

??????

لماكلاب — Detect-Decide-Respond — تاوطخ ثالث نم ةقلح لال خ نم لمعت :**ةرصتخملا ةباجإ** ةبسوح تاليلحت كرحم مادختساب ،(kernel) ةاونلا يوتسم يلع (Endpoint) ةياهنلا ةطقن يلع ةمدخ يلإ تانايب لاسرإ يلإ ةجالحا مدعل أرطنو .عارتخا ةءاربب لّجسم (edge computing) ةيفرط لقا يف اهلماكب ةرودلا لمتكت ،ةقلحلا يف يرشب لخت دوجو مدعو ،دوعت يتح راطتنا لاو ةيباحس ةيناث يليم 200 نم

??????

1. **فاشتكالا (Detect)** — ديدحتب ةاونلا يوتسم يلع ةركتبم تارعتشم موقت — **فاشتكالا** .تافلما يلإ لوصولاو ،تايلمعلا طاشنو ،ةركاذلا يف ةراضلا ةيكلولسلا طامأل
2. **رارقلا (Decide)** — ةينمي يقيقتب يغانطصالا ءاكذلاب ززعلم يكلولسل جذومنلا موقي — **رارقلا** .روفلا يلع تانايبلا يلإ جمانربلا لوصو
3. **ةباجتسالا (Respond)** — هفاقيإو جمانربلا ضارعا متي ،ةراض ةينلا تناك اذإ — **ةباجتسالا** .

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

?? ??? ???

يقلت م ث ،لليحتلا راطتناو ،يباحس مداخ يلإ (telemetry) دُغْب نع سايقلا تانايب لاسرإ نإ ةعرسل مجح حيضوتللو .رورس لكب مجاهملا هلغتسي س ام تقولا نم فيضي ،ةباجتسالا ي .كغامد يلإ كنيع نم ةبصعلا ةضبنلا لاقتنا نم عرسأ لكشب رارقلا اذه ثدحي :ةبولطملا اذه ترسخ دق نوكت جرحلا راسملا نمض (round trip) ةيكبش لاصتا ةلوج يلع دمتعت ةينب لعفلا ب قابسل

نكل — ءارثإلاو ةلدألا ضارغأل أقحالا مداوخللا يلإ خسُنُت دُغْب نع سايقلا ماخلا تانايبلا لازت ال .أدبأ كلذ رطتني ال ةيماحلا رارق

?? ?? ????? ??? ????????? ????????? (Rogue Process Prevention – RPP)?

دض لخدتلل عارتخا ةءارب ىلع لصاحل Cyber Crucible جهن وه ةقراول تايلمعلل عنم **ةنجوم ةباح**!
تافللمل ريفشت ي ف تءدب ةيذف ةيجمرب تناك ءاوس . اهتبقارم درجم نم ءلدب ةثيبلل ةيلمعلل
جرخت نأ لبق ةيلمعلل فاقيا متي ، ةسلج زمر ىلإ لوصولو لواحت تامولعم ةقرس ةيجمرب وأ
زاهجل نم تانايبلا .

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

ىلع ينبمف Rogue Process Prevention امأ . ةبقارملا ىلع ينبم ةياهنلا طاقن نمأ قوس مظعم
سراحو ، اقحال اهتجارمل ةقرس ةيلمعلل لّجست ةبقارم اريماك نب قرفلل هبشي قرفلل . لخدتلل
ةنزلل دنل صللل فقوي ينمأ .

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

تامهلل نأل ، اعم ةثالثل ةيساسأل تاديدهتل عم Rogue Process Prevention ةزيم لماعتت
بناوجل ةددعتم ابلالغ نوكت ةثيدحل :

- لعافت ي أ نودب ابلالغو ، رورملا تاملكو زومرلاو حيئاتفملا ىلإ لوصولو — **ةيوهلا ةقرس**
قلاطلال ىلع فظوملا نم
- ةلآل ةعرسب تانايبلا نم ةريبك تايماك جارختسا — **تامولعملل ةقرس**
- ريفشت عنمت ي تال ةنصارقلل عاذه ةنقت عم يكلولس ليلحت — **ةيذفل تايجمرب**
دحاو فلم ىتح

ىلوالا نيتلحرملا توفيس طقف ةيذفل تايجمرب ىلع قيض لكشب زكري يذلا عافدلا
يقيقلل ررضلا أدبي ثيح ابلالغامهو ، ةيناثلاو

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

ردصملا يهف .رخآءيش لك هيلع ىنبُي يذلا ساسألأ يه ةركاذلا تاليلحت :**ةرصتخملا ةباجإلا**
و ،ةيوهلا ةيامحو ،تانايبل ةيامح — ةيكلولسل جدامنلأ عيمج يذغي يذلا يليلحتلاو يراعشتسالأ
أيلعف جمانربلل هلعف ي ام ةفرعم ىلع موقى تاردقلا هذه هذخت رارق لكف .ءاوس دح ىلع FortressAI
ةركاذلا يف .

