China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Media Outlets

fireeye.com/blog/threat-research/2015/11/china-based-threat.html

Threat Research

FireEye Threat Intelligence

Dec 01, 2015

8 mins read

Malware

FireEye Threat Intelligence analysts identified a spear phishing campaign carried out in August 2015 targeting Hong Kong-based media organizations. A China-based cyber threat group, which FireEye tracks as an uncategorized advanced persistent threat (APT) group

and other researchers refer to as “admin@338,” may have conducted the activity.[1] The email messages contained malicious documents with a malware payload called LOWBALL. LOWBALL abuses the Dropbox cloud storage service for command and control (CnC). We collaborated with Dropbox to investigate the threat, and our cooperation revealed what may be a second, similar operation. The attack is part of a trend where threat groups hide malicious activity by communicating with legitimate web services such as social networking and cloud storage sites to foil detection efforts.[2][3]

A Cyber Campaign Likely Intended to Monitor Hong Kong Media During a Period of Crisis

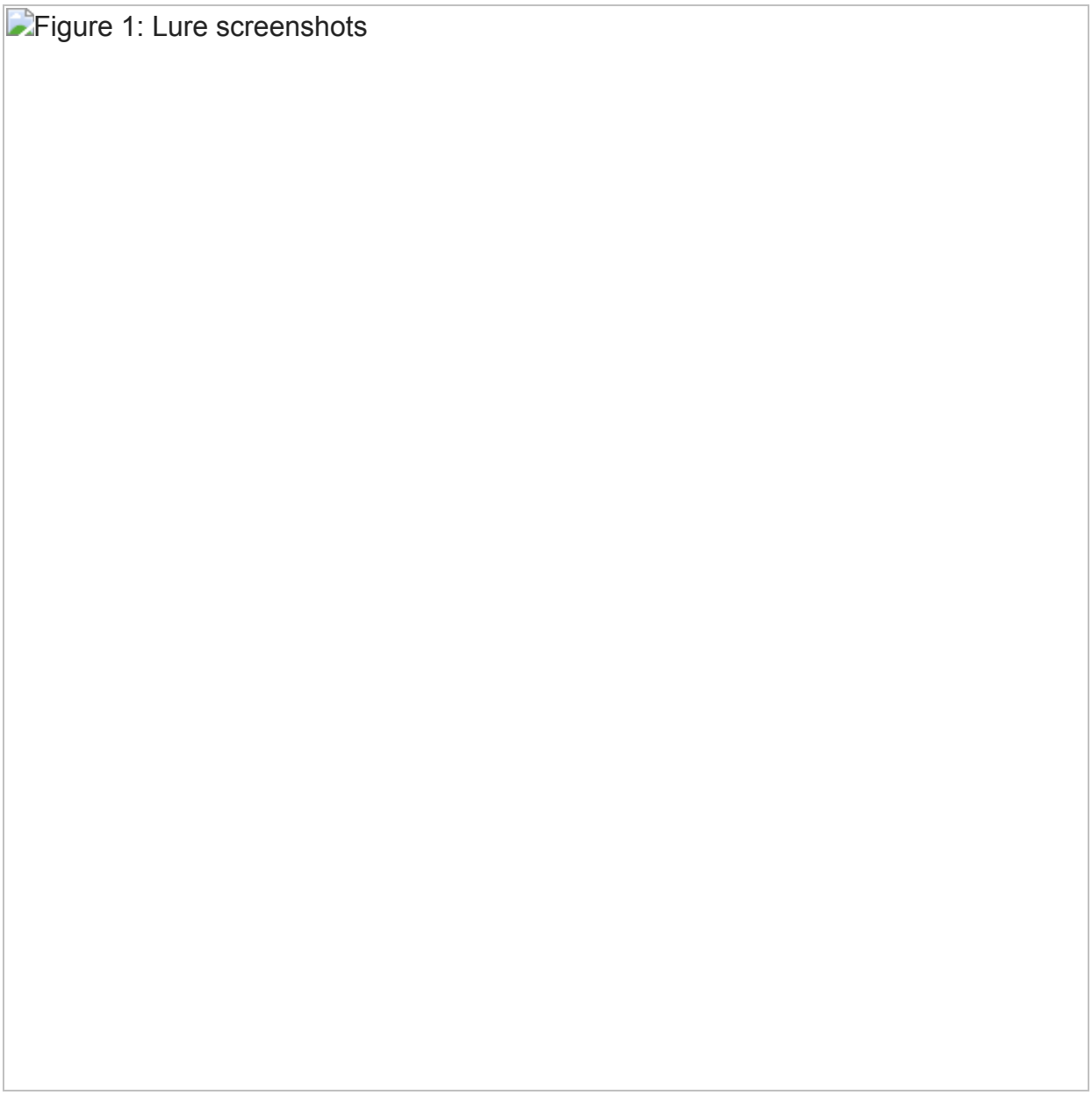
The threat group has previously used newsworthy events as lures to deliver malware.[4] They have largely targeted organizations involved in financial, economic and trade policy, typically using publicly available RATs such as Poison Ivy, as well some non-public backdoors.[5]

