

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

تايجمربل - اهفاقي إ Cyber Crucible تم مُصّيتال موجهال بيلاسأل ةحضاو ةغلب طسبم حرش وقراسو، ةنصارقل اهمدختسي يتال ةتمتأل او، ةركاذل لخاذ تامجهال او، تافلمال ةميدع ةثيبلال (session-token) ةسلجلال زومر ةقرسو، تامولعملال

- [مجاهم لل ةبنجلال ةكرحال فاقيل Cyber Crucible - لن كميل له](#)
- [تاقيبطللل ءاضيبلال مئاوللل لمعت له](#)
- [تاقيبطللل ءاضيبلال ةمئاولل ي ف جاردال وه ام](#)
- [صصخملا كولسلال دوجو الاول هقيلعت متيس ناك ام ةفرعم يننكمي فيك](#)
- [ةصصخملا تايكولسلال ةرادل ةيفيك](#)
- [\(ةركاذل ي ف\) تافلمال ميدع موجهال وه ام](#)
- [ةيديلقللل عافدل لئاسو يلعل بلغتت اذاملو، ةنصرقلال ةتمتأ يه ام](#)
- [بوساح لك ي ف عقاوملا سفن ةلآال تامجهال فدهتست اذامل](#)
- [\(session token\) ةسلجلال زمر ةقرس دغت اذاملو، \(info-stealer\) تامولعملل قراسل سوريفال وه ام](#)
[رطخال اذهب \(token\)](#)
- [ةمئاوللل لشفت اذاملو، \(Living-off-the-Land - LotL\) "ماظنل ضرأ يلعل شيعل" تامجه يه ام](#)
[اهل يدصتلال ي ف تاقيبطللل ءاضيبلال](#)
- [ةركاذل ي ف System32 DLL موجه وه ام](#)
- [ينمأ رابتخا ربتخم ي ف أمئاد اهسفن ةثيبلال تايجمربل لل عفُت ال اذامل](#)

?? ????? ?? Cyber Crucible

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

??????????

ةيبناجل ةكرحل ىلع ةلدأل عمجب Zero Trust تايجهنم وجتنم لاب صاخلا كولسل كرحم موقي ةيلاعفب.

نأ نكمي وأ، هسفن زاهجل ىلع ىرخأ ىلإ ةيلمع نم ةيبناجل ةكرحل ىلع اليلد كلد نوكي نأ نكمي ببسل ليلحت ءارجإ ءانثأ، ديعب ماطن نم ماطنلا ىلإ مجاهملا لوخد ةطقنل آفاشتكا نوكي (Root Cause Analysis) يرذجل.

تايلمعو (process injection) تايلمعل نقحب بيلاسأب ةطبترملا اهطئاسوو جماربلا طاقنلا متي Cyber Crucible ىلإ اهلاسرا مث، ىرخأ تايلمع حتفت يثلا (living off the land) "ضرأل جراح شيعلا".

تازايتما تاذ نوكت تايلمع يادجوتلا، (kernel) ءاونلا يوتسم ىلع كولسل تاليلحتل ارطن ءاونلا ليغشت جمارب كلذ ي فامب) اهنع غالبإلاو Cyber Crucible ةبقارم عنمي لكشب ةيلع (ىرخألا ةياهنلا طاقن نام تاودأ ىتح وأ، ىرخألا).

ريفشت وأ تانايبلا زازتبا تاءارجإ نم يءدب دنع يلى لكشب زازتبالل ةداضم تاباجتسا ثدحت ةيدفلل جمارب.

تايثقت مادختساب، ام زاهج ربع ةيبناجل ةكرحل حضوي ويديف يلى اميف، لاثملا ليلبس ىلع ةيلمعلل يلىل ءال قيلعتلا نأ ةطحالم يجرى. Log4j ةرغث لالغتساو، (in-memory) ةركاذلا يف لمعت ةيدفلل جماربو تانايبلا ةقرس تايكولسل ءدب دعب ثدح ةرثأتملا (تايلمعلا وأ).

[rr-log4j-procinj-3mins.mp4](#)

Windows (Windows shell) فالغ حتفل مجاهم مادختسا حضوي ةيكيمانيدلا هذه ىلع رخآ لاثم ءلواحم يف Windows فالغ أدب نأ درجمب طاشنلا قيلعت مت نكلو، ةلدأل عيمج ةبقارملا تطقنلا (تانايبلا ةقرس، ءلاحلا هذه يف) تانايبلا زازتبا ةطشنأ.

[rr-com-dll.mp4](#)

أدبأ مجاهملا حجني مل ءلاحلا هذه يفو، هلالغتسا مت حفصتم نم لاقننالا دصرأضيأ متي، أريخأ: حفصتملا ةركاذ ءلاح ةبقارم لصفب كلذو، لغتسُملا Chrome حفصتم نم لاقننالا يف.

[rr-untrusted-chrome.mp4](#)

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

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

لعمل الابل اهل حومسمال جماربال عمئاق كيدل نأ ينعي موهفم يه تاقيبطلل ااضيبال عمئاقلا،
لعملالابل اهل حومسم ريغ رخآ يشي أو.

ةهولاول ردصمال قطنم نم ام أعون أمدقت تاقيبطلل ااضيبال مئاوقلا تاي نقت رثكأ عمجتس
Windows notepad جمارب" نأ يلع ام قيبطلل ااضيبال عمئاق صنت دق، لاثمال ليلبس يلع
ريغ Microsoft Word نكل، يب صاخال بتكلمل حطس يلع بئارضال دلجم يلل لوصولالابل اهل حومسم
"كلذب اهل حومسم.

