# Sofacy Using Two Zero Days in Recent Targeted Attacks – early warning

Version: 1.0 (26.April.2017)

## Executive summary

On April 18th , Kaspersky Lab received multiple reports that a new Microsoft Office document zero day was being exploited in the wild. An analysis of the document indicated that it was configured to drop a payload commonly referred to as GAMEFISH, which is specific to the Sofacy threat actor. The document targeted a large amount of European based users, spanning both government and private industry. Timing for this wave of attacks was over the Easter holiday and most likely was deliberately sent to a large number of targets due to a patch released by Microsoft on April 11th.

The Office exploit utilizes an Encapsulated PostScript (EPS) embedded in a Microsoft Word document. We are currently working on determining the root cause for the exploit, but in the meantime have verified this to be a zero day from other sources also looking into the matter.

After successful exploitation of Word, another Local Privilege Escalation (LPE) exploit is executed. This exploit has also been confirmed by Microsoft to be a zero day. The LPE used in this attack appears to have originated from a well known exploit developer "Volodya". Sofacy has used exploits purchased from this individual before, with the most recent one used in October 2016.

This report serves as an early warning report for customers in an effort to responsibly disclose as much information as possible for defensive purposes. As a reminder, the information in this report should be handled as TLP:AMBER, allowing for the sharing of information ONLY within the customer's organization.

This paper in a nutshell:

- There was a spear-phishing campaign, mostly targeting European users, most likely over Easter holiday;
- The campaign exploited two zero days, exploiting Microsoft Word and Windows (LPE);
- It seems that Sofacy purchased the LPE exploit from the developer "Volodya";
- The payload installed after exploitation is Gamefish, malware specific to Sofacy.

For more information please contact: intelreports@kaspersky.com

# Technical Analysis

## EPS Exploit

The metadata for the original malicious document being distributed in the malicious campaign is as follows:

```
Name: Trump's_Attack_on_Syria_English.docx
Size: 268950
MD5: f8e92d8b5488ea76c40601c8f1a08790
CreateDate: 2017:04:18 08:41:00Z
```

The original document appears to have been pulled from a US-based Armenian newspaper called "The California Courier"[1] and contains content related to the recent strikes launched by President Trump in Syria. Screenshots of the content of the document are provided below:

[1] http://www.thecaliforniacourier.com/trumps-attack-on-syria-wrong-for-so-many-reasons

Trump's Attack on Syria:
Wrong for so Many Reasons

Many Americans and people around the world followed with great concern the off-the-cuff and zany ideas Donald Trump voiced during the presidential campaign and more ominously after becoming President.

It is one thing to disagree with him on a domestic policy issue like banning Muslim tourists or healthcare or building a wall, it is quite another when he issues threats to foreign countries such as Iran and North Korea, and even worse when he orders a missile attack on Syria!

What is wrong with such a disastrous decision? Pres. Trump does not have the requisite background knowledge about the Syrian conflict, except for what he has read in some fringe publications and seen on his favorite TV Channel, FOX News.

Pres. Trump stated that he was deeply touched by the images of babies he had seen on TV who had been hurt by a chemical attack. Who would not be? Certainly, he had an emotional and impulsive reaction to heart-wrenching pictures, which cannot be a substitute for a well-thought out foreign policy without a thorough examination of the facts of this tragic incident and careful consideration of the consequences of an extreme action like launching 59 tomahawk missiles on a Syrian air base.

Fortunately, Pres. Trump's aides alerted Russia shortly before the attack, to avoid any Russian casualties which could have had catastrophic consequences for the entire world!

