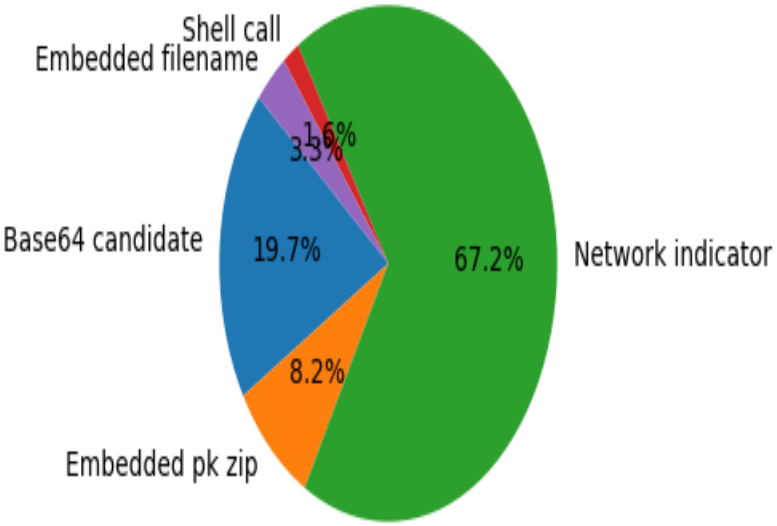
Analysis Report

/home/kaorise/Documents/uni/bit/semestralny-projekt/skodlive-subory/cfbf/macro_shell_cfbf.report.pdf

Verdict: Medium risk
Total Score: 66.40
Total Hits: 61



Name	Score	Hits	Description
Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['0x01010027C5F2A8E850404A893F4AB49FD29F78'], ...
Embedded pk zip	20	5	Document likely contains embedded CFBF/zip
Network indicator	15	1	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/drawingml/2006/main'], IPs: []
Shell call	20	1	Shell calls are detected
Embedded filename	40	1	Embedded filenames are detected: ['exe']
Embedded filename	40	1	Embedded filenames are detected: ['DLL']
Network indicator	15	1	Network indicators are detected: URLs: ['http://schemas.microsoft.com/sharepoint/v3/contenttype/forms'], IPs: []
Network indicator	15	2	Network indicators are detected: URLs: ['http://schemas.microsoft.com/sharepoint/v3/contenttype/forms', 'http://schemas.openxmlformats.org/officeDocument/2006/customXml'], IPs: []

Network indicator	15	26	Network indicators are detected: URLs: ['http://purl.org/dc/terms/', 'http://schemas.openxmlformats.org/package/2006/metadata/core-properties', 'http://schemas.microsoft.com/internal/obd', 'http://dublincore.org/schemas/xmls/qdc/2003/04/02/dcterms.xsd', 'http://dublincore.org/schemas/xmls/qdc/2003/04/02/dc.xsd', 'http://www.w3.org/2001/XMLSchema', 'http://schemas.microsoft.com/office/2006/metadata/properties', 'http://schemas.microsoft.com/office/infopath/2007/PartnerControls', 'http://schemas.microsoft.com/office/2006/metadata/properties/metaAttributes', 'http://www.w3.org/2001/XMLSchema-instance', 'http://purl.org/dc/elements/1.1/', 'http://schemas.microsoft.com/office/2006/metadata/contentType', 'http://schemas.microsoft.com/office/2006/documentManagement/types'], IPs: []
Base64 candidate	15	8	Base64 candidates found (which could be a way to obfuscate content): ['com/office/2006/documentManagement/types', '0x01010027C5F2A8E850404A893F4AB49FD29F78', 'com/office/infopath/2007/PartnerControls'], ...
Network indicator	15	11	Network indicators are detected: URLs: ['http://purl.org/dc/terms/', 'http://schemas.openxmlformats.org/package/2006/metadata/core-properties', 'http://schemas.microsoft.com/internal/obd', 'http://www.w3.org/2001/XMLSchema', 'http://schemas.microsoft.com/office/2006/metadata/properties', 'http://schemas.microsoft.com/office/infopath/2007/PartnerControls', 'http://schemas.microsoft.com/office/2006/metadata/properties/metaAttributes', 'http://purl.org/dc/elements/1.1/', 'http://schemas.microsoft.com/office/2006/metadata/contentType', 'http://schemas.microsoft.com/office/2006/documentManagement/types', 'http://schemas.openxmlformats.org/officeDocument/2006/customXml'], IPs: []
Base64 candidate	15	3	Base64 candidates found (which could be a way to obfuscate content): ['com/office/2006/documentManagement/types', 'com/office/2006/metadata/properties/metaAttributes', 'com/office/infopath/2007/PartnerControls'], ...