

درل مدع ةلظم نامأ ةعجارم تابلط مي دقت ةعيرسلا

تايوت حمل

[ةمدقملا](#)

[ةماع قرظن](#)

[لاسرا لاقيسنت](#)

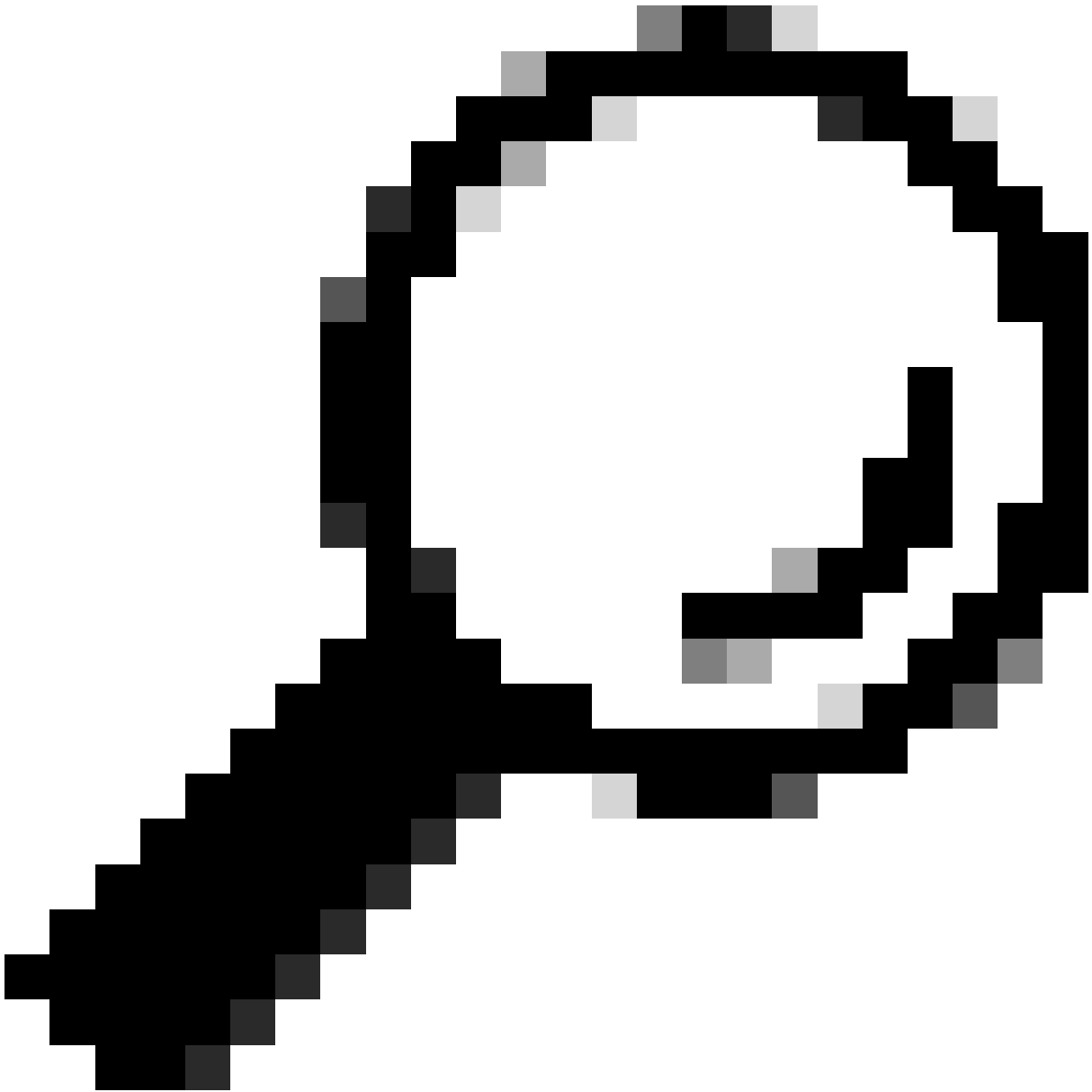
ةمدقملا

درل مدع ةعيرسلا Umbrella نامأ ةعجارم تابلط لاسرا ةيفيك دنتسملا اذه حضوي

ةماع قرظن

يطخت قيرط نع ةعرسب نامألا ةعجارم لاسرا ةجلاعمل ةديج ةقيرط Umbrella معد قيرف مدقي
ةلمعلل ينمزل لودجل جراخ مايأ ل لصي ام رفوي امم - لمك لاب يرشبل معدل قيرف

