

[Inspiratron.org](https://inspiratron.org) - [Natural language processing, machine learning and cybersecurity](#)

Chasing script-kiddies and hackers on my blog

by Nikola Milošević - Tuesday, May 26, 2015

<https://inspiratron.org/blog/2015/05/26/chasing-script-kiddies-blog/>

This morning, I was wondering over my admin dashboard and realized there are couple of guys (hackers or script-kiddies) trying to hack me. Well, to be honest guess my user name and password. So far, they were failing, but some of them were returning and trying every couple of hours, when my blocking mechanism release the block. Particularly, one guy from Moldova, one from Romania and one from Ukraine. To say it on the beginning... I ain't gonna say something very smart here, I was just playing a bits of forensics here and there, to find out who they are. And to be honest, I am not satisfied, since I have not found much apart from IP address of machine that was used, IP WhoIs record with some names, phone numbers and addresses. So it started this morning.

Looking deeper on hacking attempts

As you can see, I have WordPress website. And quite long time ago I realized there are from time to time guys trying to guess my user name and password. However, I have some security plugins installed, like [Wordfence](#) and [Bullet Proof Security](#). So basically hacker who tries it will get his IP blocked after couple of attempts. Whole thing would be logged. So I found out that these "hackers" were trying quite simple thing... guess password for admin user or Administrator. The only bad thing is that these default usernames does not exist on my website. They get soon blocked and whole attack is over.

Then today, I decided to look deeper. So I found out that the attack is happening from the static IP address 193.104.41.186. I could ping this machine. I looked at IP WhoIs record and I got the following information:

Chasing script-kiddies and hackers on my blog - 05-26-2015

by Nikola Milošević - <https://inspiratron.org>

The screenshot shows a web browser window with the URL <https://www.whatismyip.com/ip-whois-lookup/>. The page displays the results of an IP whois lookup for the IP address 193.104.41.0. The information is organized into two main sections: one for the IP block and another for the individual person.

IP Block Information:

- inetnum: 193.104.41.0 - 193.104.41.255
- netname: VVPN-NET
- descr: PE Voronov Evgen Sergiyovich
- country: MD
- org: ORG-PESV2-RIPE
- admin-c: ESV1-RIPE
- tech-c: ESV1-RIPE
- status: ASSIGNED PI
- mnt-by: VVPN-MNT
- mnt-by: RIPE-NCC-END-MNT
- mnt-routes: VVPN-MNT
- mnt-domains: VVPN-MNT
- created: 2009-10-12T11:34:50Z
- last-modified: 2015-05-05T02:16:11Z
- source: RIPE Filtered
- sponsoring-org: ORG-IL316-RIPE

Person Information:

- organisation: ORG-PESV2-RIPE
- org-name: PE Voronov Evgen Sergiyovich
- org-type: OTHER
- descr: PE Evgen Sergeevich Voronov
- address: 25 October street, 118-15
- address: Tiraspol, Transdnistria
- phone: +373 533 50404
- admin-c: ESV1-RIPE
- tech-c: ESV1-RIPE
- mnt-ref: VVPN-MNT
- mnt-by: VVPN-MNT
- created: 2009-07-24T18:52:57Z
- last-modified: 2010-01-12T19:38:04Z
- source: RIPE Filtered
- person: **Evgen Sergeevich Voronov**
- address: 25 October street, 118-15
- address: Tiraspol, Transdnistria
- phone: +373 533 50404
- nic-hdl: ESV1-RIPE
- mnt-by: VVPN-MNT
- created: 2009-07-24T18:52:56Z
- last-modified: 2010-01-12T19:38:04Z
- source: RIPE Filtered

The right sidebar contains an advertisement for the Samsung Galaxy Tab S, featuring the text "with the Galaxy Tab S" and a "Find out more" button.

There is pretty lot of information. IP is registered to the organisation PE Voronov Evgen Segiyovich, registrant is *Evgeny Sergeevich Voronov* who basically is a [Russian basketball player](#) (plays in national team as well). Address and phone number are from Tiraspol in eastern Moldova. I googled for PE Voronov Evgen Segiyovich and found also following information:



Summary for as49934

The Autonomous System (AS) number **49934** is assigned to **PE Voronov Evgen Sergiyovich**. AS49934 is assigned on **2009-10-14** by the Regional Internet Registry **ripe**. The country of registration is **Ukraine**. At least **129 domains** are hosted on AS49934. Examples of domains are androidam.org and droidofile.com. **No name servers** are hosted on AS49934. There is **one IPv4 prefix** announced by AS49934. This prefix is 193.104.41.0/24. There are **no IPv6 prefixes** announced by AS49934. AS49934 does not have any bogon prefixes.

