Insider Information

An intrusion campaign targeting Chinese language news sites

By Jakub Dalek, Geoffrey Alexander, Masashi Crete-Nishihata, and Matt Brooks July 5, 2017

"内幕消息"：一起针对中文新闻媒体的入侵行动

Key Findings

- This report reveals a campaign of reconnaissance, phishing, and malware operations that use content and domains made to mimic Chinese language news websites.
- We confirm the news portal China Digital Times was the target of a phishing operation and show how content and domains were made to mimic four other newsgroups in reconnaissance and malware operations: Mingjing News, Epoch Times, HK01, and Bowen Press. We cannot confirm if these other groups were directly targeted. These news websites report on issues sensitive to the government of China and are blocked in the country. However, this report does not conclusively attribute the campaign to a publicly reported threat actor or state sponsor.
- The malware operation made efforts to evade detection and frustrate analysis. The operation combined obfuscated, packed executables and custom shellcode with an additional step of using compromised servers to host the malicious payload. We identify the payload as NetWire, a commodity remote access trojan typically seen used in cybercrime activities and not commonly observed in Asia.
- We connect the infrastructure used in the campaign to previous malware operations targeting a Tibetan radio station and the Thai government. We also connect one of the code signing certificates we observed to a campaign targeting gaming companies. It is notable that NetWire was also used as a payload in that campaign.

Summary

A journalist at China Digital Times (CDT), (an independent Chinese and English language news portal), receives an email from a source claiming to have a tip on a sensitive story: "I have insider information that is different from what you've published". The email includes a link to an article from the news portal. Clicking on the link displays the article with a pop-up message asking the journalist to enter their username and password in prompt designed to look like a WordPress login page. What is normally a routine interaction for the journalist has become increasingly threatening. The tip from the source is actually an attempt to steal the journalist's WordPress credentials used to manage and publish content to the news portal.

The rouse used in the phishing email was clever, but it did not work. The journalist was immediately suspicious of the phishing attempts and shared them with researchers at the Citizen Lab to analyze, which led to the discovery of a wider campaign targeting Chinese language news sites using various tactics including reconnaissance, phishing, and malware. The campaign used domains and copied content that masqueraded as Epoch Times, Mingjing News, HK01, and Bowen Press. It is not clear if these other news groups were directly targeted. These organizations often report on issues that are politically sensitive to the government of China and their websites are blocked in the country. Our analysis of the infrastructure used in this campaign reveals connections to previous malware operations targeting Tibetan journalists and the Thai government. These incidents includes targets that are generally within the geopolitical interest of the government of China. However, this report does not conclusively attribute the campaign to a publicly reported threat actor or state sponsor.

There are numerous incidents of journalists and news organizations reporting on China being targeted by digital espionage operations. In 2009, as part of the GhostNet investigation, Citizen Lab found that China-based operators had infiltrated the mail servers of Associated Press offices in London and Hong Kong. Another investigation in 2009, by Nart Villeneuve and Greg Walton uncovered a targeted malware campaign against China-based journalists working at Reuters, the Straits Times, Dow Jones, Agence France Presse, and Ansa. In recent years other major news organizations, including the The New York Times, the Wall Street Journal, and the Washington Post, have reported intrusions of their networks and systems by China-based operators. In each incident, the operators were suspected to be sponsored by the government of China with the motivation of gathering information on China-related reporting that the newspapers were covering.

These historical incidents and the campaign we analyze in this report serve as a general reminder that the media are targets for digital espionage and, as a result, news organizations and journalists need to reflect on their business practices and behaviours and adopt a more systematic approach to information security.

This report proceeds in five parts outlined below:

Part 1: Phishing Operation Targeting China Digital Times

This section describes phishing messages sent to China Digital Times and our subsequent investigation into the tactics and server infrastructure used in the operation.

Part 2: Uncovering a Wider Campaign

This section reveals how the operation against China Digital Times was part of a wider campaign of phishing, reconnaissance, and malware operations that used domains and content made to mimic four other Chinese-language news organizations, Epoch Times, Mingjing News, HK01, and Bowen Press.

Part 3: Malware Operation

This section describes a malware operation that used content and domains made to mimic Chinese-language news organizations HK01 and Bowen Press. The malware operation made efforts to evade detection and frustrate analysis. The operation combined obfuscated, packed executables and custom shellcode with an additional step of using compromised servers to host the malicious payload. We identify the payload as NetWire, a commodity remote access trojan that is not commonly observed in Asia and typically seen used in cybercrime activities.

Part 4: Campaign Connections

This section links infrastructure used in the campaign against Chinese-language news site to previous malware campaigns targeting a Tibetan radio station and the Thai government. It also shows the same certificate information used to sign the malware in this campaign was used by other malware operations targeting gaming companies.

Part 5: Discussion and Conclusions

This section summarizes the characteristics of the campaign and how it reflects wider information security challenges for news organizations and journalists.

Part 1: Phishing Operation Targeting China Digital Times

This section describes a phishing messages sent to China Digital Times and our subsequent investigation into the tactics and server infrastructure used in the operation.

A Suspicious Tip: "I Have Insider Information"

China Digital Times is a multi-language news portal that reports on political issues in China and aggregates Internet content that has been censored in the country. It was founded by Xiao Qiang, a Professor at the University of California, Berkeley who has been engaged in human rights activism since the 1989 Tiananmen Square Massacre.

On February 12, 2017, a CDT staff member received an email from a person claiming to be a UC Berkeley student with "insider information" on claims made by 郭云贵 (Guo Yungui) on "hacker attacks" against the Chinese language news site Mingjing News. The characters 郭云贵 (Guo Yungui) appears to be a slight variation of Guo Wengui (郭文贵), a Chinese billionaire who has gained notoriety after voicing allegations that high ranking officials in the Communist Party of China are engaged in corruption. In January 2017 he had an interview with Mingjing News in which he made further unconfirmed allegations regarding official corruption and abuse. Following this interview, the editor of Minjing News, claimed "several sites and channels of Mingjing were attacked by vicious groups controlled by corrupt parties."

The email sent to CDT included a link that directly referenced an IP address rather than a domain name. The staff member was immediately suspicious and did not click on the link (see below):

Original Email Text

From: papa papa hellomice@mail.com
Date: February 12 2017
Subject: 我是伯克利加州大学的学生，我想认识一下您，我有爆料
To: [REDACTED]我想向您爆料，关于郭云贵说中国黑客攻击明镜具体内幕。
hXXp://43.240.14.37/asdasdasadqddd12222111[.]php/article.asp=search.php

English Translation

From: papa papa hellomice@gmail.com
Date: February 12 2017
Subject: I am a student of UC Berkeley. I want to get to know you and I have some explosive revelations for you
To: [REDACTED]I'd like to reveal some detailed insider information on Guo Yungui's claims that Chinese hackers attacked Mingjing News
website.hXXp://43.240.14.37/asdasdasadqddd12222111[.]php/article.asp=search.php

Three days later, the staff member received another email offering insider information on the Mingjing attacks. This email included a link that, at first glance, appeared to be the domain of China Digital Times, but with a slight misspelling. Instead of chinadigitaltimes.net the link sent was `chinadagitaltimes[.]net` with an added **'a'** instead of an **'i'** in the word digital. A day after this email was sent, other staff members at CDT received similar emails with the same link (see below).

Original Email Text

From: sda daua caisia.anmindo@mail.com
Date: February 14 2017
Subject: 您好，我想向您提供相关内幕
To: [REDACTED]您好：
我有关于中国时代日报上的一篇文章最新的消息，中国黑客攻击的后续事件以及最近明镜网被攻击的内幕信息
文章地址:hXXp://www.chinadagitaltimes[.]net/2016/07/chinese-hackers-blamed-multiple-breaches-fdic/文中写的与我这边得到的消息有些差异点

English Translation

From: sda daua caisia.anmindo@mail.com
Date: February 14 2017
Subject: Hi, I'd like to offer you some insider information.
To: [REDACTED]I have the latest information on an article published by China Daily. It's about follow-ups on the incident of Chinese hackers and some insider information on the recent attacks against Mingjing News.
Link to the article.
hXXp://www.chinadagitaltimes[.]net/2016/07/chinese-hackers-blamed-multiple-breaches-fdic/The information presented in the article is slightly different from the information I know.

The link connects to a web page that mirrors content from the real CDT website displaying an article related to hacker groups from China (see **Figure 1** for comparison of the real and fake content).

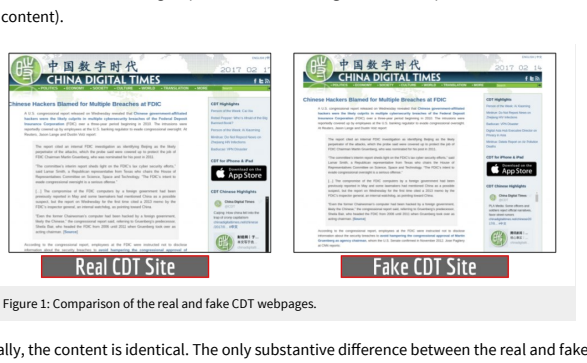


Figure 1: Comparison of the real and fake CDT webpages.

Visually, the content is identical. The only substantive difference between the real and fake content is a few lines of javascript code (see **Figure 2**).

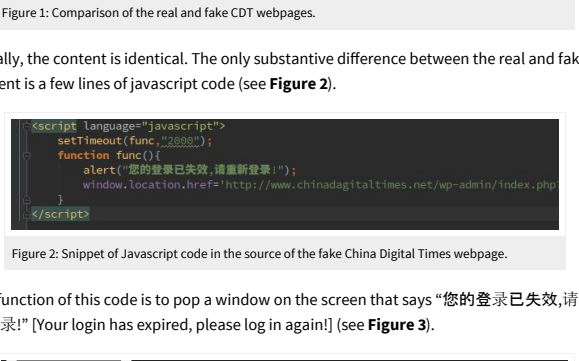


Figure 2: Snippet of Javascript code in the source of the fake China Digital Times webpage.

The function of this code is to pop a window on the screen that says "您的登录已失效,请重新登录!" [Your login has expired, please log in again!] (see **Figure 3**).

Figure 3: Screenshot of the fake China Digital Times webpage and the popup message displayed.

If the OK button is clicked, the user is forwarded to what appears to be a WordPress login page (see **Figure 4**).

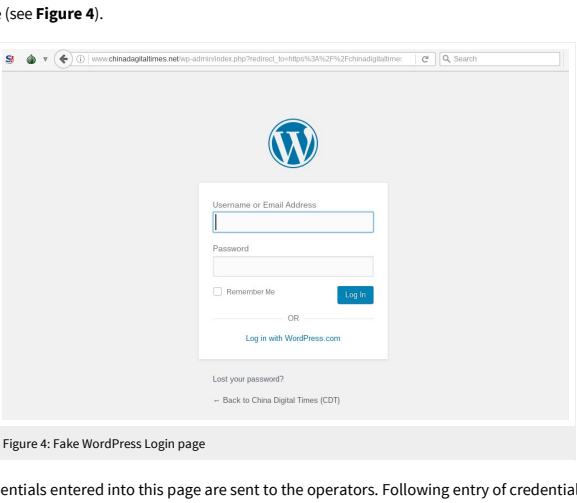


Figure 4: Fake WordPress Login page

Credentials entered into this page are sent to the operators. Following entry of credentials, users are forwarded to the real CDT site. The real CDT website runs on WordPress, and therefore the purpose of this phishing campaign is to steal credentials to the actual CDT website and gain access. The operators customized a fake domain to host real content and developed custom phishing pages for stealing the WordPress credentials demonstrating a substantial level of effort.

