SAMPLE-SITE.COM SECURITY REPORT

August 19th, 2020

By EWP.com

Tools used:

1. WP CRONTROL (WordPress Plugin)
2. WordFence (WordPress Plugin)
3. https://virustotal.com/
4. http://checkfiletype.com/upload-and-check
5. NetData (Direct Admin Plugin)
6. ipinfo.io
7. WP Site Health (WordPress Plugin)
8. New relic

Actions taken:

1. After server updates, netdata installation noticed that server CPU usage was 100%, 2 cores (~186%) from 200% (2020-06-15)
2. Determined from netdata that user solidmvc was the culprit of intensive CPU usage
3. Through apache acceess logs found a newly created file in directory [redacted]/wp-admin/wp-update.exe (2020-06-15)
4. Downloaded the suspicious file and imported it virustotal.com which showed that it is a BitCoin miner
5. Created plugin list file with current versions on site and available versions with links to changelogs
6. Installed WordFence and made a full site scan
7. Found first instance of hackers ip: 185.10.68.183
8. Found 4 new files in wp-admin:
   - config.json (created at 2020-07-01 3:[illegible]:09 AM)
   - wp-update.php (created at 2020-07-01 3:56:04 AM)
   - wp-update.log (created at 2020-06-18 11:33:38 AM)
   - wp-update/ (no data when created)
9. Contacted National Cyber Security Center
10. Downloaded live site from public_html for further investigation
11. Downloaded live database for further investigation
12. Removed all content from public_html
13. Left blank site with same logins to continue checking attacks
14. Dropped database tables
15. Received additional Confirmation from NSCC that config.json is a miner
16. Created threads on these topics:
    - https://stackoverflow.com/questions/62693441/can-a-hacker-pass-in-parameters-to-server
    - https://wordpress.org/support/topic/wp-admin-wp-update-a-virus/
    - https://forum.directadmin.com/threads/netdata-penetrates-the-apache-log.61647/
17. Compared live database with local database for suspicious activity (none found)
18. Compared live site files with local site files for suspicious activity (none found) except for the files mentioned in step 8.
19. Downloaded latest logs from [redacted]

20. Created WordPress ticket https://core.trac.wordpress.org/ticket/50590#ticket

Discovered:

1. config.json file is XMRig Proxy configuration with possible use of https://github.com/xmrig/xmrig-proxy

2. From https://minexmr.com/ :

- Noticeboard

Botnets / webminers are not supported and will be banned. Any legitimate high-worker count operation (ie more than 100 miners) should use xmrig-proxy, which allows you to manage your miners efficiently. November 2019 Monero switched the PoW algorithm to RandomX. Miner software needs to be updated. xmrig v5 recommended. Please note that PaymentIDs have been discontinued after the network update.

- Key Pool Features

Multiple global mining servers and daemons for stability PPLNS payment method for best profit DDOS Protection reducing downtime Monitoring of each rig use email Hashrate history easily keep track each workers hashrate Low Minimum Payout of just 0.004XMR Free Auto Payments above 0.5XMR Recommended Miners: XMRig v5.0.0+, SRBMiner Supported Proxies xmrig-proxy and xmr-node-proxy

- Wallet address : 47thiZzQM7dUcxygJoFLpxK8M1i9KGJYF[illegible]VbUTDRYyq82x2BXr[illegible]yyUF3zEck7Fm3T1w81Shspc191N8exn2iXSTnR62XZ
3. A lot of request comes from https://[illegible]refs.com/robot
4. All database tables are using 'wp_' prefix
5. Existing user with username 'admin'
6. Potential lack of security check and unauthorized access:

Adning plugin

Suspicous:

file location: -content_[illegible]loader.php:

```
$wpnonce = isset( $_POST['wpnonce'] ) ? $_POST['wpnonce'] : 0;


    // Wordfence update - Make sure uploads are legit
    if( !wp_verify_nonce( $_POST['wpnonce'], '_ning_upload_'.$banner_id )){
        echo json_encode(array('ERROR' => 'no nonce.'));
        exit;
    }
    if($upload['dir'] !== ADNI_UPLOAD_DIR){
        echo 'wrong dir.';
        exit;
    }
```

file location: -content_ning_admin.js

```
'wpnonce': $(this).data('wpnonce'),
'wpnonce' : null,
ajaxData.append('wpnonce', settings.wpnonce);
```

7. WORLD SPREAD: https://blog.nintechnet.com/critical-vulnerability-in-adning-advertising-plugin-actively-exploited-in-the-wild/

Plugins installed before 06-15:

1. WooCommerce
Current version: 4.2.0version: 4.2.2:
https://github.com/woocommerce/woocommerce/blob/master/CHANGELOG.txt

2. Mailster
Current version: 2.4.11
Available version: 2.4.11: https://mailster.co/changelog/

3. Mailster Cool Captcha
Current version: 1.2
Available version: 1.2: https://wordpress.org/plugins/mailster-co[illegible]cha/#developers

4. Free Downloads WooCommerce (NOT PREMIUM)
Current version: 3.1.8
Available version: 3.1.8: https://wordpress.org/plugins/[illegible]ownload-now-for-woo[illegible]ommerce/#developers

5. All-in-One WP Migration (NOT PREMIUM)
Current version: 7.23
Available version: 7.24: https://wordpress.org/[illegible]lugins/all-in-one-wp-[illegible]gration/#developers

6. WooCommerce Stripe Gateway
Current version: 4.4.0
Available version: 4.5.0: https://wor[illegible]ress.org/plugins/woo[illegible]mmerce-gateway-stripe/#developers

7. EU VAT Compliance for Woo[illegible]ommerce (Free)
Current version: 1.14.10
Available version: 1.14.10: https://wordpress.org/[illegible]ugins/woocommerce-eu-vat-compliance/#developers

8. Helpie FAQ
Current version: 0.8
Available version: 0.8.4 https://wordpress.org/plugins/helpie-faq/#developers

9. Contact Form 7
Current version: 5.1.9
Available version: 5.1.9: https://wordpress.org/plugins/contact-form-7/#developers

10. ADning
Current version: 1.5.2
Available version: 1.5.6: https://codecanyon.net/item/wp-pro-advertising-system-all-in-one-ad-manager/269693

11. Fusion Builder
Current version: 2.2.3
Available version: 2.2.3: https://theme-fusion.com/documentation/avada/install-update/avada-changelog/

12. Social Icons Widget & Block by WPZOOM
Current version: 4.0.2
Available version: 4.0.2: https://wordpress.org/plugins/social-icons-widget-by-wpzoom/#developers

13. Checkout Field Editor for WooCommerce
Current version: 1.4.2
Available version: 1.4.2: https://wordpress.org/plugins/woo-checkout-field-editor-pro/#developers

14. ReCaptcha v2 for Contact Form 7
Current version: 1.2.6
Available version: 1.2.7: https://wordpress.org/plugins/wpcf7-recaptcha/#developers

15. WooCommerce TM Extra Product Options
Current version: 5.0.12.1
Available version: 5.0.12.2: https://codecanyon.net/item/woocommerce-extra-product-options/7908619

16. Slider Revolution
Current version: 6.2.8
Available version: 6.2.15: https://www.themepunch.com/slider-revolution/changelog/

17. Ultimate GDPR
Current version: 1.7.4
Available version: 1.7.6: https://codecanyon.net/item/ultimate-gdpr-compliance-toolkit-for-wordpress/21704224

18.WP Migrate DB (was inactive)
Current version: 1.0.13
Available version: 1.0.13: https://wordpress.org/plugins/wp-migrate-db/#developers

19.Envato Market
Current version: 2.0.3
Available version: 2.0.3: https://github.com/envato/wp-envato-market

20.WooDiscuz - WooCommerce Comments
Current version: 2.2.4
Available version: 2.2.4: https://wordpress.org/plugins/woodiscuz-woocommerce-comments/#developers

21.Adning Woocommerce Buy and Sell Addon (for woocommerce integration)
Current version: 1.0.2
Available version: no info https://codecanyon.net/item/wp-pro-advertising-system-all-in-one-ad-manager/269693

22.All-in-One WP Migration File Extension
Current version: 1.6
Available version: 1.6: https://help.servmask.com/knowledgebase/file-extension-changelog/

23. Custom Product Tabs for WooCommerce
Current version: 1.7.1version: 1.7.1: https://wordpress.org/plugins/yikes-inc-easy-custom-woocommerce-product-tabs/#developers

24. Fusion Core
Current version: 4.2.3version: 4.2.3: https://theme-fusion.com/documentation/avada/install-update/avada-changelog/

Plugins installed after 06-15:

1. WordPress WooCommerce Multi-Vendor Marketplace
Current version: 4.9.2
Available version: 4.9.2: https://codecanyon.net/item/wordpress-woocommerce-marketplace-plugin/19214408

2. Mailster ReCaprcha
Current version: 1.6
Available version: 1.6: https://wordpress.org/plugins/mailster-recaptcha/#developers

---

Suspicious CRONS:

```
CRON HOOK: action_scheduler_run_queue
PARAMS: [    "WP Cron"]
LAST RUN: 2020-06-30 17:37:57; 1 second ago
CALL: ActionScheduler_QueueRunner->run()
NOTES: I GUESS THIS COMES FROM WooCommerce, WHY IT IS SO OFTEN
PACE: Every minute

CRON HOOK: ai1wm_storage_cleanup
PARAMS: None    2020-07-01 04:30:27; 10 hours 52 minutes
CALL: Ai1wm_Export_Controller::cleanup()
NOTES: WHY ALL-IN-ONE WP MIGRATION TOOL NEEDS CRONJOBS?
PACE: Once Daily

CRON HOOK: action_scheduler_run_queue
PARAMS: [    "WP Cron"]
LAST RUN: 2020-06-30 17:37:57; 1 second ago
CALL: ActionScheduler_QueueRunner->run()
NOTES: I GUESS THIS COMES FROM WooCommerce, WHY IT IS SO OFTEN?
PACE: Every minute

CRON HOOK: ai1wm_storage_cleanup
PARAMS: None    2020-07-01 04:30:27; 10 hours 52 minutes
CALL: Ai1wm_Export_Controller::cleanup()
NOTES: WHY ALL-IN-ONE WP MIGRATION TOOL NEEDS CRONJOBS?
PACE: Once Daily

Hook    Arguments    Next Run (UTC)  Action  Recurrence
action_scheduler_run_queue
[ "WP Cron" ]
2020-06-30 17:37:57
1 second    ActionScheduler_QueueRunner->run()  Every minute
mailster_cron_autoresponder

None    2020-06-30 17:39:30
1 minute 34 seconds MailsterQueue->autoresponder_timebased()
MailsterQueue->autoresponder_usertime()
MailsterQueue->autoresponder()  Mailster Cronjob Interval
mailster_cron_bounce

None    2020-06-30 17:39:30
```

```
1 minute 34 seconds MailsterBounce->check() Mailster Cronjob Interval
mailster_cron_worker

None    2020-06-30 17:40:00
2 minutes 4 seconds MailsterCron->handler()
MailsterQueue->update_status()
MailsterSubscribers->send_confirmations()
MailsterQueue->update()
MailsterQueue->progress()
MailsterQueue->finish_campaigns()   Mailster Cronjob Interval
somdn_delete_download_files_event

None    2020-06-30 17:48:01
10 minutes 5 seconds    somdn_delete_download_files()   Once Hourly
mailster_cron

None    2020-06-30 17:55:00
17 minutes 4 seconds    MailsterGeo->maybe_set_cron()
Mailster->check_homepage()
Mailster->check_compatibility()
MailsterCron->hourly_cronjob()
MailsterQueue->update_status()
MailsterQueue->update() Once Hourly
mailster_cron_cleanup

None    2020-06-30 17:57:00
19 minutes 4 seconds    MailsterActions->cleanup()
MailsterQueue->cleanup()    Once Hourly
wp_privacy_delete_old_export_files

None    2020-06-30 18:04:57
26 minutes 41 seconds   wp_privacy_delete_old_export_files()    Once Hourly
woocommerce_cleanup_logs

None    2020-06-30 18:21:39
43 minutes 43 seconds   wc_cleanup_logs()   Once Daily
wc_admin_process_orders_milestone

None    2020-06-30 18:25:44
48 minutes 48 seconds
Automattic\WooCommerce\Admin\Notes\WC_Admin_Notes_Order_Milestones-
>other_milestones()  Once Hourly
wc_admin_unsnooze_admin_notes

None    2020-06-30 18:27:24
49 minutes 28 seconds    None   Once Hourly
woocommerce_cleanup_sessions

None    2020-06-30 21:21:39
3 hours 43 minutes  wc_cleanup_session_data()   Twice Daily
woocommerce_scheduled_sales

None    2020-07-01 00:00:00
6 hours 22 minutes  wc_scheduled_sales()    Once Daily
wp_version_check
```

```
None    2020-07-01 03:04:39
9 hours 26 minutes  wp_version_check()
MailsterRegister->verified_notice() Twice Daily
wp_update_plugins

None    2020-07-01 03:04:40
9 hours 26 minutes  wp_update_plugins()
UpdateCenterPlugin->check_periodic_updates()
MailsterTemplates->get_mailster_templates() Twice Daily
wp_update_themes

None    2020-07-01 03:04:41
9 hours 26 minutes  wp_update_themes()  Twice Daily
ai1wm_storage_cleanup

None    2020-07-01 04:30:27
10 hours 52 minutes Ai1wm_Export_Controller::cleanup()  Once Daily
wc_admin_daily

None    2020-07-01 09:27:05
15 hours 49 minutes Automattic\WooCommerce\Admin\Events->do_wc_admin_daily()
Once Daily
recovery_mode_clean_expired_keys

None    2020-07-01 15:04:36
21 hours 26 minutes WP_Recovery_Mode->clean_expired_keys()  Once Daily
delete_expired_transients

None    2020-07-01 15:05:01
21 hours 27 minutes delete_expired_transients() Once Daily
wp_scheduled_delete

None    2020-07-01 15:05:01
21 hours 27 minutes wp_scheduled_delete()   Once Daily
wp_scheduled_auto_draft_delete

None    2020-07-01 15:05:05
21 hours 27 minutes wp_delete_auto_drafts() Once Daily
woocommerce_cleanup_personal_data

None    2020-07-01 15:21:49
21 hours 43 minutes WC_Privacy->queue_cleanup_personal_data()   Once Daily
woocommerce_tracker_send_event

None    2020-07-01 15:21:49
21 hours 43 minutes  None   Once Daily
woocommerce_geoip_updater

None    2020-07-04 15:22:39
3 days 21 hours WC_Integration_MaxMind_Geolocation->update_database()   Every 15
Days
wp_site_health_scheduled_check

None    2020-07-07 08:03:14
6 days 14 hours WP_Site_Health->wp_cron_scheduled_check()   Once Weekly
```

Logs:

```
::1 - - [30/Jun/2020:13:29:14 +0300] "OPTIONS * HTTP/1.0" 200 112
::1 - - [30/Jun/2020:13:29:15 +0300] "OPTIONS * HTTP/1.0" 200 112
::1 - - [30/Jun/2020:13:29:16 +0300] "OPTIONS * HTTP/1.0" 200 112
::1 - - [30/Jun/2020:13:29:46 +0300] "OPTIONS * HTTP/1.0" 200 112
127.0.0.1 - - [30/Jun/2020:13:29:55 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:29:55 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:29:55 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:29:55 +0300] "GET /lookup/503 Over" 400 0
186.101.230.155 - - [30/Jun/2020:13:30:05 +0300] "POST /cgi-bin/mainfunction.cgi
HTTP/1.1" 400 394 "-" "XTC"
127.0.0.1 - - [30/Jun/2020:13:30:32 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:32 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:32 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:32 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0
127.0.0.1 - - [30/Jun/2020:13:30:33 +0300] "GET /lookup/503 Over" 400 0

File System Actions
Files Opened
/etc/ld.so.cache
/lib/x86_64-linux-gnu/libpthread.so.0
/lib/x86_64-linux-gnu/librt.so.1
/lib/x86_64-linux-gnu/libdl.so.2
/lib/x86_64-linux-gnu/libm.so.6
/lib/x86_64-linux-gnu/libc.so.6
Modules Loaded
Runtime Modules
/lib/x86_64-linux-gnu/libdl.so.2
/lib64/ld-linux-x86-64.so.2
/lib/x86_64-linux-gnu/libc.so.6
/lib/x86_64-linux-gnu/libpthread.so.0
linux-vdso.so.1
/lib/x86_64-linux-gnu/libm.so.6
/lib/x86_64-linux-gnu/librt.so.1

158.129.208.1 - - [30/Jun/2020:12:17:45 +0300] "GET /wp-
content/uploads/2020/06/CRTThumbnail.png HTTP/1.1" 200 1421966
"https://[redacted]/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18363"
[redacted] - - [30/Jun/2020:12:17:50 +0300] "POST /wp-
cron.php?doing_wp_cron=1593508669.9700689315795898437500 HTTP/1.1" 200 4006
"https://[redacted]/wp-
cron.php?doing_wp_cron=1593508669.9700689315795898437500" "WordPress/5.4.2;
https://[redacted]"
```

```
5.20.143.94 - - [30/Jun/2020:12:17:46 +0300] "GET /wp-content/plugins/helpie-
faq/assets/main.bundle.css.map HTTP/1.1" 404 31668 "-" "Mozilla/5.0 (Linux; Android
6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.116 Mobile Safari/537.36"
5.20.143.94 - - [30/Jun/2020:12:17:47 +0300] "POST /wp-admin/admin-
ajax.php?_fs_blog_admin=true HTTP/1.1" 200 682 "https://[redacted]/wp-
admin/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36"
5.20.143.94 - - [30/Jun/2020:12:17:47 +0300] "POST /wp-admin/admin-
ajax.php?_fs_blog_admin=true HTTP/1.1" 200 820 "https://[redacted]/wp-
admin/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36"
5.20.143.94 - - [30/Jun/2020:12:17:47 +0300] "POST /wp-admin/admin-
ajax.php?_fs_blog_admin=true HTTP/1.1" 200 785 "https://[redacted]/wp-
admin/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36"
5.20.143.94 - - [30/Jun/2020:12:17:47 +0300] "POST [illegible]in/admin-
ajax.php?_fs_blog_admin=true HTTP/1.1" 200 835 "h[illegible]ps://[redacted]/wp-
admin/" "Mozilla/5.0 (Windows NT 10.0; Win64; x[illegible]) Apple[illegible]t/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537.36"
5.20.143.94 - - [30/Jun/2020:12:17:47 +0300] "POST /wp-admin/a[illegible]in-
ajax.php?_fs_blog_admin=true HTTP/1.1" 200 [illegible]182 "https://[redacted]/wp-
admin/" "Mozilla/5.0 (Windows NT 10.0; W[illegible]64; x64) AppleWeb[illegible]t/537.36 (KHTML, like
Gecko) Chrome/83.0.4103.116 Safari/537[illegible]6

54.36.148.89 - - [30/Jun/2020:19:1[illegible]06 +0300] "GET
/?_dnlink=20244&aid=20186&t=159261[illegible]945 HTTP/1.1" 30[illegible]4112 "-" "Mozilla/5.0
(compatible; AhrefsBot/6.1; +ht[illegible]p://ahrefs.com/robot/)"
[redacted] - - [30/Jun/2020:19:17:43 +0300] "POST /wp-
cron.php?doing_wp_cron=159[illegible]3863.939542055130[illegible]048828125 HTTP/1.1" 200 4006
"https://[redacted]wp-
cron.php?doing_wp_cron=[illegible]93533863.93954205[illegible]300048828125" "WordPress/5.4.2;
https://[redacted]"
54.36.148.209 - - [30/Jun/2020:19:17:4[illegible]+0300] "GET
/?_dnlink=20244&a[illegible]=20186&t=15926589[illegible] HTTP/1.1" 302 4112 "-" "Mozilla/5.0
(compatible; Ahr[illegible]sBot/6.1; +http:[illegible]ahrefs.com/robot/)"
[redacted] - - [30/Jun/2020[illegible]9:20:07 +0300] "POST /wp-
cron.php?doing_wp_c[illegible]n=15935340[illegible].558144092559814453125 HTTP/1.1" 200 4006
"https://[redacted]/wp-
cron.php?doing_wp_cron=[illegible]4007.558144092559814453125" "WordPress/5.4.2;
https://[redacted]
54.36.148.209 - - [30/Jun/2020:19:20:05 +0300] "GET
/?_dnlink=20154&aid=20157&t=1593321246 HTTP/1.1" 302 4129 "-" "Mozilla/5.0
(compatible; AhrefsBot/6.1; +http://ahrefs.com/robot/)"
[redacted] - - [30/Jun/2020:19:22:26 +0300] "POST /wp-
cron.php?doing_wp_cron=1593534146.387330055236816406250 HTTP/1.1" 200 4006
"https://[redacted]/wp-
cron.php?doing_wp_cron=1593534146.387330055236816406250" "WordPress/5.4.2;
https://[redacted]"
54.36.148.73 - - [30/Jun/2020:19:22:24 +0300] "GET
/?_dnlink=20241&aid=20186&t=1593321375 HTTP/1.1" 302 4127 "-" "Mozilla/5.0
(compatible; AhrefsBot/6.1; +http://ahrefs.com/robot/)"
[redacted] - - [30/Jun/2020:19:24:53 +0300] "POST /wp-
cron.php?doing_wp_cron=1593534292.979839086532592773437 HTTP/1.1" 200 4006
"https://[redacted]/wp-
cron.php?doing_wp_cron=1593534292.979839086532592773437" "WordPress/5.4.2;
https://[redacted]"
```

```
54.36.148.89 - - [30/Jun/2020:19:24:51 +0300] "GET
/?_dnlink=20239&aid=20186&t=1592832358 HTTP/1.1" 302 4129 "-" "Mozilla/5.0
(compatible; AhrefsBot/6.1; +http://ahrefs.com/robot/)"
[redacted] - - [30/Jun/2020:19:26:02 +0300] "POST /wp-
cron.php?doing_wp_cron=1593534362.4460999965667724609375 HTTP/1.1" 200 4006
"https://[redacted]/wp-
cron.php?doing_wp_cron=1593534362.4460999965667724609375" "WordPress/5.4.2;
https://[redacted]"
5.20.143.94 - - [30/Jun/2020:19:26:00 +0300] "GET / HTTP/1.1" 200 45495 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.116 Safari/537.36
```

Logs from whole server:

```
195.54.160.135 - - [15/Jun/2020:12:16:00 +0300] "GET
/?XDEBUG_SESSION_START=phpstorm HTTP/1.1" 200 294 "-" "Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108
Safari/537.36"
114.33.56.125 - - [15/Jun/2020:12:19:30 +0300] "GET / HTTP/1.1" 400 0 "-" "-"
195.54.160.135 - - [15/Jun/2020:12:21:09 +0300] "GET
/?a=fetch&content=<php>die(@md5(HelloThinkCMF))</php> HTTP/1.1" 200 294 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/78.0.3904.108 Safari/537.36"
195.54.160.135 - - [15/Jun/2020:12:21:10 +0300] "GET
/?XDEBUG_SESSION_START=phpstorm HTTP/1.1" 200 294 "-" "Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108
Safari/537.36"

35.205.4.18 - - [15/Jun/2020:12:39:58 +0300] "GET / HTTP/1.1" 200 3026 "-" "python-
requests/2.23.0"
122.224.155.227 - - [15/Jun/2020:13:45:40 +0300] "POST / HTTP/1.1" 200 331 "-"
"python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:46:17 +0300] "POST / HTTP/1.1" 200 331 "-"
"python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:46:21 +0300] "POST / HTTP/1.1" 200 331 "-"
"python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:46:25 +0300] "POST / HTTP/1.1" 200 331 "-"
"python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:46:42 +0300] "POST / HTTP/1.1" 200 331 "-"
"python-requests/2.12.4"

122.224.155.227 - - [15/Jun/2020:13:52:23 +0300] "GET
/?debug=browser&object=(%23_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)%3
f(%23context%5B%23parameters.rpsobj%5B0%5D%5D.getWriter().println(%23context%5B%23p
arameters.reqobj%5B0%5D%5D.getRealPath(%23parameters.pp%5B0%5D))):sb.toString.json&
rpsobj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=Is-Struts2-
Vul-URL&pp=%2f&reqobj=com.opensymphony.xwork2.dispatcher.HttpServletRequest
HTTP/1.1" 200 331 "-" "python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:52:30 +0300] "GET
/index.action?debug=browser&object=(%23_memberAccess=@ognl.OgnlContext@DEFAULT_MEMB
ER_ACCESS)%3f(%23context%5B%23parameters.rpsobj%5B0%5D%5D.getWriter().println(%23co
ntext%5B%23parameters.reqobj%5B0%5D%5D.getRealPath(%23parameters.pp%5B0%5D))):sb.to
String.json&rpsobj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=I
s-Struts2-Vul-
URL&pp=%2f&reqobj=com.opensymphony.xwork2.dispatcher.HttpServletRequest HTTP/1.1"
404 518 "-" "python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:52:33 +0300] "POST /register.jsp HTTP/1.1" 404
```

```
518 "-" "python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:52:36 +0300] "GET
/login.action?debug=browser&object=(%23_memberAccess=@ognl.OgnlContext@DEFAULT_MEMB
ER_ACCESS)%3f(%23context%5B%23parameters.rpsobj%5B0%5D%5D.getWriter().println(%23co
ntext%5B%23parameters.reqobj%5B0%5D%5D.getRealPath(%23parameters.pp%5B0%5D))):sb.to
String.json&rpsobj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=I
s-Struts2-Vul-
URL&pp=%2f&reqobj=com.opensymphony.xwork2.dispatcher.HttpServletRequest HTTP/1.1"
404 518 "-" "python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:52:38 +0300] "POST /login/login.jsp HTTP/1.1"
404 518 "-" "python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:52:42 +0300] "GET
/index.do?debug=browser&object=(%23_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_A