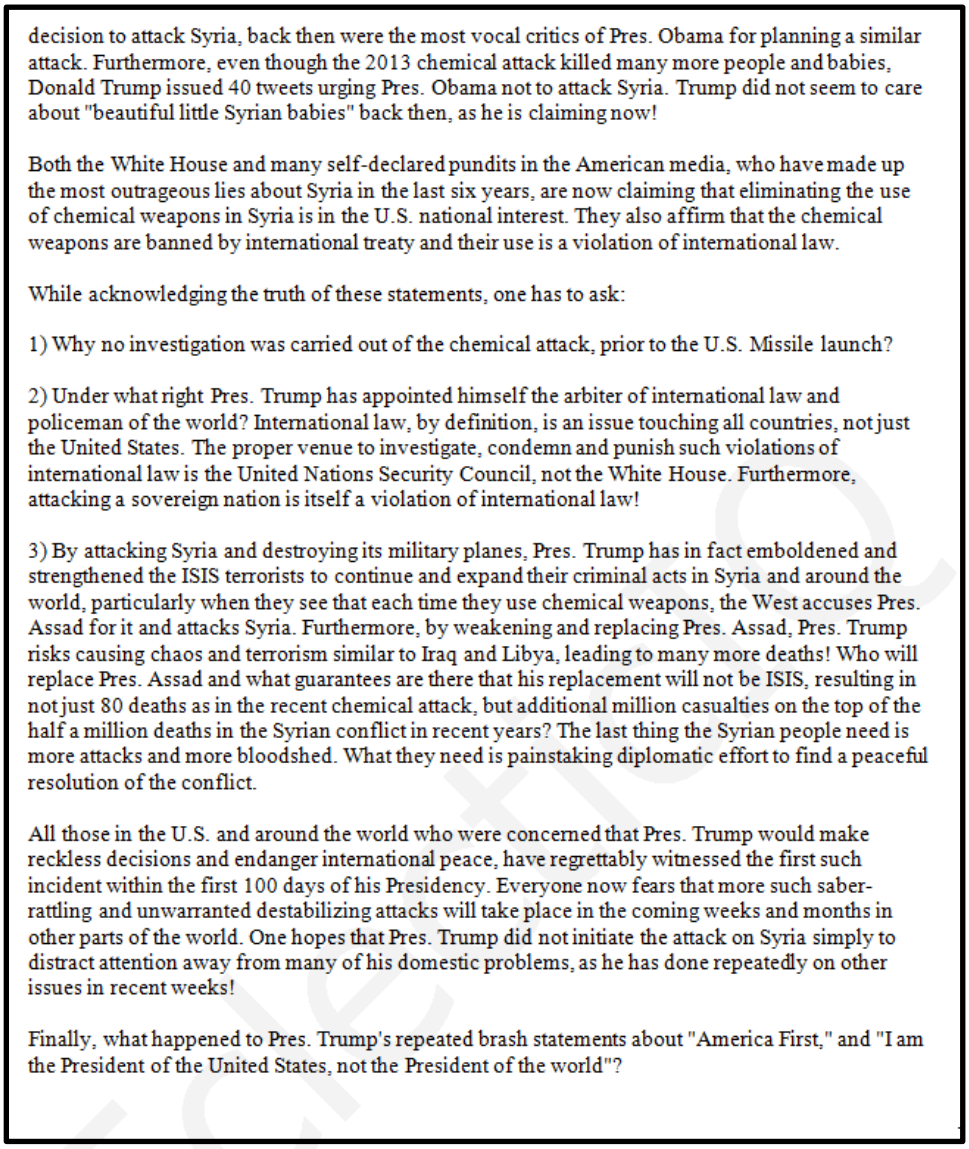
Furthermore, Pres. Trump's actions violated the U.S. Constitution, as he neither sought nor received the legally required authorization from the U.S. Congress to launch a war on another sovereign state.

Pres. Trump had neither the wisdom nor the patience to wait for the outcome of the investigation of the circumstances of the chemical attack -- to verify who is truly responsible for this terrible attack.

The Trump Administration accused the Syrian Air Force of carrying out a chemical attack near Idlib. The Syrian and Russian governments have a different version of these events. They affirm that Syria does not possess any chemical weapons after its 2003 agreement to dispose of all such hazardous materials. Furthermore, Syria claims that the chemical explosion was caused by its Air Force bombing a warehouse belonging to Syrian terrorists who had stored these dangerous materials. It makes no sense for Pres. Assad to use chemical weapons while he is winning, risk antagonizing the West, and precipitating a military backlash.

