If you run an independent news blog or are a "Citizen Journalist" here is who will attack you and how they will do it.\

Huge Increase in Brute Force Attacks in December and What to Do

This entry was posted in General Security, Wordfence, WordPress Security on December 16, 2016 by mark 61 Replies

At Wordfence we constantly monitor the WordPress attack landscape in real-time. Three weeks ago, on November 24th, we started seeing a rise in brute force attacks. As a reminder, a brute force attack is one that tries to guess your username and password to sign into your WordPress website.

In today's post we show you how attacks have increased during the past 3 weeks and share some data about where attacks are originating from.

First: How to protect yourself from these attacks

Brute force attacks are unsophisticated. They are simple password guessing attacks. A machine will automatically try to sign into your website over and over in the hope that it can guess your password.

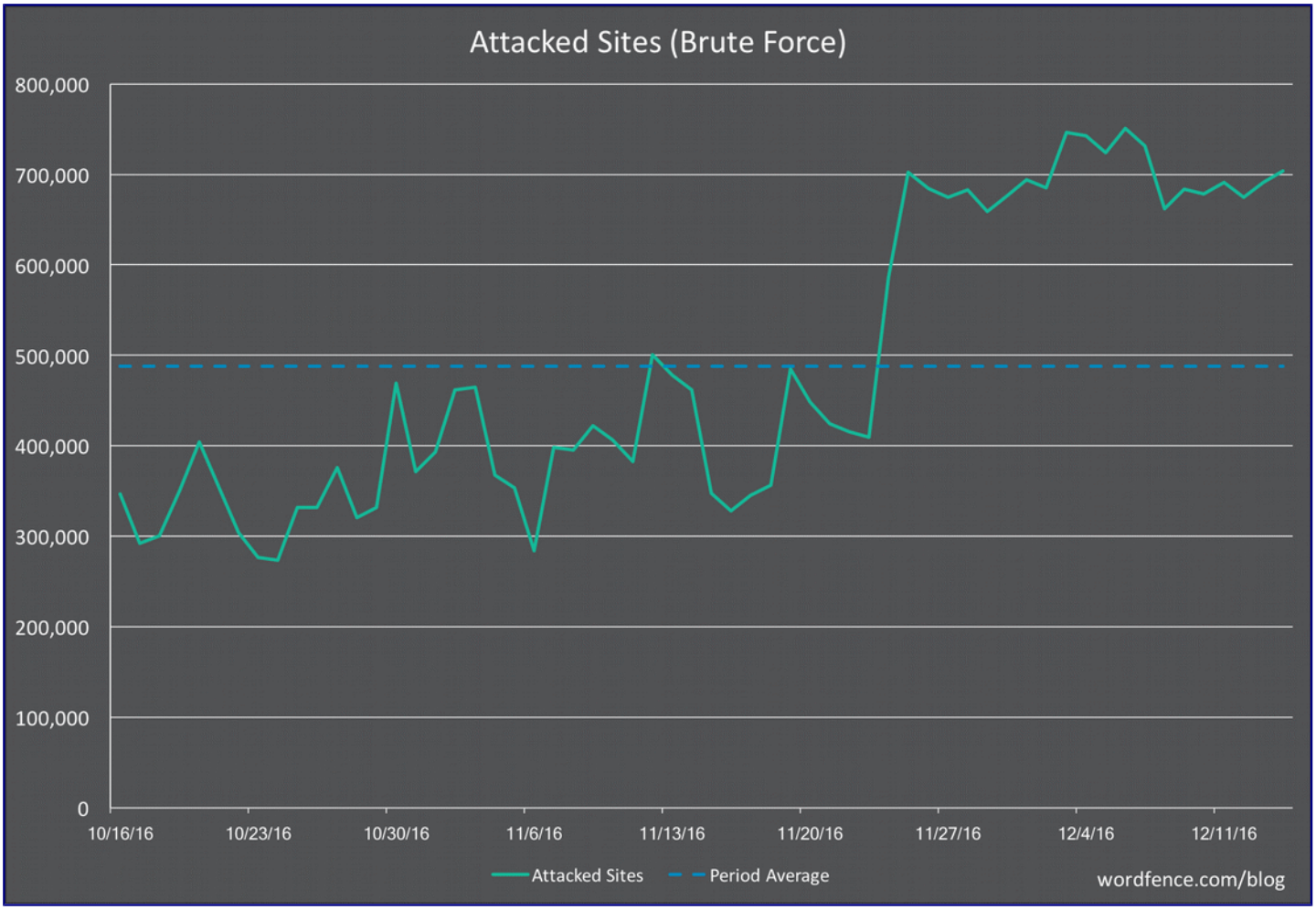
If you install the free version of Wordfence, you are automatically protected against brute force attacks. It's that simple. We also automatically block the worst offenders completely, and we share some information below on who those are.