Phishing Operation Timeline

Through analysis of the server used to host the phishing pages and the phishing emails sent to CDT we documented the activities and timeline of the operation, which lasted for approximately 20 days (see **Figure 5**). The operation began with the operators scanning the real CDT website for vulnerabilities. Five days later the first phishing email was sent. The next day the operators registered the domain mimicking the CDT site, set up the fake site, and sent out phishing emails with links to it. Over the next week further phishing emails were sent to CDT. Through analysis of log files found on the server we observed what appears to be the operators testing the phishing page during this period. The last phishing email sent to CDT was on February 20. Eight days later the fake CDT website was taken down and no further phishing emails were sent.

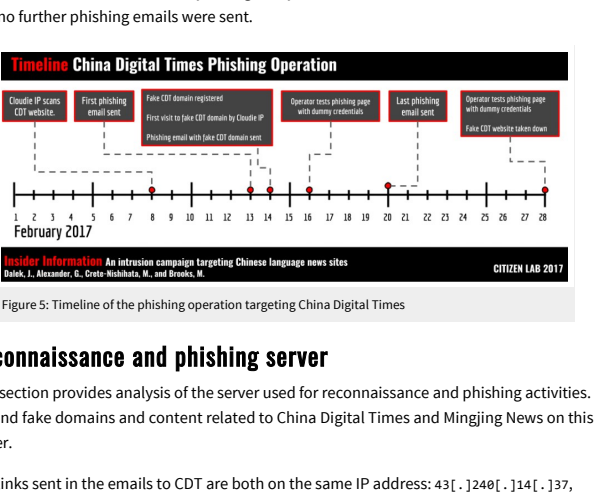


Figure 5: Timeline of the phishing operation targeting China Digital Times

Reconnaissance and phishing server

This section provides analysis of the server used for reconnaissance and phishing activities. We find fake domains and content related to China Digital Times and Mingjing News on this server.

The links sent in the emails to CDT are both on the same IP address: `43[.]240[.]14[.]37`, hosted by Cloudie, a hosting provider based in Hong Kong. The link provided in the first phishing email sent to CDT included the full IP address of the server.

```
hXXp://43.240.14.37/asdasdasadqddd12222111[.]php/article.asp=search.php
```

Four days after the first phishing email was sent to CDT we accessed the content on the page and found it served content copied from a Mingjing News article about illicit sales of Chinese visas (See **Figure 6** for comparison of the real and fake content).

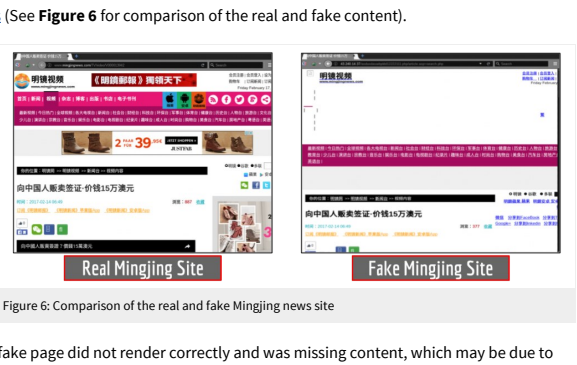


Figure 6: Comparison of the real and fake Mingjing news site

The fake page did not render correctly and was missing content, which may be due to improper mirroring of the content, or possibly because the page relies on external content in a location that changed since the initial copy. Comparing the legitimate page to the fake page finds no addition of code by the operator on the fake page.

Reconnaissance Server Log Analysis

We investigated the directory of the fake Minjing News page and found the content was modified on February 14, 2017 and discovered a file '`log.txt`'. This file is a custom log that captures three pieces of information from every visitor to the page: IP address, web browser user agent, and time visited (see **Figure 7**). There is no malicious content on the page. We suspect that the purpose of this page is to perform reconnaissance of targets by testing if users will click on the link, and by retrieving IP addresses and user agent information.

Figure 7: Server directory containing the log.txt file.

The first visit in the log file is on February 2, 2017 from the IP address `45[.]124[.]24[.]39` which is also hosted on Cloudie. This visit is likely from the operators because it was the first visit and from the same provider on which the server is hosted. There are also two visits in the logs within seconds of each other, from the IP address `125[.]86[.]123[.]47` (ChinaNet, Chongqing China)

Examining the email headers from the phishing emails reveals two IP addresses, including the same Cloudie IP and another ChinaNet Chongqing IP (see below):

```
45[.]124[.]24[.]39 Cloudie HK
141[.]30[.]39[.]155: ChinaNet Chongqing
```

We shared these IP addresses with CDT to check if the addresses had visited the real CDT website around the period of the phishing emails. We found that the Cloudie IP address (`45[.]124[.]24[.]39`) visited the real CDT web site 42,000 times on February 8 2017, during a four hour period. The rate of the requests, user agents utilized, and information requested indicates that these visits were attempts to enumerate HTTP paths on the website to test for vulnerabilities. This scan occurred less than a week before the operators staged the phishing page sent to CDT.

Phishing Server Log Analysis

Between February 14 and 28, 2017, a direct visit to the URL `hXXp://43[.]240[.]14[.]37` returned a copy of the CDT homepage (see **Figure 8**).

Figure 8: Comparison of the real frontpage of CDT (as seen on day the emails were sent) and the fake webpage

This fake homepage was not included in the emails sent to CDT. The operators potentially included this homepage if users clicked the link in the email and then viewed the top level URL to ensure they were on the right site (see below).

Email Link: `chinadagitaltimes[.]net/2016/07/chinese-hackers-blamed-multiple-breaches-fdic`
Home page: `chinadagitaltimes[.]net`

The directory of `chinadagitaltimes[.]net/2016/07` shows the content listed on the server and lists the last modified date of the content as February 15, 2017 (see **Figure 9**).

Figure 9: An index listing on the phishing server.

We found a file '`log.txt`' on the fake CDT home page and article web pages. This log file records the IP address, browser user agent, and timestamp of visitors to the pages. We found an additional log in the URL of the fake WordPress login page that captures username, password and date to record credentials that are entered.