The group started targeting Hong Kong media companies, probably in response to political and economic challenges in Hong Kong and China. The threat group’s latest activity coincided with the announcement of criminal charges against democracy activists.[6] During the past 12 months, Chinese authorities have faced several challenges, including large-scale protests in Hong Kong in late 2014, the precipitous decline in the stock market in mid-2015, and the massive industrial explosion in Tianjin in August 2015. In Hong Kong, the pro-democracy movement persists, and the government recently denied a professor a post because of his links to a pro-democracy leader.[7]

Multiple China-based cyber threat groups have targeted international media organizations in the past. The targeting has often focused on Hong Kong-based media, particularly those that publish pro-democracy material. The media organizations targeted with the threat group’s well-crafted Chinese language lure documents are precisely those whose networks Beijing would seek to monitor. Cyber threat groups’ access to the media organization’s networks could potentially provide the government advance warning on upcoming protests, information on pro-democracy group leaders, and insights needed to disrupt activity on the Internet, such as what occurred in mid-2014 when several websites were brought down in denial of service attacks.[8]

Threat Actors Use Spear Phishing Written in Traditional Chinese Script in Attempted Intrusions

In August 2015, the threat actors sent spear phishing emails to a number of Hong Kong-based media organizations, including newspapers, radio, and television. The first email references the creation of a Christian civil society organization to coincide with the anniversary of the 2014 protests in Hong Kong known as the Umbrella Movement. The second email references a Hong Kong University alumni organization that fears votes in a referendum to appoint a Vice-Chancellor will be co-opted by pro-Beijing interests.[9]



The group's previous activities against financial and policy organizations have largely focused on spear phishing emails written in English, destined for Western audiences. This campaign, however, is clearly designed for those who read the traditional Chinese script commonly used in Hong Kong.

LOWBALL Malware Analysis

The spear phishing emails contained three attachments in total, each of which exploited an older vulnerability in Microsoft Office (CVE-2012-0158):

MD5	Filename
b9208a5b0504cb2283b1144fc455eaaa	使命公民運動 我們的異象.doc

ec19ed7cddf92984906325da59f75351	新聞稿及公佈.doc
6495b384748188188d09e9d5a0c401a4	(代發)[采訪通知]港大校友關注組遞信行動.doc

In all three cases, the payload was the same:

MD5	Filename
d76261ba3b624933a6ebb5dd73758db4	time.exe

This backdoor, known as LOWBALL, uses the legitimate Dropbox cloud-storage service to act as the CnC server. It uses the Dropbox API with a hardcoded bearer access token and has the ability to download, upload, and execute files. The communication occurs via HTTPS over port 443.

After execution, the malware will use the Dropbox API to make an HTTP GET request using HTTPS over TCP port 443 for the files:

MD5	Filename
d76261ba3b624933a6ebb5dd73758db4	WmiApCom
79b68cdd0044edd4fbf8067b22878644	WmiApCom.bat

The “WmiApCom.bat” file is simply used to start “WmiApCom”, which happens to be the exact same file as the one dropped by the malicious Word documents. However, this is most likely meant to be a mechanism to update the compromised host with a new version of the LOWBALL malware.

The threat group monitors its Dropbox account for responses from compromised computers. Once the LOWBALL malware calls back to the Dropbox account, the attackers will create a file called “[COMPUTER_NAME]_upload.bat” which contains commands to be executed on the compromised computer. This batch file is then executed on the target computer, with the results uploaded to the attackers’ Dropbox account in a file named “[COMPUTER_NAME]_download”.

We observed the threat group issue the following commands:

```
@echo off
dir c:\ >> %temp%\download
ipconfig /all >> %temp%\download
net user >> %temp%\download
net user /domain >> %temp%\download
ver >> %temp%\download
del %0
```

```
@echo off
dir "c:\Documents and Settings" >> %temp%\download
dir "c:\Program Files\
" >> %temp%\download
net start >> %temp%\download
net localgroup administrator >> %temp%\download
netstat -ano >> %temp%\download
```

These commands allow the threat group to gain information about the compromised computer and the network to which it belongs. Using this information, they can decide to explore further or instruct the compromised computer to download additional malware.

We observed the threat group upload a second stage malware, known as BUBBLEWRAP (also known as Backdoor.APT.FakeWinHTTPHelper) to their Dropbox account along with the following command:

```
@echo off
```

ren "%temp%\upload" audiodg.exe
start %temp%\audiodg.exe
dir d:\ >> %temp%\download
systeminfo >> %temp%\download
del %0

We have previously observed the admin@338 group use BUBBLEWRAP. This particular sample connected to the CnC domain accounts.serveftp[.]com, which resolved to an IP address previously used by the threat group, although the IP had not been used for some time prior to this most recent activity:

MD5		
0beb957923df2c885d29a9c1743dd94b	accounts.serveftp.com	59.188.0.197

BUBBLEWRAP is a full-featured backdoor that is set to run when the system boots, and can communicate using HTTP, HTTPS, or a SOCKS proxy. This backdoor collects system information, including the operating system version and hostname, and includes functionality to check, upload, and register plugins that can further enhance its capabilities.

A Second Operation

FireEye works closely with security researchers and industry partners to mitigate cyber threats, and we collaborated with Dropbox to respond to this activity. The Dropbox security team was able to identify this abuse and put countermeasures in place.

Our cooperation uncovered what appears to be a second, ongoing operation, though we lack sufficient evidence to verify if admin@338 is behind it. The attack lifecycle followed the same pattern, though some of the filenames were different, which indicates that there may be multiple versions of the malware. In addition, while the operation targeting Hong Kong-based media involved a smaller number of targets and a limited duration, we suspect this second operation involves up to 50 targets. At this time, we are unable to identify the victims.

In this case, after the payload is delivered via an exploit the threat actor places files (named upload.bat, upload.rar, and period.txt, download.txt or silent.txt) in a directory on a Dropbox account. The malware beacons to this directory using the hardcoded API token and attempts

to download these files (which are deleted from the Dropbox account after the download):

- upload.bat, a batch script that the compromised machine will execute
- upload.rar, a RAR archive that contains at least two files: a batch script to execute, and often an executable (sometimes named rar.exe) which the batch script will run and almost always uploads the results of download.rar to the cloud storage account
- silent.txt and period.txt, small files sizes of 0-4 bytes that dictate the frequency to check in with the CnC

The threat actor will then download the results and then delete the files from the cloud storage account.

Conclusion

LOWBALL is an example of malware that abuses cloud storage services to mask its activity from network defenders. The LOWBALL first stage malware allows the group to collect information from victims and then deliver the BUBBLEWRAP second stage malware to their victims after verifying that they are indeed interesting targets.

A version of this article appeared first on the FireEye Intelligence Center. The FireEye Intelligence Center provides access to strategic intelligence, analysis tools, intelligence sharing capabilities, and institutional knowledge based on over 10 years of FireEye and Mandiant experience detecting, responding to and tracking advanced threats. FireEye uses a proprietary intelligence database, along with the expertise of our Threat Intelligence Analysts, to power the Intelligence Center.

[1] FireEye currently tracks this activity as an “uncategorized” group, a cluster of related threat activity about which we lack information to classify with an advanced persistent threat number.

[2] FireEye. Hiding in Plain Sight: FireEye and Microsoft Expose Obfuscation Tactic. https://www2.fireeye.com/rs/fireye/images/APT17_Report.pdf

[3] FireEye. HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group.

[4] Moran, Ned and Alex Lanstein. FireEye. “Spear Phishing the News Cycle: APT Actors Leverage Interest in the Disappearance of Malaysian Flight MH 370.” 25 March 2014. https://www.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.

[5] Moran, Ned and Thoufique Haq. FireEye. “Know Your Enemy: Tracking a Rapidly Evolving APT Actor.” 31 October 2013. FireEye. Poison Ivy: Assessing Damage and Extracting Intelligence

[6] BBC News. “Hong Kong student leaders charged over Umbrella Movement.’” 27 August 2015. http://www.bbc.com/news/world-asia-china-34070695.

[7] Zhao, Shirley, Joyce Ng, and Gloria Chan. “University of Hong Kong’s council votes 12-8 to reject Johannes Chan’s appointment as pro-vice-chancellor.” 30 September 2015. http://www.scmp.com/news/hong-kong/education-community/article/1862423/surprise-move-chair-university-hong-kong.

[8] Wong, Alan. Pro-Democracy Media Company’s Websites Attacked. “Pro-Democracy Media Company’s Websites Attacked.” New York Times. 18 June 2014. http://sinosphere.blogs.nytimes.com/2014/06/18/pro-democracy-media-companys-websites-attacked/.

[9] “HKU concern group raises proxy fears in key vote.” EIJ Insight. 31 August 2015. http://www.ejinsight.com/20150831-hku-concern-group-raises-proxy-fears-in-key-vote/.