We have a few other really cool options, like preventing username discovery and immediately locking out invalid usernames. All these techniques help protect you against brute force attacks.

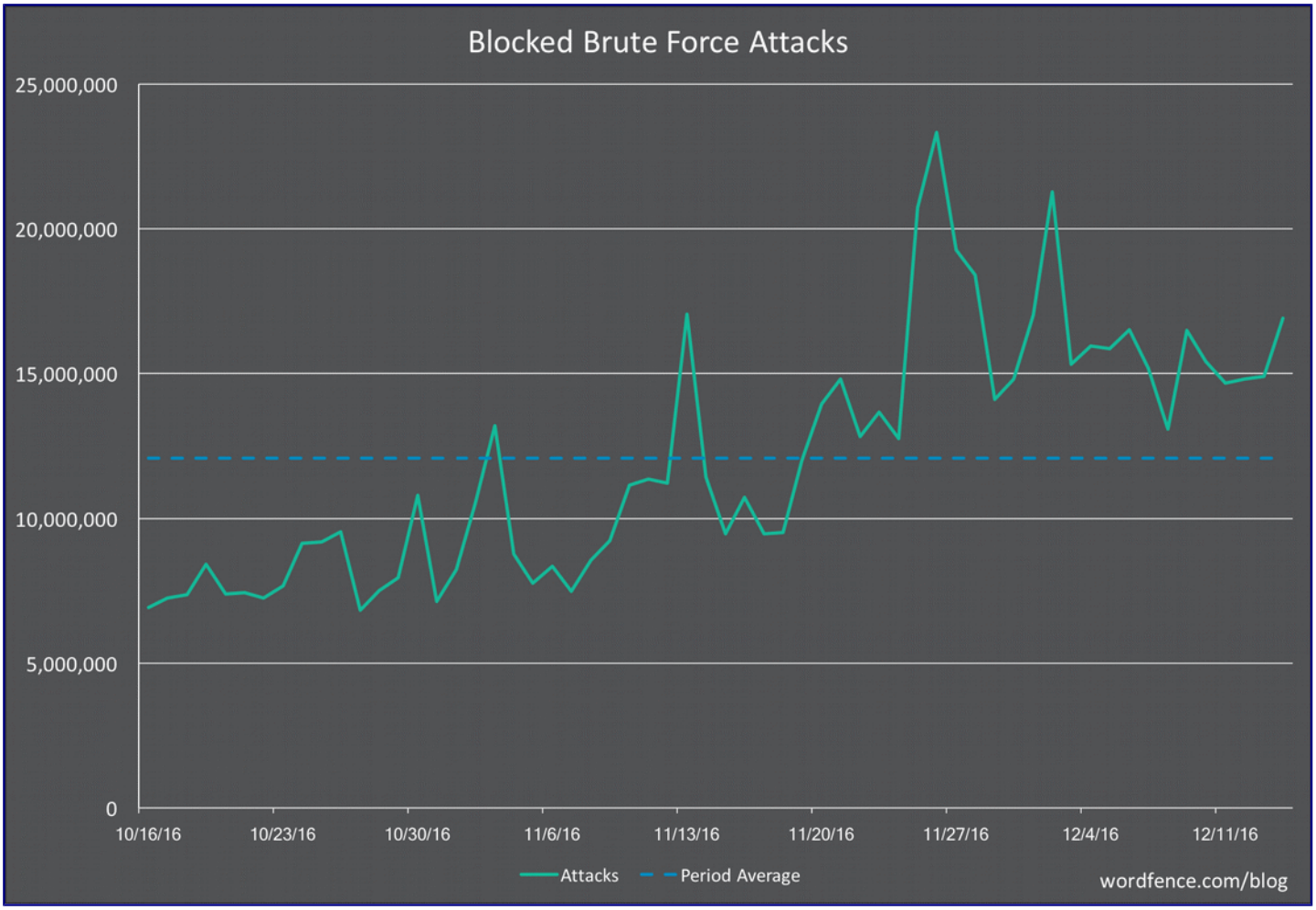
Download and install the free version of Wordfence today to get instant protection against brute-force attacks.

