

تالجس و ةنمآلـا بيـولا ةـزهـجـأ عـاطـخـأ فـاشـكـتـسـأ ةـراـضـلـا جـمـارـبـلـا نـم ةـمـدـقـتـمـلـا ةـيـامـحـلـا (ـمـاـكـحـأـلـا رـادـصـا) اـحـالـصـاـوـ)

تـايـوـتـحـمـلـا

ـمـدـقـمـلـا

[ـيـسـاسـأـلـا تـابـلـطـتـمـلـا](#)

[ـاـبـلـطـتـمـلـا](#)

[ـمـدـخـتـسـمـلـا تـانـوـكـمـلـا](#)

[ـيـسـاسـأـتـامـوـلـعـمـ](#)

[ـاـحـالـصـاـوـ WSA AMP تـالـجـسـ عـاطـخـأـ فـاشـكـتـسـأـ](#)

[ـلـصـ تـاذـ تـامـوـلـعـمـ](#)

ـمـدـقـمـلـا

صـاخـلـا "ـاعـاطـخـأـلـا حـيـحـصـتـوـتـامـوـلـعـمـلـا لـجـسـ يـوـتـسـمـ يـفـ مـاـكـحـأـلـا مـسـقـ دـنـتـسـمـلـا اـذـهـ فـصـيـ
(WSA). بـيـولا نـامـا زـاهـجـبـ صـاخـلـا (AMP) ةـراـضـلـا جـمـارـبـلـا نـمـ ةـمـدـقـتـمـلـا ةـيـامـحـلـا كـرـحـمـبـ.

ـيـسـاسـأـلـا تـابـلـطـتـمـلـا

ـاـبـلـطـتـمـلـا

ـيـلـاتـلـا عـيـضـاـوـمـلـا ـفـرـعـمـ كـيـدـلـ نـوـكـتـ نـأـبـ يـصـوـتـ:

- ـيـبـثـتـ مـتـ WSA
- ـاـفـلـمـلـا لـيـلـحـتـوـفـلـمـلـا ـعـمـسـ نـيـكـمـتـ مـتـ
- ـراـضـلـا جـمـارـبـلـا نـمـ ةـمـدـقـتـمـلـا ةـيـامـحـلـا
- ـمـلـ Cisco نـمـ نـمـآلـا بـيـولا زـاهـجـ
- ـيـمـعـ SSH

ـمـدـخـتـسـمـلـا تـانـوـكـمـلـا

ـنـيـعـمـ ةـيـدـامـ تـانـوـكـمـوـجـمـارـبـ تـارـادـصـاـىـلـعـ دـنـتـسـمـلـا اـذـهـ رـصـتـقـيـ الـ.

ـصـاخـ ةـيـلـمـعـمـ ةـيـيـبـ يـفـ ةـدـوـجـوـمـلـا ةـزـهـجـأـلـا نـمـ دـنـتـسـمـلـا اـذـهـ يـفـ ةـدـرـاوـلـا تـامـوـلـعـمـلـا ءـاشـنـا مـتـ
ـتـنـاكـ اـذـاـ. (ـيـضـاـرـتـفـاـ) حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـا اـذـهـ يـفـ ةـمـدـخـتـسـمـلـا ةـزـهـجـأـلـا عـيـمـجـ تـأـدـبـ
ـرـمـأـ يـأـلـ لـمـتـحـمـلـا رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ ،ـلـيـغـشـتـلـا دـيـقـ كـتـكـبـشـ.

ـيـسـاسـأـتـامـوـلـعـمـ

ـنـمـ ةـيـامـحـلـا AMP رـفـوتـ .ـيـلـحـمـلـا كـرـحـمـلـا طـاقـنـلـا عـمـ لـمـاـكـتـلـا WSA رـفـويـ
ـةـدـيـجـلـا ـعـمـسـلـاـوـ تـافـلـمـلـا لـيـلـحـتـ تـازـيـمـ لـالـخـ نـمـ اـدـحـاـوـ اـمـوـيـ زـوـاجـتـتـ اـلـ ةـدـمـلـ ةـراـضـلـا جـمـارـبـلـا
ـلـبـقـ اـيـلـخـادـ تـافـلـمـلـا صـحـفـ نـعـ لـوـفـسـمـ فـيـنـصـتـلـا لـبـقـ اـمـ كـرـحـمـ WSA نـمـضـتـيـ .ـتـافـلـمـلـلـ

كرحمب ةطبترم يلاتل مسقلاب يف ةحصو ملأ تالجسلأ. ةماعلأ ةكبشلا نم ققحتلا تايملع AMP ديدهتلأ ةكبش وأ ةباحسب سيلو WSA ئلعي.

