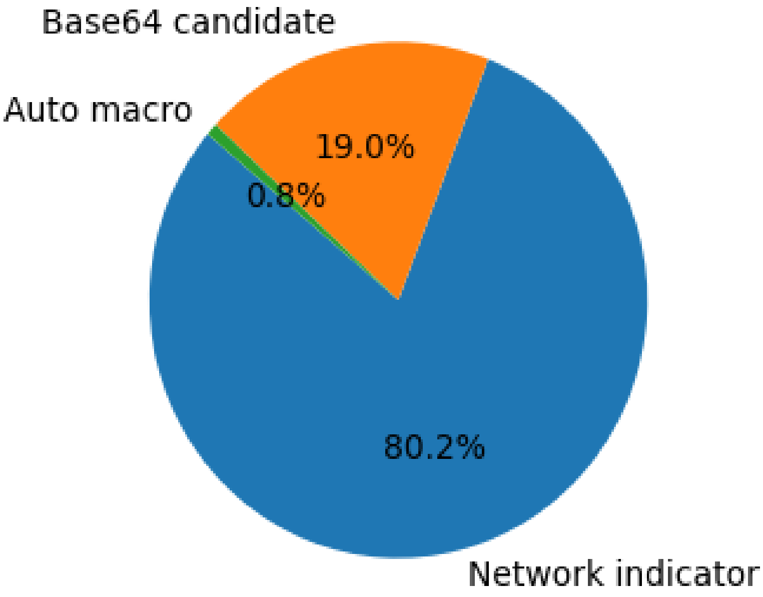
Analysis Report

/home/kaorise/Documents/uni/bit/semestralny-projekt/skodlive-subory/ooxml/higly_malicious_ooxml.report.pdf

Verdict: High risk
Total Score: 75.14
Total Hits: 258



Name	Score	Hits	Description
Network indicator	15	1	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/package/2006/content-types'], IPs: []
Network indicator	15	5	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/package/2006/relationships', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/extended-properties', 'http://schemas.openxmlformats.org/package/2006/relationships/metadata/core-properties', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/officeDocument', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/custom-properties'], IPs: []
Base64 candidate	15	4	Base64 candidates found (which could be a way to obfuscate content): ['org/officeDocument/2006/relationships/officeDocument', 'org/package/2006/relationships/metadata/core', 'org/officeDocument/2006/relationships/extended'], ...

Network indicator	15	32	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/word/2018/wordml/cex', 'http://schemas.openxmlformats.org/wordprocessingml/2006/main', 'http://schemas.microsoft.com/office/drawing/2016/ink', 'http://schemas.microsoft.com/office/drawing/2015/10/21/chartex', 'http://schemas.microsoft.com/office/drawing/2016/5/14/chartex', 'http://schemas.openxmlformats.org/markup-compatibility/2006', 'http://schemas.microsoft.com/office/drawing/2016/5/13/chartex', 'http://schemas.microsoft.com/office/word/2018/wordml', 'http://schemas.microsoft.com/office/word/2006/wordml', 'http://schemas.microsoft.com/office/word/2010/wordprocessingGroup', 'http://schemas.microsoft.com/office/word/2023/wordml/word16du', 'http://schemas.openxmlformats.org/officeDocument/2006/math', 'http://schemas.microsoft.com/office/word/2010/wordprocessingInk', 'http://schemas.microsoft.com/office/word/2010/wordml', 'http://schemas.microsoft.com/office/word/2020/wordml/sdtdatahash', 'http://schemas.microsoft.com/office/drawing/2014/chartex', 'http://schemas.microsoft.com/office/drawing/2016/5/10/chartex', 'http://schemas.microsoft.com/office/word/2024/wordml/sdtformatlock', 'http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing', 'http://schemas.microsoft.com/office/word/2015/wordml/symex', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships', 'http://schemas.microsoft.com/office/word/2016/wordml/cid', 'http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas', 'http://schemas.microsoft.com/office/word/2012/wordml', 'http://schemas.microsoft.com/office/drawing/2016/5/9/chartex', 'http://schemas.microsoft.com/office/drawing/2017/model3d', 'http://schemas.microsoft.com/office/word/2010/wordprocessingShape', 'http://schemas.microsoft.com/office/drawing/2016/5/11/chartex', 'http://schemas.microsoft.com/office/drawing/2016/5/12/chartex', 'http://schemas.microsoft.com/office/2019/extlst', 'http://schemas.microsoft.com/office/drawing/2015/9/8/chartex', 'http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing'], IPs: []
Base64 candidate	15	6	Base64 candidates found (which could be a way to obfuscate content): ['com/office/word/2010/wordprocessingDrawing', 'com/office/word/2010/wordprocessingShape', 'com/office/word/2024/wordml/sdtformatlock'], ...