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

امب ،ةياهنلا ىلإ ةيادبل نم ،ةلماكلل هتايح ةرود ربع جمانربلل ةركاذ ةلاح Cyber Crucible عبات
لجع ي ام وه دحاولا يليلحتلا قفدتلا اذهو .رخآلأ جماربل عم ةركاذلا لخاد هتالعات كلذ ي
ةنكمم تاردقلا ةيقب :

- كشو ىلع اهنأ ىلإ ريشت ةقيرطب ةيلمعلل هذه فرصتت له — **تانايبل ةيامح**
ببئرسنلا وأ ريشفنلا
- لواحت يتيلا دامتعالا تانايبل يعرشلل كللملأ يه ةيلمعلل هذه له — **ةيوهلا ةيامح**
؟اهيلع يلوُتسا اهنأ أم ،اهيلإ لوصولا
- **FortressAI** — ىلإ اهلوصو عقي لهو ،اهتعي بط ىلع هذه يعانطصالأ ءاكذلا ةادأ تلاز ام له
؟ةدحملل ةسايسلل نمض تانايبل

ثالث يه لب .يراعشتسالأ ةزهجأ نم ةلقنسم تاعومجم ثالثب ةلصفنم تاكرحم ةثالث تسيل هذه
ةركاذلل دحاو يكلولس جذومن قوف اهسفن نع رُبُغت تاسايس .

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

نقح متيف .هصحف نكمي فلم يأ كرت مدع ىلإ ديازتم لكشب ةثيدحلل تامجهل لي مت
يذلا ديجولناكمل نوكي ثيحب ،ةركاذلا يف اهؤانبو ةقوئوم تايلمع لخاد ةيجمربلل تاميلعتلا
يف ةيؤرلل عيطتسي ال عافدي أو .ليغشتلا دي ق جمانربلل ةركاذ ةلاح وه طاشنلأ ةيؤر هيف نكمي
تامجهل نم ةلماكلل ةئفلل هذه دصر نع أمامت أزجاع نوكي ناكملا اذه .

اده لاز ام له :ساسح ءيش يأ ىلإ لوصولا حنم لب ق مهأل لاؤسلل نع ةركاذلا ليلحت ببجي امك
مل هتابتكمب وأ هتيلمعب ثبعلل ىرج يذلا قوئومل قيببطتلاف ؟**هنأ معزي امك جمانربلل**
ةركاذلا ىوتسم ىلع صحتللالل نم الإ كلذ نع فشكلل نكمي الو ،ةثلاثلأ آري دج دع .

??? ??? ?????????? (Memory Scanning)

يأ — عطقلللا كلت لللحيو ةركاذلا نم أءزج خسني صحتلاف .يرون صحتف ال ،يحي كولس عبتت اذه
ةلاح نوكت دق ،طشن زاهج ىلعو .ةرشابم ويديف عطقلل ال ةيفارغوتوف ةروص ةبائتمب هنأ
تاقيقحتللا يف ةديفم ةبائتل تاطقللل لعجي امم ،ةدحاو ةطحتل دعب أمامت ةفلتخم جم انربلل
يقيقحتللا تقوللا يف عافدلل ةادأك ريثكب فعضأ اهنكل ،ةطوبضللا ةيمقرلل ةيئانجللا

لليصافتللا ىلع لوصحلل ةيلالحلا Memory Analytics تالاقم أضيأ عجار ١١
دنع ثدحي امو ،ةركاذلا صحتف نع بولسألا اذه فالتخا ةيفيكل لوح ةينقتللا
ةركاذلا فدهتسي موجه فاشتكا

????? ????? Cyber Crucible ??? ?????? ??????????

