How do I decode the X−IronPort−AV header on the ESA?

TAC **Document ID: 117887**

Contributed by Scott Roeder and Enrico Werner, Cisco TAC Engineers.

Jul 09, 2014

Contents

Question

How do I decode the X−IronPort−AV header?

As part of anti−virus scanning the ESA will add an X−IronPort−AV header which encodes details of the AV scanning result. This header can be disabled if desired as part of the anti−virus configuration. Here are some example headers.

```
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"
```

Although a few of the codes contained are specific to the Sophos engine and are not documented here, you can derive a lot of information from understanding the structure of this header. Here is the key to decode the X−IronPort−AV header:

Code	*Meaning*	*Content*
i	Version information	• product version • number of ides • IDE serial
e	Errors	Error code (hex) plus one of: • "i" ignored • "u" unscannable • "e" encrypted • "t" timeout • "f" fatal • "j" savi−bug (ignored) • "s" savi−bug (unscannable) • "z" unknown

v	Virus list	• virus name • part number • infos: "r" repair "d" drop "u" unscannable "e" encrypted "v" viral
d	File details	• extension • type code list
a	Message actions	• mid ':' (action section) • "a" archived ? • "s" sent | "d" dropped | "f" forwarded • "x" certain errors (timed−out, rpc conn fails, etc) • 'N' (notification section) • "s" sender • "r" recipient • "o" other • 'H' (headers section) • "s" subject modified • "h" custom header modified • "T" (time section) • NNNN elapsed time