Network indicator	15	10	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/package/2006/relationships', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/customXml', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles', 'http://schemas.microsoft.com/office/2006/relationships/vbaProject'], IPs: []
Base64 candidate	15	9	Base64 candidates found (which could be a way to obfuscate content): ['org/officeDocument/2006/relationships/webSettings', 'org/officeDocument/2006/relationships/fontTable', 'org/officeDocument/2006/relationships/settings'], ...
Network indicator	15	2	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/drawingml/2006/main', 'http://schemas.microsoft.com/office/thememl/2012/main'], IPs: []
Network indicator	15	2	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/package/2006/relationships', 'http://schemas.microsoft.com/office/2006/relationships/wordVbaData'], IPs: []
Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['com/office/2006/relationships/wordVbaData'], ...
Auto macro	50	2	Suspisious macros are detected

Network indicator	15	32	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/word/2018/wordml/cex', 'http://schemas.openxmlformats.org/wordprocessingml/2006/main', 'http://schemas.microsoft.com/office/drawing/2016/ink', 'http://schemas.microsoft.com/office/drawing/2015/10/21/chartex', 'http://schemas.microsoft.com/office/drawing/2016/5/14/chartex', 'http://schemas.openxmlformats.org/markup-compatibility/2006', 'http://schemas.microsoft.com/office/drawing/2016/5/13/chartex', 'http://schemas.microsoft.com/office/word/2018/wordml', 'http://schemas.microsoft.com/office/word/2006/wordml', 'http://schemas.microsoft.com/office/word/2010/wordprocessingGroup', 'http://schemas.microsoft.com/office/word/2023/wordml/word16du', 'http://schemas.openxmlformats.org/officeDocument/2006/math', 'http://schemas.microsoft.com/office/word/2010/wordprocessingInk', 'http://schemas.microsoft.com/office/word/2010/wordml', 'http://schemas.microsoft.com/office/word/2020/wordml/sdtdatahash', 'http://schemas.microsoft.com/office/drawing/2014/chartex', 'http://schemas.microsoft.com/office/drawing/2016/5/10/chartex', 'http://schemas.microsoft.com/office/word/2024/wordml/sdtformatlock', 'http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing', 'http://schemas.microsoft.com/office/word/2015/wordml/symex', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships', 'http://schemas.microsoft.com/office/word/2016/wordml/cid', 'http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas', 'http://schemas.microsoft.com/office/word/2012/wordml', 'http://schemas.microsoft.com/office/drawing/2016/5/9/chartex', 'http://schemas.microsoft.com/office/drawing/2017/model3d', 'http://schemas.microsoft.com/office/word/2010/wordprocessingShape', 'http://schemas.microsoft.com/office/drawing/2016/5/11/chartex', 'http://schemas.microsoft.com/office/drawing/2016/5/12/chartex', 'http://schemas.microsoft.com/office/2019/extlst', 'http://schemas.microsoft.com/office/drawing/2015/9/8/chartex', 'http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing'], IPs: []
Base64 candidate	15	6	Base64 candidates found (which could be a way to obfuscate content): ['com/office/word/2010/wordprocessingDrawing', 'com/office/word/2010/wordprocessingShape', 'com/office/word/2024/wordml/sdtformatlock'], ...

