

[Full-Disclosure] Re: Online Script Decoder

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-12/0249.html>

From: Paul Szabo (psz_at_maths.usyd.edu.au)

Date: 12/07/04

To: full-disclosure@lists.netsys.com, security@greymagic.com

Date: Wed, 8 Dec 2004 06:20:06 +1100 (EST)

GreyMagic Security <security@greymagic.com> kindly made an online decoder available at

<http://www.greymagic.com/security/tools/decoder/>

On occasions it may be more useful to have a "local" decoder: I often use the following perl script.

Cheers,

Paul Szabo – psz@maths.usyd.edu.au <http://www.maths.usyd.edu.au:8000/u/psz/>
School of Mathematics and Statistics University of Sydney 2006 Australia

```
#!/usr/bin/perl -w --
```

```
# VBScript/JScript.Encode Decoder
```

```
# Based on Full-Disclosure message "VBScript/JScript.Encode Decoder"
```

```
# by Andreas Marx <amarx@gega-it.de>, dated 16 Sep 03
```

```
# http://lists.netsys.com/pipermail/full-disclosure/2003-September/010155.html
```

```
#
```

```
# See also:
```

```
# http://www.saltstorm.net/lib-soya/examples/Soya.Encode.ScriptDecoder.wbm
```

```
# http://www.saltstorm.net/lib-soya/Soya/Encode/ScriptDecoder.js
```

```
# http://www.virtualconspiracy.com/scrdec.html
```

```
# http://www.virtualconspiracy.com/download/scrdec14.c
```

```
# http://www.r4k.net/dec/dec.pl
```

```
@itab = ( # table order
```

```
0,2,1,0,2,1,2,1,1,2,1,2,0,1,2,1,
```

```
0,1,2,1,0,0,2,1,1,2,0,1,2,1,1,2,
```

```
0,0,1,2,1,2,1,0,1,0,0,2,1,0,1,2,
```

```
0,1,2,1,0,0,2,1,1,0,0,2,1,0,1,2);
```

```
@dectab0 = ( # tables to decrypt
```

```
"\x00", "\x01", "\x02", "\x03", "\x04", "\x05", "\x06", "\x07", "\x08", "\x57", "\x0A", "\x0B", "\x0C", "\x0D", "\x0E", "\x0F",
```

```
"\x10", "\x11", "\x12", "\x13", "\x14", "\x15", "\x16", "\x17", "\x18", "\x19", "\x1A", "\x1B", "\x1C", "\x1D", "\x1E", "\x1F",
```

Full-Disclosure: [Full-Disclosure] Re: Online Script Decoder

"\x2E", "\x47", "\x7A", "\x56", "\x42", "\x6A", "\x2F", "\x26", "\x49", "\x41", "\x34", "\x32", "\x5B", "\x76", "\x72", "\x43", "\x38", "\x39", "\x70", "\x45", "\x68", "\x71", "\x4F", "\x09", "\x62", "\x44", "\x23", "\x75", "\x3C", "\x7E", "\x3E", "\x5E", "\xFF", "\x77", "\x4A", "\x61", "\x5D", "\x22", "\x4B", "\x6F", "\x4E", "\x3B", "\x4C", "\x50", "\x67", "\x2A", "\x7D", "\x54", "\x2B", "\x2D", "\x2C", "\x30", "\x6E", "\x6B", "\x66", "\x35", "\x25", "\x21", "\x64", "\x4D", "\x52", "\x63", "\x31", "\x7B", "\x78", "\x29", "\x28", "\x73", "\x59", "\x33", "\x7F", "\x6D", "\x55", "\x53", "\x7C", "\x3A", "\x5F", "\x65", "\x46", "\x58", "\x31", "\x69", "\x6C", "\x5A", "\x48", "\x27", "\x5C", "\x3D", "\x24", "\x79", "\x37", "\x60", "\x51", "\x20", "\x36

@dectab1 = (

"\x00", "\x01", "\x02", "\x03", "\x04", "\x05", "\x06", "\x07", "\x08", "\x7B", "\x0A", "\x0B", "\x0C", "\x0D", "\x0E", "\x0F", "\x10", "\x11", "\x12", "\x13", "\x14", "\x15", "\x16", "\x17", "\x18", "\x19", "\x1A", "\x1B", "\x1C", "\x1D", "\x1E", "\x1F", "\x32", "\x30", "\x21", "\x29", "\x5B", "\x38", "\x33", "\x3D", "\x58", "\x3A", "\x35", "\x65", "\x39", "\x5C", "\x56", "\x73", "\x66", "\x4E", "\x45", "\x6B", "\x62", "\x59", "\x78", "\x5E", "\x7D", "\x4A", "\x6D", "\x71", "\x3C", "\x60", "\x3E", "\x5", "\xFF", "\x42", "\x27", "\x48", "\x72", "\x75", "\x31", "\x37", "\x4D", "\x52", "\x22", "\x54", "\x6A", "\x47", "\x64", "\x2D", "\x20", "\x7F", "\x2E", "\x4C", "\x5D", "\x7E", "\x6C", "\x6F", "\x79", "\x74", "\x43", "\x26", "\x76", "\x25", "\x24", "\x2E", "\x28", "\x23", "\x41", "\x34", "\x09", "\x2A", "\x44", "\x3F", "\x77", "\x3B", "\x55", "\x69", "\x61", "\x63", "\x50", "\x67", "\x51", "\x49", "\x4F", "\x46", "\x68", "\x7C", "\x36", "\x70", "\x6E", "\x7A", "\x2F", "\x5F", "\x4B", "\x5A", "\x2C", "\x5

@dectab2 = (

"\x00", "\x01", "\x02", "\x03", "\x04", "\x05", "\x06", "\x07", "\x08", "\x6E", "\x0A", "\x0B", "\x0C", "\x06", "\x0E", "\x0F", "\x10", "\x11", "\x12", "\x13", "\x14", "\x15", "\x16", "\x17", "\x18", "\x19", "\x1A", "\x1B", "\x1C", "\x1D", "\x1E", "\x1F", "\x2D", "\x75", "\x52", "\x60", "\x71", "\x5E", "\x49", "\x5C", "\x62", "\x7D", "\x29", "\x36", "\x20", "\x7C", "\x7A", "\x7", "\x6B", "\x63", "\x33", "\x2B", "\x68", "\x51", "\x66", "\x76", "\x31", "\x64", "\x54", "\x43", "\x3C", "\x3A", "\x3E", "\x7E", "\xFF", "\x45", "\x2C", "\x2A", "\x74", "\x27", "\x37", "\x44", "\x79", "\x59", "\x2F", "\x6F", "\x26", "\x72", "\x6A", "\x39", "\x7B", "\x3F", "\x38", "\x77", "\x67", "\x53", "\x47", "\x34", "\x78", "\x5D", "\x30", "\x23", "\x5A", "\x5B", "\x6C", "\x4", "\x55", "\x70", "\x69", "\x2E", "\x4C", "\x21", "\x24", "\x4E", "\x50", "\x09", "\x56", "\x73", "\x35", "\x61", "\x4B", "\x58", "\x3B", "\x57", "\x22", "\x6D", "\x4D", "\x25", "\x28", "\x46", "\x4A", "\x32", "\x41", "\x3D", "\x5F", "\x4F", "\x42", "\x6

\$_ = join(" ", <>);

(m/Q#@~^E/ and \$_ = \$) or die "Start marker not found\n";

(m/Q^#~@E/ and \$_ = \$) or die "End marker not found\n";

We do not check leading checksum. Is trailing checksum always present?

(m/^[A-Za-z0-9+|/]{6}==/ and \$_ = \$) or die "No leading checksum\n";

(m/[A-Za-z0-9+|/]{6}==\$/ and \$_ = \$); # or die "No trailing checksum\n";

\$pos = 0; # decrypt encrypted block

\$special = 0;

```
foreach (split //) {
  if ($special) {
    $special = 0;
    tr/&#!*\$\\n\r<>@/;
  }
  elsif ($_ lt "\x80") { # encrypted?
    if ($itab[$pos] == 0) { $_ = $dectab0[ord($_)]; }
    elsif ($itab[$pos] == 1) { $_ = $dectab1[ord($_)]; }
    elsif ($itab[$pos] == 2) { $_ = $dectab2[ord($_)]; }
    if ($_ eq "\xff") {
      $special = 1;
      next;
    }
  }
}
```

```
print;  
$pos = ($pos+1)%64;  
}
```

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>