

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

- [CRL/OCSP تاداهشل رادصلإ هج لوصو رطحت ةيامحل اناردج \(DMZ عضو\)](#)
- [Cyber Crucible تيبتت ةيفيك](#)
- [تيبتتال تالاجس عقوم ديدحت يننكمي فيك](#)
- [AD قاطن لىلإ تبتتل لىرسقلا عفدلا](#)
- [تيبتتال تبتريكس لىل عماع ةرطن](#)
- [SCCM مادختساب تيبتتال](#)

????? ????????? ???? ???? ???
????? ?????????? CRL/OCSP (
??? DMZ)

يُمكنكم الوصول إلى لوحة التحكم من خلال الرابط التالي: <https://dashboard.cybercrucible.com>

85131265.png?width=680

85229569.png?width=340

لوؤسم نم بلطت نأ وأ ،ةومجمل ءاشنإ إلی اجاتحت نأ ام إف ،ةمئاقلا یف ةومجمل رهظت مل اذإ .ةدوجومل ةومجمل إلی إکتفاضإ ةومجمل

?????? ?????

Cyber Crucible كرمو مة مدخ لى محتوتو تي بثل زاهجلا لى لع ةيراد ا تاي حالص لى لع لو صحلل مزلي

عقووم اللى هنى وكوتو تيبت التاجمان رب ليزنتب اديحت (Script) جمرربل صلل تيبت موقى
عقووم اللى لوصولا عى حالص كللمى رود وأمدختسمك جمرربل صلل ذىفنت بجى. C:\ يضرارفال
الذىفنتالاولىزنتال.

صنن الل ليدعت وأ، تيبتتالءا ثأ C:\مادختسا ةيحالص هيدل مدختسم امإ مزلي، يلاتلابو
فلتخم عقوم ي هذيفنتو تيبتتال ليزنتل (هاندا حوضوملا) يجرمربلا.

??????? ???? ???? ????
 ???????? (GUI)

١٩. اى ودى تىبثتاللا ةىلمعم تىبثتو نىوكت مدختسم لل هذه تىبثتاللا ةقيرط حىت

،ةددملا ةعومجملا يف تيبتثتلا تايحالص كللم ي أم دختسم هذه تيبتثتلا ةقيرط بلطتت
ل.ل و دلا ليحست نم نكم تي

،دحاو مدختسم ةطساوب ،نيزاهج وأ دحاو زاهج تيبتثتلا اهمادختسا لّضفُي

??????? ???? ???? ??????? (Script)

عزانم الب أعويش رثكأل تيبتثتلا ةقيرط يه هذه

،تيبتثتلا ةيلمع نيوكتب أيئاقلت Cyber Crucible بيو قيبتطت موقي ،ةقيرطلا هذه مادختساب
ب.يولا قيبتطت نمأل ليمعلا لاصتا ديمتو

هذه نأ إا ،أديقت رثكأ ىرخأ تيبتثت قرط دوجو مغرو .(Batch File) يعفد Windows فلم مدختسُي
دغُب نع ةرادإلا تاودأ عم قفاوت عسوأب عتمتت ةقيرطلا

هخسن وأ ،(لوؤسملا ةداع) ةبسانملا تايحالصلا كللم ي مدختسمك يعفدلا فلملا ليغشت نكمي
كيذل ةلضفملا يئاقلتلا رشنلا ةادأ يف هقصلو

ك.تاجايتحال أقفو هنيوكت نكمي يذلاو ،يعفدلا فلملا تايوتحمل ينقت صحف يلي امي

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

oauth زمر كلذك و ،يجمرربلا صنلا يف يجمرربلا صنلا ءاشنإ ءانثأ ددملا ةعومجملا فّرعم لاخدا متي
ةددملا ةعومجملا ىلإ ءالمعلا مامضنالا بولطملا

47480849.png?width=680

نكمي الو .مدختسم ي أب الو ،بيولا قيبتطت طبترم ريغ اذه OAuth ةقداصملا زمر نأ ةطحال ميجري
ب.يولا قيبتطت (API) تاقيبطت ةجررب ةهجاو ىلإ REST تاءاعدتسا ءارجإل همادختسا