دنع لمعلال. ليغشلتالماظن يف آزايتما رثكأل او قمعأل ةقبطلاليه ةاونللا: **ةرصتخملا ةباجإلا** ةين ديدحتو، اهي ف مكحتلالو ماطنلال ةطشنأ عي مج ةيؤر Cyber Crucible -لحي تي يوتسملا اذه مجاهملا يلع آدج بعصلال نم لعجي امك — ةيناثلال نم ءازجأ نوضغي ف اهفاقيإو، ةثبخلال ةيلمعلال اهليطعت وأ ةادلأاب ثبعلال.

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

- كلذ يف امب، تافللملا يلى لإ لوصولو، تايلىمعلال كولسو، ةركاذلال كولسل **ةلماك ةيؤر** صرقلال يلى لإ آدبأ لصتال تي ةطشنأل.
- قيلعتو تانوذأل ءاغلإ نكمي ذإ — ةبقارملا درجم سيلو، **فرصتلا يلع ةردقلا**، ةثبخلال ةينللا فاشتكأ ةظحل يف تايلىمعلال.
- اهسفن نامأل ةادلأليطعت آمتحنولواحي سني مجاهملا نأل، **ةنورملا**.

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

ةاونلال يوتسم يلع تايجمرب ريوطت نع نيللحملاو قوسلال يف نيخسارلال نيبعلالل ضعب ينيثي ام وهو — اهل قوسلال نم ريبيك عذج بنجت ببس طبضللاب اذهو، أقح ةفللكمو ةبعص ةاونلال ةسدنهف نكمي يتللو، مدختسملا ةحاسم يف دعبنع سايقلال تانايب يلع دمعتت ةياهنلال طاقن لعج اهليطعت رذجلال يوتسم يلع تامجهلل.

Windows ةزهجأ قفاوت جمانرب لالخال نم ثبعلل اهتوماقمو Cyber Crucible ةدوج نم ققحتللا متي (WHCP) تفوسوركيا م بصاخال.

???? ???? ?? Cyber Crucible ????? ? ???? Windows?

دق ف .اهتيامحب موقت يتي ال Windows ماظن تابتكم ىل ع Cyber Crucible دمتعت ال :ةزجوم ةباح|
وأ اهلطعت ي ف نوببستتي وأ تابتكالم كلت نومجاهمالم قرتخي امندن ثيحب ،أدمع اهنع اهلصف مت
(enforcement) قيبطتال ي ف رمتستو ،لمعال ي ف Cyber Crucible رمتست ،اهيلع ءاليتسال
ريراقتال دادع| ي ف رمتستو .

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

ي ف ةيساسأل Windows تابتكم ةباص| ىل |نومجاهمالم لّوت ،2025 ماع نم ينالال فصلال ي ف
لمعلل اهتاذ تابتكالم هذه ىل ع نودمتعي آبيريقت ةينمأل لولالال يدوزم مطعم نأل أرطنو .ةركاذل
قوسال نم ريبيك ءج ءامع| ىل |ةدحاولا ةوطخال هذه تدأ دق ف .

دهج ىل |ةفاضي| ،(sensors) ةديج تارعتشتسم راكتبال رهشأ ةعست وحن Cyber Crucible تقرغتسا
كلذ ي ف امب — لمكالاب Windows تابتكم ىل ع دامتعالا ءالزال ىرخأ رهشأ ةسمخ رمتسا يسندنه
MiniFilter ىل ع ةبلقمتالم تاي دامتعالا ءالزا .

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

كلذ ي ف امب ،(kernel) ءاونال لخال دامت ءلقتسم ةيعرف ةمظنأ ةعبس ةيرامعالم ةينبال لّغشُت
عبتتو ،(metadata) ةيفصولا تانايبال لي لحتو ،تاكبشالو ،لوزعالم اهب صالال ريفشتال
(ws32_2.dll) ةيسايقال Windows تاكبش ةبتكم لمعال اذه نم ةيفاضي ءلحرم لدبتستو .ثالأل
ءاونال ىوتسم ىل ع صصخم تاكبش سّذكمب .

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

،نيمجاهمالم عنمب (kernel-only) طقف ءاونال ىوتسم ىل ع لمعي يذل رارقال كرحم ماق ،نيليمعم عم
ماظن ب ءصالال تاكبشال ءقبط ءمجاهم لالال نم ليمعال ءالبل عنم كلذ دعب نومجاهمالم ءالؤه لواحف
تلت ،ليغشتال ماظن نع ءلقتسم Cyber Crucible ي ف ءكبشال تالاصتا نأل أرطنو .ليغشتال
كلذ مغل ليمعال ىل |ةيتارابختسال تاملولعالم تلصوو ءمئاق ةيالحال .