تاي جيتار تسامدتت، ماع لكشب نكلو، أقحال ليلصفال نم ديزمب رمألا اذه مييقتب موقنس
نيريغتمال نيذه يلع ريبك لكشب تاقيبطلل ااضيبال مئاوقلا يلع عمئاقلا عافدل:

1. نمألا ةادأب قلعتي اميف مهل اهتعضوي تال دعاقول عابتا يلع نومجاهمال قفاوي
كيدل تاقيبطلل ااضيبال عمئاقلا بصاخال يناربيلسال
2. دح يلل ةرقتسم لظت تي تال تاقيبطلل نم ليلق ددع يلع يوتحتو آدج ةريغص كتئيبي
لالغتسالل ةلباق تارغت نودبو، ام.

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

?????????

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

رصح ال تايكولس اهل ورمتسم ريغت يفي تانايك يه ةريغصل تامولعمل اينيقت تاكشب يتح
جماربال وروطم موقيا امك. اهتلازاول تاقيبطلل افاضلابل رارمتساب نومدختسمال موقيا. اهل
أريخأو. ثيدحتال دنع ةصاخ، اهتلازاول تاقيبطلل لخد (modules) تادحول افاضلابل رارمتساب
تايكولس نإف، كولسال يفي تاريغت يلل يدؤت تي تال ةيجمربال ةرفيشال تاريغت يلل افاضلابل

تاقوأي في نیفلتخم نیمدختسم لبق نم ةفلتخم قرطب مدختسُت افسن تاقیبطتال
ینفل معدل ركاذتو ،رارمتساب كلذ ةعباتم هیلع نیعتیسی ذل قیرفل آلآ لیخت .ةفلتخم
تامولعمل ةینقت ةدعاسم بتكم یلإ رارمتساب درتسی تل

ثیح ،(kiosks) كاشكأ طساوب لمعت یتل كلت یه ةدیحوال ةرقتسمل ةینقتال ةئیبل ،آیغقاو
ءادأ نیمدختسمل لحمسُیو ،ةلازالا وأ ةفاضإلا وأ ةقیرتال ةیناكمإ نود جماربلا تیبتت متی
،ةلاحل هذه یف .هباش ام وأ روصلال ةعابطل كشك امبر .قیض لكشب طقف نیتیظو وأ ةفیظو
زاهج ةقیرت اهیف متت ةرم لك الإ ثیدحتال یلإ تاقیبطتلل ءاضیبل ةمئاقلا جاتحت نل
،ةنسلال یف نیترم امبر ،كشكال

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

اهدوجوب حومسمل جماربلا ب مئاق یلع ةطاسب یوتحت تاقیبطتلل ءاضیبل مئاقول طسبأ
مدختسمل ماظن یف .

ةلمتحمال تانیسحتال نم ةعونتم ةعومجم یلإ یدؤی هنكل ،ةرادإلا بعصأرمأ هتاذ دحب اذه نوکی دق

ال ،ةكرشل باتاور ماظن عم لعافتلل قیبطت هیدل بتاورلا مسق نأ درجمل ،لاثمل لیبس یلع
تاقیبطت هیدل یذل ،عدوتسمل قیرفل دعاوقلا نم ةلصفنم ةعومجم كانه نوكت نأ یغبنی
؟(بتاورلاب ةقلعتم ریغ) ةفلتخم

لیغشتب مهل حومسمل نیمدختسمل وأ ماسقألا دیحبت ةقلعتمل تانیسحتال إف ،اذل
درج یلإ ةفاضإلاب ،آیفاضإدیقت نآلا دجوأ نیسحت .حضاو نیسحت یه ةنیعم تاقیبطت
.كشكبش یلع ةدوجومال جماربلا تارادصاوغاوناو ددع عبتت

هیدل مدختسم یأ دیحت یلإ جاتحن - تانیسحتال نم یرخأ ةعومجم یلإ ةجاحب اننأ ضررتفنل ،نآلا
.تانایبل نم ةعومجم یألو ،قیبطت یأ یلإ لوصول ةیحالص

یلإ لوصول نم كیدل عدوتسمل قیرف كنكمتی نأ دیرت ال ؟كلذك سیلأ ،أمامت یقطنم آضیأ اذهو
تانایب یلإ لوصول یلإ جاتحی ال حجرألا یلع ةیرشبلا دراومل قیرفو ،ةیرشبلا دراومل تالجس
.عدوتسمل میلست قیرف تایلعم

عقاوم تفیضُأ نأ دعب نآلا ،اهعبتت بجی یتل تابكیرتال نم فیخس لكشب ةدقعم ةعومجم هذه
.ریغتمك تانایبل

ةرادإلا إف ،ةلاعف تاقیبطتلل ءاضیبل مئاقول تانینقت لعجل ریورض نیسحت لك عم - اذل
یلع طاफलل مزاللا (رارمتساب دعاصتیو یهتنی ال هنإ لوقلل كنمی) رمتسمل معدلاو ةئییهتلاو
نم ةریبك تاعومجم نأ یه ةداع ةجیتنلاو .مادختسالل ةلباق ریغ ةینقتال لعجی اهلعم
مطعم یلإ حجرألا یلعو ،تاقیبطتال نم ةریبك تاعومجم یلإ لوصول ةیحالص حنُمُت نیمدختسمل
دراومل اهیذل ةكرش دجوت ال هنأل ،ةینقتلل ةدئافل ةمیدع هبش ةئییهت - یلاتلابو .تانایبل
.جیحصل لكشب اهترادإ یلع طاफलل ةیفاكل

