

ةي باجيإل تافلما لي لحت ءاطخأ فاشكتسأ ةي اهنل طاقنل AMP في اهال صاو

تايوت حمل

[ةمدقملا](#)

[ةيساسأل تابلطتلا](#)

[تابلطتلا](#)

[ةمدختسمل تانوكملا](#)

[ةيساسأ تامولعم](#)

[ةي اهنل طاقنل AMP في اهال صاو ةي باجيإل تافلما لي لحت ءاطخأ فاشكتسأ](#)

[SHA 256 فلملا ةئزجت](#)

[فلملا جذومن خسن](#)

[AMP مكحت ةدحو نم هي بنتلا ثدح طاقنلا](#)

[AMP مكحت ةدحو نم ثدحلا لي صافات طاقنلا](#)

[فلملا لوح تامولعم](#)

[حرشلا](#)

[تامولعمل ري فوت](#)

[رارقلا](#)

ةمدقملا

نم ةمدقتملا ةي امحل" في فئاز بجوم فلم لي لحت عي مجت ةي فيكي دنتسمل اذه حضوي
ةي اهنل طاقنل (AMP) "ةراضل جماربل

Cisco نم TAC س دنهم ،زي نيترام ري في فاخ عوسي هي ف مهاس

ةيساسأل تابلطتلا

تابلطتلا

ةيلال عيضاوملاب ةفرعم كي دل نوكت نأ Cisco ي صوت

- AMP في مكحتلا ةدحو تامولعم ةحول
- لوؤسمل تازاي تباب باسح

ةمدختسمل تانوكملا

6.X.X ةي اهنل طاقن رادصل Cisco AMP لي دنتسمل اذه في ةدراول تامولعمل دنتست
ثدحأل تارادصل او

ةصاخ ةي لمعم ةئيبي في ةدوجوملا ةزهجال نم دنتسمل اذه في ةدراول تامولعمل عاشنإ مت
تنالك اذا. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه في ةمدختسمل ةزهجال عي مج تادب
رما يال لم تحملا ري ثاتلل كمهف نم دكأتف ،ةرشابم كتكبش

ةيساسأ تامولعم

(SHA) ةئزجت ةيمزراوخ ىلع ةطرفم تاهيبننت عاشنإب ةياهنلا طاقنل AMP موقى نأ نكمي ةئطاخ ةيباجيإ فشك تايلمع يأ ثودح يف كشنت تنك اذا. نامأل/ةيلمعلا/فلملاب ةصاخ 256 لصاوي ف Cisco، نم (TAC) ةينقتلا ةدعاسملا زكرمب لاصتالا كنكمي ف، كتك بش يف اذه دوزي نأ جاتحت تنأ، Cisco TAC، تنأ لصت ي ام دنع. قمعأ فلم لي لحت عارجا صيخشنتلا قيرف ةمولعم:

- SHA 256 فلملا ةئزجت
- فلملا جذومن خسن
- AMP مكحت ةدحو نم هيبنتلا ثدح طاقنلا
- AMP مكحت ةدحو نم ثدحل لىصافت طاقنلا
- ةئيبل ي ف نوكي نأ بجي اذامل وه يلع لوصحل مت نيأ نم) فلملا لوح تامولعم
- ةئطاخ ةيباجيإ نوكت دق ةيلمعلا/فلملاب نأ دقتعت اذامل حرش