?? ????? Cyber Crucible ?? ??? ??? ?????????? ?? ?? ?????????? ???????????? ?? ????????? (air- gapped)?

،ةياهنلا ةطقن ىلع آي لحم قي بطتلاو لي لححتلا تاي لمع عي مج متت .معن :ةرصتخملا ةباجإلا
يأ وأ ،ةباجس ةمدخ وأ ،تنرتنإلاب لاصتا إلى إجحاحلا نودة لماك ةيامح Cyber Crucible رفوت اذل
ةيليغشتلا تاي نقتلا تائي بو ،(air-gapped) ةلوزعملا تاكبشلل ةبسانم يهو .عون ي نم ةراشإ
،ةلصتملا ريغ ةيناديملا تاي لمعلاو ،(ICS) يغانصللا مكحتلا ةمظنأو (OT)

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

الف ،زاهجلا ىلع (kernel) ةاونلا لخاد لماكلاب لمعت Detect-Decide-Respond ةقلح نأل آرطن
لكشب (telemetry) دُعب نع سايقلا ةنمازم متت .ةيامح رارق ذاخاتال أدبأ لاصتا دوجو طرئتشي
لكذ ىلع دمتعت ال ةيامحلا نكل ،لاصتا رفوت دنع ريراقتلا دادعإو ةلدألا ضارغلأ يزاهتنا

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

نود مايأ ةدع ترمتسا تالحر لالخال لقتسم لكشب Cyber Crucible تلمع ،ةيرحب رشن ةيلمع يف
تاذه ةيغانصللا رامقألا طباور عم تفكيكو ،ةنيفسلا نتم ىلع تامولعم ةينقت يفظوم دوجو
تالجبسب تظفتحاو ،ةيوجل لاوحألا ببسب تااعاطقنا عم ةعطقتملاو صفخنملا يدرتلا قاطنلا
ةمظنألا تحوارتو .ةلحرلا ءاهتنا دعب اهليلحتلا ةليوطلا اعاطقانالا تارثف لاوط ةينغ ةيئانج
ماهملل ةيمهألا ةغللاب ةيرحبلا مكحتلا ةمظنأو باكترلل ةهجوملا هيفرتلا تاطحم نيب ةيمحمل

تامدخللا ليطاسأو ،عينصتلا عناصم بسانم هتاذ لي لمعلا نأ يف ببسلا وه أضيأ اذهو
آبئاع وأ قوئوم ريغي باحسلا لاصتالا نوكتي ثيح ةيفرطللا تائيبل نم اهريغو ،ةيتسجوللا
أدمع

????? ?????? Cyber Crucible

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

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

يئاقتنالا ديمجتلا مسا أنايح أهيلع قلطويو — طقف ةثبخلال ةيلمعلا قيلعت :ةزجوم ةباج!
(Selective Freeze) — لملعلا يف رخآ ءيش لك رمتسي امنيب موجهلا لوعفم لطبئي —
عورشملا لمعلل عاطقنا الو ،ليغشت ةداعإ الو ،ماطنلل لماك

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

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

وأ زاهجلا لزع :ةظف ةحاتملا ءاوتحال تاراخي نوكت ،ذوذش دوجو فشكلا تاودأ نم ديدعلا ددحت امدنع
ةراض ةباجتسال هذه نوكت نأ نكمي ،لوات ةيلمع وأ عنصم وأ يفشتسم يف .ةمدخلال نع هجارخإ
هسفن موجهلا ردقب آبيرقت

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

ةصاخلا رشنللا ةيلمع يف .آدب أعورشملا تالماعملا فقوتت ال .ةركاذلا يف موجهلا قيلعت متي
SQL تالماعم ترمتسا ،ةثبخلال 10,000 براقبي امضارتعا مت ثيح ،ةيلاملا تامدخالاب
لمعلال نع آدب تايلمعلا فقوتت ملو — تقولا لاوط عاطقنا نود أعورشملا

اهباسح ىلع ةضياقم نوكت نأ نم آلدب لامألل ةيرارمتسا عم ةقفاوتم ةياقولا لعجي ام اذه