pedramamini Update Microsoft_Office_DDE_Command_Execution.rule History

1 contributor

105 lines (86 sloc) 6.02 KB

```
/*

 Follow the conversation on Twitter:

    https://twitter.com/i/moments/918126999738175489

 Read up on the exposure, mitigation, detection / hunting, and sample dissection from our blogs:

    http://blog.inquest.net/blog/2017/10/13/microsoft-office-dde-macro-less-command-execution-vulnerability/
    http://blog.inquest.net/blog/2017/10/14/02-microsoft-office-dde-freddie-mac-targeted-lure/
    http://blog.inquest.net/blog/2017/10/14/01-microsoft-office-dde-sec-omb-approval-lure/
    http://blog.inquest.net/blog/2017/10/14/03-microsoft-office-dde-poland-ransomware/

 InQuest customers can detect related events on their network by searching for:

    event ID 5000728, Microsoft_Office_DDE_Command_Exec

*/

rule MC_Office_DDE_Command_Execution
{
    meta:
        Author      = "InQuest Labs"
        URL         = "https://github.com/InQuest/yara-rules"
        Description = "This rule looks for a variety of DDE command execution techniques."

    strings:
        /*
            standard:
                <w:fldChar w:fldCharType="begin"/></w:r><w:r>
                <w:instrText xml:space="preserve"> </w:instrText></w:r><w:r><w:rPr>
                <w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica" w:cs="Helvetica"/><w:color w:val="333333"/>
                <w:sz w:val="21"/><w:szCs w:val="21"/>
                <w:shd w:val="clear" w:color="auto" w:fill="FFFFFF"/></w:rPr>
                <w:instrText>DDEAUTO c:\\windows\\system32\\cmd.exe "/k calc.exe"</w:instrText></w:r>
                <w:bookmarkStart w:id="0" w:name="_GoBack"/>
                <w:bookmarkEnd w:id="0"/><w:r>
                <w:instrText xml:space="preserve"> </w:instrText></w:r><w:r>
                <w:fldChar w:fldCharType="end"/></w:r>

            encompassed:
                # e 313fc5bd8e1109d35200081e62b7aa33197a6700fc390385929e71aabbc4e065
                [root@INQ-PPSandbox tge-zip-1-1]# cat xl/externalLinks/externalLink1.xml
                <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
                <externalLink xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main" xmlns:mc="http://schema
                    <ddeLink xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" ddeService="
                        <ddeItems>
                            <ddeItem name="A0" advise="1" />
                            <ddeItem name="StdDocumentName" ole="1" advise="1" />
                        </ddeItems
                        </ddeLink
                </externalLink>
        */

        // standard DDE with optional AUTO.
        $dde = />\s*DDE(AUTO)?\s*</ nocase wide ascii

        // NOTE: we must remain case-insensitive but do not wish to fire on "<w:webHidden/>".
        // NOTE: nocase does not apply to character ranges ([^A-Za-z0-9-]).
        $dde_auto = /<\s*w:fldChar\s+w:fldCharType\s*=\s*['"]begin['"]\s*\/>.+[^A-Za-z0-9-]DDEAUTO[^A-Za-z0-9-].+<w:flc

        // DDEAUTO is the only known vector at the moment, widening the detection here other possible vectors.
        $dde_other = /<\s*w:fldChar\s+w:fldCharType\s*=\s*['"]begin['"]\s*\/>.+[^A-Za-z0-9-]DDE[B-Zb-z]+[^A-Za-z0-9-].+

        // a wider DDEAUTO condition for older versions of Word (pre 2007, non DOCX).
        $magic = /^\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00\x00/
        $wide_dde_auto = /.+[^A-Za-z0-9-]DDEAUTO[^a-z0-9-].+/ nocase wide ascii

        // obfuscated with XML. use an early exit because this is an expensive regex.
        // NOTE: this is exactly the reason we have a DFI stack ... to strip, simplify, augment, transform, and make li
        // NOTE: we prefer to use $xml_obfuscated, but it's not suitable for VTI hunt, perf warnings are a no-go.
        // NOTE: xml_obfuscated_{1,6} also won't fly for VTI, they are left here for reference.
        // NOTE: xml_obfuscated_{4,5} are prone to false positives, they are left here for reference.
        $early_exit       = "fldChar" nocase wide ascii
        //$xml_obfuscated   = /!?(<[^>]*>){0,10}['"]?(<[^>]*>){0,10}D(<[^>]*>){0,10}D(<[^>]*>){0,10}E(<[^>]*>){0,10}(A(
        //$xml_obfuscated_1 = />\s*["']?D\s*</   nocase ascii wide
        $xml_obfuscated_2 = />\s*["']?DD\s*</  nocase ascii wide
        $xml_obfuscated_3 = />\s*["']?DDE\s*</ nocase ascii wide
        //$xml_obfuscated_4 = />\s*DDE["']?\s*</ nocase ascii wide
        //$xml_obfuscated_5 = />\s*DE["']?\s*</  nocase ascii wide
        //$xml_obfuscated_6 = />\s*E["']?\s*</   nocase ascii wide

        // fully encompassed in XML
        $pure_xml_dde = /<\s*ddeLink[^>]+ddeService\s*=\s*["'](cmd|reg|mshta|regsvr32|[wc]script|powershell|bitsadmin|s

        // NOTE: these strings can be broken apart with XML constructs. additional post processing is required to avoic
        $exec_action = /(cmd\.exe|reg\.exe|mshta\.exe|regsvr32|[wc]script|powershell|bitsadmin|schtasks|rundll32)/ noca

        // QUOTE obfuscation technique.
        $quote_obfuscation = /w:instr\s*=\s*["']\s*QUOTE\s+\d+\s+/ nocase wide ascii

    condition:
        ((any of ($dde*) or ($magic at 0 and $wide_dde_auto)) and ($exec_action or $quote_obfuscation))
            or
        ($early_exit and any of ($xml_obfuscated*))
            or
        ($pure_xml_dde)
            or
        (
            // '{\rt' (note that full header is *NOT* required: '{\rtf1')
            // trigger = '{\rt' nocase
            // generated via https://labs.inquest.net/tools/yara/iq-uint-trigger
            for any i in (0..30) : ((uint32be(i) | 0x2020) == 0x7b5c7274 and $exec_action)
        )
}
```