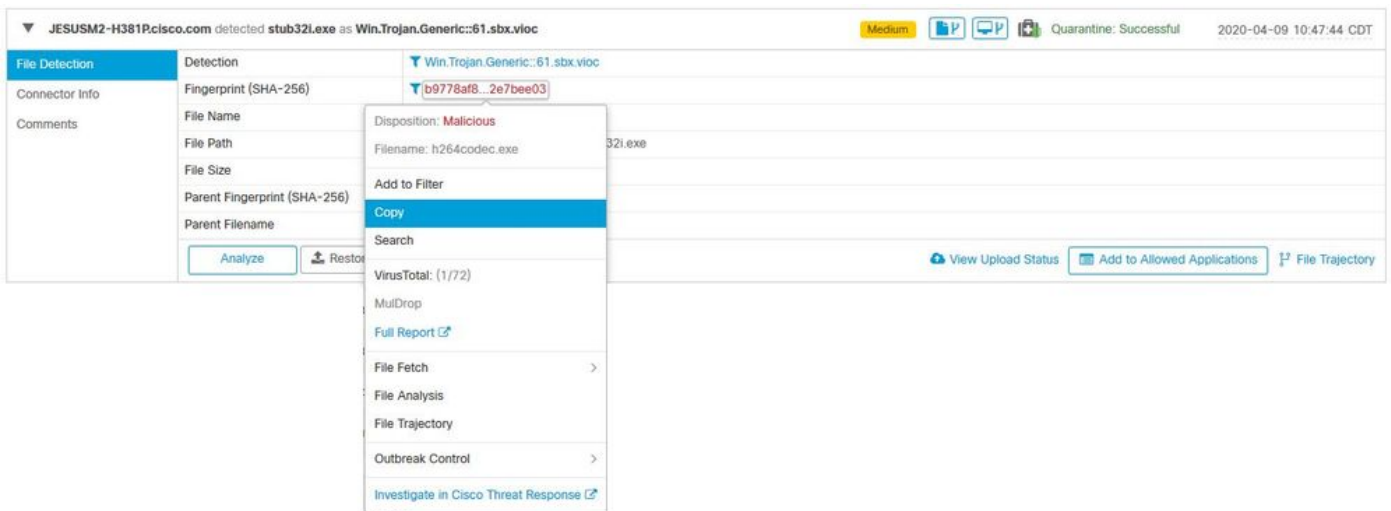
يف احوال صواو أطخ لا ييباجيإ لا فلملا لي لحت عا طخأ فاشكتسا ةياهنلا طاقنل AMP

حت في نأ جاتحي لىصافتلا لك لصحي نأ تلمعتسا عي طتسي تنأ ةمولعم مسق اذه دوزي Cisco TAC عم ةيوه ةحص أطخ

SHA 256 فلملا ةئزجت

> تامولعمل ةحول > AMP مكحت ةدحو ىلا لقتنا، SHA 256 ةئزجت ىلع لوصحلل 1. ةوطخلل اذال

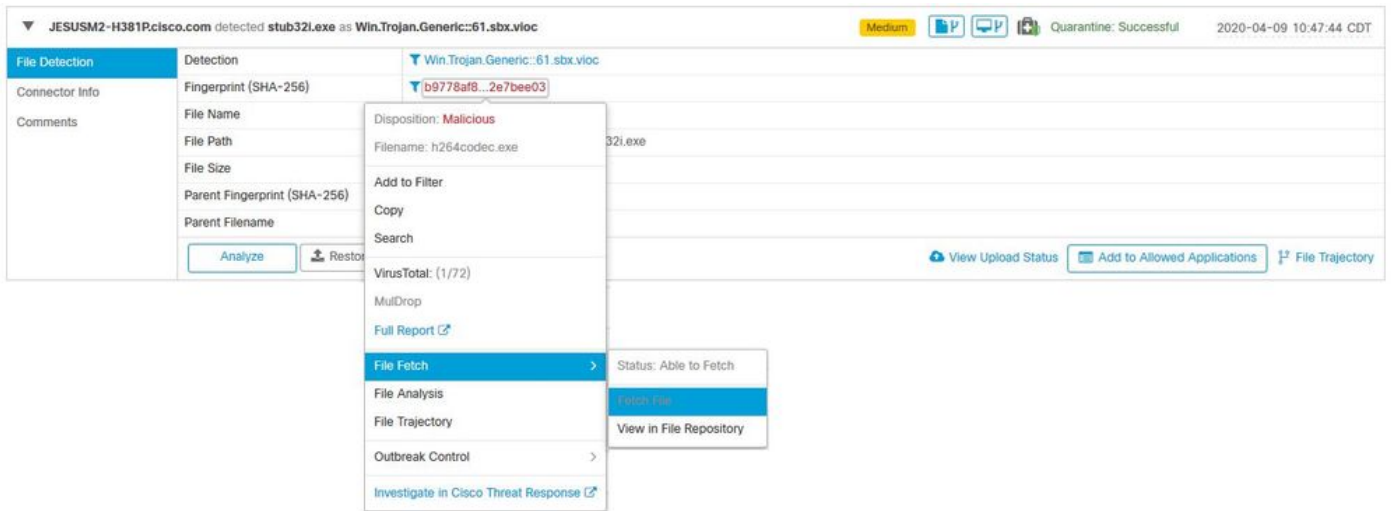
ةروصل ي ف حضوم وه امك خسن دحو SHA256 ىلع رقنا، هيبنتلا ثدح دح 2. ةوطخلل