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

، أنايحأ .ىرخأ تاقيبب طت عم تاقيبب طتلا لعافتت نأ ةثيدحل لىغشتلا ةمظنأ يف عئاشلا نم
حتف لثم - مدختسملا ةبرجت ززعي امم ، نىقيبب طت نيب لماكت نع أجتان لعافتلا اذه نوكي
تاءاعدتسا ثدحت (أدج عئاش رمأ اذهو) ىرخأ نايحأ يفو . Microsoft Photos قيبب طتلا Word دنتسم
يئاهنلا مدختسملل ةيئرم ريغ ةداع نوكت ةقيرطب جماربلا نيب

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

- [مقدم](#)
- [ينقت ريغ ف صو - تاقى ببطت لل اءاضى بل اءمئاق لى ف جاردال اعاون](#)
 - [\(دي ج رم\) قهرم ل او حضاو ل رورم لى حى رصت](#)
 - [\(اى ج ارم ا سى ل ج رال لى لى\) ماعل رورم لى حى رصت](#)
 - [ددحم ل ماعل رورم لى حى رصت](#)
 - [اى دحت ددحم ل رورم لى حى رصت](#)
 - [قرتخم ل قى ببطت ل](#)
- [تاقى ببطت لل اءاضى بل اءمئاق لى قردق ص ح ف دن ع اءرط ب جى ءلئ س ا - زاجى اب](#)
- [\(NIST\) ءى نقت ل او رى اعمل ل لى نطولا ده عم ل ن م ءم عم ءارق](#)

?????

ن ذال ا م قى ببطت ح ن م وه Cyber Crucible قاي س ف ، تاقى ببطت لل اءاضى بل اءمئاق لى ف جاردال اءراض و اءوب شم كل ذ ف ا ل خ ر ب ت ع ئ دق نى ع م اءر ج اءا ب

لى ع ءمئاق لى اءاف دل بى لاس ا ف ءءاع تاقى ببطت لل اءاضى بل اءمئاق لى ف جاردال ءى نقت دج و ت ف (ا ن ه لوم شم رى غ رم و وه) اءضى ا ن وم د خ ت سى نى م ج ا ه م ل ا ض ع ب ن ا م ر ، ك و ل س ل لى ل ح ت ل م ه ت اى ل م ع

ص ص ل ا ءا ن ث ا ت ا ر م م ل ا فى ل و ج ت ل ا ب ءءاع ب ا ل ط ل ل ح م س ئ ن كى م ل ثى ح ، ء س ر د م ل ل ث م ر م ا ل لى خ ن كى م ل ف ، ء ط ل س ت ا ذ ءى ص خ ش ل ب ق ن م ا م ل ك ش ب "رورم حى رصت" ا و ح ن م ا ذ ا ، ك ل ذ ع م و . ءى س ا ر د ل رى د م ل ب ت ك م لى لى ن و ل س ر ئ و ا س ا ر د ل م ه ل ص ف لى لى ن و د ا ع ئ ب ا ل ط ل ل

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

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

????

ولوؤسم اهملعت ةفلتخم تاي نقت دجوت نأ نكمي ،"رورم لحي رصت" هي بشت مادختسا ان لصاو اذإ
بالطل اضعب لواحي دق يتل تايكولسلال ىلع ىمسرللاباطل ءاضإ يف تدعاس ،ةسردملا ةرادإ
ةرشابم ةقالع أعيمج هذلو .اهب تالفإلا (سنيدي ذي فننتلا انسيئر سيل ديكأتلابو)
نم ألل تاي لمعب

????? ?????? ??????? ????????? (???
???)

21987331.jpg?width=278
غلابم لكشب آحضاوو آري بك ناك ،ام ةفرغل حاتفم وأ ،رورم لحي رصت ىلع لك لوصح أموي ركذتت له
هيف

كذلذل ناهيحو ناببس كانه ناك:

1. دق فُي ال ىتح .
 2. ققحتللا يف ،ةطلسلال تاذ ةيصخشلل لب ق نم رَمثتسملا دهجل او تقولا ليلقتل
ب. لاطلل ةدمتعمل ةطشنأل نم عيرسلال
- يغبني تاقيبطتلل ءاضيبلا ةمئاقلا جم انرب نكلو ،ءاضيب ةمئاق دي جلال جم انربلا "دقي" نل
هصحف مت دق قيبطتلل أن نم دراوملا ثيح نم لأغلل او عيرسلال ققحتل نم نكمُي نأ

????? ?????? ?????? (??? ????????? ???
????? ??????)

هنكل ،ءاوس دح ىلع سرادم للو تاقيبطتلل ةبقارمل ةبسنلاب ةدئاف لقألل اذه نوكي امبر
ةربخلل وأ ةرادإلا نم ردق لقأ بلطتي

- لي بس ىلع ،كلذب ملعمل ملعي دق .رمملا يف هتمهم زاجنإ بل لاطلل حمسُي ،ةلاحلا هذيف
كانه تناك اذإ ،كلذك .بل لاطللا هل عفي ام أنشب رمملا ببقارم نم ققحت دجوي ال نكل ،لاثملا
دراوملا يف ريبكلا رامثتسالال نم نايتوتسم كانهف ،ققحتلل ةلواح
1. هتي نو هتايكولس أنشب هباوجتساو بل لاطللا نم بارتقالل مزاللا دهجلل ىوتسم
 2. بل لاطللا ريسفت نم ققحتلل ،بل لاطللا قدص نم دكأتلل مزاللا دهجلل ىوتسم