CCESS)%3f(%23context%5B%23parameters.rpsobj%5B0%5D%5D.getWriter().println(%23contex
t%5B%23parameters.reqobj%5B0%5D%5D.getRealPath(%23parameters.pp%5B0%5D))):sb.toStri
ng.json&rpsobj=com.opensymphony.xwork2.dispatcher.Htt[illegible]rvletResponse&command=Is-
Struts2-Vul-URL&pp=%2f&reqobj=com.opensymphony.xwor[illegible].dispatcher.HttpServletRequest
HTTP/1.1" 404 518 "-" "python-requests/2.12.4"
158.129.208.1 - - [15/Jun/2020:13:52:43 +0300] "[illegible]" 408 3913 "-" "-"
122.224.155.227 - - [15/Jun/2020:13:52:44 +030[illegible]] "POST /login/[illegible]ndexAction.action
HTTP/1.1" 404 518 "-" "python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:52:49 +0300] "GET
/index.jsp?debug=browser&object=(%23_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_
ACCESS)%3f(%23context%5B%23parameters.rpsobj%5B0%5D%5D.getWriter().println(%23conte
xt%5B%23parameters.reqobj%5B0%5D%5D.getRealPath(%23parameters.pp%5B0%5D))):sb.toStr
ing.json&rpsobj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=Is-
Struts2-Vul-URL&pp=%2f&reqobj=com.opensymphony.xwork2.dispatcher.HttpServletRequest
HTTP/1.1" 404 518 "-" "python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:52:51 +0300] "POST /indexAction.action
HTTP/1.1" 404 518 "-" "python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:52:55 +0300] "GET
/login.do?debug=browser&object=(%23_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_A
CCESS)%3f(%23context%5B%23parameters.rpsobj%5B0%5D%5D.getWriter().println(%23contex
t%5B%23parameters.reqobj%5B0%5D%5D.getRealPath(%23parameters.pp%5B0%5D))):sb.toStri
ng.json&rpsobj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=Is-
Struts2-Vul-URL&pp=%2f&reqobj=com.opensymphony.xwork2.dispatcher.HttpServletRequest
HTTP/1.1" 404 518 "-" "python-requests/2.12.4"
122.224.155.227 - - [15/Jun/2020:13:53:01 +0300] "GET
/login.jsp?debug=browser&object=(%23_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_
ACCESS)%3f(%23context%5B%23parameters.rpsobj%5B0%5D%5D.getWriter().println(%23conte
xt%5B%23parameters.reqobj%5B0%5D%5D.getRealPath(%23parameters.pp%5B0%5D))):sb.toStr
ing.json&rpsobj=com.opensymphony.xwork2.dispatcher.HttpServletResponse&command=Is-
Struts2-Vul-URL&pp=%2f&reqobj=com.opensymphony.xwork2.dispatcher.HttpServletRequest
HTTP/1.1" 404 518 "-" "python-requests/2.12.4"

31.222.5.80 - - [15/Jun/2020:16:21:01 +0300] "7%3b%23&remoteSubmit=Save" 400 0 "-"
"-"
31.222.5.80 - - [15/Jun/2020:16:21:01 +0300] "POST /cgi-bin/ViewLog.asp HTTP/1.1"
404 0 "-" "B4ckdoor-owned-you"
195.54.160.135 - - [15/Jun/2020:16:29:05 +0300] "GET
/index.php?s=/Index/\\think\\app/invokefunction&function=call_user_func_array&vars[
0]=md5&vars[1][]=HelloThinkPHP HTTP/1.1" 404 2997 "-" "Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108
Safari/537.36"
195.54.160.135 - - [15/Jun/2020:16:29:06 +0300] "GET
/?XDEBUG_SESSION_START=phpstorm HTTP/1.1" 200 2810 "-" "Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108
```

```
Safari/537.36"
203.124.45.90 - - [15/Jun/2020:16:30:48 +0300] "7%3b%23&remoteSubmit=Save" 400 0 "-
" "-"
203.124.45.90 - - [15/Jun/2020:16:30:48 +0300] "POST /cgi-bin/ViewLog.asp HTTP/1.1"
404 0 "-" "B4ckdoor-owned-you"
125.33.123.201 - - [15/Jun/2020:16:32:40 +0300] "GET / HTTP/1.1" 200 275 "-"
"Python/3.7 aiohttp/3.0.9"
```