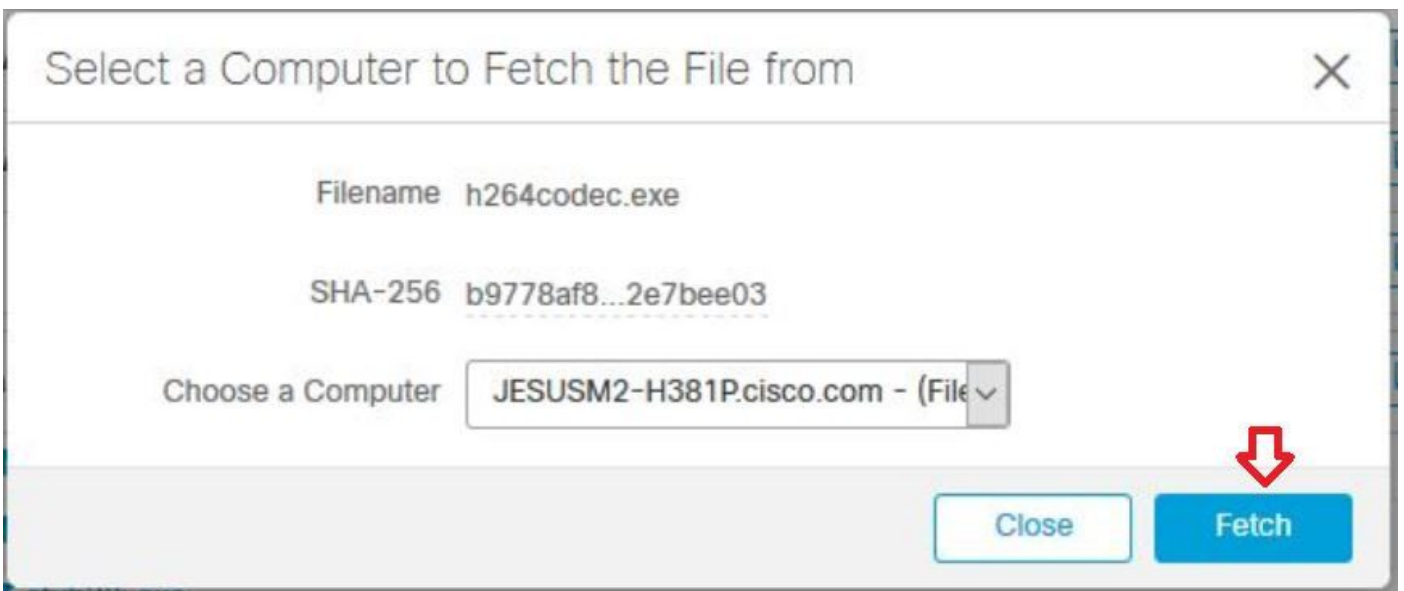
فلملا جذومن خسن

AMP مكحت ةدحو ىلا لقتنا، AMP مكحت ةدحو نم فلملا جذومن ىلع لوصحلل كنكمي 1. ةوطخلل اذال > تامولعمل ةحول >