We recall that back in 2013, there was another chemical attack on a Damascus suburb that killed many more people than the one near Idlib. Back then, Pres. Obama was close to going to war with Syria wrongly believing that the Syrian government had crossed his announced "red line." However, when he learned that the chemical attack near Damascus was a "false flag," meaning that it was orchestrated by Turkey and its terrorist allies to force the United States to intervene militarily in Syria, Pres. Obama did not go through with his plans to launch missiles on Syria. No one should forget that U.S. officials in 2003 presented fake "intelligence" evidence to the world claiming that Pres. Saddam Hussein possessed WMD (Weapons of Mass Destruction), to justify the invasion of Iraq.

Ironically, many Republican members of Congress who are now applauding Pres. Trump for his



decision to attack Syria, back then were the most vocal critics of Pres. Obama for planning a similar attack. Furthermore, even though the 2013 chemical attack killed many more people and babies, Donald Trump issued 40 tweets urging Pres. Obama not to attack Syria. Trump did not seem to care about "beautiful little Syrian babies" back then, as he is claiming now!

Both the White House and many self-declared pundits in the American media, who have made up the most outrageous lies about Syria in the last six years, are now claiming that eliminating the use of chemical weapons in Syria is in the U.S. national interest. They also affirm that the chemical weapons are banned by international treaty and their use is a violation of international law.

While acknowledging the truth of these statements, one has to ask:

1) Why no investigation was carried out of the chemical attack, prior to the U.S. Missile launch?

2) Under what right Pres. Trump has appointed himself the arbiter of international law and policeman of the world? International law, by definition, is an issue touching all countries, not just the United States. The proper venue to investigate, condemn and punish such violations of international law is the United Nations Security Council, not the White House. Furthermore, attacking a sovereign nation is itself a violation of international law!

3) By attacking Syria and destroying its military planes, Pres. Trump has in fact emboldened and strengthened the ISIS terrorists to continue and expand their criminal acts in Syria and around the world, particularly when they see that each time they use chemical weapons, the West accuses Pres. Assad for it and attacks Syria. Furthermore, by weakening and replacing Pres. Assad, Pres. Trump risks causing chaos and terrorism similar to Iraq and Libya, leading to many more deaths! Who will replace Pres. Assad and what guarantees are there that his replacement will not be ISIS, resulting in not just 80 deaths as in the recent chemical attack, but additional million casualties on the top of the half a million deaths in the Syrian conflict in recent years? The last thing the Syrian people need is more attacks and more bloodshed. What they need is painstaking diplomatic effort to find a peaceful resolution of the conflict.

All those in the U.S. and around the world who were concerned that Pres. Trump would make reckless decisions and endanger international peace, have regrettably witnessed the first such incident within the first 100 days of his Presidency. Everyone now fears that more such saber-rattling and unwarranted destabilizing attacks will take place in the coming weeks and months in other parts of the world. One hopes that Pres. Trump did not initiate the attack on Syria simply to distract attention away from many of his domestic problems, as he has done repeatedly on other issues in recent weeks!

Finally, what happened to Pres. Trump's repeated brash statements about "America First," and "I am the President of the United States, not the President of the world"?

Contained within the malicious document is an EPS file (details below), which when executed, will unpack another EPS file using a simple XOR routine. A Python script to decode the second EPS file is also shown.

```
Name: image1.eps
MD5: b137c809e3bf11f2f5d867a6f4215f95
```

```
%!PS-Adobe-3.0
%%BoundingBox:   36   36  576  756
%%Page: 1 1
 /A3{ token pop exch pop } def
 /A2 <c45d6491> def
 /A4{
    /A1 exch def 0 1 A1 length 1 sub {
        /A5 exch def A1 A5 2 copy get A2 A5 4 mod get xor put
    } for A1
} def
<bf7d4bd9a13112f4b03407f0e43b0dffa03b0bffb07d55a1f47d17f2a53101f7ab3310b1
044f8a27d25a3f27d25a0f57d25a5f57d09e4a87d25a4f07d14e4b0340ae5a12f12f0a87d
```