Network indicator	15	20	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/word/2012/wordml', 'http://schemas.microsoft.com/office/word/2018/wordml', 'http://schemas.microsoft.com/office/word', 'http://schemas.microsoft.com/office/word/2018/wordml/cex', 'http://schemas.microsoft.com/office/word/2023/wordml/word16du', 'http://schemas.openxmlformats.org/officeDocument/2006/math', 'http://schemas.microsoft.com/office/word/2020/wordml/sdtdatahash', 'http://schemas.openxmlformats.org/wordprocessingml/2006/main', 'http://schemas.microsoft.com/office/word/2024/wordml/sdtformatlock', 'http://schemas.openxmlformats.org/markup-compatibility/2006', 'http://schemas.microsoft.com/office/word/2015/wordml/symex', 'http://schemas.openxmlformats.org/schemaLibrary/2006/main', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships', 'http://schemas.microsoft.com/office/word/2016/wordml/cid', 'http://schemas.microsoft.com/office/word/2010/wordml'], IPs: []
Base64 candidate	15	2	Base64 candidates found (which could be a way to obfuscate content): ['com/office/word/2024/wordml/sdtformatlock', 'overrideTableStyleFontSizeAndJustification'], ...
Network indicator	15	26	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/2006/metadata/properties', 'http://purl.org/dc/terms/', 'http://schemas.microsoft.com/office/2006/metadata/properties/metaAttributes', 'http://schemas.microsoft.com/office/infopath/2007/PartnerControls', 'http://dublincore.org/schemas/xmls/qdc/2003/04/02/dcterms.xsd', 'http://www.w3.org/2001/XMLSchema-instance', 'http://schemas.microsoft.com/office/2006/documentManagement/types', 'http://schemas.microsoft.com/office/2006/metadata/contentType', 'http://www.w3.org/2001/XMLSchema', 'http://schemas.openxmlformats.org/package/2006/metadata/core-properties', 'http://dublincore.org/schemas/xmls/qdc/2003/04/02/dc.xsd', 'http://schemas.microsoft.com/internal/obd', 'http://purl.org/dc/elements/1.1/'], IPs: []
Base64 candidate	15	8	Base64 candidates found (which could be a way to obfuscate content): ['0x01010027C5F2A8E850404A893F4AB49FD29F78', 'com/office/2006/documentManagement/types', 'com/office/infopath/2007/PartnerControls'], ...

Network indicator	15	11	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/2006/metadata/properties', 'http://purl.org/dc/terms/', 'http://schemas.microsoft.com/office/2006/metadata/properties/metaAttributes', 'http://schemas.microsoft.com/office/infopath/2007/PartnerControls', 'http://schemas.microsoft.com/office/2006/documentManagement/types', 'http://schemas.microsoft.com/office/2006/metadata/contentType', 'http://www.w3.org/2001/XMLSchema', 'http://schemas.openxmlformats.org/package/2006/metadata/core-properties', 'http://schemas.openxmlformats.org/officeDocument/2006/customXml', 'http://schemas.microsoft.com/internal/obd', 'http://purl.org/dc/elements/1.1/'], IPs: []
Base64 candidate	15	3	Base64 candidates found (which could be a way to obfuscate content): ['com/office/2006/documentManagement/types', 'com/office/infopath/2007/PartnerControls', 'com/office/2006/metadata/properties/metaAttributes'], ...
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	3	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/2006/metadata/properties', 'http://schemas.microsoft.com/office/infopath/2007/PartnerControls', 'http://www.w3.org/2001/XMLSchema-instance'], IPs: []
Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['com/office/infopath/2007/PartnerControls'], ...
Network indicator	15	9	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/2006/metadata/properties', 'http://purl.org/dc/terms/', 'http://schemas.microsoft.com/office/infopath/2007/PartnerControls', 'http://www.w3.org/XML/1998/namespace', 'http://schemas.microsoft.com/office/2006/documentManagement/types', 'http://schemas.openxmlformats.org/package/2006/metadata/core-properties', 'http://schemas.openxmlformats.org/officeDocument/2006/customXml', 'http://purl.org/dc/elements/1.1/', 'http://purl.org/dc/dcmitype/'], IPs: []
Base64 candidate	15	2	Base64 candidates found (which could be a way to obfuscate content): ['com/office/2006/documentManagement/types', 'com/office/infopath/2007/PartnerControls'], ...