يتلا تالاحلا يف ةداع اذه ثدحي .أيئاقلت تايحالصلا ىلع لوصحلا متي دق ،تائيبلل ضعب يف
لوصولاب ةنراقم ،هيلي رقننلاب يجمرربلا تيبتثتلا صن ليغشتب مدختسملا اهيف موقي
هذيفنت متي أل لم تحملا نمف ،يلاأل رشنلا تاودأ وأ تاسسؤملا تائيبي يف امأ .يجمرربلا

47480857.png?width=680

جامارب ليزنت نكمي يذلا فلملا عقوم صيصخت نكمي ،يجمرربلا صنلا نم يلاتا عقوملا اذه يف
هنم هذيفنتو تيبتثتلا

ةزهجأ ةدع مايقف .هيلي ةادأل تيبتثت متي يذلا زاهجلا ىلع أيلحم عقوملا اذه لعجب ةدشب حصنُي
تافلملا قوف ةباتكو لاطعأ ثودح ىلإ يدؤيس عقوملا سفن ىلإ تيبتثتلا جامارب ليزنتب

أيضا ارتفا مدخستُت ال جي مبربل تي بثتال صن ربع عيئاقللتال ليغشتال اداعإ نأ عطحالم يجرى
تاي لمع ةلودج ةرادإ إلى رقتفت جي مبربل صنل اذه يف ةي لآال ليغشتال اداعإ نأ ك ل ذ يف ببسلالو
لّجسم مدخستسمال ناك اذإ امم ققحتت يتال فيظنل القالغإل بيلاسأو، ددحم تقو يف تي بثتال
ةكيشو ليغشت اداعإ نم مدخستسمال ريذحت وأ، تاقيبطت لّغشي وأ أيلا ل وخذل.

47513621.png?width=680

ي جري. زاهجال إلى ص صخم لكشب هتيمستو تي بثتال جمانرب ليزنن تب يلاتل مسقلا اذه موقى
هليزنن لاج يف، تي بثتال فلم إلى ع ديرف عباط ءافضإل نامدختسُي تقولوا خيراتال نأ عطحالم
ة. فلل تخم تارادصإ وأ تادادعإب تارم دة.

اذا زاهجال إلى ع أبلس ريثألتال نود تافللمال ليزنن لواحت Windows يف دةعاسم ةادأ يه Bitsadmin
أيلا ل ي قث ل م ح تحت ليغشتال ماطن ناك.

47448109.png?width=680

ريغ ةلاح يف Bits نو كى دق، ك ل ذ إلى ةفاضإلاب.ّالطعم Bits لوكوتورب نو كى تائي ببالضعب يف
يلاتل مسقلا مدختسي، Bits ربع ليزننل لشف لاج يف Windows. يف أطخ ببسب ةي ليغشت
ليزنن لشف اذإ إلى زمرل اذه دُف نُي ال. تي بثتال جمانرب فلم ليزننل (.net JSC) ةليدب ةقيرط
قباسل Bits.

47415316.png?width=680

جمانرب ليغشتب جي مبربل صنل نم ريخأل مسقلا اذه موقى، تي بثتال جمانرب ليزنن دعب
تادادعإ نأ نم دكأتلل، رمأوال رطس تاطيسو صيصخت رابتخا بجي هنأ عطحالم يجرى. تي بثتال
انه ةمدقمال رمأوال رطس تاطيسو عم قفاوتت installer.exe تايامحو.

تادادعإ لثم ةمدقتمال تائي بلل وأ، ةيفاضإ تادادعإ إلى عاح كانه تناك اذإ معد ةركذت تحت يجرى
SSL (SSL man in the middle) ربع طيسولال موجه.

47480877.png?width=680

اهعضوب) ذيفننل نم اهل يعفت ءاغلإ مت دقو، ةبولطم تسيل ليغشتال اداعإ نأ عطحالم يجرى
لّجست ال Windows، نم مدقأل تارادصإل يف أعويش رثكأ لكشبو، ةردان تالاج يف. (قيلعتك
ك ل ذب اهل تي بثتال جمانرب هيجوت مغر ليغشتال ماطن يف لّمُحتو (Drivers) ليغشتال جمارب
إلى ءالمعل ريذست يه ليغشتال جمانرب لي محت نم دكأتلل ةقيرط لهسأ، تالاحل ك ل ت يف
تاي لمع عي مج تناك اذإ. ك لوصأ ةمئاق نم ةدوقفمال ةزهجأل ءامسأ نع ثحبلاو، Excel دننسم
ءالمعل ددع مادختسا أضيأ نكمي، ةديدج ةعومجم يف تي بثتال.

