Re: Log Question

Source: http://www.derkeiler.com/Mailing−Lists/securityfocus/focus−ms/2004−02/0067.html

---

esardanons_at_presencia.net
Date: 02/27/04

```
Date: Fri, 27 Feb 2004 15:52:39 −0300 (ART)
To: Sean Warnock <swarnock@warnocksolutions.com>
```

check out this:
http://www.eeye.com/html/Research/Advisories/AD20010618.html

Eliel

> To all on the list;
>
> Over the past few days I have been receiving a flurry of traffic on one
> of my web servers. I suspect it to be sometime of automated scan but I
> have been unable to find anything listed on Google with this type of
> signature. Fortunately whatever is going on is only getting a 404 error
> but I would like to learn a little more about what is going on. From
> what I can tell from reading so far it looks like a buffer overrun
> attempt on the indexing service. Below my signature you will find an
> except from my log file. Any thoughts or insights would be appreciated.
>
> Sean Warnock
> swarnock@warnocksolutions.com
>
> #Software: Microsoft Internet Information Services 5.0
> #Version: 1.0
> #Date: 2004−02−27 01:28:43
> #Fields: date time c−ip cs−username s−ip s−port cs−method cs−uri−stem
> cs−uri−query sc−status cs(User−Agent) cs(Referer)
> 2004−02−27 05:03:10 211.109.254.187 − 192.168.200.202 80 GET /Default.htm
> − 200 − −
> 2004−02−27 05:03:10 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA
> CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> 404 − −
> 2004−02−27 05:03:16 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA
> CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â

> *404 − −*
> *2004−02−27 05:03:21 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA*
> *CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> *404 − −*
> *2004−02−27 05:03:26 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA*
> *CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> *404 − −*
> *2004−02−27 05:03:32 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA*
> *CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> *404 − −*
> *2004−02−27 05:03:37 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA*
> *CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> *404 − −*
> *2004−02−27 05:03:42 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA*
> *CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> *404 − −*
> *2004−02−27 05:03:47 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA*
> *CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> *404 − −*
> *2004−02−27 05:03:52 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA*
> *CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> *404 − −*
> *2004−02−27 05:03:58 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA*
> *CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> *404 − −*
> *2004−02−27 05:04:03 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA*
> *CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC*

â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> 404 − −
> 2004−02−27 05:04:08 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA
> CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> 404 − −
> 2004−02−27 05:04:13 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA
> CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> 404 − −
> 2004−02−27 05:04:18 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA
> CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> 404 − −
> 2004−02−27 05:04:24 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA
> CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â
> 404 − −
> 2004−02−27 05:04:29 211.109.254.187 − 192.168.200.202 80 GET /NULL.IDA
> CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
â„¢â„¢q_â„¢â„¢â„¢ afâ€“ /â„¢â„¢â„¢ aâ„¢Ã-Ã ++++Ã³â„¢ Â¦Å“â„¢â„¢Ã‰Ã±â„¢Â â„¢â„¢ ÃšÅ“â„¢â„¢Ã‰ Â¶Å“
¡â„¢â„¢Ã‰f+Â½Å¸â„¢â„¢ Ã¶Å¡â„¢â„¢Ã‰f+Â©Å¸â„¢â„¢ aâ„¢Ã-Â»++++ Ã©â€¢ ge4 aâ„¢Ã-Å ++++ â„¢Â¥â€œÃ
„¢â„¢Ã’ÃœÃ‹Ã—ÃœÃ•ÂªÂ«â