

SecurityFocus Incidents: RE: is this the start of something naughty?

## RE: is this the start of something naughty?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-08/0247.html>

---

**From:** DeGennaro, Gregory (*Gregory\_DeGennaro\_at\_csa.com*)

**Date:** 08/18/03

To: Charles Blackburn <charlesb@summerfield-technology.co.uk>, incidents@securityfocus.com

Date: Mon, 18 Aug 2003 11:44:20 -0700

From SANS-Incidents -

<http://isc.sans.org/diary.html?date=2003-08-18>

Regards,

Greg DeGennaro Jr., CCNP  
Security Analyst

-----Original Message-----

From: DeGennaro, Gregory

Sent: Monday, August 18, 2003 11:42 AM

To: 'Charles Blackburn'; incidents@securityfocus.com

Cc: 'Ken Eichman'

Subject: RE: is this the start of something naughty?

[http://www.cert.org/current/current\\_activity.html#icmpincrease](http://www.cert.org/current/current_activity.html#icmpincrease)

Regards,

Greg DeGennaro Jr., CCNP  
Security Analyst

-----Original Message-----

From: Charles Blackburn [mailto:charlesb@summerfield-technology.co.uk]

Sent: Monday, August 18, 2003 3:25 AM

To: incidents@securityfocus.com

Subject: is this the start of something naughty?

Hi

I received approximately 100 of these within the space of 30 minutes or so from numerous different IP addresses and on my /29 block (2/3 machines and also the broadcast/and network addresses). Now I've had a few shall we say erm, "funnies" going on on this one machine lately with problems when it's rebooted which seem to be fixed by a kernel rebuild, but that could be a hardware problem. however it could be more indicative of an attack maybe

RE: is this the start of something naughty?

SecurityFocus Incidents: RE: is this the start of something naughty?

even a successful one.

Aug 18 10:46:14 thunder snort: [1:483:2] ICMP PING CyberKit 2.2 Windows  
[Classification: Misc activity] [Priority: 3]: {ICMP} 80.253.133.136 ->  
xx.xx.xx.120/123/125/127

120/127 are the end of my 8 IP block, 125 is the machine with the funnies,  
and 123 is a windows 98 vmware session that I've only just finished  
installing windows in.

it's always those same IP's and never any of the others.

my question is, what can i do to see whether my box has been compromised (a  
rebuild's not much a problem as i was going to do it anyway :P) and if could  
any of you "1337" (i use that term loosely) help me.

regards  
charles

---

Captus Networks – Integrated Intrusion Prevention and Traffic Shaping

- Instantly Stop DoS/DDoS Attacks, Worms & Port Scans
- Automatically Control P2P, IM and Spam Traffic
- Ensure Reliable Performance of Mission Critical Applications
- Precisely Define and Implement Network Security and