The logs only included what we suspect to be fake credentials, which demonstrates the phishing attempts were unsuccessful. The first entry on February 16, 2017 may be a record of the operator testing the phishing page.

```
username:1111----password:1111----2017-02-16 09:26:14
```

On February 28, we again see what appear to be test credentials added.

```
username:12312----password:1232131----2017-02-28 10:25:33
```

Phishing Operation Final Stages

On February 20, the CDT staff member who received the original phishing email was sent a follow-up email that responded to an auto away message from the staff member and reminded the recipient about the link that was sent. This was the last phishing email sent to CDT (see below):

Original Email Text

From: papa papa hellomice@mail.com
To: [REDACTED]
Date: February 20 2017
Subject: Fwd: 我是伯克利加州大学的学生，我想认识一下您，我有爆料[REDACTED]您好:
我想写一篇文章，请如何注册与登录；thxSent: February 14 2017
From: [REDACTED]
To: "papa papa"hellomice@mail.com
Subject: Re: 我是伯克利加州大学的学生，我想认识一下您，我有爆料
谢谢来信，非常抱歉我本月20号之前都没有时间，请月底和我再联系。谢谢，2017-02-13 18:34 GMT-08:00 papa papa hellomice@mail.com
我想向您爆料，关于郭云贵说中国黑客攻击明镜具体内幕。
hXXp://43.240.14.37/asdasdasadqddd12222111[.]php/article.asp=search.php

English Translation

From: papa papa hellomice@mail.com
To: [REDACTED]
Date: February 20 2017
Subject: Fwd: I am a student at UC Berkeley. I want to get to know you and I have some exclusive information to expose. I would like to publish an article. How do I register and log in? thxSent: Tuesday, February 14, 2017 at 1:35 PM
From: [REDACTED]
Subject: Re: I am a student at UC Berkeley. I want to get to know you and I have some exclusive information to expose.
To: "papa papa" hellomice@mail.com
Thanks for the email. Unfortunately I don't have time before 20th this month. Please contact me again at the end of this month. Thank you.2017-02-13 18:34 GMT-08:00 papa papa hellomice@mail.com
I would like to expose some materials to you. It is about the insider information of Guo Yungui's claim that Chinese hackers attacked Ming Jing News.
hXXp://43.240.14.37/asdasdasadqddd12222111[.]php/article.asp=search.php

Later on the same day, the phishing pages and log files were taken offline serving a 404 error if visited. The bare IP of the server (`43[.]240[.]14[.]37`) also switched to returning a default CentOS test page. After the site was taken down on February 28 no additional phishing emails were sent and we observed no other activity.

Analysis of passive DNS records and WHOIS registration information associated with the server infrastructure used to host the fake CDT page led to the discovery that the phishing operation targeting CDT was part of a wider campaign.

Part 2: Uncovering a Wider Campaign

This section reveals how the operation against China Digital Times was part of a wider campaign of phishing, reconnaissance, and malware operations that used domains and content made to mimic four other Chinese language news organizations.

Infrastructure Connections

After examining the server used to host the fake CDT page and referencing passive DNS records and WHOIS registration information, we found other fake domains registered by the same entity with copied content from Chinese-language news sites. Our analysis shows that the operators are using the fake domains for at least three different purposes: reconnaissance, phishing, and malware. We were only able to collect phishing emails sent to CDT and cannot confirm if the other media organizations were direct targets or if the fake domains were used to target other groups. **Table 1** provides an overview of groups that the operator attempted to mimic through fake domains and / or copied content.

Organization	Fake Domain Registered	Site contents copied	Confirmed targeting	Purpose
China Digital Times	X	X	X	Phishing
Mingjing News		X		Recon
HK01		X		Malware
Bowen Press	X	X		Unknown
Epoch Times	X			Unknown

The fake domains are linked by common WHOIS registration information, which shows they were all registered by the same entity. The WHOIS registration information used to register the fake CDT domain is as follows:

```
Name: free tibet
Mailing Address: Uniter states, Phoenix Arizona 86303 US
Phone: +1.2126881188
Email: aobama_5@yahoo.com
```

We found a series of domains registered with the same information. The majority of these domains are designed to mimic domains of Chinese-language news sites. We resolved each domain to determine if they are active and which IP they resolve to (see **Table 2**).

Domain	Registration Date	Real Organization	Hosting Status (As of March 15th)
secuerserver[.]com	2015-08-31	GoDaddy (secureserver.com)	Not resolving
bowenpress[.]com	2015-10-07	Bowen Press (bowenpress.com)	Parked Page (GoDaddy)
bowenpress[.]net	2015-10-07	Bowen Press (bowenpress.com)	Parked Page (GoDaddy)
bowenpress[.]org	2015-10-07	Bowen Press (bowenpress.com)	Parked Page (GoDaddy)
bowenpross[.]com	2015-10-07	Bowen Press (bowenpress.com)	Parked Page (GoDaddy)
datalink[.]one	2016-07-07	n/a	Gorillaservers
chinadagitaltimes[.]net	2017-02-14	China Digital Times (chinadigitaltimes.net)	Cloudie HK
epochatimes[.]com	2017-02-27	Epoch Times (theepochtimes.com)	Cloudie HK

The registration dates show the operators have been registering fake domains that mimic Chinese language news websites since 2015, when they registered domains made to look like the real domain of news site Bowen Press (`bowenpress[.]com`).

We investigated the servers hosting the domains and found the operators use two servers for different purposes: one for phishing and reconnaissance activities and another to serve malware.

The phishing and reconnaissance server hosted the fake CDT domain, the fake Mingjing page, and a domain made to look like the legitimate domain of Epoch Times (a multilingual media organization started by Chinese-American Falun Gong supporters.

On February 26 2017, the operators registered a fake domain mimicking the main Epoch Times domain (epochtimes[.]com), which adds an additional **'a'** after 'epoch' (`epochatimes[.]com`).

Following our discovery of the fake Epoch Times domain we notified the organization and shared indicators of compromise. Epoch Times found a Cloudie IP (`103.200.31[.]164`) that sent 24,183 requests during a 12 hour period on March 8, 2017 to the subscription page of Epoch Times at the URL `subscribe.epochtimes.com`. These requests appear to be attempts to enumerate HTTP paths, similar to the requests sent to China Digital Times on February 8.