Network indicator	15	12	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/word/2012/wordml', 'http://schemas.microsoft.com/office/word/2018/wordml', 'http://schemas.microsoft.com/office/word/2018/wordml/cex', 'http://schemas.microsoft.com/office/word/2023/wordml/word16du', 'http://schemas.microsoft.com/office/word/2020/wordml/sdtdatahash', 'http://schemas.openxmlformats.org/wordprocessingml/2006/main', 'http://schemas.microsoft.com/office/word/2024/wordml/sdtformatlock', 'http://schemas.openxmlformats.org/markup-compatibility/2006', 'http://schemas.microsoft.com/office/word/2015/wordml/symex', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships', 'http://schemas.microsoft.com/office/word/2016/wordml/cid', 'http://schemas.microsoft.com/office/word/2010/wordml'], IPs: []
Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['com/office/word/2024/wordml/sdtformatlock'], ...
Network indicator	15	12	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/word/2012/wordml', 'http://schemas.microsoft.com/office/word/2018/wordml', 'http://schemas.microsoft.com/office/word/2018/wordml/cex', 'http://schemas.microsoft.com/office/word/2023/wordml/word16du', 'http://schemas.microsoft.com/office/word/2020/wordml/sdtdatahash', 'http://schemas.openxmlformats.org/wordprocessingml/2006/main', 'http://schemas.microsoft.com/office/word/2024/wordml/sdtformatlock', 'http://schemas.openxmlformats.org/markup-compatibility/2006', 'http://schemas.microsoft.com/office/word/2015/wordml/symex', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships', 'http://schemas.microsoft.com/office/word/2016/wordml/cid', 'http://schemas.microsoft.com/office/word/2010/wordml'], IPs: []
Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['com/office/word/2024/wordml/sdtformatlock'], ...
Network indicator	15	12	Network indicators are detected: URLs: ['http://schemas.microsoft.com/office/word/2012/wordml', 'http://schemas.microsoft.com/office/word/2018/wordml', 'http://schemas.microsoft.com/office/word/2018/wordml/cex', 'http://schemas.microsoft.com/office/word/2023/wordml/word16du', 'http://schemas.microsoft.com/office/word/2020/wordml/sdtdatahash', 'http://schemas.openxmlformats.org/wordprocessingml/2006/main', 'http://schemas.microsoft.com/office/word/2024/wordml/sdtformatlock', 'http://schemas.openxmlformats.org/markup-compatibility/2006', 'http://schemas.microsoft.com/office/word/2015/wordml/symex', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships', 'http://schemas.microsoft.com/office/word/2016/wordml/cid', 'http://schemas.microsoft.com/office/word/2010/wordml'], IPs: []

Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['com/office/word/2024/wordml/sdtformatlock'], ...
Network indicator	15	5	Network indicators are detected: URLs: ['http://purl.org/dc/terms/', 'http://www.w3.org/2001/XMLSchema-instance', 'http://schemas.openxmlformats.org/package/2006/metadata/core-properties', 'http://purl.org/dc/elements/1.1/', 'http://purl.org/dc/dcmitype/'], IPs: []
Network indicator	15	2	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/officeDocument/2006/extended-properties', 'http://schemas.openxmlformats.org/officeDocument/2006/docPropsVTypes'], IPs: []
Network indicator	15	2	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/officeDocument/2006/docPropsVTypes', 'http://schemas.openxmlformats.org/officeDocument/2006/custom-properties'], IPs: []
Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['0x01010027C5F2A8E850404A893F4AB49FD29F78'], ...
Network indicator	15	2	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/package/2006/relationships', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/customXmlProps'], IPs: []
Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['org/officeDocument/2006/relationships/customXmlProps'], ...
Network indicator	15	2	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/package/2006/relationships', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/customXmlProps'], IPs: []
Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['org/officeDocument/2006/relationships/customXmlProps'], ...
Network indicator	15	2	Network indicators are detected: URLs: ['http://schemas.openxmlformats.org/package/2006/relationships', 'http://schemas.openxmlformats.org/officeDocument/2006/relationships/customXmlProps'], IPs: []
Base64 candidate	15	1	Base64 candidates found (which could be a way to obfuscate content): ['org/officeDocument/2006/relationships/customXmlProps'], ...