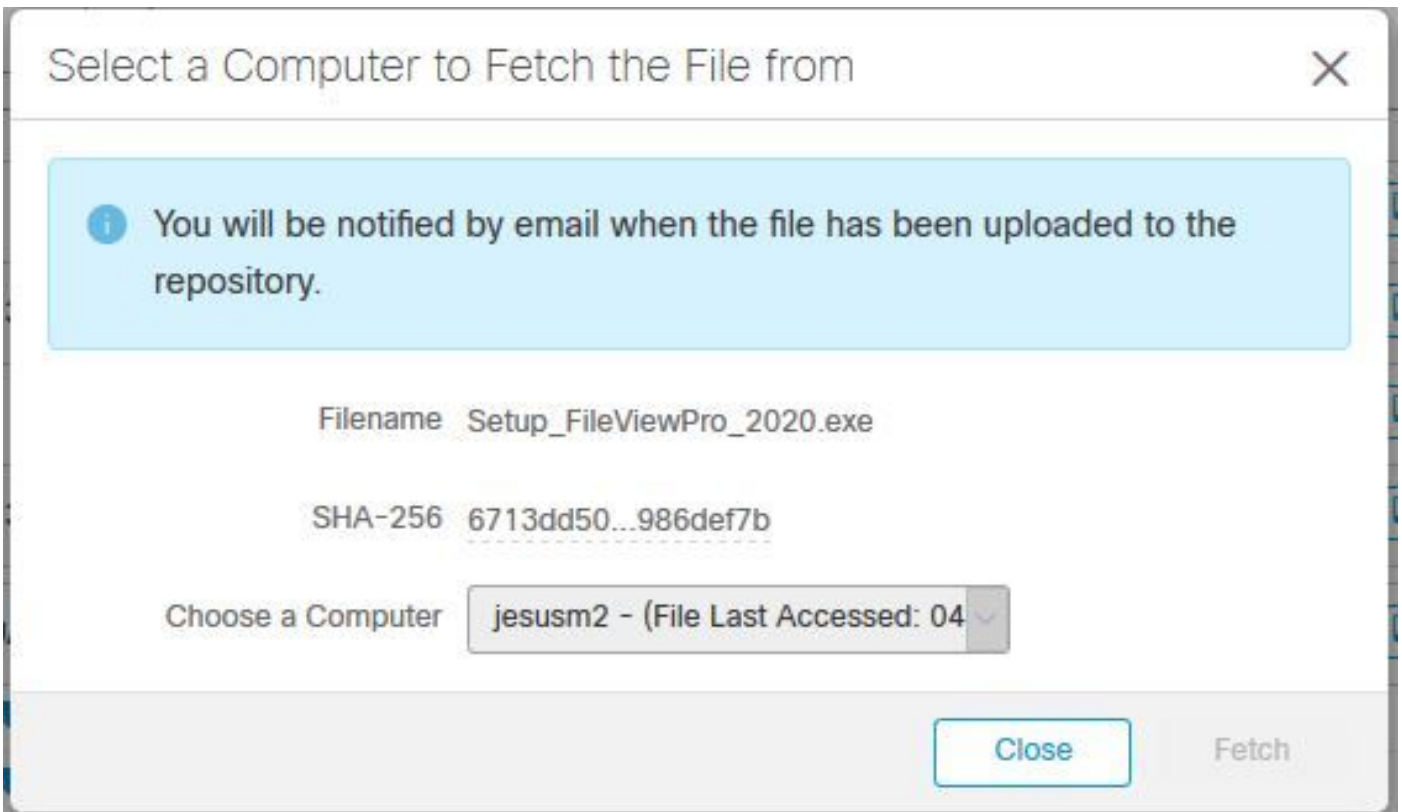
امك فللمل راضح|اضح|ى لى لقتناو SHA256 ى لى رقنا ،هېبنتال شىح دىح . 2 ةوطخال
ةروصلال ى ف حىوم وه