Figure 1. Snippet of first EPS file

```
import sys

encData = bytearray(open(sys.argv[1], 'rb').read())
dataLen = len(encData)

key = bytearray([0xc4, 0x5d, 0x64, 0x91])
keyLen = len(key)

outFileName = str(sys.argv[1]) + '.dec'
outFile = open(outFileName, 'wb')

keyPosition = 0
output = bytearray()
for i in range(0, dataLen):
    output.append(encData[i] ^ key[keyPosition % keyLen])
    keyPosition += 1
outFile.write(output)
outFile.close()
```

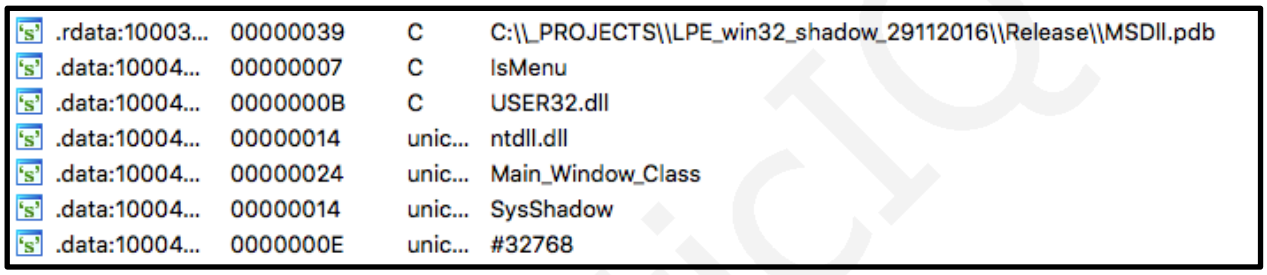
Figure 2. Python Script used to decode second EPS file

The decoded, second EPS (MD5: 237e6dcbc6af50ef5f5211818522c463) contains what appears to be a heap spray or some other memory corruption which will subsequently load a large chunk of shellcode into memory. This shellcode, when executed will then unpack the LPE exploit into memory and transfer execution flow to it.

## LPE Exploit

The LPE binary (MD5: 88009adca35560810ec220544e4fb6aa) is unpacked into memory and executed. We are currently still analyzing this exploit to determine the root cause, but Microsoft has at least confirmed this to be a zero day and is working on a patch.

One interesting note for this exploit is that it appears to have been purchased from the prolific exploit writer "Volodya" based on certain strings shown below which are a sort of "calling card" for their exploits. Volodya seems to enjoy using the class name "Main_Windows_Class", and targets the SysShadow class in many of his previous LPE exploits. Also, the debug path is typical of his exploits in the past.



| | | | |
|---|---|---|---|
| .rdata:10003... | 00000039 | C | C:_PROJECTS\\LPE_win32_shadow_29112016\\Release\\MSDll.pdb |
| .data:10004... | 00000007 | C | lsMenu |
| .data:10004... | 0000000B | C | USER32.dll |
| .data:10004... | 00000014 | unic... | ntdll.dll |
| .data:10004... | 00000024 | unic... | Main_Window_Class |
| .data:10004... | 00000014 | unic... | SysShadow |
| .data:10004... | 0000000E | unic... | #32768 |

The last known Sofacy LPE was also purchased from Volodya and used in a wave of attacks in October 2016. Based on a timestamp in the debug string for the new LPE (*C:_PROJECTS\LPE_win32_shadow_**29112016**\Release\MSDll.pdb*), it may indicate that once Microsoft patched the last Sofacy LPE, they turned around and purchased a new one from the same developer.