A sustained increase in Brute Force WordPress Attacks

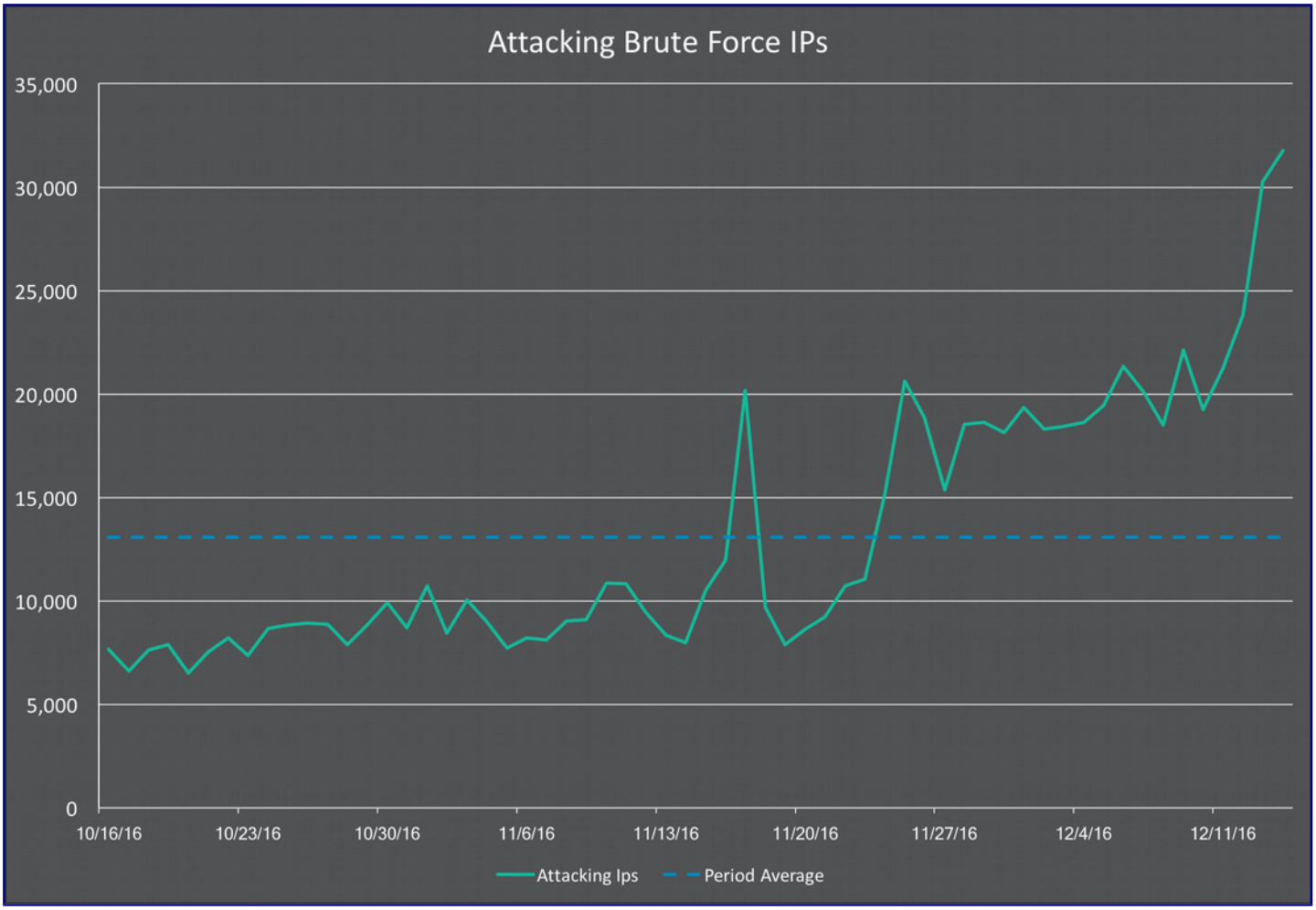
During the past three weeks we have seen the **number of sites attacked** each day almost double. The dotted blue line indicates the average number of attacked sites for the 60 days shown. The charts below show attack patterns over the past 2 months.



We have observed the **number of brute force attacks blocked** increase significantly above our 60 day average.



And what most concerns us is that we have seen a rise in **unique IP addresses that are attacking WordPress websites** per day. This rise started on November 24th and has spiked significantly during the past week.



This has now increased far above our baseline. Usually we see an average of around 13,000 unique IP's attacking each day. We're currently seeing over 30,000 unique attacking IPs and this is continuing to increase.

Who is Brute Force Attacking WordPress sites?

The charts above show data for the past two months. We then analyzed attacks during the past 24 hours to see who is currently attacking WordPress sites.

The following table shows the top 20 countries sorted by attacks during the past 24 hours. As you can see, Ukraine is by far the main culprit, responsible for over 15% of total attacks. That is a lot when you consider that the population of Ukraine is only 45 million people.

countryName	totalAttacks	percentage
Ukraine	2349087	15.7%
France	1663554	11.1%
Russia	1016810	6.8%
United States	991529	6.6%
India	874440	5.8%
China	638020	4.2%
Germany	482269	3.2%
Italy	367162	2.4%
United Kingdom	331594	2.2%
Japan	310467	2.0%
Indonesia	295746	1.9%
Brazil	272819	1.8%
Republic of Korea	260668	1.7%
Poland	203052	1.3%
Romania	202120	1.3%
Canada	184237	1.2%
Turkey	183994	1.2%
Pakistan	178648	1.1%
Philippines	177972	1.1%
Malaysia	171361	1.1%

Most of the attacks come from 8 IP addresses in Ukraine.

IP	attacks	hostname	asNumber	Organization	countryName
91.200.12.18	271160	kehuqyuda.com	35804	Pp Sks-lugan	Ukraine
91.200.12.42	229631	wangzhanpaim0901.com	35804	Pp Sks-lugan	Ukraine
91.200.12.92	213829	kehu1101.com	35804	Pp Sks-lugan	Ukraine
91.200.12.81	187734	1030.2016.com	35804	Pp Sks-lugan	Ukraine
91.200.12.86	168090	huangdiqda0515.com	35804	Pp Sks-lugan	Ukraine
91.200.12.29	161644	a170786572.example.com	35804	Pp Sks-lugan	Ukraine
91.200.12.93	146310	huangdi0910.com	35804	Pp Sks-lugan	Ukraine
91.200.12.114	139835	a170786571.example.com	35804	Pp Sks-lugan	Ukraine

These IPs all belong to the same organization and are on the same network. Doing a Google search on the top IP brings back many reports of abuse around the Internet. They belong to a hosting company in Ukraine called “Pp Sks-lugan“. The servers are a mix. Some aren’t running any services. Others appear to be running Windows IIS web server.

These IPs are using brute force attacks exclusively. They don’t launch any sophisticated attacks. They are hammering away at WordPress sites at a rate of over a quarter million login attempts each, in some cases, during a 24 hour period.

When we add up attacks during the past 24 hours and group by the organization that owns the attacking IP address, you can really see the impact that the Ukrainian host is having.

Keep in mind that as you look at the data below, some organizations like GoDaddy are very large. They actually make up a large percentage of total WordPress sites on the Net. And so before you call out a hosting provider for being ‘insecure’, you should consider their size and that it takes the operations team at each hosting provider some time to respond to a hacked site and take it offline.

We also think the table below illustrates how most attacks originate from specific networks that are relatively obscure.

Organization	totalAttacks
Pp Sks-lugan	1650353
Iliad-Entreprises	959617
OVH SAS	372433
GoDaddy.com, LLC	329723
Korea Telecom	177553
BSNL	176991
China Unicom Liaoning	170729
NTT	170288
Leaseweb Deutschland GmbH	147776
FOP Tokarchuk Oleksandr Stepanovich	144322
Netplan Internet Solutions Ltd	140077
ISP Datasvit network	130866
HETZNER	126853
1&1 Internet AG	124294
PT Telkom Indonesia	120596
Kyivstar GSM	115879
ONLINE SAS	109892
TM Net	108601
Philippine Long Distance Telephone	104639
Telecom Algeria	103079
Bharti Airtel	94721
NTT America	82062
OVH Srl	78463
Rostelecom	77128
PTCL	77016
OVH Hosting	75805
China Telecom	73769
Telekom Srbija	71902
myLoc managed IT AG	69754
BSNL Wimax	69426
Private Entrepreneur Shantyr Yuriy	69146
Reliance Communications	66562
Phoenix LLC	66315
TE Data	63893
Telecom Italia	63609
Cloudie Limited	63411
RCS & RDS Residential	63242
PE Tetyana Mysyk	55298
Emirates Telecommunications Corporation	55033
Comcast Cable	54454
Orange	54009
Turk Telekom	53026
Netvigator	52973
PT Jasa Utama Capital	51743
Fastweb	51133
SaudiNet	50482
Hangzhou Alibaba Advertising Co.,Ltd.	49796
Serbia BroadBand-Srpske Kablovske mreze d.o.o.	49061
Vietnam Posts and Telecommunications(VNPT)	48813
Oi Internet	48793