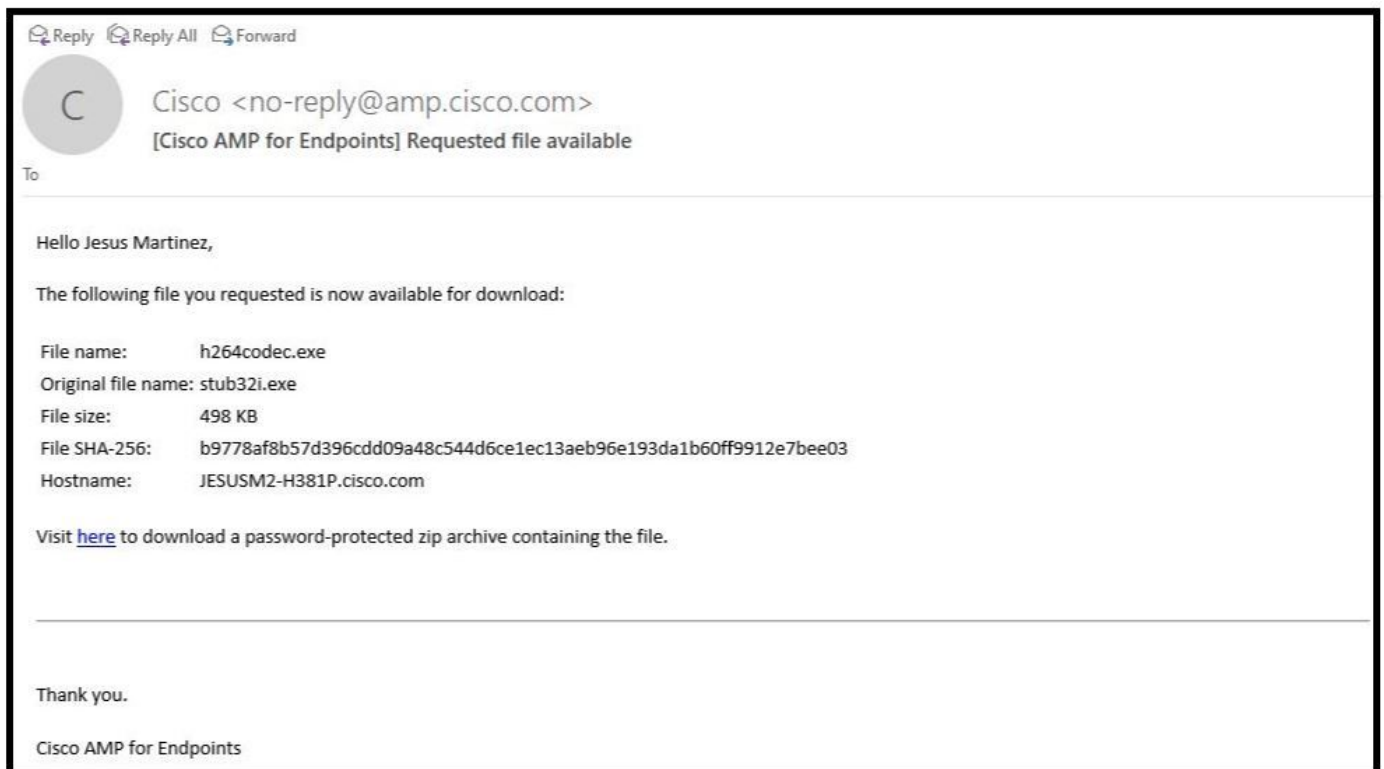
ةروصلال ى ف حىوم وه امك راضح|ى لى رقناو فللمل نى ف شىكال م تىح زاهجال دىح . 3 ةوطخال
ةروصلال ى ف حىوم وه امك (زاهجال لىغشى بىجى)



