

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

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

م ا ط ن ل ا ي ف ف ل ت خ م ع ق و م ي ل ا ا ه خ س ن م ت ي ا م ة د ا ع و ، ة ر ك ا ذ ل ا ن م ة ل ت ك ذ خ ا ة س ر ا م م و ه ة ر ك ا ذ ل ا ص ح ف
ل ل ل ح ت ل ا ض ا ر غ ا ل ا ه ص ح ف م ث ، ل ل ل ح ت ل ا ض ر غ ل .

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

ه ن ا ك و ر م ا ل ا ي ف ر ك ف . ج م ا ن ر ب ل ل ة ي ن م ز ة ط ق ل و ه ل ب ، ه ل م ع ا ن ث ا ج م ا ن ر ب ل ل ا ي ح ا ص ح ف س ي ل ا ذ ه
ى ل ا ة ط ح ل ن م ا ر ي ب ك ا ف ا ل ت خ ا ج م ا ن ر ب ل ل ا ة ل ا ح ف ل ت خ ت د ق . ر ش ا ب م ث ب ب ة ن ر ا ق م ة ي ف ا ر غ و ت و ف ة ر و ص
ة ئ ي ب ي ف ة د ئ ا ف ل ق ا و ه و . ة ر ط ي س ل ل ة ع ض ا خ ة ئ ي ب ي ف ي ئ ا ن ج ن ي ر م ت ك ة د ئ ا ف ر ث ك ا ل ا و ه ف ا ذ ل ، ي ر خ ا
ه ب م و ق ي ا م د ا ذ ا و ا ، ز ا ه ج ل ا ة ي ل و غ ش م ت د ا ذ a ا م ل ك ف . ل ي م ع ل ا ة ئ ي ب ل ث م ، ة ر ط ي س ل ل ة ع ض ا خ ر ي غ
ج م ا ن ر ب ل ل ة ي ل ا ح ل ا ة ل ا ح ل ل ة ق ي ق د ة ر و ص ي ل ع ل و ص ح ل ا ة ب و ع ص ت د a ذ a ، ج م a ن ر ب ل a
ت a ل a ح ل " ر و ص ل a " ن م ر ي ث ك ل ا ط ا ق ت ل ا ة ل و ا ح م ، ة ر ك a ذ ل a ص ح ف ل ف ث ك م م a د خ ت س a ب Cyber Crucible ت ا د ب
، ة ر ك a ذ ل a ت a ط ق ل ذ خ ا ة ع ر س ي د م ب ق ل ع ت ت ة د د ع ت م ت a ق a ن ت خ a ا ن ه ج a و ، ا ن ت ع ر س د a ي ذ a ع م و . ج م a ر ب ل a ة ر ك a ذ
، ة د د ع ت م ج م a ر ب ر ب ع و .

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

ت ق و ل ا ض ر ع ب ق ر غ ت س ي د ق و ، ر ي ب ك ل ك ش ب د ر a و م ل ل ا ك ل ه ت س م ا ذ ه ة ر K a ذ ل a ص ح ف ن و ك ي ن ا ن ك م ي
ن م ا ل د ب ، ة ر K a ذ ل a ص ح ف م د خ ت س ت Cyber Crucible ت ن ا ك ا م د ن ع . ة ر ي ب ك ل a ج م a ر ب ل ل ة ب س ن ل a ب

هـيـلـمـعـل (CPU core) هـلـمـاـك هـجـلـاعـم هـاـون صـيـصـخـت مـتـي نـاـك ،هـركـاـذـلـل هـيـكـذـلـا هـيـكـولـسـلـا هـبـقـارـمـلـا صـحـفـلـا .

يـلـع هـمـئـاق هـدـدـم تـاـيـرـاـمـعـم يـلـع هـرفـوتـم يـهـو ،[Intel TDT AMS](#) يـعـذـت هـركـتـبـم هـيـنـقـت Intel كـلـتـمـت مـ Intel نـم هـجـمـدم (GPU) تـاـمـوسـر هـجـلـاعـم هـدـحـوب هـدـوزـم Intel تـاـجـلـاعـم .

هـجـلـاعـم هـدـحـو هـمـدـخـتـسـم ،هـرم لـوـأـل هـلـيـغـشـت هـدـب دـنـع جـمـانـرـبـلـا هـركـاـذ صـحـفـب هـيـنـقـتـلـا هـذـه مـوقـت هـجـلـاعـم هـدـحـو نـأ مـاـك . (CPU) هـيـزـكـرمـلـا هـجـلـاعـمـلـا هـدـحـو لـاـقـثـا مـدـع يـلـع هـدـعـاـسـمـلـل (GPU) تـاـمـوسـرـلـا (أـقـحـال كـلـذ لـوح دـيـزـمـلـا) هـذـيـفـنـت مـتـي يـذـلـا صـحـفـلـا عـون هـاـدـأ يـف هـاـفـك رـثـكـأ تـاـمـوسـرـلـا .