Given the timeframe of the registration of the fake Epoch Times domain, we suspect the operators may have moved from targeting CDT to Epoch Times. The fake Epoch Times domain was hosted on the same server as the fake CDT and Mingjing pages (`43.240.14[.]37`). However, we did not find content copied from any Epoch Times websites on the operator's infrastructure during the investigation and did not have any phishing emails reported to us. It is possible that the fake Epoch Times domain is being used for phishing or reconnaissance, but we are unable to confirm.

In addition to phishing and reconnaissance activities the operators are also engaged in malware operations and have a dedicated server for this purpose. We discovered the malware server by resolving the domain: `datalink[.]one`, and found it hosted NetWire, a commodity remote access trojan, and included bait content and domains designed to mimic Chinese-language news organizations HK01 and Bowen Press.

Part 3: Malware Operation

This section describes a malware operation that used content and domains made to mimic Chinese-language news organizations HK01 and Bowen Press. The malware operation made efforts to evade detection and frustrate analysis. The operation combined obfuscated, packed executables, and custom shellcode with an additional step of using compromised servers to host the malicious payload. We identify the payload as NetWire, a commodity remote access trojan that is not commonly observed in Asia and typically seen used in cybercrime activities.

Malware server and analysis

Our investigation of the malware operation began with analysis of the server used to host the malware. The malware server is on the IP address: `23[.]239[.]106[.]119` hosted by GorillaServers, a provider based in the United States. We found the server by resolving the domain datalink[.]one, which was one of the domains registered by the operators.

On the server we found domains and copied content mimicking HK01 and Bowen Press, but cannot confirm if these groups were direct targets of the malware operation or if the content was used as lures to target other groups.

Passive DNS records for the IP address: `23[.]239[.]106[.]119` show a number of other domains that we have connected to the operators including:

Domains
datalink[.]one
get.adobe.com.bowenpress[.]org
hk.secuerserver[.]com
pop.secuerserver[.]com
smtpout.secuerserver[.]com
www.bowenpress[.]org
www.mail.secuerserver[.]com
www.secuerserver[.]com
www.vnews[.]hk

We found that some of these domains were used as command and control servers for the malware we found hosted on the domain.

HK01 Lure

When we first investigated the malware server on March 6, 2017 we found it was hosting what appears to be a copy of the frontpage of HK01, a Hong Kong-based news site (see **Figure 10**).

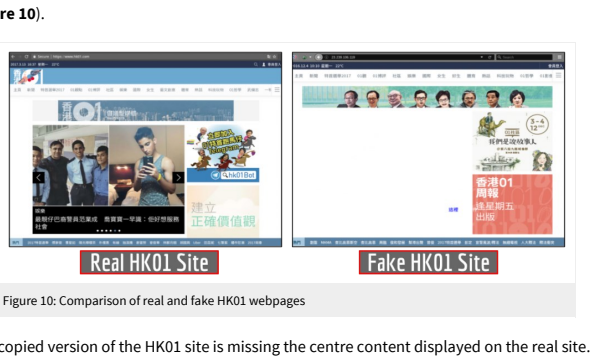
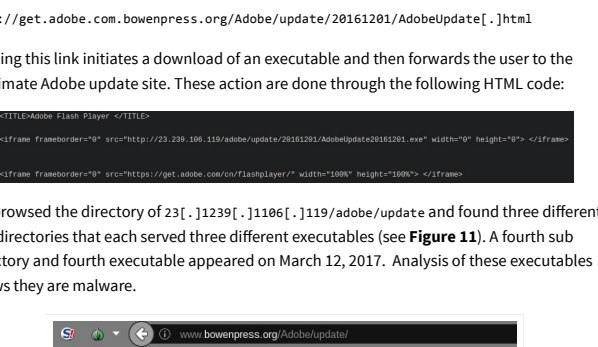


Figure 10: Comparison of real and fake HK01 webpages

The copied version of the HK01 site is missing the centre content displayed on the real site. Instead it shows a link with the following text: "Adobe Flash Player 版本過低，請點擊" [Adobe Flash Player this version is outdated. Please click].

The link connects to:
`hXXp://get.adobe.com.bowenpress.org/Adobe/update/20161201/AdobeUpdate[.]html`

Clicking this link initiates a download of an executable and then forwards the user to the legitimate Adobe update site. These action are done through the following HTML code:



We browsed the directory of `23[.]239[.]106[.]119/adobe/update` and found three different sub directories that each served three different executables (see **Figure 11**). A fourth sub directory and fourth executable appeared on March 12, 2017. Analysis of these executables shows they are malware.

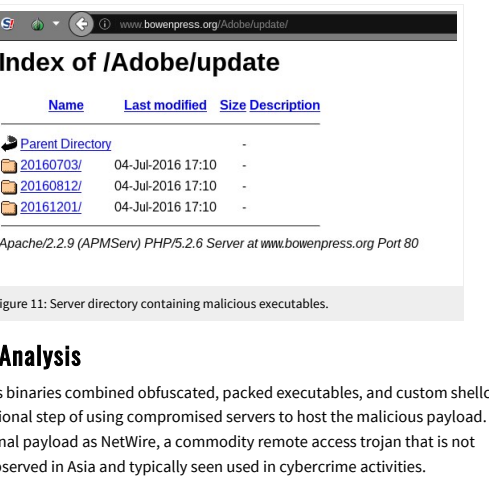


Figure 11: Server directory containing malicious executables.

Malware Analysis

The malicious binaries combined obfuscated, packed executables, and custom shellcode with an additional step of using compromised servers to host the malicious payload. We identify the final payload as NetWire, a commodity remote access trojan that is not commonly observed in Asia and typically seen used in cybercrime activities.

The four executables we found in the "Adobe update" directory are named to appear as an update for Adobe Flash followed by a date stamp (e.g., `AdobeUpdate20160703.exe`).