ةروصلال ى ف حىوم وه امك لىاسرللا ى قلىتت . 4 ةوطخال



ليزنت ل احاتم فلمل نوكي ام دنع ينورت كلال دي رب ل اب اراخ | يقلتت ، قئاق د عضب دعب
ةروصلال ي ف حضوم وه امك



قوف رقناو فلمل ددحو تافللمل عدوتسم > ل لحت > AMP م كحت ةدحو ل لقتنا 5. ةوطخال
ةروصلال ي ف حضوم وه امك ل ل زنت

Connector Diagnostics Feature Overview

Search by SHA-256 or file name...

Status

Group

Type

▼ **h264codec.exe is Available** Requested by **Jesus Martinez** 2020-04-16 03:37:42 CDT

Original File Name	stub32i.exe
Fingerprint (SHA-256)	b9778af8...2e7bee03
File Size	498 KB
Computer	JESUSM2-H381P.cisco.com

لېزنت مټي و، ډروصلال ي ف حضورم وه امك، لېزنت قوف رقنا، مالعإل عېرم ره ظي 6. ؤوطخل ZIP فلم يل ع فلمل.

Warning ✕

You are about to download **h264codec.exe**

This file may be malicious and cause harm to your computer. You should only download this file to a virtual machine that is not connected to any sensitive resources.

The file has been compressed in zip format with the password: **infected**

AMP مكحت ؤدحو نم هېبنتال ثدح طاقنال

ثادخال > تامولعمل ؤحول > AMP مكحت ؤدحو يل لقتنا 1. ؤوطخل

ډروصلال ي ف حضورم وه امك طاقنالال طاقنال او هېبنتال ثدح ددح 2. ؤوطخل

▼ JESUSM2-H381P.cisco.com detected stub32i.exe as Win.Trojan.Generic::61.sbx.vloc Medium Quarantine: Successful 2020-04-09 10:47:44 CDT

File Detection	Detection	Win.Trojan.Generic::61.sbx.vloc
Connector Info	Fingerprint (SHA-256)	b9778af8...2e7bee03
Comments	File Name	stub32i.exe
	File Path	C:\Users\jesum2\Downloads\stub32i.exe
	File Size	498.49 KB
	Parent Fingerprint (SHA-256)	2fb898ba...7bf74fef
	Parent Filename	7zG.exe

AMP مكحت ؤدحو نم ثدخال لېصافات طاقنال

ثادخال > تامولعمل احوول > AMP مكحت دحو ىل القتنا 1. ةوطخال

ةروصلال ىف حضوم وه امك زاوجل راسم راىخ ىلع رقناو وهى بنتلا ثح دح 2. ةوطخال



JESUSM2-H381Pcisco.com detected stub32l.exe as Win.Trojan.Generic:61.sbx.vioci Medium Quarantine: Successful 2020-04-09 10:47:44 CDT

File Detection	Detection	Win.Trojan.Generic:61.sbx.vioci
Connector Info	Fingerprint (SHA-256)	b9778af8...2e7bee03
Comments	File Name	stub32l.exe
	File Path	C:\Users\jesusm2\Downloads\stub32l.exe
	File Size	498.49 KB
	Parent Fingerprint (SHA-256)	2fb898ba...7bf74fef
	Parent Filename	7zG.exe

Analyze Restore File All Computers View Upload Status Add to Allowed Applications File Trajectory

ةروصلال ىف حضوم وه امك زاوجل راسم لىصافات ىل اىجوتلا دىع ىن

Device Trajectory

JESUSM2-H381Pcisco.com in group jesu20r - Oscar Group 2 compromise events (spanning less than a ...)