47480889.png?width=680

جمانرب ليزننل ةمدختسمال (Function) ةلادل وه جي مبربل تي بثتال صن ةيانه يف مسقلا اذه
ليزننل .net JSC. لب ةناعستالال مت اذإ إلى هذيفننل متي ال. رمأال مزل اذإ JSC مادختساب تي بثتال
Bits. لشف لاج يف امك، تي بثتال جمانرب.

47480895.png?width=680

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

ىلإ اهتالاجسو اهتلاح (Headless) ةيموسرر ةهجاو نودب (CLI) رماوأل رطس نم تيبتتال تاودأ جرخت لكشب. تبثملاب صاخال exe فلمل ليلدلل ي ف دوجوم، لاجس فلم ىلإو `stdout` نم لك نم اهليزنت متي يتال bat و ps1 صوصن لثم، أقبسّم أبغّم يجمرّب صن مادختسا دنع، يضارتفا C: صارقأل كرحم رذج ي ف أدوجوم لاجسلا فلم نوكتيس، <https://dashboard.cybercrucible.com>.

تيبتتال لاجس تافلم ىمسّت `cc_installer.log`

نودب تسيل اهنإ ثيح، لاجسلا تافلم سفن (GUI) ةيموسررل ةهجاوالتا تبثملال جتنتال ةهجاوالتا ف ريرمتلل لباقلا لىصنلا مسقلا ي ف تالاجسلا عيج ضرغتو، (Headless) ةهجاو ةيموسررل.

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

????? AD

رشنل نوکي ال دق ،ثيدح عاطقنا وأ موجه نم يفاعتلا دنع اميس ال ،ةشهلا تائيبل وضعب ي ف ج دومن ةبائتم نوکي نأ نكمي ايجمر ب ا صن انه دجتس .احاتم ارايخ SCCM وأ/و RMM ربع يداعلا active directory ةئي ب ربع ايرسق CC تيبثت عفد ةيفيكل

بلطتيو ،كمادختسا ةلاحل اقفو صيصخت ىل ايجمر ب ل ص نلا اذه جاتحي نأ حجرمل نم :**ةطحال م** ص نلا اذه ليغشت متي نأ عقوتمل نم .ليغشتلل (domain credentials) قاطنلا دامتعا تانايب (ةيساسال) قاطنلا مكحت ةدحو ىلع ةرشابم ايجمر ب ل

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

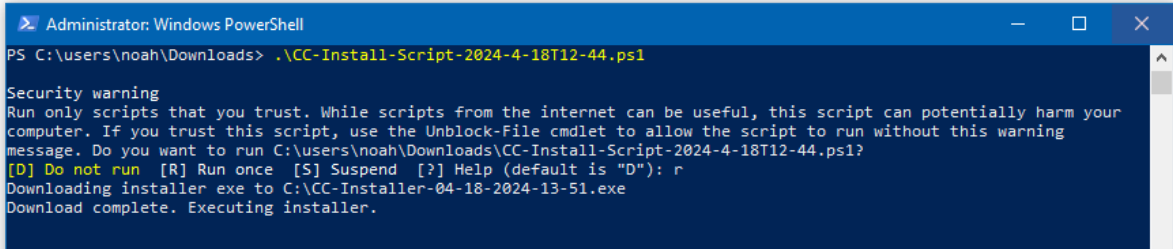
1. فيضم عامسأ وأ (NETBIOS) ةزهجال عامسأ ةمئاقب `$install_targets` ريغتمل ثيدحتب مق (ةهباشم)
2. [Cyber Crucible](#) مكحت ةحول نم `ps1` ةغيصب تبثملل يداع ايجمر ب ص ن لي زنتب مق
3. ةقباطم نوكتل `push_installer_ad.ps1` ايجمر ب ل ص نلا ي ف تاريغتمل ثيدحتب مق مكحتل ةحول ص ن نم ةصاخلا كتعومجم تاريغتمل
 1. `${GroupId}`
 2. `${ClientAuth}`
 3. تاريغتم ي أ `--rest-pub-key`
4. [Cyber Crucible](#) مكحت ةحول نم (CLI) رماوال رطس ةهجاو ليصلأ يذيفنت فلم لي زنتب مق
 1. ةزهجال ايجم نم هي ل لوصولو نكمي ناكم ي ف وأ ،ةكبش ةكراشم ىلع CLI فلم عض اهي ل اهتيتبثت دارملا
 1. س فن لي زنت ةداعل ايدررتل قاطنلا ضرعو تقولا رادهل نم زاهج لك اذه عنمي فلمل يذيفنتل فلمل
 2. ثيح ،ةفلتخم ليغشت ةمظنأل يذيفنتل فلمل س فن يذيفنت نكمي ةلصلل اذ تيبثتال/فيرعتال/ةمدخلل تافل م بحسب تبثمل موقيس زاهجلل نيفشتكمال رودل او ليغشتل ماطن ب
 2. ةكبشلا ةكراشمال ىلع CLI فلم راسم ىل `${OutputFilePath}` نييعتب مق
5. (كتئي بل حل اص ريغ / ايرورص نكي مل اذل) ICMP ربع لاصلتال نم ققحتل ةلازا نكمي
6. مادختساب ايجمر ب ل ص نلا ليغشتب مق `-credential`
 1. لاثمل ليبس ىلع: `./push_installer_ad.ps1 -credential ad1\kyle`

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

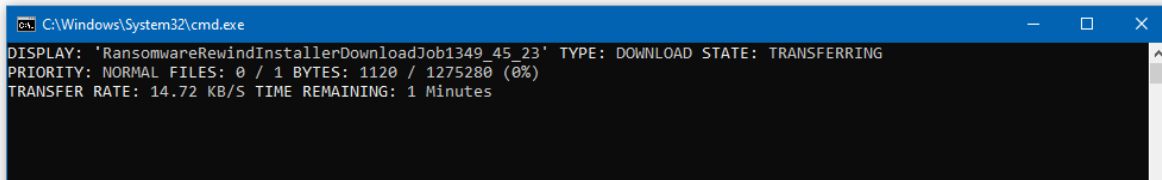
1. نم تي بـثـتـ جـمـانـرـبـ ثـدـحـاً لـيـزـنـتـ مـتـي

<https://installerfiles.rpp.cybercrucible.com/installers/64/installer-cli.exe>

1. WebClient ةـخـسـن PowerShell (PS1) عـون نم تي بـثـتـ الـتـاـتـبـيـرـكـس مـدـخـتـسـتـس



2. اذـا JScript وـا BitsAdmin، ةـاـدـا Batch (BAT) عـون نم تي بـثـتـ الـتـاـتـبـيـرـكـس مـدـخـتـسـتـس
تـلـشـف BitsAdmin.