Each malware file was digitally signed:

File	Certificate Details
AdobeUpdate20160703.exe	无锡凯扬电子科技有限公司 **Serial:** 57 be 1a 00 d2 e5 9b db d1 95 24 aa a1 7e d9 3b **Valid From:** Thursday, November 19, 2015 5:45:01 PM **Valid To:** Saturday, November 19, 2016 5:45:01 PM
AdobeUpdate20160812.exe	深圳市乐途儿科技有限公司 **Serial:** 68 be c5 c0 26 4c c9 09 6d 2f b2 0a 98 86 e9 4d **Valid From:** Monday, June 15, 2015 4:00:00 PM **Valid To:** Thursday, June 15, 2017 3:59:59 PM
AdobeUpdate20161201.exe AdobeUpdate20170312.exe	Elex do Brasil Participações Ltda **Serial:** 06 71 ee 52 6a cb 6f 9b e2 01 f5 a8 e2 03 c4 1c **Valid From:** Sunday, April 12, 2015 4:00:00 PM **Valid To:** Wednesday, July 12, 2017 3:59:59 PM

All four samples are packed with VMProtect, software used to obfuscate source code to make anaylsis and reverse engineering more difficult. When executed the samples unpack and drop a second VMProtect-packed `DLL` to the following location:

```
C:\Program Files\Common Files\Microsoft Shared\VGX\Stub.dll
```

Before executing the dropped `DLL` via `rundll32` as shown:

```
rundll32.exe C:\Program Files\Common Files\Microsoft Shared\VGX\Stub.dll,Install
```

This stub `DLL` unpacks itself and then gains persistence by creating a new autorun service: `COM+ Event Log`. The `DLL` edits the following registry keys to create this new service:

```
HKLM\Software\Microsoft\Windows NT\CurrentVersion\SvcHost\EventSystemLog
HKLM\System\CurrentControlSet\Services\EventSystemLog
HKLM\System\CurrentControlSet002\Services\EventSystemLog
HKLM\System\CurrentControlSet003\Services\EventSystemLog
```

Once the `DLL` has gained persistence it starts the newly created service. When run as part of a service, the `DLL` unpacks itself and attempts to download what appears to be a `jpg` file hosted on one of three websites: a Chinese-language news organization, a University, and a software company.

Each of the 4 samples uses a different URL. Each of these files begins with a 631 byte `jpg` header followed by encrypted shellcode. The malware first decrypts the payload immediately after the `jpg` header using the following algorithm:

```
for i = 0; i < len(payload); i++ payload[i] = (16 * ~((((payload[i] ^ 0x50) >> 4) ^ 1) & 0xf) & 0xef) ^ payload[i]
```

The decrypted payload begins with a short header consisting of an unsigned 32 bit integer that is the size of the stage 2 payload, an unsigned 32 bit integer used as a checksum, and 64 bytes of padding. This header is followed by a block of shellcode and a second encrypted payload (see **Figure 12**). The shellcode decrypts the stage 2 payload using RC4 with different 256-bit keys for each sample.

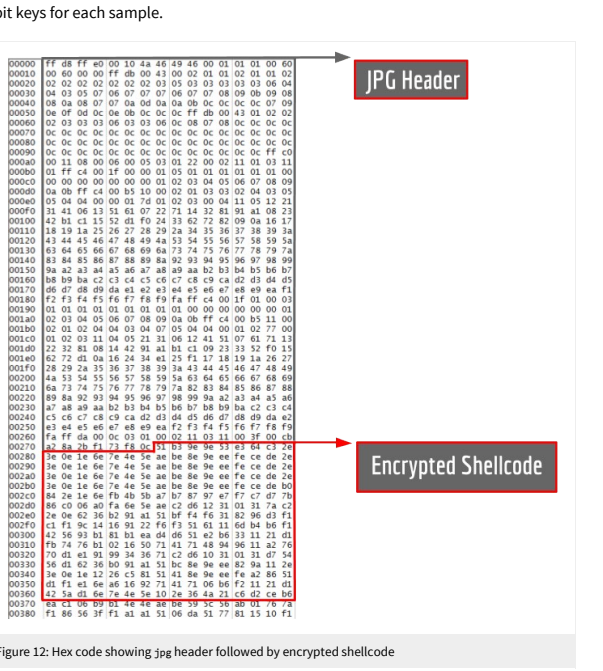


Figure 12: Hex code showing `jpg` header followed by encrypted shellcode

This decrypted data contains additional shellcode followed by a PE file. We identify the PE file as the Netwire RAT. The final stage shellcode acts as a loader and maps the RAT into memory and resolves the RAT's imports before jumping to the RAT's entrypoint.

Netwire RAT is a multi-platform RAT (Remote Access Tool) that first appeared in 2012. Since its appearance, Netwire RAT has been used in a variety of attacks ranging from stealing credit card data to targeted campaigns against health care and banking sectors. The Netwire samples we analyzed are capable of a wide-range of behavior including:

- Reading stored usernames and passwords from common apps including:
  - Web Browsers
  - Email Clients
  - Instant Messaging Clients
- Keylogging
- Taking Screenshots
- Audio capture
- Screen recording
- Process listing, creation, killing, etc.
- Uploading and downloading files

Each of the 4 fake `jpg` files contains a Netwire sample containing different configuration settings. After analyzing the samples we recovered the configuration settings for each sample (see **Appendix A**). The use of multiple layers of packed or obfuscated payloads is likely an attempt to evade detection and analysis. Downloading the RAT each time the malware runs could be an attempt to hide the final payload, as the Netwire samples are never written to disk. This process makes direct analysis difficult without memory images or an understanding of the payload decryption and shellcode routines to decrypt the RAT manually. Using different configurations for each sample could be an attempt to use specific domains tailored to each target, or to allow for the use of multiple domains as fallbacks in case previously used domains are discovered and blocked.

Each of the four binary samples we analyzed downloaded a copy of the Netwire RAT as a different "`jpg`" file. The three hosts used are all legitimate servers with active web pages. In each case, the `jpg` downloaded by the malware is noticeably larger than other files in the same directory on the server and was last modified more recently. We believe that each of the three servers used to host the "`jpg`" files have been compromised and that the operator is using these legitimate servers to host their payload in an effort to hide their activities.