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

يـه هـذـه نـوكـت اـم أـبـلـاـغـو .هـدـدـم (strings) "هـيـصـن لـسـالـس" وـأ دـاـوكـأ نـع ثـحـبـلـل هـركـاـذـلـا صـحـف اـرـجـا مـتـي لـمـتـخـي يـتـلـا تـاـفـلـمـلـا يـف EDR/تـاـسـورـيـفـلـا هـجـفـاـكـم تـاـودـأ هـنـع ثـحـبـت يـتـلـا تـانـاـيـبـلـا اـزـجـا سـفـن هـرـاض نـوكـت نـأ .

هـؤـاـرـجـا نـكـمـي يـتـلـا هـدـقـعـمـلـا ثـحـبـلـا تـاـيـلـمـع ضـعـب نـم هـيـدـودـم رـثـكـأ دـيـدـحـتـلـا هـجـو يـلـع هـركـاـذـلـا صـحـف فـلـم يـلـع .

هـثـيـبـخـلـا تـاـيـجـمـرـبـلـا لـثـم ،أـقـبـسـم هـفـورـعـم رـصـانـع نـع يـضـارـتـفـا لـكـشـب صـحـفـلـا ثـحـبـي ،كـلـذـل كـلـذـب مـاـيـقـلـا يـلـع هـتـردـق يـف دـودـم هـنـكـل ،هـمـيـدـقـلـا .

تـبـثـأ كـلـذ نـكـل ،هـيـرـيـفـشـت دـاـوم نـع اـثـحـب هـركـاـذـلـا اـزـجـا صـحـفـب أـقـبـاس مـوقـت Cyber Crucible تـنـاـك هـبـقـارـمـلـا هـفـلـتـخـم هـقـيـرـطـا نـرـكـتـبـا فـ ،هـثـيـدـحـلـا تـاـيـيـبـلـل هـبـسـنـلـاب هـدـيـدـشـلـا هـتـيـدـودـم (kernel-based logic) هـاـونـلـا يـلـع مـئـاق قـطـنـم مـادـخـتـسـاب ،تـاـيـكـولـسـلـا .

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

هـدـعـل كـولـسـلـا يـلـع هـمـئـاق هـيـجـهـنـم يـلـا صـحـفـلـا يـلـع هـمـئـاق هـيـجـهـنـم نـم Cyber Crucible تـلـقـتـنـا بـابـسـأ .

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

هـبـعـص هـيـنـمـزـلـا تـاـطـقـلـلـا تـنـاـك .جـمـارـبـلـا عـيـمـج رـبـع هـيـح هـروـص مـادـخـتـسـا هـرورـض هـو لـوـأـلـا بـبـسـلـا طـاشـن نـم رـيـثـكـلـا نـاـك .يـرـخـأ هـطـقـلـلـا يـلـا هـجـاـح كـاـنـه نـوكـت نـأ لـبـق ،دـودـم لـيـلـحـت يـتـح لـاـمـكـاـلـا هـيـاـغـلـلـا رـمـأـلـا اـذـه مـقـاـفـت دـقـو .أـدـج ضـفـخـنـم تـارـاـطـا لـدـعـمـب لـمـعـت وـيـدـيـف اـرـيـمـاـك لـثـم اـمـامـت ،تـوـفـي جـمـانـرـبـلـا يـتـلـا و ،هـمـحـزـمـلـا لـمـعـلـا تـاـطـحـم وـأ مـدـاـوـخـلـا .هـسـفـن تـقـولـا يـف جـمـارـبـلـا عـيـمـج هـبـقـارـم يـلـا هـجـاـحـلـا عـم

نم ةبس ن لقأب رمألا اب هت نا ،ةيمهأ رثكألاو ةبقارم لل ةجاح رثكألا ةزهجألا اهنإ لوقلا نكمي ريغو ةحضاو ةينقتلا دويقلا تناك ،جتنملا وأ ةكرشلا نع رظنلا ضغبو .ةيلعفل ةبقارملا ةيلمع .

نع ثحبلا يضارتفا 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 ةليئض ةصرف كانهو ؛تاونسلا تافللملا ىلع ةمئاقلا تاعيقوتلا تاعافد نم برهنتلا .ةردق لقأ تاعيقوتلا ىلع مئاق ماظن ةطساوب نيجمجاهملا فاشتكال

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

ىلإ لوصول نم ديفتستو ،تاعيقوت Cyber Crucible نم ةركاذلل ةيكولسللا ةبقارملا بلطتت ال لصفن انوعد .هسفن تقولا يف جماربلا عيمج تايكولس عبتتل (kernel memory) ةاونلا ةركاذ كلذ .

يتلا كلت وأ ،ةديجلل ةثبخلل تايجمربلا فاشتكا نكمي هنأ ةيكولسللا ةبقارملا يئنت ،ألاو ىلع مئاقلا صحفل دمتعي .يلعفل تقولا يف 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 ةيكولسللا ةبقارملا نكمتت ،آيئانث نم ةركاذلا صحف يئاعي .لمالكلا اب جماربلا 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 .ةميدق وأ (zero day) ةديج ةثبخل