لاجل لاسرا تاي لمعب حمسي. ةينمأ بابسأل رظح بلط ةمومدملا لاسرا تاي لمع نمضتت
ةديج نامأ لتك ةفاضل تابلط ةدعتمل



وأثناء طاقم التاي باجاي إلى عجارم وأتالاجم الدأ رطح عاغلإ تابلط لوبق متي ال: حيملت
ةئف نمضتي اذهو. يلالحال تقولا يفة يحيابإل داومل لثم يوتحملم فينصت عجارم
Talos Intelligence إلى تابلطال هذه لاسرا بجي. اتقؤم اهافاقيإ متي تالالاجم
تاميلعت يلع لوصحلل Talos فينصت بلط لاسرا: ةيفيك ةلاقم رظنا

تبات قيسنتب umbrella-research-noreply@cisco.com ديرب لاسراب مق، عجارم لل لاسرالل

موقيو Cisco Umbrella، عم معد ةلاح حتف يجري - تمؤم الماظنل اذه يفلطع يأ شودح ةلاح ي
يسايقال ةباجتسالال تقوي فكب صاخال عجارم الماظنل بملط ةبب لتب انيدل معدل قيرف

لاسرالل قيسنت

يتال لاسرالل تاي لمع ضفر متي. ةدحم لاسرا ةرامتسإ يلع درلل لاسرا تاي لمع يأ دمتعت ال

دودرياً لبقت ملو. هلج بجي ام لوح تاداشرا نمضتي دحاو در عم قيسنتلا اذه يفوتست ال ديربلة جلاع ممت. هاندأ يلاتل عرفال رظنا، ةلمتحملا دودرلا ليصافت ىلع عالطاللو. ىرخأ طقف umbrella-research-noreply@cisco.com ناوئعلا ىلإ لسرمل

تاقيسنتلا عم ضرورعلا لوبق مت

(رقنلل لباق طابترا) umbrella-research-noreply@cisco.com يديربل ناوئعلا

دحاو لاجم

Domain: domain.comRequest: blockComments: Include background information or attribution and rationale here

ةددعتم تالاجم

Domaincsv: domain.com, moredomains.com,moredomain.comRequest: blockComments: Include background information or attribution and rationale here
Comments: (Additional comments are supported - must start with comments:)Desired: malware

وأ

Domaincsv: domain.com, moredomains.com,moredomain.com
moredomains.com, evenmoredomains.com, stillmoredomains.com,
afewmoredomains.com
enddomains:Request: blockComments: Include background information or attribution and rationale here
more comments are supported (and optional). Include additional comment lines
here. End with
endcomments:Desired: malware

لوقحلا

الو طقف هسفن لاجملا مسا ىلع اذه يوتحي. ةعجارملا لاسرا متي يذلا لاجملا وه اذه: لاجملا
رطسلا اذه ىلع كلذ نم رثكأ دجوي

رداصللا ينورتكللا ديربلة يفصت لماع لخادتت نأ نم اقلق تنك اذلا لاجملا طبرءاغلإ مق
ي: لي امك وه لوبقملا لكشلا. لاسرالا اذه عم

domain[.]com

تالاجم لاسرا مت اذلا. ةعجارملا لاسرا متي يتلا تالاجملا ةمئاق يه هذو: يف سايسنامود
بطلال عون ةلتك عم طقف لقحلا اذه مادختسا متي. لقحلا لهاجت متي: لاجملا ناف، ةددعتم

؟(ةلتك) هرظح متيل نامأ فينصت ىلإ لاجملا ةفاضإ بلطي لاسرا اذه له: بطل

بطلال ةلوبقملا ةميقيلا

- رطح

ديصتلا طابترا لىصافت كلذى فامب ةيساسأ تامولعم ةيأ ني مضت :تاقىلعتلا لاجملا ةعجارمل ثحبلا قيرف اهمدختسي تامولعم وأ ةراضلا جماربلا وأ يلاي تحالا

مت يذلا لاجملا اب طبترملا جرعتملا ريغ URL ناو نع ىلع اضيأ تاقىلعتلا يوتحت نا نكمي :ةلثمألا .نامك " .ريغت نم دكأت نكلو ،هلاسرا

hxxp://domain[.]com/badstuff.exe

hxxps://domain[.]com/badstuff.exe

ةلوبقملا ميقلل ىدحإ ري فو تب مق .لاسرا لل ةبولطملا ةجيتنلا لقحلا اذه دكؤي :بوغرم بولطملا فينصت لل

بوغرم ل ةلوبقم ميقي :

- شي بخ جمارب
- يلاي تحا ديصت
- تابنلا ملع

ةمچرتل هذه ل و ح

ةل آل ا ت ا ي 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 ي 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 و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل آل ا 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 م ا ة 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