نم يفاضإ ققحت يأ نود ،ءاضيب ةمئاق ىلإ جم انرب فاضُي ام دنع آبللاغ اذه دَهاشُي ،تاقيبطتلل عم
تايكولس قاي س باستكا ىلع ةردقلا نإف ،طحلا ءوسلو .اهب حومسملا ةطشنأل وأ تايكولسلال
رخآ لمع راطإ ةطساوب آي جراح عُبَتُت مل ام اهيلي لوصحلل ةحاتمَّ دَعا نوكت ال قيبطتلل

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

"!ءاشت ام لعفا ،قيبطتلا اهيأ لضفت"، نيبو هنيب طلخُي ال

أيبسن لهسل نم ،حيرصتلا حوضول أرطن .انه أدج مئالم هنأل ،هايمل ةرود حيرصت ىلإ دعنل قاطن نع جرت يتلا ءحذافلا تاكولسل ميريقت نكمي .بلالطلا هب موقى نأ يغبنى ام ميريقت .ةريبك ءبوعص نود "هايمل ةرود ىلإ باهذلا" تاكولسل

نأ مغر ،أعويش رثكألا وه ءطشنأل ءماعلا دودحل تاذ تاقىبطتلل ءاضيبلا ءمئاقلا يف جاردإلا يف بعللابل هايمل ةرود حيرصت لمحي بلالطل حامسل لداعت تالاحل نم ريثك يف دودحل هذه .بعلمل

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

"!دحمل ماعلا رورمل حيرصت" نيبو هنيب طلخُي ال

22642689.jpg?width=340

،ةريبك ءسردم يف - هايمل ةرود مدختسي بلالطل نأ ،دحمل ماعلا رورمل حيرصت عم ،ملعن امنيب ملعن ال

1. نذال بلالطل حنم نم .
2. وتلل ىتأ نى نم .
3. ءقفاومل تحنم امذن ءطلسل تاذ ءيصخشلل نهذ يف تناك هايمل ةرود ي .
4. "ألوجتمو آجراخ" بلالطل اوىتم ذنم .

،ءسردم لابل صاخلا ءطلسل راطل ىلع لمعل نم آديزم اذه بّلطت

املك ءقد رثكأ كوكولسل لىلحتلا نوكى ،تاقىبطتلل ءاضيبلا ءمئاقلا يف جاردإلا ىلإ ءدوعللو رارقلا ذاختا ىلع ءردق ي ىلإ ءفاضملا تاريغتملا تدار .

5 نم ءلسلس عبتت ىلإ ءءاع جاتحت ال ،رداص رورم حيرصت نم ققحتلا دنع ،كلذل ىلإ ءفاضلابل نم آعون نكي مل ملعلم نأب قوثلابل رقت آمائاد كنكمي امك .ردصملا ىلإ لوصولل نيملمعم ءاضيبلا ءمئاقلا يف جاردإلا .قئال ريغ لكشب فرصتلل بلالطل ءجوي يذلا "ئيسل ملعلملا" صحفل ،يسكع لكشب لمعل بلطتي ،آديحت ءدحمل ءاضيبلا ءمئاقلا لاثم يف ،تاقىبطتلل نم ءعطق نوكت دق ،لاثملا لىبس ىلع .لياتل قىبطتلا حتفلس وأ بأ قىبطتلك Windows تاودأ نم ءيعرش ءادأ تحتف دق ءثيبخلا تايجمربلا

هالءأ "بلالطل رورم حيرصت" أبرقت لداعت ءيلاتلا ءلئسلأ :

1. دوصقملا كوكولسل ءفرعم ىلإ جاتحن ؟لءفى نأ هنم بلط اذام وأ ،قىبطتلا أدب ضرغ يأل .
2. رخآ آجامنرب اذه نوكى ام ءءاع ؟قىبطتلا لىغشتب ماق نم .

يوني وأ،لعفي اهنم لك ناك اذام ؟جمانربل اذه حتف ىلإ تدأ "فلس" وأ "بأ" جمارب ي 3. هلعف

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

ام لاتحم يلوتسي امدنع ،بعرل مالفأو بدأ وأ ،يملعل لايلخل لامعأ فلتخم يف ركذت له ام ةقيرطب

22413315.jpg?width=226

نئاك يلوتسي نأل ركذت ةصرف دجوت ال ،سرادمال يف ؟ام ةيصخش كولس ىلع ةرطيسلا ىلع مّلع ىلع ىلغاضف

طحالي ال ،مالفأال يف امك ،هنأل ني مجاهملا ىدل ةلصفم ةينقت وه قيربطلتلا ىلع ءاليتسالا .ناوأل تاوف ىتح يعي بط ريغ آئيش ني بقارملا مطعم

لهاجتُي ،كلذبو .ةركاذلا يف آيلاحّ المحم ،ليغشتلا ديق آجامنرب مجاهملا دخأي ،ةلاحل هذه يف ةفاضلا ةركاذلا يف دوجوملا جمانربلا لّدغُي .تافلما لماظن يف دوجوملا أمامت ميلسللا جمانربلا ،ةيمارجلال هتطشنأب مجاهملا موقي .ناسنإ دسج لخاد ىلغاضف نئاك لثم أمامت .مجاهملا ةرفيش اذإ ،ىرخأ ةرم يعرشللا جمانربلا لمعي امدنع .ةلدألا مطعم يف تخت ،جمانربلا ليغشت يهتني امدنعو .نويلصلأل نويعرشللا نوجمرملا دصق امك أمامت لمعي هنإف ،ىرخأ ةرم ةرفيشلا مجاهملا لّدغُي مل ؟بئذتسملا وه ،ةلاحل هذه يف ،بسنألل هيبشتلا نوكي امبر