اوحالص او WSA AMP تالجس عاطخاً فاشكتسأ

تالجس لييذتو (CLI) رمأولا رطس ةهجاو رباع لودلا ليجستب مق. تالجس ئلإ لوصولـا اهتئزجت وأ amp:

1. ليمع لالخ نم رمأولا رطس ةهجاو ئلإ لودلا لجس SSH.

2. لاخدالا حاتفم طغض او grep رمألا بتكا.

3. بـلـط دـنـع amp_log مـقـرـلـخـدا.

4. رـاـيـخـلـاـ رـتـخـأـ،ـ رـشـابـمـ روـرـمـ ةـكـرـحـ لـيـغـشـتـبـ تـمـقـ (ـاـذاـ)ـ ةـيـلـاتـلـاـ تـارـايـخـلـاـ ئـلـعـ ةـبـاجـإـلـابـ مقـ).ـ تـالـجـسـلـاـ لـيـذـتـلـ).

5. حـاتـفـمـلـاـ ئـلـعـ طـغضـاـ Enter.

6. تـالـجـسـلـاـ ضـرعـ مـتـيـ.

يـوـتـسـمـ دـيـدـحـتـ كـنـكـمـيـ،ـ تـامـوـلـعـمـلـاـ نـمـ ةـفـلـتـخـمـ تـايـوـتـسـمـ يـفـ WSA AMP يـفـ ةـحـضـوـمـ ةـفـيـفـطـ تـافـالـتـخـاـ ئـلـعـ يـوـتـحـتـ يـتـلـاـ جـئـاتـنـلـلـ عـاطـخـأـلـاـ حـيـحـصـتـ وأـ تـامـوـلـعـمـلـاـ يـلـاتـلـاـ مـسـقـلـاـ.

تـالـجـسـ دـيـدـحـتـلـ WSA صـيـخـرـتـ تـيـبـثـتـ مـزـلـيـ:ـ ةـظـاحـاـلـمـ.

تـامـوـلـعـمـ يـوـتـسـمـ تـالـجـسـ:

```
Wed Apr 27 12:21:26 2022 Info: Txn 18210 Binary scan on instance[0] Id[1345]: AMP allocated  
memory = 0, AMP used memory = 0, Scans in flight = 1, Active faster connections = 1, Active  
slower connections = 0  
Wed Apr 27 12:21:35 2022 Info: Binary scan on instance[0] id[1345]:  
filename[npp.8.4.Installer.x64.exe] filemime[application/x-dosexec] file_extension[exe]  
length[4493047b] ampverdict[(1, 1, 'amp', '', 0, 0, True)] scanverdict[0] malwareverdict[0]  
spyname[] SHA256[ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1] From[Cloud]  
uploadreason[Enqueued in the local queue for submission to upload] verdict_str[FILE UNKNOWN]  
is_slow[0] scans_in_flight[0] Active faster connections[0] Active slower connections[0]  
Wed Apr 27 12:22:28 2022 Info: File uploaded for analysis. Server:  
https://panacea.threatgrid.com, SHA256:  
ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1, Filename:  
npp.8.4.Installer.x64.exeTimestamp: 1651044116 sampleid[]
```

(ماـكـحـأـلـاـ رـادـصـاـ)ـAMPـ تـامـوـلـعـمـ يـوـتـسـمـ تـالـجـسـ:

```
ampverdict[(1, 1, 'amp', '', 0, 0, True)]  
(analysis_Action, scan_verdict, 'verdict_source', 'spyname', malware_verdict, file_reputation,  
upload_action)]
```

عاطخاً حـيـحـصـتـ يـوـتـسـمـ تـالـجـسـ AMP:

```
Fri Apr 29 01:38:40 2022 Debug: Binary scan: proxid[3951] filename[favicon.ico] len[41566b]  
readtime[109.721680ms] scantime[2.205322ms] ampverdict[(1, 1, 'amp', '', 0, 0, False)]  
scanverdict[0] malwareverdict[0]
```

SHA256[e7a2345c75a03e63202b12301c29bb8b6bae7cef9e191ed58797ec028def7c4f] From[Cloud]

FileName[favicon.ico] FileMime[application/octet-stream]

(ماكحألا رادصا) AMP ءاطخأ حيحصت ىوتسم تالجس:

ampverdict[(1, 1, 'amp', '', 0, 0, False)]

ampverdict[(analysis_action, scan_verdict, disposition, 'spyname: policy name if amp registered with console', file_reputation, upload_action, 'sha256', 'threat_name')]

ةميق لباقم يليصفت لقح تاريغ:

لـقـحـلـا

ةـمـيـقـلـا

نـلـاـ جـمـارـبـلـاـ نـمـ ةـمـدـقـتـمـلـاـ ةـيـامـحـلـاـ "ـنـأـ ـىـلـاـ"ـ ـ0ـ"ـ رـيـشـيـ

لـيـلـحـتـلـلـ فـلـمـلـاـ لـيـمـحـتـ بـلـطـتـ مـلـ

نـلـاـ جـمـارـبـلـاـ نـمـ ةـمـدـقـتـمـلـاـ ةـيـامـحـلـاـ "ـنـأـ ـىـلـاـ"ـ ـ1ـ"ـ رـيـشـيـ

لـيـلـحـتـلـلـ فـلـمـلـاـ لـيـمـحـتـ تـبـلـطـ

رـاضـ رـيـغـ فـلـمـلـاـ ـ0ـ:

فـلـمـلـاـ عـوـنـ بـبـسـ بـاـيـئـوـضـ فـلـمـلـاـ حـسـمـ مـتـيـ مـلـ ـ1ـ:

بـ صـاـخـلـاـ

تـافـلـمـلـاـ صـحـفـ ةـلـهـمـ تـهـتـنـاـ ـ2ـ:

حـسـمـلـاـ يـفـ أـطـخـ ـ3ـ:

رـاضـ فـلـمـلـاـ ـ3ـ نـمـ رـبـكـأـ

تـافـلـمـلـاـ لـيـلـحـتـ:AMP

فـورـعـ رـيـغـ ـ1ـ:

فـيـظـنـ ـ2ـ:

رـاضـ (AMP) ـ3ـ:

(يـئـوـضـلـاـ حـسـمـلـلـ لـبـاـقـ رـيـغـ)ـ حـسـمـلـلـ لـبـاـقـ رـيـغـ ـ4ـ:

يـشـفـتـ جـهـنـ مـاـدـخـتـسـاـ مـتـيـ مـلـ اـذـاـ غـرـافـAMP

سـجـتـلـاـ مـسـاـ Simple_Custom_Detection: تـجـهـنـ مـاـدـخـتـسـاـ ةـلـاحـ يـفـ

AMP

ةـيـامـحـلـاـ عـضـوـىـلـعـ فـلـمـلـاـ طـبـضـ مـتـ: حـيـحـصـ

يـلـمـرـلـاـ عـبـرـمـلـاـ ـىـلـاـ فـلـمـلـاـ لـاـسـرـاـ مـتـيـ مـلـ: ءـاطـخـ

SHA256

ةـيـامـحـلـاـ تـادـيـدـهـتـ عـاوـنـأـ ـىـلـاـ اـدـانـتـسـاـ دـيـدـهـتـلـاـ مـسـاـ

ةـمـدـقـتـمـلـاـ (AMP)

مـكـحـلـاـ رـدـصـمـ

ةـيـلـبـاـقـ

سـسـجـتـلـاـ مـسـاـ

ءـاـجـاـ لـيـمـحـتـ

SHA256

دـيـدـهـتـلـاـ مـسـاـ

ةـلـصـ تـاـذـ تـاـمـوـلـعـمـ

• [عـمـ تـادـيـدـهـتـلـاـ ةـكـبـشـ وـةـيـاهـنـلـاـ طـاقـنـلـ \(AMP\)ـ قـمـدـقـتـمـلـاـ ةـيـامـحـلـاـ جـمـدـ WSA](#)

• [فـلـمـلـاـ لـيـلـحـتـ وـفـلـمـلـاـ ةـعـمـسـ ةـيـفـصـتـ](#)

• [ةـمـظـنـأـلـاـ Cisco - تـادـنـتـسـمـلـاـوـيـنـقـتـلـاـ مـعـدـلـاـ](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).