



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.Н.Овсяник

Date	Weekday	Holiday name	Holiday type
01-01	Monday	New Year's Day	Public Holiday
01-02	Tuesday	New Year's Day	Public Holiday
01-03	Wednesday	New Year's Day	Public Holiday
01-04	Thursday	New Year's Day	Public Holiday
01-05	Friday	New Year's Day	Public Holiday
01-06	Saturday	New Year's Day	Public Holiday
01-07	Sunday	New Year's Day	Public Holiday
01-08	Monday	New Year's Day	Public Holiday
01-09	Tuesday	New Year's Day	Public Holiday
01-10	Wednesday	New Year's Day	Public Holiday
01-11	Thursday	New Year's Day	Public Holiday
01-12	Friday	New Year's Day	Public Holiday
01-13	Saturday	New Year's Day	Public Holiday
01-14	Sunday	New Year's Day	Public Holiday
01-15	Monday	New Year's Day	Public Holiday
01-16	Tuesday	New Year's Day	Public Holiday
01-17	Wednesday	New Year's Day	Public Holiday
01-18	Thursday	New Year's Day	Public Holiday
01-19	Friday	New Year's Day	Public Holiday
01-20	Saturday	New Year's Day	Public Holiday
01-21	Sunday	New Year's Day	Public Holiday
01-22	Monday	New Year's Day	Public Holiday
01-23	Tuesday	New Year's Day	Public Holiday
01-24	Wednesday	New Year's Day	Public Holiday
01-25	Thursday	New Year's Day	Public Holiday
01-26	Friday	New Year's Day	Public Holiday
01-27	Saturday	New Year's Day	Public Holiday
01-28	Sunday	New Year's Day	Public Holiday
01-29	Monday	New Year's Day	Public Holiday
01-30	Tuesday	New Year's Day	Public Holiday
01-31	Wednesday	New Year's Day	Public 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):

- 3fe0cbdec6969803a72b8c76a4a0a03
- 50064d33625970a8145add7e3e242fe3
- 6a6a8cb2e59439891e53b04024573d37
- e1b4a5a565dfccec52346d3b6063c587
- 9b6af5f8878a3fde32a3e8ff3cf98906
- 6d55eb3ced35c7479f67167d84bf15f0
- 21bb2d447247fd81c42d4262de36adb6
- 375e51a989525cfec8296faaffdefa35
- 445886e6187cb36ee33ef7e27b7d5dbe
- f4c1e96717c82b14ca76384cb005f5e5
- aae962611da956a26a76d185455f1d44

Email alerts
Join today to receive email alerts when we publish new articles

Search the site

Search our archive

Articles by category

Articles by month

Are you ready for the new data privacy world?
Register for our live webcast on Wednesday 2 March 2016

Latest posts from Cyber security updates

- [Exploring CVE-2015-2545 and its users](#)
- [Social Media – The Hacking Revolution](#)
- [Taiwan Presidential Election: A Case Study on Thematic Targeting](#)
- [Cyber security - Are you ready for the new data privacy world?](#)
- [Amazing what you see over lunch...](#)
- [What the recent JANET attack tells us about Social Media Risk](#)
- [The concept of 'cyber' in a criminal world](#)
- [ELISE: Security Through Obesity](#)
- [Why 2015 was the tipping point for cybersecurity](#)
- [#PrivateBizChat: Cybersecurity - 15 December, 12.30pm - 1.30pm](#)

Cyber security
Building confidence in your digital future

Breach aid
Are you suffering a cyber, privacy or data breach?

Data protection and privacy

c591263d56b57dfadd06a68dd9657343
03a537ff04deaf2c30b23122d795fee2
a4144b9bc99ab39d16c8125a19382316
bfc4133a64a8a8a53c02f9d471c79c16
07614906c9b0ed9cfae07306c32555b9
e63896f2dfcc2ee2173944ef16ddc131
805a522481056441e881c46c69b808f6
c48521d427f40148ee6e5a953ea23622
ebc3f26c0bfc473c840c9e4f3393671d
238ca1ab29f191b767837748fb655c8e
2689515f0bbdf4f3fd4448d0fdc9f2a7
f89c4fb64edc993604d53e5fad6585d4
e95f65bfe3e54d58dcbef3275d0c3f49
e61211931319eace42ec4755a6f6fc815
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>



 **Comments**

Post a comment

Comments are moderated and will not appear until the author has approved them.

If you have a TypeKey or TypePad account, please [Sign in](#)

© 2012-2016 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

[Privacy Statement](#) [Cookies info](#) [Legal Disclaimer](#) [Provision of Services](#) [Diversity](#)