

# OceanLotus: Extending Cyber Espionage Operations Through Fake Websites

[volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites](https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites)

November 6, 2020

by Steven Adair, Thomas Lancaster, Volexity Threat Research



Since Volexity's 2017 discovery that OceanLotus was behind a sophisticated massive digital surveillance campaign, the threat group has continued to evolve. In 2019, Volexity gave a presentation at RSA Conference that provided a historic and up-to-date look at various operations of the Vietnamese threat actor OceanLotus. Notably, the presentation revealed that, for years, OceanLotus set up and operated multiple activist, news, and anti-corruption websites. At first glance, it appeared these were real websites that had been compromised. These fake websites were convincingly legitimate and allowed OceanLotus to have full control over the tracking of and attacks against website visitors. The most popular of these websites even had a corresponding Facebook page with over **20,000 followers**. Shortly after the presentation was given, these websites were shut down or abandoned. However, old habits and successful techniques die hard. Volexity has identified multiple new attack campaigns being launched by OceanLotus via multiple fake websites and Facebook pages that have been set up within the last year. In addition to targeting those within Vietnam, Volexity has seen renewed targeting of OceanLotus's neighbors throughout Southeast Asia. These websites have been observed profiling users, redirecting to phishing pages, and being leveraged to distribute malware payloads for Windows and OSX. This post will focus on one of the larger campaigns where OceanLotus has leveraged multiple fake news websites to target users.

## Newsorthy Websites

Throughout the year, Volexity identified multiple Vietnamese-language news websites that appeared to be compromised, as they were being used to load an OceanLotus web profiling framework. The exact functionality varied from site to site, but the goal of these frameworks was to gather information about site visitors and, in some cases, deliver malware. This code appears to be a variation of what Volexity has previously described as Framework A.

However, upon closer inspection of the websites, Volexity found the sites were not compromised, instead they were created and operated by OceanLotus. Each of the websites appears to have had a decent level of effort to build it, as there are numerous variations in themes, content, and even custom images and slogans. The websites all claim to be news sites and contain a great deal of benign content, with no malicious redirects or profiling in place on the vast majority of pages including the main index page. Instead, generally speaking, only a handful of specific articles within each site contain malicious content. The sites vary in theme, with some focused on Vietnamese news while others are focused on news themed around other Southeast Asian countries.

A list of websites that Volexity has identified is provided below. Each listing includes a thumbnail image that can be clicked to see a larger screen shot of the website. The majority of these websites are still live at the time of this blog post and Volexity recommends against visiting them.

## Website

## Theme/Notes

### baodachieu.com





This website covers general news and is written in Vietnamese. It has a custom logo and slogan indicating it publishes things that others want to hide.



### baomoivietnam.-com

This website covers general news and is written in Vietnamese. It has a custom logo and tagline indicating it has short and reliable news.



Website	Theme/Notes
<b>ledanvietnam.org</b> 	<p>This website shares “the people’s news” and is written in Vietnamese. It is designed to provide news that is different than that of official government news. It has a custom logo and slogan mentioning truth and responsibility.</p>
<b>nhansudaihoi13.org</b> 	<p>This website is dedicated to news surrounding the upcoming 13th National Congress of the Communist Party of Vietnam, which convenes in January 2021. There is no custom logo or slogan for this website.</p>
<b>tocaonline.org</b> 	<p>This website is dedicated to news and the “truth.” The website has a customized header image that is displayed on all pages.</p>
<b>thamcungbisu.org</b> 	<p>This website covers general news and is written in Vietnamese. There is no custom logo or slogan for this website. It uses many WordPress defaults to include the website description of “Just another WordPress site.”</p>

**Website**

**Theme/Notes**

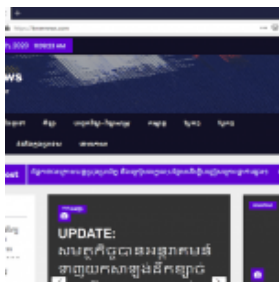
**tinmoivietnam.com**

This website covers general news and is written in Vietnamese. There is no custom logo or slogan for this website. The domain name is very similar in naming to a non-malicious website that is accessible via tinmoivietnam.net.