وأ فالسأي أو ،جمانربلا نأ نامضل ىلغاضف لمع ىلإ تاقيربطلتلا ءاضيبلا ةمئاقلا جاتحت ىلغاضف .اهليغشت ءانثأ ةنصارقلال اهلّدغُي نأ نود ةميسل ،بأ جمارب

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

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

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

ءاضيبلا ةمئاقلا يف جاردإلا ةشقانم دنع ،ءاضيبلا ةمئاقلا هب حمست ام دودح مهف ىلع صرحا .كيدل دروملا وأ ةينقتلا قيرف عم تاقيربطلتلا

1. تايكولسلال نراقو ،جمانربلا هب موقي نأ ضررتفُي ام عّبتتو ةردقلا هذه صحت له ؟ةطّحالّملا ةيلعلل تايكولسلالاب ةقوتملا
2. رارقلا داخا ةيلمع يف ءاضيبلا ةمئاقلا ةردق اهطقتلت تيلا ليصافتلا رادقم ام ؟لّصفم بلاط رورم حيرصت نم لقأ مأ رثكأ
3. ةيني أي نع اثحب اهصحتو فلسلاو بألا جماربلا ءاضيبلا ةمئاقلا ةردق عّبتت له (أدج عئاش رمأ - D حتفي ،C حتفي ،B حتفي A جمانربلا) ؟ةثب

4. هب ثبغئي مل ليغشتلا دي قجم انربلا نأ نم ااضيبللا ةمئاقلا ةردق ققحتت له .

????? ?????? ?? ??????? ???????
????????? ??????????? (NIST)

ةياغلل يفصو هنكل ،ةرباعلا ةءارقلل اصصخم سيل قوئوم روشنم

لك ةبك او مل يفكي امب رركتم لكشب ليصافتلل تئخت الو ،ويراني سلك يطغي ال هنأ مغر
فورظلا مظعم يف ةميق تاذ نوكتل يفكي امب ةيجيتارتسا فاصوالا نإف ،ويراني س

أقفو كلذل آتقو صصخي و ،NIST تاروشنم نم ةدمتسملا ىؤرلا أمئاد Cyber Crucible قيرف رّدئي
كلذل .

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf>

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

كولس دوجو مدع لاج يف قُلْغُتس تناك يتلا زازتبالا تاباجتسا ةفرعم ني مدختس ملل نكمي
بيوبتلا ةمالع نمض ةدوجوملا زازتبالا تاباجتسا ةحفص ىلإ الوأ لاقنتالاب كلذو، صصخم
بيبناجال طيرشلا يف تاي لمعلا

لماع ضرعيو، ال مأ اهداعبتسا مت دق زازتبالا ةباجتسا تناك اذا ام "دعبتسمل" دومع رهطي
ةتاماصل ريغو ةدعبتسمل ريغ تاباجتسال دومعلل يضارفتالا ةيفصتلا

ExcludedColumn.png

طقف "دعبتسم" ددحو "دعبتسمل" دومع ةيفصت لماع حتفا، ةدعبتسمل تاباجتسال ضرعل

ExcludedFilter.png

قُلْغُتس تناك يتلا ةدعبتسمل زازتبالا تاباجتسا لودجال ضرعيس، "قيبطت" ىلع رقنلا دعب
صصخمل كولسل دوجو الول

دوجوملا مهسل ىلإ الوأ رقنا، ةنيعم ةباجتسا ىلع هقيبطت مت يذلا صصخمل كولسل ةفرعمل
مهسل ىلإ رقنلا دعب رهطي يذلا يلدال لودجال يف. ددحمل فصلل "ثداوحلا ددع" دومع يف
ةباجتسال ىلع هقيبطت مت يذلا صصخمل كولسل مسا "ءافخإل ةدعاق" دومع ضرعيس

ExcludedResponses.png

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

- [صصخم ككولس ءاشن إةففيك](#)
- [ةتقؤملا ةصصخملا تايككولسل ليدعتو ءاشن إةففيك](#)
- [ةصصخملا تايككولسل فذح ةففيك](#)
- [ةفلتخم ةعومجم لىل ةصصخملا تايككولسل خسن ةففيك](#)
- [زازتبالل ةباجتسال ءحفص نم صصخم ككولس ءاشن إ](#)

طيرشلل ي ف تايلمعلل بيوبتلل ةمالع نمض ةصصخملا تايككولسل ءحفص لىل روثعلل نكمي "ةصصخملا تايككولسل ضرع" ةيحالص نومدختسملل كلتمى نأ بجى هنأ ةطحالل ىجُرى .يبناجل ءحفصلل هذه يف ةعومجملا كلتل ةصصخملا تايككولسل ةيؤر نم اونكمتيل ام ةعومجمل

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

ةدوجوملا ةيلمعلل داعبتسا ةنوقيأ لىل رقنا ،ةصصخملا تايككولسل ءحفص لىل لاقنتاللا دعب لودجلل اذه لىلأ .

صصخملا ككولسل ءاشن إة قثبنم ءذفان روهظ لىل ةنوقيألال هذه لىل رقنلل يدؤيس .

CreateTailoredBehaviorIcon.png
Create Exclusion.png

ءانثتساللا عم (parent program) يسىئر جم انرب ديدحت راىخ ني مدختسملل ىدل

94732291.png?width=504
اهق ببطت يف ببغرت يتلل ةففاضلال دويقلا لخدأ

CreateTailoredBehaviorAdditionalRestrictions.png
نوكتو ،ةدحمتافلم لوصو تازفحمب ءانثتساللا ديقت راىخ نألل ني مدختسملل ىدل حبصأ رادصللاب (agents) ءالكولل نأ ةطحالل ىجُرى .أىضارتفا ةنمضُم تافلملا لوصو تازفحم عيمج .هذه تافلملا لوصو زفحم ةردق نوكلتمى طقف قوف امو 4.4.6.2 .