2. ةـقـدـاصـم تـاـنـاـيـبـو (group ID) ةـومـجـمـال فـرـعـم رـيـرمـتـو تي بـثـتـ الـتـاـتـبـيـرـبـ ذـيـفـنـتـ مـتـي
هـيـلـل كـب صـاـخـال تـبـيـرـكـسـال يـف ةـرفـوتـمـال لـيـمـعـال
 1. exe، فـلـم ذـيـفـنـتـ ةـيـلـمـعـى لـل --reuse-agent-by-machine-name ةـاـضـا اـيـرـاـيـتـخـا نـكـمـي،
صـيـخـرتـالـاو (agent) لـيـكـولـنـئـاك مـاـدـخـتـسـا دـيـعـي تي بـثـتـ الـتـاـتـبـيـرـب لـعـجـل كـلـذو
NetBIOS مـسـا سـفـن لـمـحـي اـقـبـسـم هـتـي بـثـت مـت لـيـكـوب صـاـخـال
3. ةـبـولـطـمـال تي بـثـتـ الـتـاـتـبـيـرـب فـوتـن نم تي بـثـتـ الـتـاـتـبـيـرـب قـقـحـتـي
 1. (Administrator) لوؤسـمـال تـاـيـحـالـصـب لـيـغـشـتـال.
 2. Windows نم مـوـعـدم رـاـدـصـا بـ زـاـهـجـال لـمـعـي نـا.
 3. لـعـفـالـاب لـيـغـشـتـال دـيـق رـخ آ تي بـثـت جـمـانـرـب دـوـجـو مـدـع.
 4. اـقـبـسـم لـيـكـول تي بـثـت مـدـع.
4. ةـبـولـطـمـال مـداـوـخـلـلـب لـاصـتـالـا لـعـ زـاـهـجـال ةـردـق نم تي بـثـتـ الـتـاـتـبـيـرـب قـقـحـتـي
 1. Amazon OAuth 2.0 نـاـوـنـعـالـا لـيـل ransomwarerewind-agents.auth.us-west-2.amazoncognito.com
 2. نـاـوـنـعـالـا لـيـل Cyber Crucible صـاـخـال الـ (backend) ةـيـفـلـخـال agent.tasking.rpp.cybercrucible.com
5. HTTPS رـبـع installerfiles.rpp.cybercrucible.com نم لـيـكـول تـاـفـلـم لـيـزـنـت مـتـي
6. هـلـيـغـشـتـو لـيـكـول تي بـثـت مـتـي.

???????? ?????????? SCCM

طاقننلا ىرخأ ةيجمرب ةمزح يأ تيبتت نع SCCM مادختساب Cyber Crucible تيبتت فلتخي ال
يه SCCM ربع رشنلل ةيساسأل

1. نم هليزنت متي يذلا ،زهاج ال PS1 تبركس مادختساب رشنا
<https://dashboard.cybercrucible.com>
2. قيرطك ،صرقلال ىلع ةدوجوم وأ ،ليغشتلا ديقي **Cyber Crucible Agent** ةمدخ نع ثحبا
C:\Program Files\CyberCrucible\service.exe وه ليغملا ةمدخل يضارثفالا عقوملا .فشكلل
ليجستلا حاتفم دوجو نم ققحتلا اضيأ كنكمي ،أيرايتخا
1. دق ،تيبتتلا اغلل دعب هنأ ةطحالم عم ،**HKLM\Software\CyberCrucibleAgent** ،
أدوجوم حاتفملا اذه لظي

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

1. ةمزح **سيو** (package) ،أقبيطت ئشنأ
2. أيودي ةئيهتلا دح

image-20250807-175116.png

3. كلذلى إامو ،فصولاو ،درومل مساو ،قبيطتلا مسا ةئيهت مق
4. **Script Installer** ددحو ،(Deployment Type) رشنلا عون ةئيهت مق

image-20250807-175303.pngimage-20250807-175332.png

5. لثم ةيكبش ةكراشم حجرألال ىلع ،تبركسلا عقوم دح **\\cc-dc01\share**
6. لاثم ،قفرم ال ps1 فلم ذيفنتل تيبتتلا جمانرب دح : Powershell.exe -file "CC-Install-Script-2025-8-7T13-55.ps1"
1. خيراتلا ىلىل هرييغت مقو ،تبركسلا مسا يفيراتلل ينمزللا عباطلا طحال
كب صاخلا
2. ىلىل جاتحت دق ،كتئيهت ىلع ادامتعا نكلو ،PowerShell تاسايس زواجتت حصني ال
هباش ام وأ **-executionpolicy Bypass** ديدحت
7. "Add Clause" ىلىل رقنلاب فشك ةقيرط فضا
1. ةحفصلا هذه ىلعأ يفيراب ىصوصملا فشكلا قرط عجار
8. (UX) مدختسملا ةبرجت رشن تادادع دح
1. تيبتتلا تابلطتم إف ،ليغشت ةداعإ بلطتي ال Cyber Crucible رشن نأل ارظن
كتسسؤم ريديقتل عوضخت لوخدلا ليجستو

image-20250807-175906.png

9. جلاعالم قالغإ نم نكمتت ىتح ءاهنإ / ىلاتلا رتخا