**kmernews.com**

This website covers general news and is written in Cambodian. It purports to be an “online newspaper” and does not have a custom logo or slogan.



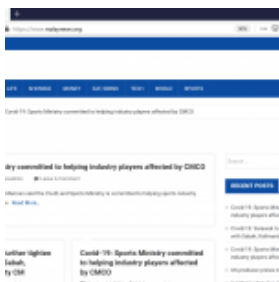
**laostimeneews.com**




This website covers general news and is written in English and Laotian. It looks to take much of its content from the website of the Laotian Times (lao-tiantimes.com). The website does not have a custom logo or slogan.



**malaynews.org**

This website covers general news and is written in English and Malay. The website does not have a custom logo or slogan.



Website	Theme/Notes
<p><b>philiippines-news.net</b></p> 	<p>This website covers general news and is written in English. The website does not have a custom logo or slogan.</p>
<p><b>khmer-liveneews.-com</b></p> 	<p>This website covers general news and is written in Cambodian. The website does not have a custom logo or slogan.</p>
<p><b>khmerleaks.com</b></p> 	<p>This website focuses specifically on Cambodia-centric news and offers content in both Cambodian and English. The slogan for the site is “Stay up to date with the hottest news about the country.”</p>

While a couple of the websites above may use a similar layout, the vast majority have their own theme and layout which makes the sites appear to have nothing to do with one another. The sites also largely stick to a wide variety of news that would be interesting to the masses across the different targeted user bases.

However, one of the sites is a bit more specific than the rest and is quite political in nature. The website **nhansudaihoi13[.]org** pertains to the upcoming 13th Vietnamese Communist Congress where new political leaders will be elected. This website has a corresponding Facebook page filled with posts copied from other Vietnamese media outlets focusing on corruption within Vietnamese politics. The page has over 1,000 likes and interactions from a number of individuals in Vietnam. Notably, the Facebook page has a Messenger account associated with it which could be used to send messages to individuals of interests.

## Targeting Visitors

---

The websites contain numerous articles and content to make them seem legitimate; in some cases the websites have over 10,000 individual news articles. Volexity has found the content is largely scraped and reposted in full from various other legitimate online news outlets. This appears to be done in an automated fashion and most likely through WordPress plugins. Numerous posted articles and images can be directly tracked back to other online blogs and newspapers; sometimes the byline or even watermark in images show directly where the article was sourced. In some cases, only a small number of pages on the site contains malicious code; in other cases, the profiling code is pervasive.

Volexity believes it is likely that individuals are targeted through these websites in two ways. The first is through profiling frameworks that exist on many of the pages that can be used to identify and evaluate information about users that visit the website by happenstance. The second is through individually targeting victims who are sent links to specific news containing malware delivery logic through spear phishing and social media messages.

When the users visit a page with an infection chain on it, malicious JavaScript is loaded. The exact workflow of the script varies between different infected pages but generally there are two parts:

