

Wie decodiere ich den X-IronPort-AV-Header auf der ESA?

Inhalt

[Frage](#)

Frage

Wie decodiere ich den X-IronPort-AV-Header?

Im Rahmen des Anti-Virus-Scans fügt die ESA einen X-IronPort-AV-Header hinzu, der Details des AV-Scanergebnisses codiert. Dieser Header kann bei Bedarf im Rahmen der Virenschutzkonfiguration deaktiviert werden. Hier sind einige Beispiel-Header.

```
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"
```

Obwohl einige der enthaltenen Codes spezifisch für die Sophos-Engine sind und hier nicht dokumentiert sind, können Sie viele Informationen aus dem Verständnis der Struktur dieses Headers ableiten. Der Schlüssel zum Decodieren des X-IronPort-AV-Headers lautet wie folgt:

Code	Bedeutung	Inhalt
i	Versionsinformationen	<ul style="list-style-type: none">• Produktversion• Idenzahl• IDE-Serie
o	Fehler	Fehlercode (hex) plus einer der folgenden Werte: <ul style="list-style-type: none">• "i" wird ignoriert• "u" nicht scanbar

		<ul style="list-style-type: none"> • "e" verschlüsselt • "t"-Zeitüberschreitung • ,f' tödlich • "j" savi-bug (ignoriert) • "s" savi-bug (nicht scannbar) • "z" unbekannt
v	Virenliste	<ul style="list-style-type: none"> • Virusname • Teilenummer • infos: "r" Reparatur "d" Drop "u" unscannable "e" verschlüsselte "v" virale
g	Dateidetails	<ul style="list-style-type: none"> • Verlängerung • Typencodelist
a	Nachrichtenaktionen	<ul style="list-style-type: none"> • mid ':' (Aktionsabschnitt) • "a" archiviert ? • "s" gesendet "d" verworfen "f" weitergeleitet • "x" bestimmte Fehler (Timeout, RPC-Verbindung fällt aus usw.) • 'N' (Abschnitt "Benachrichtigung") • s-Absender • Empfänger "r" • "o" andere • 'H' (Kopfzeilen-Abschnitt) • Betreff "s" geändert • Benutzerdefinierter Header "h" geändert • ,T' (Zeitabschnitt) • Verstrichene NNN-Zeit

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.