Filters Search Device Trajectory

Systems

- svchost.exe [PE]
- DpAgent.exe [PE]
- smartscreen.exe [PE]
- ciscoobdhubclient.exe [PE]
- ciscoobdhub.exe [PE]
- wlan32.zip.part [ZFP]
- firefox.exe [PE]
- winword.exe [PE]
- 8099542a935c0c3f68a4...ink [Link]
- downloads (31) link [Link]
- 677d9fe07b83767...automa... [OLEDB]
- stub32l.exe [PE]
- 7zG.exe [PE]
- explorer.exe [PE]
- shupdate.exe [PE]
- ptoneck.exe [PE]
- webexapplauncherlatest.exe [PE]
- atimg.exe [PE]
- webexmcs.exe [PE]
- CiscoWebEXStart.exe [PE]
- gpg-agent.exe [PE]
- gpg.exe [PE]
- scolson.exe [PE]
- dmimg.exe [PE]
- gpgconf.exe [PE]
- gpgme-w32api.exe [PE]
- explorer.exe [PE]
- explorer.exe [PE]
- mfteddiag.exe [PE]
- lenovo.modern.incontrol...exe [PE]
- Lenovo.Modern.InControl.exe [PE]
- clip_themedata.thmx [ZFP]
- msdftool.exe [PE]
- services.exe [PE]
- mtbamagent.exe [PE]
- sdhelper.exe [PE]

Event Details

Medium

2020-04-09 10:47:43 CDT

Detected stub32l.exe, h264codec 4.1.0.0 [b9778af8...2e7bee03] [PE_Executable] as Win Trojan Generic: 61.sbx.vioci.

Created by 7zG.exe, 7-Zip 19.0.0.0 [2fb898ba...7bf74fef] [Unknown] executing as.

The file was quarantined.

Process disposition Design.

File full path: C:\Users\jesusm2\Downloads\stub32l.exe

File SHA-1: 6e055e270bc13a0aa4871b399ac3e15e2197225

File MD5: e74325e74009a868e37887ea011102

File size: 510450 bytes

Parent file SHA-1: ar22612647e8404d15e88eaa490349682950a

Parent file MD5: 648c3ae765c8bc333129972e607398

Parent file size: 581632 bytes

Parent file age: 0 seconds

Parent process id: 24084

Detected by the SHA engines.

ةروصلال ىف حضوم وه امك ثدخال لىصافات ع برم طاقنتلا 3. ةوطخال

Event Details

Medium

2020-04-09 10:47:43 CDT

Detected **stub32i.exe**, h264codec 4.1.0.0 (b9778af8...2e7bee03)
[PE_Executable] as **Win.Trojan.Generic::61.sbx.vioc**.

Created by **7zG.exe**, 7-Zip 19.0.0.0 (2fb898ba...7bf74fef)
[Unknown] executing as .

The file was **quarantined**.

Process disposition Benign.

File full path: C:\Users\jesusm2\Downloads\stub32i.exe

File SHA-1: 6e055a270bdc13dcaa4871b39fac3d15a2137225.

File MD5: f74325a740d0a9cf68e37887ce017102.

File size: 510450 bytes.

Parent file SHA-1: df22612647e9404a515d48ebad490349685250de.

Parent file MD5: 04fb3ae7f05c8bc333125972ba907398.