يلاتل مسقلل يف ديزملا رطانا ،ةتقؤم تايككولس ءاشن إة لىل ةردقلا اضىأ نومدختسملل كلتمى

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

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

امك كولس ءاشنل ةي داي تالال ةي لمعلال عابتاب تقؤم صصخم كولس ءاشنل ني مدختسملل نكمي
نكمي. "أتقؤم صصخملا كولسلا اذه لعج" ليدبت حاتفم ليعفت م، هالعأ حضوم وه
يصقأ دحب) تقؤملا كولسلا ةي حالص ءاهتنا ىتح تاعاسلا ددع لاخدإ كلذ دعب ني مدختسملل
(دحاو عوبسأ).

Temporary Exclusion.png

لودجل ىلع ءاهتنا لالخيرات دومع يف كولسلا ةي حالص ءاهتنا لالخيرات ةيؤر نكمي.

مئاد كولس لعجل وأ، أمئاد تقؤم كولس لعجل وأ، ءاهتنا لالخيرات ديدمتل تقؤم كولس ليدعتل
ءاهتنا لالخيرات دومع يف بولطملا كولسلا ب ةصاخلا ليدعتل ةنوقيأ ىلع رقنا، أتقؤم

Edit Temp Behavior Icon.png

ليدعت اهللخ نم ني مدختسملل نكمي ةقثب نم ةذفان حتف ىلإ ةنوقيأ ال هذ ىلع رقنل ي دؤيس
ةبغرلل بسح كولسلا ةي حالص ءاهتنا لالخيرات

Edit behavior modal.pngScreenshot from 2024-09-09 15-21-58.png

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

ىلع اهفدح دارملا (تاي كولسلا) كولسلا ألوأ ددح، دحاو نآ يف تاي كولس ةدع وأ، دحاو كولس فذحل
لودجل ىلعأ تالمهمل ةلس ةنوقيأ ىلع رقناو لودجل.

فذل رز ىلع رقناو "delete" بتكا، آيئاث.

RemoveTailoredBehaviorIcon.pngRemoveTailoredBehaviorModal.png

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

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

دارملا (تاي كولسلا) كولسلا ددح، ىرخأ ةعومجم ىلإ (دحاو نآ يف تاي كولس ةدع وأ) دحاو كولس خسنل
لودجل ىلعأ خسنل ةنوقيأ ىلع رقناو لودجل ىلع اهخسن.

يتل ةعومجملا ديدحت اهللخ نم كنكمي ةقثب نم ةذفان روهظ ىلإ ةنوقيأ ال هذ ىلع رقنل ي دؤيس
اهلإ (تاي كولسلا) كولسلا خسن بجي.

عومجمل اي لاج ةدوجومل تايكولسل فذل راخي يلع اُضي ةقثبنملا ةذفانلا هذه يوتحت طقف ةخوسنملا تايكولسل ابءافتكال او ،(ايقائل ةأشنُملا تايكولسل اءاثساب) ةدحمل بلطل لاسرا دعب ةدحمل ةعومجمل اي

CopyTailoredBehaviorIcon.pngCopyTailoredBehaviorModal.png
ةدحمل ةعومجمل نآل ةخوسنملا تايكولسل رهظتس ،بلطل لاسرا دعب

ResultGrid.png
????? ???? ???? ?? ????
???????????? ???? ?????

زازتبال تاباجتسا ةحفص نم ةصصخم تايكولسل ءاشنإ يلع ةردقل نيمدختسملا ىدل لودجل راهظإل ثداوحلا ددع دومع نمض ةبولطملا زازتبالا ةباجتسا فص يف مهسللا يلع رقنا ،آلأا يلخادل روهظ ىلإ يدؤيس امم ،ةباجتساللا مسا دومع يف ةباجتساللا داعبتسا ةنوقي ىلعل رقنا ،ايناث صصخملا كولسل ءاشنإل ةقثبنملا ةذفان

ExcludeResponseIcon.png
ةيذيفنتلا تافللملا تاراسم مادختساب تايكولسل ءاشنإ كنكمي ،ةقثبنملا ةذفانلا هذه يف ةحرتقملا تاراسملا نمض هجاتحت ام دجت مل اذا ةعجارملا ةباجتساللا لاسرا وأ ةحرتقملا

Exclude Modal.png
كلويحتب موقيس يذلاو ،"ةصصخملا تايكولسل ةحفص ىلإ يذخ" رز ىلعل رقنلا اُضي كنكمي سفنب كولسل ءاشنإل ةقثبنملا ةذفانلا ايقائل ألميو ةصصخملا تايكولسل ةحفص ىلإ ةباجتساللا نم جامنربلا طئاسو وراسملاو ةعومجمل

AutofilledModal.png
آلطمع نوكي "يسئرلا جامنربلا + جامنربلاب ءاثتساللا ديقت" دادعإ نأ ةطحالم ىجرُي ايقائل زازتبالا ةباجتسا نم هطئاسوو يسئرلا جامنربلا راسم ءلم اُضي متيس .ايسارتفا دادعإلا اذه ليعفتب تمق اذا

PrefilledArgs.png
ءاثتساللا ديقت" دادعإ ليعفت عم ءاشنإ ىلعل رقنلا دعب صصخملا كولسل ءاثتسا "يسئرلا جامنربلا + جامنربلاب

ExlusionResult.png

يُف. اتافلم لصحف نمّ الدب (kernel) ةاونللا يوتسم يلعل ةنللاو كولسل Cyber Crucible بقارت
مأ فلم ةباتك تمت ءاوس، ةيناث يللم 200 نم لقأ يف اهفاقيإ متي راض لكشب فرصتت ةيلمع
ال.

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

تمت أو يعان طصاا اءا ذلا و ةيج مرربا صوصنلا ماذخسا يا ةنصرقلا ةتمأ : **ةزوم ةباج** !
أ تمؤم موجهل نكمي . ةلآا ةعرسب موجهل لءارم نم ةلءرم لك ذيفننل ةيتوبورلا تايللمعلا
عرسا — ناوئ نوضغ يف ةركاذلا يف ةدوجوملا ءاودأ فذحيو ، تانايبلا قرسيو ، آزاهج قرتخي
هل ةباجتسالا يرشب للحم يأل نكمي امم ريئكب

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

- **ةطيرخ مسرو ةفيعضلا ةمظنألا** نع آئحب تنرتنإلا ءسمب تاودألا موقت : **ءالطتسالا**
عساو قاطن ىلع ةعنقم يلايئا ءيصت لئاسر ديلوتو ءناوئ نوضغ يف فءهلا ةكبشل
- **لالغتسالا** رشنب ةيج مرربا رطألا موقت ، فعض ةطقن فاشتكا ءرجمب : **لالغتسالا**
طءالي نأ لب ق ءزهجال نييالا م ربع (zero-day) رفصللا موي ةرغئ ماذخسا نكمي ذا — آروف
هيبنتلا ناسنإ
- **مبيقتب ةئيءل ءايبءل** تايج مرربا موقت ال : **"ءيرسالا ءاليئسالا و فاطئءالا"**
ام عرسأب ، هيلإ لوصولا هانكمي ام لك بيريست وأ ريفشئتب موقت لب . ةمّيقلا تافلما
هيلإ لوصولا هانكمي

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

يري يكل مزاللا تقولا . ةيرشبالا ةعيبطالا يف لب . نيفظوملا ءءع وأ قيرفلا ءءوج يف سيل ءءلا
هءمأئل موجهلا ءقرغتسي يءلا تقولا نم لوطأ ، هيلعءأنا بفرصتيو ، هءلاءيو ، هيبنتلا صءشللا
قوف ريءأئلا نم آءيزم فيضي اهءءاعإ مئ ليلءلل يباءس مءا ءلا ءبئتلا تانايب هءءوتو
كلذ

ءازء نوضغ يف ، ةياهنلا ةطقن ىلع ، لقتسم لكشب فرصتيو ررقي عافء وه ءيءولا يلمعلا لءلا
(ةيئاثل يلم) .

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

ةيلآل مهتايچمرب بتكُت اذل ،ةدحمل كئئيب نع آئيش نومجاهملا فرعي ال :نجوم ةباح!
تاكرحم فرحأو ،نيمدختسملا فيرعت تافلم تادلجم — زاهج لك يف آي لمع ةدوجوم عقاوم فادهتسال
ني عفادملل نكمي فعض ةطقن وبنتلل ةيلبالا اذه .تاقيبطتلا تانايب لئالدو ،صارقألا
اهلالغتسا.

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

- طفتحي Windows، ماظن يف :بتكملا حطسو نيمدختسملا فيرعت تافلم
ربع يصنللا جمانربلا رمي .ةمّيق تانايبب قوئوم لكشب `C:\Users\[Username]` راسملا
ماظنلا مهف ىلإ ةجالحا نود مدختسم ليلد لك
- ىلع روئعلل اهدعب امو `D:\` و `C:\` دادعتب ةيلآلا تاودألا موقت :صارقألا تاكرحم فرحأ
اهري فشتل ةلمخُمل ماسقألاو ،ةيجراخلا صارقألاو ،ةيكبشلا تاكراشملا
- تافلمو دامتعالا تانايبب ليغشت ماظن لك طفتحي :تاقيبطتلا تانايب تادلجم
تانايب ةقرسل ةيسيئر فادهأ هو — ةفورعم تاراسم يف تادادعإلاو طابتزالا فيرعت
دامتعالا.

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

Cyber Crucible بقارت .آديج ةفورعمل عقاوملل طاف حسم وه لب ؛أسوردم سيل موجهلا طمن
لوصولا لواحي جمانرب ي أعضي .تانايبلاو ةيوهلا ةقرسل كلت ةفورعمل لوخدلا طاقن ديدحتلاب
هب ةطبترملا ةيعرفلاو ةيلصألا تايلمعلا بناج ىلإ — عقاوملا كلت يف تانايبلا ىلإ
كلت تناك اذإ هضارتعا متي و ،ةيناثلا نم عزج يف هتي مييقتل — اهب ةطبترملا تابتكملاو
ةثببخة نللا.

?? ?? ????????? ???????
????????????? (infostealer)?
???????? ?????? ?????? ??? ???????
(session token) ????? ????????

ءاليتسالى ةممصم ةثي ب خ ةيجمرب وه (infostealer) تامولعملل قراسل سوريفال :ءجوم ةباج!
ءجمرب تاهج اوحي تافمو ،(session tokens) ةسلجل زومرو ،رورملا تاملك — ةيمقرلا ةيوهلا داوم ىلع
اهب ىرسو — (VPN) ةصاخلا ةيضارتفالا ةكبشل دامتعانا ابو ،(API keys) تاقىب طتلا
ةددعتم ةقداصملاو رورملا تاملك زواجتي ام ابلاغ هنأل اري طخ قورسمل ةسلجل زمر دغىو .ةعرسب
يعرش مدختسمك لوخدلا ليجست مجاهملل حي تي امم ،لماكلاب لم اوعل

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

يف ءاقبل اف .ةليوط تارتفل ةكبشل ل خاد ءاقبل ديازتم لكشب نورصاعملا نومجاهملا بئجتي
امم ،نورداغيو ةيوهلا داوم ىلع نولوتسي ،كلذ نم الدبو .فاشكالا ةيلامتحا نم عفرى ةئيبلا
ئيتزي م مهنمى :

1. مهبسانى يذلا تقولا يف ةنمآ ةئيب نم هوقرس ام ليلىحتب نوموقي ذإ — **لقأ ةرطاخم**
2. ةيضارتفا ةكبشحاتفم وأ ،رورم ةملك وأ ،حلاص ةسلج زمر دوجوبف — **ةدوعلا ةلوهس**
ةقداصملا ماظنل امامت نىي عرش نودبىو ،اوعاش ىتم ةدوعلا مهنكمى ،(VPN) ةصاخ

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

يباحس هيبنت رداغى نأ نم عرسأ — نئاوٲ يف ي تاذاذل فزحل ىلى لىلستلا نم تاودألا هذو لقتنت
نم لقأ يف ةيلمعل قلعنو ةيوهلا تانايب ىلى لوصولو ةطحل ةئىلا Cyber Crucible أرقو .ناكمل
ب.بىرستلا أدبى نأ لبق ،ةئىناٲ ىلىم 200

[illegible]

?? ?? System32 DLL ??

????????

اهليغشت ءانثأ (System32 DLLs) ةيساسأل Windows دو ك تابت كم بيصي موجه ه نإ : **ةنجوم ةباح** !
نإف ، لمعتل تابت كم ال كلت ىل ع دمتعت ةينمأ ةادأ لك و أبيرقت قي بطت لك نأل و . ةركاذل ا يف
أ دج ليئض رثأ عم ةياهنل ةطقن ىل ع ةلماك ه بش ةرطيس مجاهم لحنمي اهقارتخا

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

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

— هتاقى بطت و Windows اهلي ع دمتعي يتل ةيساسأل تاي لمعل DLL System32 تابت كم رفوت
متيل سيل و ، ةيقو وثومل او ةعرسل ل جأ ن م تمم ص دق و . تاك بشل او ، ريفش ل او ، ةركاذل ا صيصخت
جاتنإل ةئي ب يف لمعل ءانثأ اهضارتعا و اهحيصت

ريمدت و أرييغت و ءاشنإ و أ صحف ىل ع ةردقل بستكي ةركاذل ا يف اهلي دعت ىل ع رداقل مجاهم ل
عبتتل لحي تسم نو كي داكي فختب ، ماطنل ىل ع جمارب ل او تانايب ل

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

مكحب ، دمتعت Microsoft ن م ةدوزمل تارعش تسم ل تانايب ىل ع دمتعت يتل ةينمأل تاجت نمل
اذه فاشتكال ةمزالل تارعش تسم ل اف . موجهل لضرعت يتل اهتاذ تابت كم ال ىل ع ، فيرعتل
امنيب ةادأل تمصت اذل — ةيسايق ل تاودأل تاعومجم يف ةدوجوم ريغ ةطاسبب تامجهل ن م عونل
ماري ام ىل ع ءيش لك نأ ب غلبت

ليغش ل ماطن ن كم تي ال تح Windows تابت كم ن ع آلقتسم نو كي ل آدمع Cyber Crucible م م ص
اهلي طعت و ةادأل ءامع ن م قرتخم ل

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

نم ققحت ةراشإ قللت مل ام ةلماخ ىقبتل ةثيبلخال تايجمربلال نومجاهملا ممصري :ةزجوم ةباح!
ةدعاق ىلإ ةنيعلال هيف لصت يذلا تقولا لولحبو .هليل نورطيسي ي ح (C2) مكحتو ةدايق مداخ
اذل — رخآ ناكم ىلإ ةداع تلقتنا دق ةيتحتال C2- ال ةينب نوكت ،ةثيبلخال تايجمربلال تانايب
ءيش أب موقت ال ةميتي ةنيع نوئحابال ربتخي ام أبلاغ

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

- ي أب ةلماخال ةثيبلخال تايجمربلال موقت ال :ةيتارابختسالال تامولعملال ليلقت
أردق نيئئابلللو هقيثوتل لقأ أردق نيلللحملل كرتي امم ،اهتطحالم نكمي ةراض تاءارجإ
هليلعأ ءانب تاعيقوتال ءانبل لقأ
- ي لوتسي ثحاب وأ سفانم ي أن "ةيرسلال ءحفاصلال" طارتشا نمضي :فاطتخالال عنام
تانايبال عمجو ةثيبلخال ةيجمربلال ليغشت ةطاسبب عيطتسي ال C2- ال مداخ ىلع
ةقورسمل

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

ام سيل مهملا لاؤسلاف .أدج ليلقلا الإ لاصلتالال ةعوطقم ةنيع لباقم ربتخملال رابتخا سريقي ال
ةيحل تامجهل فقوت تناك اذا ام لب ،ةدكار ةلماخ ةثيبلخال ةيجمربلال عم لعافتت ةأالال تناك اذا
طاقن بقاري وهف :ريخأال ضرغل اذل Cyber Crucible مُمص .أليلعاف اهعوقو ءانثأ ءكرحال ءعيرس
يف ةينلل مّقيو ،ةيقيقحل تامجهل اهفدهتست يتل تانايبال او ءوهل ءقرسب ءصاخال لوخذل
حجنت نأ لبقة قرسلال فقويو ،ةيناث يلللم 200 نم لقأ