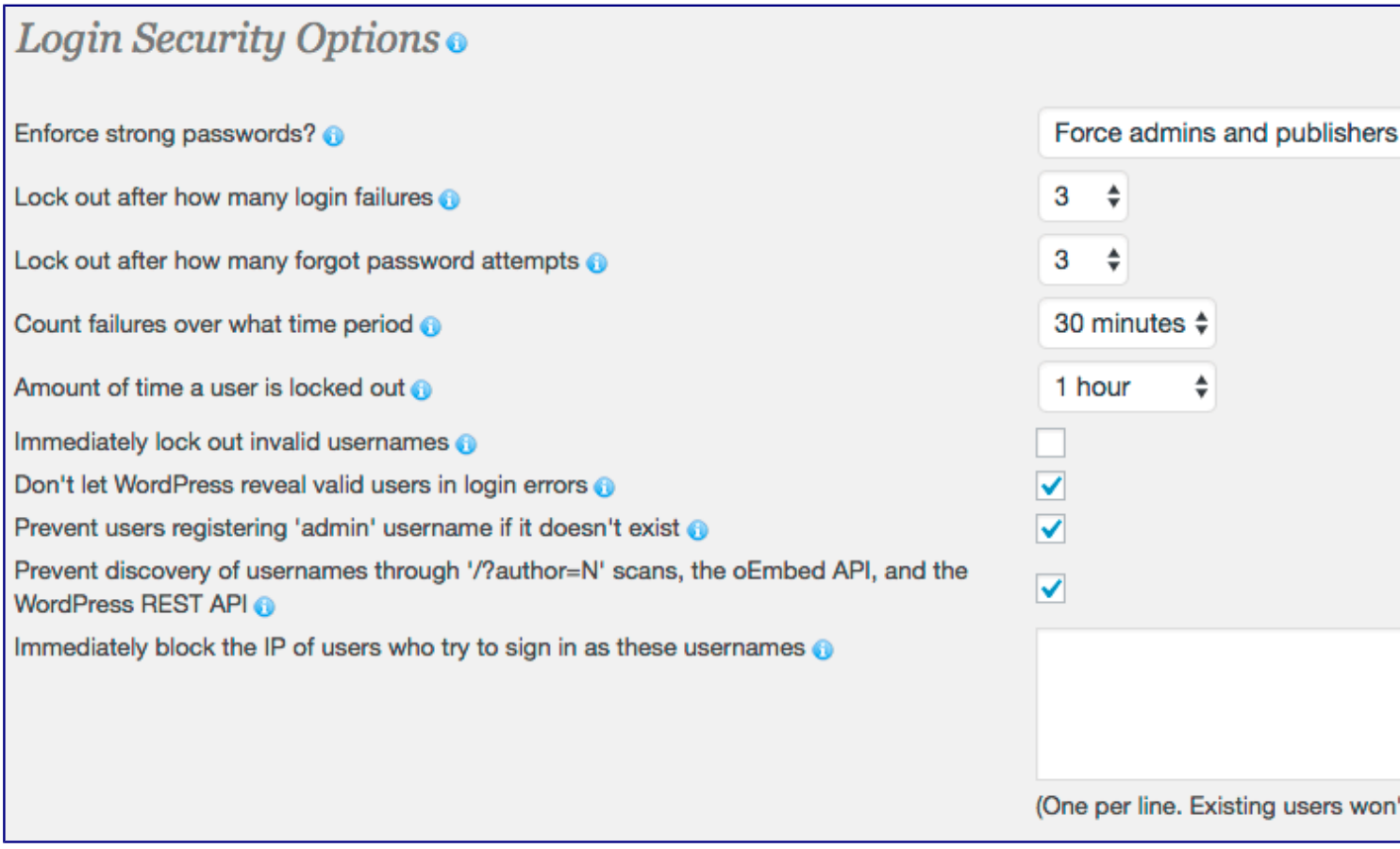
The top hosting provider is a tiny organization you've probably never heard of. But they're head and shoulders above most other companies on this list for the number of attacks that originate from their network.

The second company on the list, "Iliad-Entreprises", has 8 IP addresses in particular that launched between 50,000 and 210,000 attacks each during the past 24 hours. That is what makes up the bulk of the action on their network.

The difference between the top two networks and the network in third place is dramatic. OVH is a very large hosting provider, but we're seeing more than 4 times fewer attacks originating from their network than from the #1 Ukrainian host.

Lock it down and stay safe this holiday season

If you run a WordPress site, make sure you lock it down so that you can relax over the holiday season. Brute force attacks are easy to protect against if you have the right tools. I've included a screenshot below of the Wordfence Login Security options that give you an idea of the many different ways we stop brute force attacks in their tracks. Click for a larger image.



As always I would love to hear your feedback and comments below and will be around to respond.

Mark Maunder – Wordfence Founder/CEO