General information

AS number	49934
Alias	AS49934, ASN49934
Organization	PE Voronov Evgen Sergiyovich
Country	Ukraine (UA) 
Regional Internet Registry (RIR)	ripe
Allocation or assignment date	2009-10-14
Number of IPs originated (v4)	256
ASRank (based on number of IPs)	46,753
Number of IPv4 prefixes	1
Number of IPv6 prefixes	0
AS has bogon prefixes	No
Number of IPv4 peers	2
Number of IPv6 peers	0

Hosting information

Number of domains hosted	129
Number of adult domains hosted	2
Number of name servers hosted	0
Number of SPAM hosts hosted	8
Number of open proxies hosted	0
Number of mail servers hosted	8

Prefixes IPv4

Prefix	Country	Description
193.104.41.0/24	MD 	PE Voronov Evgen Sergiyovich

Prefixes IPv6

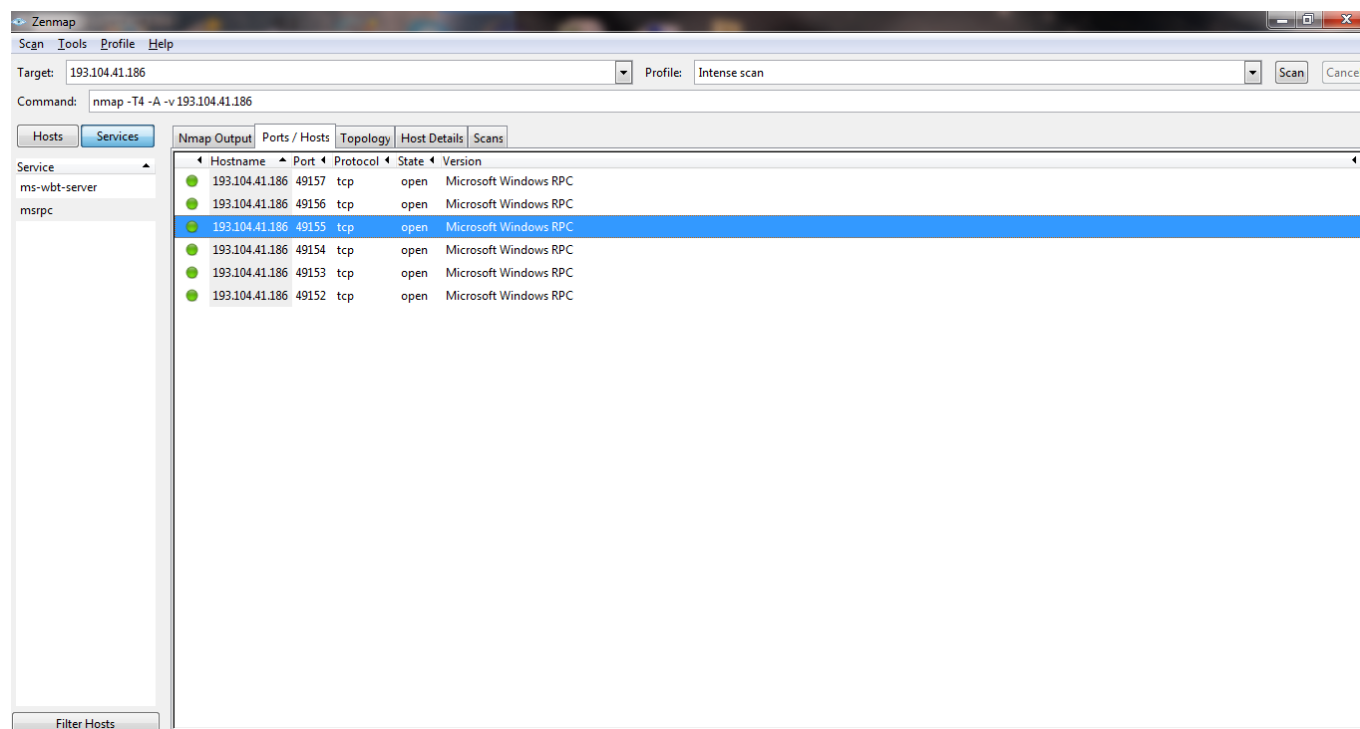
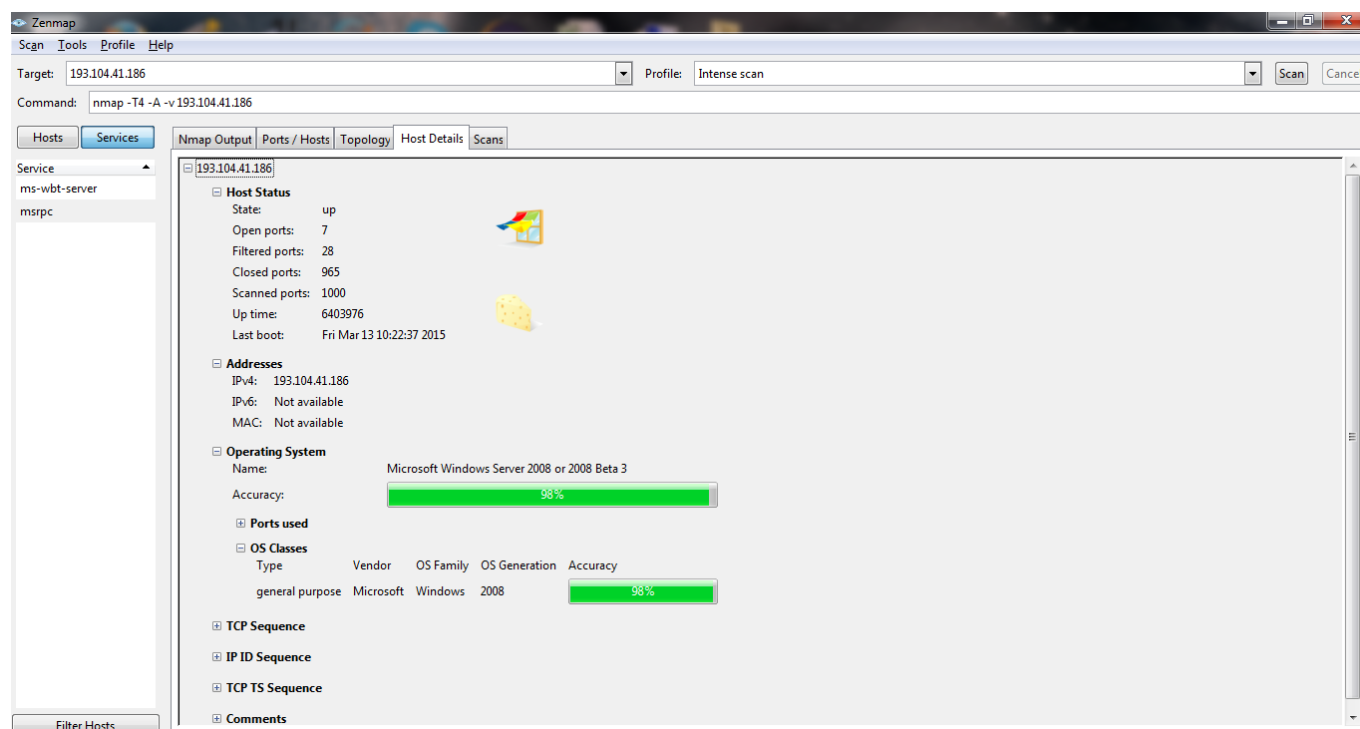
No IPv6 prefixes defined. AS49934 is not IPv6 ready.

IP address mathes subnetwork. I also had similar attack, with different registrant from Ukraine... so might be connected. However, I am not sure and not really sure how to find out. However, this AS is registered to some organisation. It does not looks like they would be malicious as a whole. I had to look deeper. I runned nmap on the IP address.

What I found is in the following pictures:

Chasing script-kiddies and hackers on my blog - 05-26-2015

by Nikola Milošević - <https://inspiratron.org>



So basically machine attack happened from is Windows Server 2008 with open ports for Remote Procedure Calls. Windows Remote Procedure Calls were vulnerable to couple of exploits. Here is an example of [exploit](#).

I would conclude that this attack was done from this machine, which was pwned by the attacker. Maybe he even uses some script that just

probes different wordpress sites. However, I decided not to go deeper and try to get access to machine from which was attack performed in order to know more about execution. So it looked like a dead end for my passive forensics ability. I just blocked these IPs. However, if you know more on IP level forensics and how can I know more about attacker, please let me know and leave a comment.

All rights reserved and copyrighted by inspiratron.org and Nikola Milosevic