

如何解碼ESA上的X-IronPort-AV報頭？

目錄

[問題](#)

問題

如何解碼X-IronPort-AV報頭？

作為防病毒掃描的一部分，ESA將增加X-IronPort-AV報頭，該報頭編碼AV掃描結果的詳細資訊。如果需要，可以停用此報頭作為防病毒配置的一部分。以下是一些標題範例。

```
X-Ironport-AV: i=""3.84,87,1091404800"";
d=""scan'217,208""; a=""76:sNHT50174724""
X-Ironport-AV: i=""3.83,108,1088978400"";
d=""scan'208""; a=""0:sNHT0""
X-Ironport-AV: i=""3.83,93,1089000000"";
d=""scan'217,208""; a=""1233:sNHT25086908""
X-Ironport-AV: i="3.81R,139,1083556800"; e="0x80040202'u";
d="scan'217,208?doc'217,208,186,179,178,32";
a="2645030:sNHsT231932724"
```

雖然其中的一些代碼是專為Sophos引擎而設計的，此處沒有介紹，但是透過瞭解此標題的結構，您可以獲得大量資訊。以下是解碼X-IronPort-AV報頭的金鑰：

代碼	意義	內容
i	版本資訊	<ul style="list-style-type: none">• 產品版本• IDE數量• IDE序列
e	錯誤	錯誤代碼（十六進位制）加上以下其中一項： <ul style="list-style-type: none">• 「i」被忽略• 「u」無法掃描• 「e」已加密• 「t」超時• 「f」致命• 「j」savi-bug（已忽略）

		<ul style="list-style-type: none"> • 「s」 savi-bug (無法掃描) • 「z」 未知
v	病毒清單	<ul style="list-style-type: none"> • 病毒名稱 • 零件編號 • infos : 「r」 修復 「d」 丟棄 「u」 不可掃描的 「e」 加密 「v」 病毒
d	檔案詳細資料	<ul style="list-style-type: none"> • 延伸 • 型別代碼清單
答	訊息動作	<ul style="list-style-type: none"> • mid 「 : 」 (操作部分) • 「a」 查扣 ? • 已傳送 「s」 已捨棄 「d」 已轉發 「f」 • 「x」 某些錯誤 (超時、rpc連線失敗等) • 'N' (通知部分) • 「s」 寄件者 • 「r」 收件人 • 「o」 其他 • 'H' (標頭區段) • 「s」 主題已修改 • 已修改 「h」 自訂標頭 • 「T」 (時間段) • NNNN經歷時間

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。