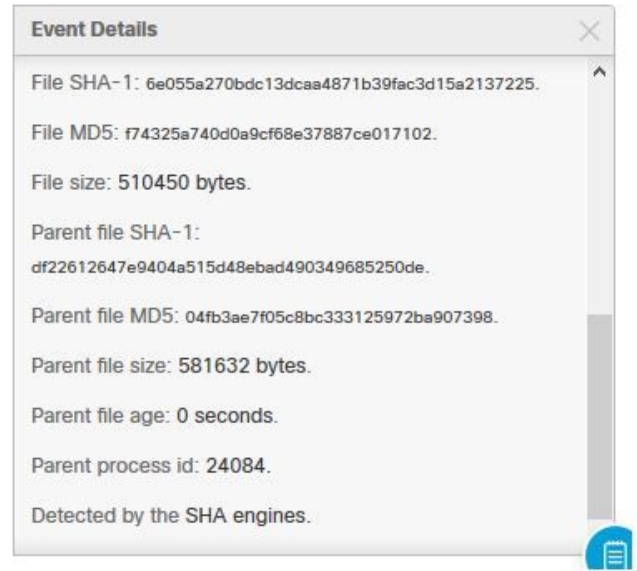
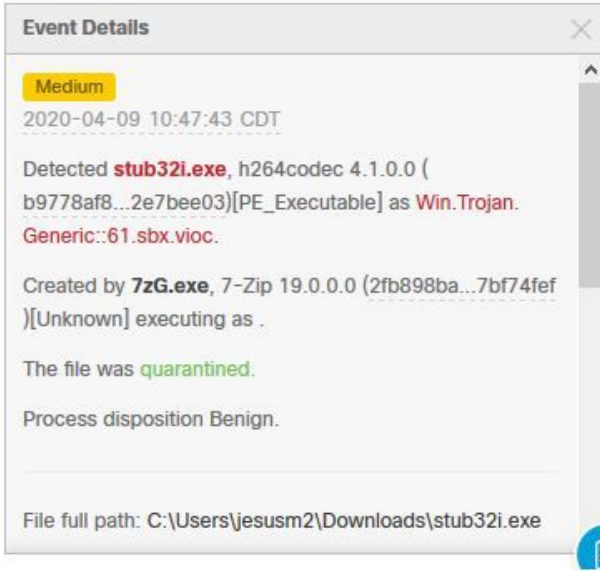
Parent file size: 581632 bytes.

Parent file age: 0 seconds.

Parent process id: 24084.

Detected by the SHA engines.

يُعدّ لوصول طاقّات لال اضعب طاقّات لال لفسأل قلزنا، يرورض لال نم ناك اذا. 4. ةوطخلال
ةروصلال يف حضوم وه امك ثادخالال عيمج لى صافات تامولعم.



فلمل لوج تامولعم

- فلمل ردصم لوج تامولعم
- بېولل URL ناو نع ةكراشمب مقف ، بېوقوم نم فلمل اءا اءا
- فلمل ةفيظو حرشب مقو فلمل اريغص افصو كراش

حراش

- ةئطاخ ةبءاچي نوكت نا نكمي فلمل ةي لمع نا دقتعت اءامل
- فلمل يف اءب قئت يتل بابسأل كراش

تامولعم ريفوت

- عقوم لىل ةبولطمل تامولعمل اعيمج لي مءب مق ، لي صافتل اعيمج عيمجت درجمب <https://cway.cisco.com/csc/>
- ةمدخل بلط مق رىل ةراشال نم دءا

رارقل

ةياهنل طاقنل AMP ةينقءب صاخلل ديهتلل ءاكذ نيسحت لىل امءاد Cisco عىست ، حءص رىغ لكشب هبنت لىغشءب كءدل AMP for Endpoints لءام اءا ، لكذ عمو ، هعيسوتو قوئو اءه مدقو . كءئبب لىل ءافاضل رىءاىل اءنمل ءاءارءال ضعب ءاءءل كنكمي فقلعتي امي ف Cisco TAC عم ءءا حءفي نا ةبولطمل لي صافتل لك لىل صءى نا guidelines رىصم رىغء نكمي ، "صءىءشءل قىرف" فلم لىل حءل لىل اءانءسا . ةئطاخ ةبءاچي ءلءسم رفوي نا نكمي وا AMP مءءء ءءو لىل ءل لىل هبنتل ءاءءا فاقىل فلمل يف لكاشم ءوءء نوء ءل لمءل/فلمل لىل ءشءب ءامسلل بسانمءل ءالصال Cisco TAC كءئبب .

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل