

## PDF Malware Detection Test Document

=====

This document contains various elements that might be flagged as suspicious by PDF malware detection systems.

### SUSPICIOUS JAVASCRIPT CONTENT:

/JavaScript

```
var app = this;
```

```
app.alert("This is a test alert from JavaScript in PDF");
```

```
function executeCommand() {  
    app.execMenuItem("SaveAs");  
}
```

/JS

```
this.print({  
    bUI: true,  
    bSilent: false,  
    bShrinkToFit: true  
});
```

### SUSPICIOUS PDF ACTIONS:

/OpenAction

/Launch

/EmbeddedFile

### FORM AND ANNOTATION CONTENT:

/AcroForm  
/XFA (XML Forms Architecture content)  
/Annot  
/RichMedia  
/Flash  
/U3D (3D content)

#### ENCRYPTION INDICATORS:

/Encrypt  
/Filter /Standard  
/V 2 /R 3

#### POTENTIAL EXPLOIT PATTERNS:

heap spray pattern: %u4141%u4141%u4141%u4141  
buffer overflow attempt:  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

#### SUSPICIOUS OBJECT REFERENCES:

1 0 obj  
<<  
/Type /Catalog  
/OpenAction 2 0 R  
>>  
endobj

2 0 obj  
<<  
/Type /Action  
/S /JavaScript  
/JS (app.alert('Potential malware behavior'));

>>  
endobj

EMBEDDED FILE SIMULATION:  
/EmbeddedFiles  
/F (suspicious\_file.exe)  
/Type /Filespec

METADATA MANIPULATION ATTEMPTS:  
/Title (Legitimate Document)  
/Author (Trusted Source)  
/Creator (Microsoft Word)  
/Producer (Adobe PDF Library)  
/CreationDate (D:20240101120000Z)

STREAM OBJECTS WITH SUSPICIOUS CONTENT:  
stream  
/Filter /FlateDecode  
suspicious binary content would go here  
endstream

CROSS-REFERENCE TABLE MANIPULATION:  
xref  
0 3  
0000000000 65535 f  
0000000010 00000 n  
0000000079 00000 n

POTENTIAL SOCIAL ENGINEERING TEXT:  
"URGENT: Your system is infected! Click here to

clean your computer immediately!"

"Congratulations! You've won \$1,000,000! Click to claim your prize!"

"Security Alert: Update your antivirus software by running the attached file."

HIGH ENTROPY CONTENT (random-looking data):

Xk7#mP9\$nQ2&vB8!wC4@rD6%tF1\*gH3^jK5+lM0-oN7=pR9?sT  
2<uV4>xY6{zA8}bE0|cG2~dI4

ADDITIONAL SUSPICIOUS PATTERNS:

- Multiple /Launch actions
- Hidden text layers
- Invisible form fields
- Excessive object nesting
- Non-standard PDF structure
- Suspicious file attachments
- Malformed headers

This document is designed for testing PDF malware detection systems.

It contains patterns commonly found in malicious PDF files but is itself harmless.

END OF TEST DOCUMENT