## Payload

Once privileges are elevated using the above exploit, the GAMEFISH payload is then written to the victim's %TEMP% folder and executed, resulting in a callout to Google first, then a subsequent callout to the embedded C2 below.

**MD5:** 2163a33330ae5786d3e984db09b2d9d2
**Filename:** apisecconnect.dll
**C2:** wmdmediacodecs[.]com
**TCP Port:** 443

Since the payload is written using elevated privileges, the "System File" and "Hidden File" flags are set as attributes in an effort to better hide from plain sight.

## Persistence

Persistence for the GAMEFISH payload is achieved using the Microsoft Office Perf technique[2] first detailed in 2014. While this was first written about in 2014 as a research project, the use of it in the wild was not known until June 2016[3], when Palo Alto described it being used by Sofacy in another wave of attacks.

The DLL is referenced in the following registry key, allowing it to be loaded any time a Microsoft Office application is started on the victim's system:

```
Key: HKCU\Software\Microsoft\Office test\Special\Perf\
Value: <TEMP_PATH>\apisecconnect.dll
```

## Catalyst for Attacks

On April 11th , Microsoft released a patch[4] for Office which disabled, by default, the Encapsulated PostScript (EPS) filter. Once this patch was announced publicly, our current theory is that Sofacy realized they had limited time before this exploit would become useless. Coincidental timing with the Easter holiday throughout the World allowed the actor to mass spam this exploit over the holiday in hopes that systems had not been patched and the target would read their mail first thing when returning from holiday.

# Conclusions

Sofacy continues to show they possess access zero day exploits seemingly at will. As stated in previous reports, this threat actor does not appear to be slowing down in any way even after the large amount of publicity they received following the U.S. election cycle. Their targeting continues to fall in line with what has previously been observed, focusing on government and policy influencers. This specific wave of attacks also shows their agility as they were able to mount a large attack within one week of Microsoft pushing a patch that would render this exploit virtually useless.

Customers are advised to implement the below indicators of compromise on any defensive system they can, specifically at mail gateways and network monitoring devices. While we believe this wave of attacks has subsided and was intended as a final "shot over the bow", the possibility exists that they may use one or both exploits in another wave in the near future.

---

[2] http://www.hexacorn.com/blog/2014/04/16/beyond-good-ol-run-key-part-10
[3] http://researchcenter.paloaltonetworks.com/2016/06/unit42-new-sofacy-attacks-against-us-government-agency
[4] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV170005

## Appendix I - Indicators of Compromise

**Hashes**

f8e92d8b5488ea76c40601c8f1a08790
b137c809e3bf11f2f5d867a6f4215f95
237e6dcbc6af50ef5f5211818522c463
88009adca35560810ec220544e4fb6aa
2163a33330ae5786d3e984db09b2d9d2

**Domains**

Wmdmediacodecs[.]com

**File Paths / Names**

*%TEMP%*\apisecconnect.dll

**Registry Keys / Values**

**Key**: HKCU\Software\Microsoft\Office test\Special\Perf\
**Value**: *%TEMP%*\apisecconnect.dll

**Yara rules**

```
rule Word_with_Encapsulated_PS {

meta:

      description = "Rule to find Sofacy zero day documents with embedded
image1.eps file"
      author = "Kaspersky Lab"
      copyright = "Kaspersky Lab"
     distribution = “DISTRIBUTION IS FORBIDDEN. DO NOT UPLOAD TO ANY MULTISCANNER
OR SHARE ON ANY THREAT INTEL PLATFORM”
      date = "2017-04-25"

strings:

        $a1="docProps/app.xmlPK"
        $a2="docProps/core.xmlPK"
        $a3="word/document.xmlPK"
        $a4="word/fontTable.xmlPK"
        $a5="word/settings.xmlPK"
        $a6="word/styles.xmlPK"
        $a7="word/webSettings.xmlPK"
        $a8="word/media/image1.epsPK"
        $a9="word/theme/theme1.xmlPK"

condition:

      (filesize>50000) and (uint16(0)==0x4b50) and (all of them)

}
```