Like the phishing operation, the malware setup shows a significant level of effort. We observe custom shellcode paired with an additional step of using likely-compromised servers to host the payload. While Netwire has been seen in some targeted intrusions, it has primarily been used in cybercrime activities and is not common in Asia.

Bowen Press Lures

The earliest domains registered by the operators that follow the pattern of mimicking China related news organizations were decoys for Bowen Press. The real Bowen Press domain is `bowenpress[.]com`, the operators registered bowenpress[.]org. We were unable to retrieve the content that originally appeared on the domains in 2015. However, we were able to find copied Bowen Press content on the malware server through Google searches on the "news" subdirectory of the server. The content was an iframe of the front page of Bowen Press and results in rendering additional error messages (See **Figure 13**). The existence of Bowen Press content on this server suggests that the operators may have been using Bowen Press lures to serve malware.

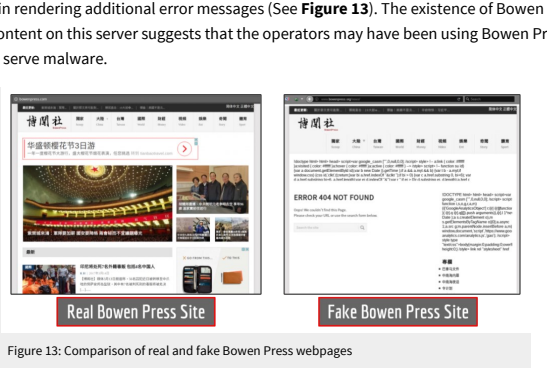


Figure 13: Comparison of real and fake Bowen Press webpages

Additionally,we found the Netwire samples in a directory under the URL `www.bowenpress[.]org/Adobe/update`, even though the website serving the sample was a copy of HK01. The use of this URL path further suggests that the fake Bowen Press domain and content were used to serve malware at some point. The operators may have simply reused the domain for the HK01 related campaign.

On March 15, 2017, the front page of the malware server was changed to a copy of the Bowen Press website that mirrored content from the same day (see **Figure 14**). The copied page did not contain any malicious code and we were unable to find a `log.txt` file on the server.

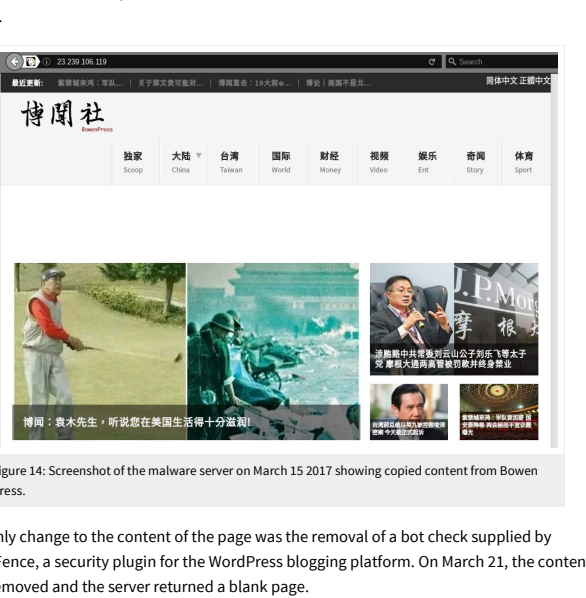


Figure 14: Screenshot of the malware server on March 15 2017 showing copied content from Bowen Press.

The only change to the content of the page was the removal of a bot check supplied by WordFence, a security plugin for the WordPress blogging platform. On March 21, the content was removed and the server returned a blank page.

We cannot confirm what was the purpose of the recently copied Bowen Press content. However, it shows that the operators have had a continued interest in using Bowen Press content as lures potentially to serve malware.

Part 4: Campaign Connections

This section links infrastructure used in the campaign against the Chinese-language news sites to previous malware campaigns targeting a Tibetan Radio Station and the Thai government. It also highlights connections between certificate information used to sign the Netwire samples we analyzed and malware used in campaigns targeting gaming companies.

Infrastructure Connections to Malware Operations against Tibetan Radio Station

Domain registration information for some of the infrastructure used in the campaign have links to earlier targeted malware operations against civil society and government groups in Asia.

The WHOIS records for the domains used in the phishing and malware operations include the phone number (`12126881188`). Searching other WHOIS records for this number reveals a known command and control server with a Tibet theme. The WHOIS information for this domain matches all the fields with the exception of the email address. All other fields used match including the same address and misspelling of United States as 'Uniter States'.

```
Domain: www.tibetonline[.]info
Name: free tibet
Mailing Address: Uniter states, Phoenix Arizona 86303 US
Phone: +1.2126881188
Email: rooterit@outlook.com (admin)
fightfortibet@ymail.com (billing)
```

The registrant e-mail is linked to another domain in addition to `tibetonline[.]info` which is `rooter[.]tk`. Both these domains are linked to a 2013 campaign targeting Voice of Tibet, an independent radio station reporting on Tibetan issues. In this campaign, the two domains were reported by ThreatConnect as being used as a command and control server (`rooter[.]tk`) and hosting an Adobe Flash heap spray vulnerability (`tibetonline[.]info`) as well as an IE exploit (CVE-2013-1347).

Infrastructure Connections to Malware Operations against Thai Government

The domain `tibetonline[.]info` was also identified by Palo Alto Networks as a command and control server used for FFRAT malware recently described by Cylance. This infrastructure overlapped with servers used by a threat actor targeting Thai government entities with the Bookworm trojan in 2015. The general tactics, techniques, and procedures used by this threat actor also show similarities to the campaign we analysed. Both used the same hosting provider on one IP: Cloudie HK (`103.226.127[.]47`), and used fake Adobe updates to lure targets into installing malware. The threat actor documented by Palo Alto also used fake news site domains (*e.g.*, `vancouversun[.]us`, `yomiuri[.]us`, `voanews[.]hk`, and `nhknews[.]hk`) Finally, both operations leveraged compromised web servers for command and control.

Certificate Connections to Malware Targeting Gaming Companies

In October 2016 Cylance disclosed information on a threat actor called "PassCV", which targeted the gaming industry and used stolen code signing certificates to sign malware.

The disclosure was an update to information published by Symantec in July 2014 and Kaspersky's 2013 view into Winnti.

Cylance lists three malware samples signed with one of the same certificates used to sign one of the Netwire dropper files in the operation we report on:

```
57 BE 1A 00 D2 E5 9B DB D1 95 24 AA A1 7E D9 3B
```

In addition, Cylance also notes the discovery of Netwire being used in the same campaign. The use of Netwire is notable as it is the only other mention of it being used in Chinese-nexus malware operations of which we are aware.

The disclosure was an update to information published by Symantec in July 2014 and Kaspersky's 2013 view into Winnti.

Explaining the Connections

These overlaps point to a number of potential scenarios. The campaign we analyzed may have been conducted by the same threat actors as the previous operations. Alternatively the overlap may be an artifact of resource sharing between separate but unrelated threat actors — potentially through the use of a "digital quartermaster" (a group that supplies operators with malware and other resources), or more informal means. While the first scenario is possible, we do not have enough information to fully substantiate it. We suspect that at the least there is some level of sharing and reuse of infrastructure by the same operator or group of operators. The targets in most of these other campaigns (ethnic minority groups, government in Southeast Asia, and news sites reporting on China) generally fall into the geopolitical interests and strategic concerns of the government of China. However, we have insufficient information to conclusively attribute the campaign to a specific threat actor or state sponsor.

Part 5: Discussion and Conclusion

This section summarizes the characteristics of the campaign and how it reflects wider information security challenges for news organizations and journalism.

A Patient and Persistent Operator

While the tactics used in these campaigns are technically simple, the operators demonstrate patience and persistence. They have been using content and domains mimicking Chinese-language news sites as lures since at least 2015, and appear to carefully move from one target to another. The phishing campaign against China Digital Times was stood up and taken down in the span of 20 days. In this period, the operators scanned the CDT site for vulnerabilities, registered a lookalike domain, created a fake CDT decoy site, and sent the group a wave of customized phishing emails. When these efforts were not successful the operators quickly shut down the campaign and moved on to new targeting. The malware operation also showed efforts to bypass detection and analysis. The operators combined obfuscated, packed executables and custom shellcode with an additional step of using compromised servers to host the payload.

The news sites used for lures and targeting in the operation all report on topics seen as politically sensitive by the government of China, and follow a general pattern of news organizations reporting on China being targeted by digital espionage. While there are connections between these targets and the geopolitical concerns of the Chinese government we cannot conclusively attribute this operation to a state sponsor. What we can clearly determine is that this operation was conducted by a threat actor active for at least 2 years that targets Chinese language news organizations with intrusion attempts and appears to carefully move from target to target.

Information Security Challenges for Journalism

This campaign reflects general information security challenges for news organizations and journalists. Journalists operate in high-paced environments under intense time pressures. As part of their practice, they regularly receive information from unknown sources in a variety of media (*e.g.*, social media, email, chat messages, etc). Gathering sources and material requires journalists to be open and accessible online. Journalists also may handle sensitive information and contacts. Ideally, information security should be part of their standard work process, but information security is but one consideration out of many other competing priorities. Journalists and management may not have the same level of awareness or concern for information security threats. Bridging these gaps, balancing conflicting necessities for openness, availability, and security all within a resource-constrained environment are major challenges. Nonetheless, information security needs to be addressed.

The case we analyzed (and many others like it) shows journalists and news groups are being targeted by digital espionage operations designed to access confidential information and systems. The threat is not only against journalists reporting on China. Previous research has found digital espionage operations targeting journalists reporting on the Middle East, Latin America, Russia, and elsewhere. More work is needed to understand the nature of the threats and ways to mitigate them that are sensitive to the practicalities and realities of journalism.

Acknowledgements

We are grateful to China Digital Times, Epoch Times, Bowen Press, and HK01 for their participation.

Thanks to our colleagues for review and assistance: John Scott-Railton, Lotus Ruan, Jeffrey Knockel, Lokman Tsui, Valkyrie-X Security Research Group, Andrew Hilts, Ron Deibert, and TNG.

This project was supported by the John T. and Catherine D. MacArthur Foundation.

Appendix A: Malware Configuration Settings

```
File name: 7.jpg
ConnectionString: email23.secuerserver[.]com:443;
ProxyString: -
Password: Password
HostId: HostId-%Rand%
Mutex: -
InstallPath: -
StartupKeyName1: -
StartupKeyName2: -
KeyLoggerFilePath: -
BoolSettingsByte: 000
ConnectionType: 000
```

```
File name: 8.jpg
ConnectionString: hk.secuerserver[.]com:443;
ProxyString: -
Password: Password
HostId: HostId-%Rand%
Mutex: -
InstallPath: -
StartupKeyName1: -
StartupKeyName2: -
KeyLoggerFilePath: -
BoolSettingsByte: 000
ConnectionType: 001
```

```
File name: HHBcampus.jpg
ConnectionString: HK.SECUERSERVER[.]COM:443;
ProxyString: -
Password: Password
HostId: HostId-%Rand%
Mutex: -
InstallPath: -
StartupKeyName1: -
StartupKeyName2: -
KeyLoggerFilePath: -
BoolSettingsByte: 000
ConnectionType: 001
```

```
Filename: icon_sad.jpg
ConnectionString: dns.bowenpress[.]org:443;
ProxyString: -
Password: Password
HostId: HostId-%Rand%
Mutex: -
InstallPath: -
StartupKeyName1: -
StartupKeyName2: -
KeyLoggerFilePath: -
BoolSettingsByte: 000
ConnectionType: 001
```

Appendix B: Indicators Of Compromise

Indicators of compromise for this report can be found on our github page.

Media Mentions

Gizmodo, China Digital Times, Threat Post, Epoch Times, Times of India, Democracy Now