

مادختساب لوخدلا ليجست شادحاً نع ثحبلا LogSearch.ps1

تايوتحملا

[ةمدقملا](#)

[ةيساسأ تامولعم](#)

[يصننلا جمانربلا ليغشت](#)

ةمدقملا

جمانرب مادختساب لوخدلا ليجست شادحاً نع ثحبلا ةيفيك دنتسملا اذه حضوي PowerShell ل يصن جمانرب وهو، LogSearch.ps1.

ةيساسأ تامولعم

Umbrella معدلة ةديفم تامولعم عمجي PowerShell نم ريغص يصن جمانرب وه LoginSearch.ps1 ال اذامل احوال صا واطخال فاشكتسا دنع ديفملا نم. احوال صا واطخال فاشكتسا ضارغأل هيف ثحبلا متي يذل طاشنلا وأ ريراقتلا يف حيحصل طاشنلا ني مدختسملا ضع رهطي ااطخال فاشكتسال همدختسا اضيأ نكمي كلذ عمو، OpenDNS Umbrella تامولعم ةحول ىلع احوال صا واطخال نم ىرخال عاونال.

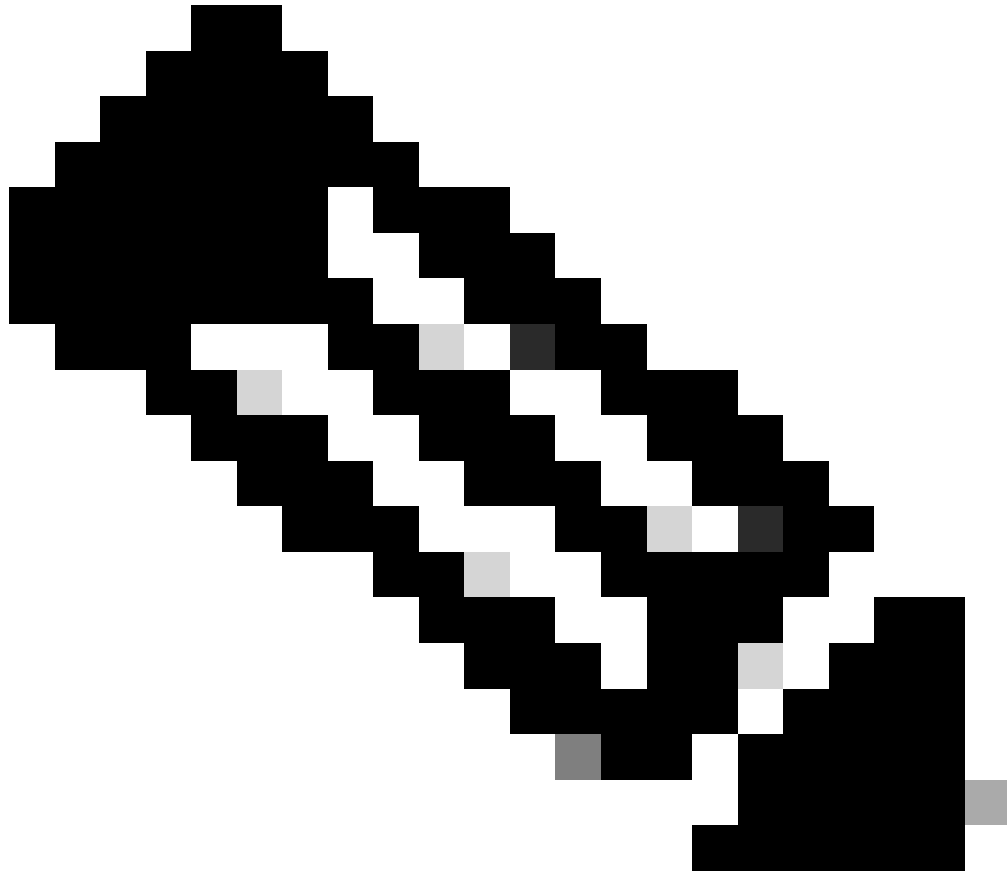
لوخدلا ليجست شادحاً خسن متي شيح ةيسايق لاجملاب مكحت ةدحو ي ىلع اذه ليغشتب مق اهتدهاشم عقوتتو ثحبلا اناثأ شادحاً ةيأ دهاشت مل اذا، كلذ عمو. لاجملاب مكحتلا تادحو نيب اذه يف. مداوخل نيب شادحال تالجس خسن يف ةلكشم كانه نوكت دق، نيعم فيضم نم ليغشتب مق مث، فيضملا اذه لبق نم مدختسملا %LOGONSERVER% فشكتسا ليثمل ةيأ روهظ مدع ةلاح يف. ددحم لكشب اهيلي راشملا لاجملاب مكحتلا ةدحو ىلع يصننلا جمانربلا. لوخدلا ليجست شادحاً قيقدت نم دكأت، نال ىتح شادحاً.

اهعيمجت متي تال تامولعمل مادختسا نكمي. ةلاقملا هذه لفسا ىل صننلا قافرا مت OpenDNS معد ةطساوب وأ كسفنب اما احوال صا واطخال فاشكتسال.

يصننلا جمانربلا ليغشت

ةيلاتلا تاوطخل لمكأ:

1. 'ps1' ىل 'txt' نم قحلملا ةيمست ةداعا و قفرملا يصننلا فلملا ليزننن مق.



"txt.ps1". دصق نودب اهيمست الو ةجودزمل تادادتمال نم رذخا :ةطحال م

2. 'Right-Click' ةطساوب اهلي غشت ءدب مت ةديج PowerShell ةذفان حتفا، Windows مداخل نم م ث
-->Run as Administrator'. هيل يذيفنتل صننلا ظفحب تمق يذلا ناكملا ىل لقتنا (eg: 'cd
C:\Users\admin\Downloads'. ةباتك لال يذيفنتل صننلا ذيفنتب مقو (C:\Users\admin\Downloads\loginsearch.ps1).
3. ثادحأ تالجس ي ف هنع ثحبلا ديرت يذلا مدختسملا مسا الوأ ي صننلا جامانربلا بلطي
تابل اطملا مدختسأ IP. ةطساوب ثحبلا لصفنت تنك اذا ددحم IP ناو نع م ث Windows نامأ
وأ مدختسملا مسا) ىرخأ وأ ةدحاو ثحب ةيلمع مادختسا نكمي. ةشاشلا ىلع رهظت ي تل
دبيقت ي ف بغرت تنك اذا، تقولا س فن ي ف امه ي لك مادختسا نكمي وأ، يدر ف لكشب (IP
تقولا س فن ي ف IP ناو نع و ددحم مدختسم ىلع ثحبلا جئاتن
4. ةشاشلا نم لك ىلع تاجرخملا ىرتس، هئاهتنا دنع. لي غشتلا عيرس ي صننلا جامانربلا
لك ري دصت لامكإ نوكي نأ نكمي، كلذلى إ ةفاضلإاب. ةينمز ماتخأ ىلع يوتحت يتلاو
ءارجإل اذه 'C:\%hostname%.txt' ي ف ةدوجوملا ةشاشلا ىلع هلي ثمت متي ثادحأ لالجسل لاخدا
ني عم ثدح ىل لاقتنال ديرت تنك اذا ادي فم.

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا