Exploring CVE-2015-2545 and its users

06 May 2016

By Pierre Montagnier and Tom Lancaster

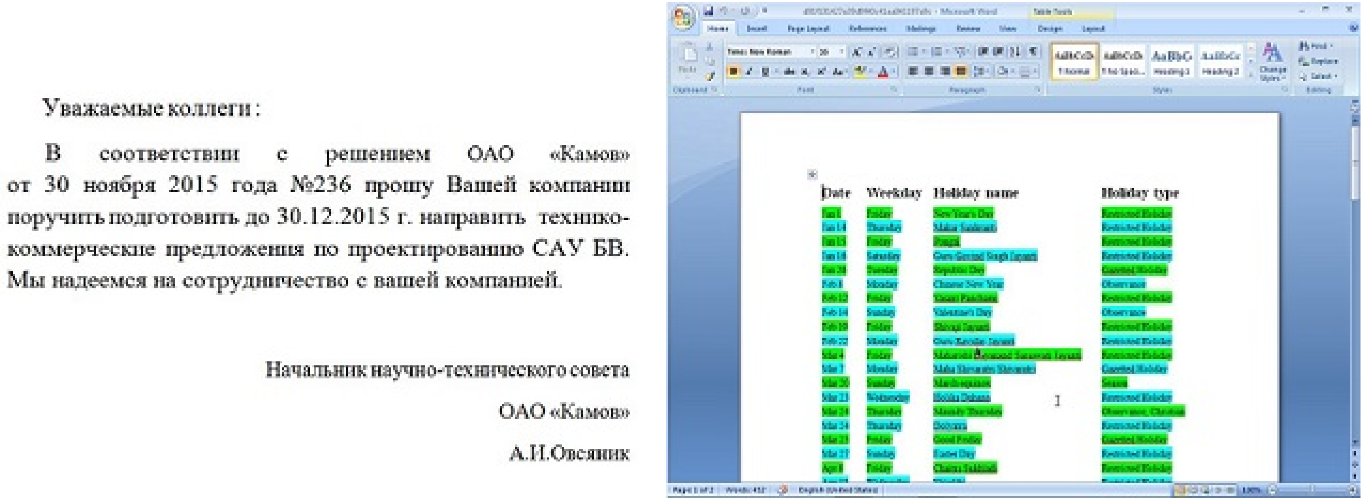
Executive Summary

This report, available at TLP:GREEN to researchers and network defenders, gives an overview of different attacks using CVE-2015-2545. Specifically we look at the different ways attackers are triggering the vulnerability, and the possibility that the exploit is shared amongst various groups. Based on overlaps in the samples analysed, our findings show that there are several clusters of documents, with the majority of the document-based builders sharing similar constructs in terms of how the final payload is discovered and executed. We also found that more recently some attackers are triggering the vulnerability through the use of MHTML files with .doc extensions.

Background

Back in November 2015, FireEye published a report titled 'Two For One'[1] detailing two new zero days, one affecting Microsoft (MS) Word and the other affecting the Windows operating system. Our report focuses on the former, CVE 2015-2545.

The vulnerability stems from a flaw in the processing of Encapsulated PostScript (EPS) files and allows an attacker to execute arbitrary code. We have been tracking samples exploiting this vulnerability as well as tracking the associated malware, much of which has been already discussed in public reporting.



Уважаемые коллеги :

В соответствии с решением ОАО «Камов» от 30 ноября 2015 года №236 прошу Вашей компании поручить подготовить до 30.12.2015 г. направить технико-коммерческие предложения по проектированию САУ БВ. Мы надеемся на сотрудничество с вашей компанией.

Начальник научно-технического совета

ОАО «Камов»

А.И.Овсяник

Date	Weekday	Holiday name	Holiday type
Jan 1	Friday	New Year's Day	Restricted Holiday
Jan 14	Thursday	Makar Sankranti	Restricted Holiday
Jan 15	Friday	Pongal	Restricted Holiday
Jan 16	Saturday	Guru Govind Singh Jayanti	Restricted Holiday
Jan 26	Tuesday	Republic Day	Gazetted Holiday
Feb 8	Monday	Chinese New Year	Observance
Feb 12	Friday	Vasant Panchami	Restricted Holiday
Feb 14	Sunday	Valentine's Day	Observance
Feb 19	Friday	Shivaji Jayanti	Restricted Holiday
Feb 22	Monday	Guru Ravidas Jayanti	Restricted Holiday
Mar 4	Friday	Maharishi Dayanand Saraswati Jayanti	Restricted Holiday
Mar 7	Monday	Maha Shivaratri/Shivaratri	Gazetted Holiday
Mar 20	Sunday	March equinox	Season
Mar 23	Wednesday	Holika Dahana	Restricted Holiday
Mar 24	Thursday	Maundy Thursday	Observance, Christian
Mar 24	Thursday	Dolyatra	Restricted Holiday
Mar 25	Friday	Good Friday	Gazetted Holiday
Mar 27	Sunday	Easter Day	Restricted Holiday
Apr 8	Friday	Chaitra Sukhladi	Restricted Holiday

Figure 1: Examples of decoy documents used in conjunction with the exploit

The report summarises our findings based on samples collected in 2016, and explores similarities and differences in the shellcode between different documents exploiting this vulnerability.

To request your copy, e-mail threatintelligence@uk.pwc.com - note this is not for lead generation purposes, but is rather to avoid disclosing to adversaries how their attacks can be linked.

The samples analysed & their command & control addresses are given below:

Samples (initial MD5s):

3fe0cbedec6969803a72b8c76a4a0a03

50064d33625970a8145add7e3e242fe3

6a6a8cb2e59439891e53b04024573d37

e1b4a5a565fdfcec52346d3b6063c587

9b6af5f8878a3fde32a3e8ff3cf98906

6d55eb3ced35c7479f67167d84bf15f0

21bb2d447247fd81c42d4262de36adb6

375e51a989525cfec8296faaffdefa35

445886e6187cb36ee33ef7e27b7d5dbe

f4c1e96717c82b14ca76384cb005fbe5

aae962611da956a26a76d185455f1d44

c591263d56b57dfadd06a68dd9657343

03a537ff04deaf2c30b23122d795fee2

a4144b9bc99ab39d16c8125a19382316

bfc4133a64a8a8a53c02f9d471c79c16

07614906c9b0ed9cfae07306c32555b9

e63896f2dfcc2ee2173944ef16ddc131

805a522481056441e881c46c69b808f6

c48521d427f40148ee6e5a953ea23622

ebc3f26c0bfc473c840c9e4f3393671d

238ca1ab29f191b767837748fb655c8e

2689515f0bbdf4f3fd4448d0fdc9f2a7

f89c4fb64edc993604d53e5fad6585d4

e95f65bfe3e54d58dcbef3275d0c3f49

e61211931319ece42ec4755a6f6fc815

b49de68758f2c1c2f7dfe60fe67d1516

d0533874d7255b881187e842e747c268

e560dfba68e5bd9a84aeb7b79c9b11ea

edde511d4872c4b2551e7ad22e746fb6

40fdca3c932b12b6740cea1266021c6e

07614906c9b0ed9cfae07306c32555b9

03726d30ebffaf5455a932dee69ce6e7

03726d30ebffaf5455a932dee69ce6e7

07614906c9b0ed9cfae07306c32555b9

C2s:

sent[.]leeh0m[.]org

found[.]leeh0m[.]org

64[.]62[.]238[.]73

newsupdate.dynssl[.]com

121[.]127[.]249[.]74

carwiseplot[.]no-ip[.]org

goback[.]strangled[.]net

win7_8d90f[.]dns04[.]com

37[.]10[.]71[.]35

www[.]kashiwa-js[.]com

78[.]128[.]92[.]49

news[.]rinpocheinfo[.]com

59[.]188[.]13[.]204

coffeol[.]com

updo[.]nl

[1] https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/twoforonefinal.pdf