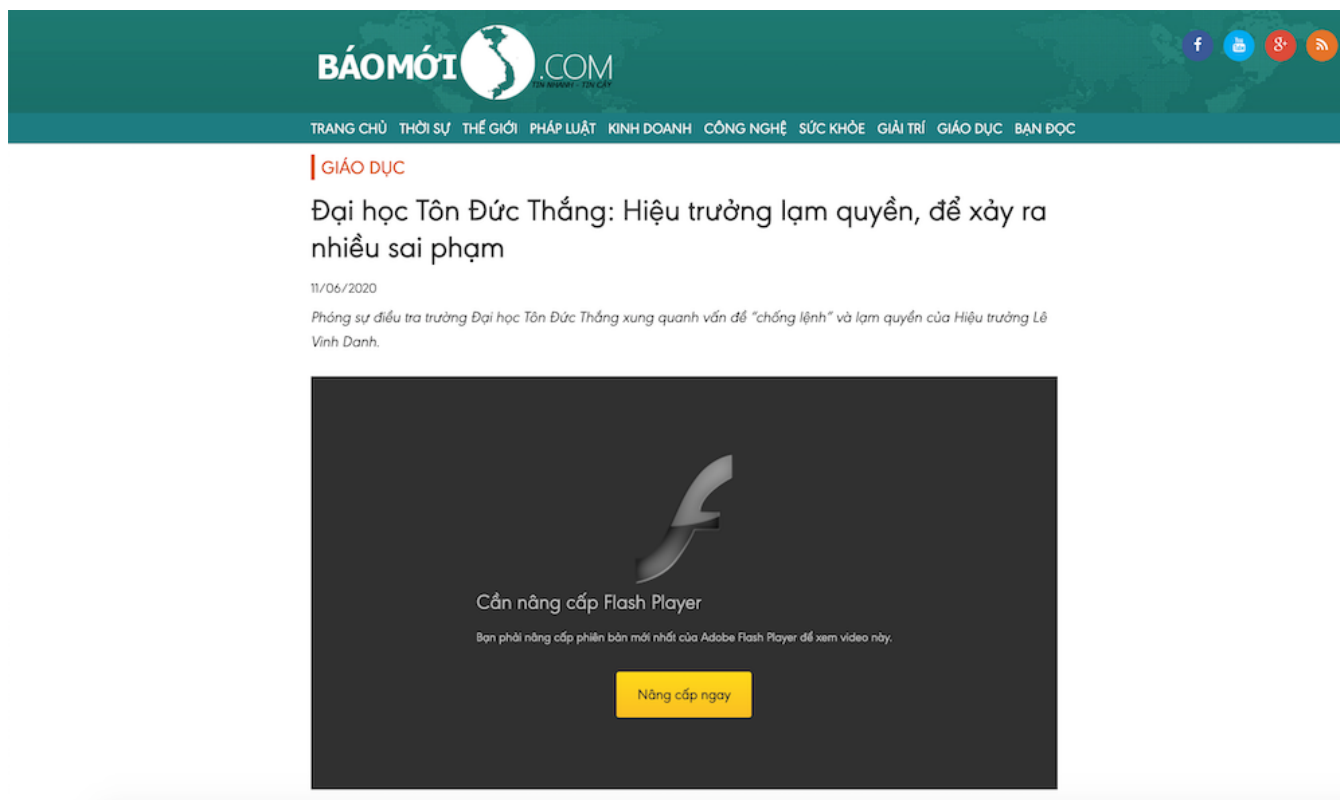
1. A script to capture and store information about the visitor;
2. A second script which socially engineers targets into downloading a fake software update or document. The exact nature of the malware downloaded is sometimes configured based on the user's browser and the content.

To illustrate a real example of how this worked and looked to a website visitor, the following section will use one of the few pages of the fake site **baomoivietnam[.]com** that was designed to profile visitors and deliver malware or a phishing link. On this site, a news story ([https://www.baomoivietnam\[.\]com/dai-hoc-ton-duc-thang-hieu-truong-lam-quyen-de-xay-ra-sai-pham/](https://www.baomoivietnam[.]com/dai-hoc-ton-duc-thang-hieu-truong-lam-quyen-de-xay-ra-sai-pham/)) about an investigation into potential improper conduct by a university professor in Vietnam contained malicious content. Once the page was accessed, a special OceanLotus server on the hostname **cdn.arbenha[.]com** would be leveraged to load malicious JavaScript to load a fake video player. At first, the page would display a dialog indicating that the video was loading (Đang tải) as shown in Figure 1 below.



Figure 1. Fake video player dialog indicating a video is loading

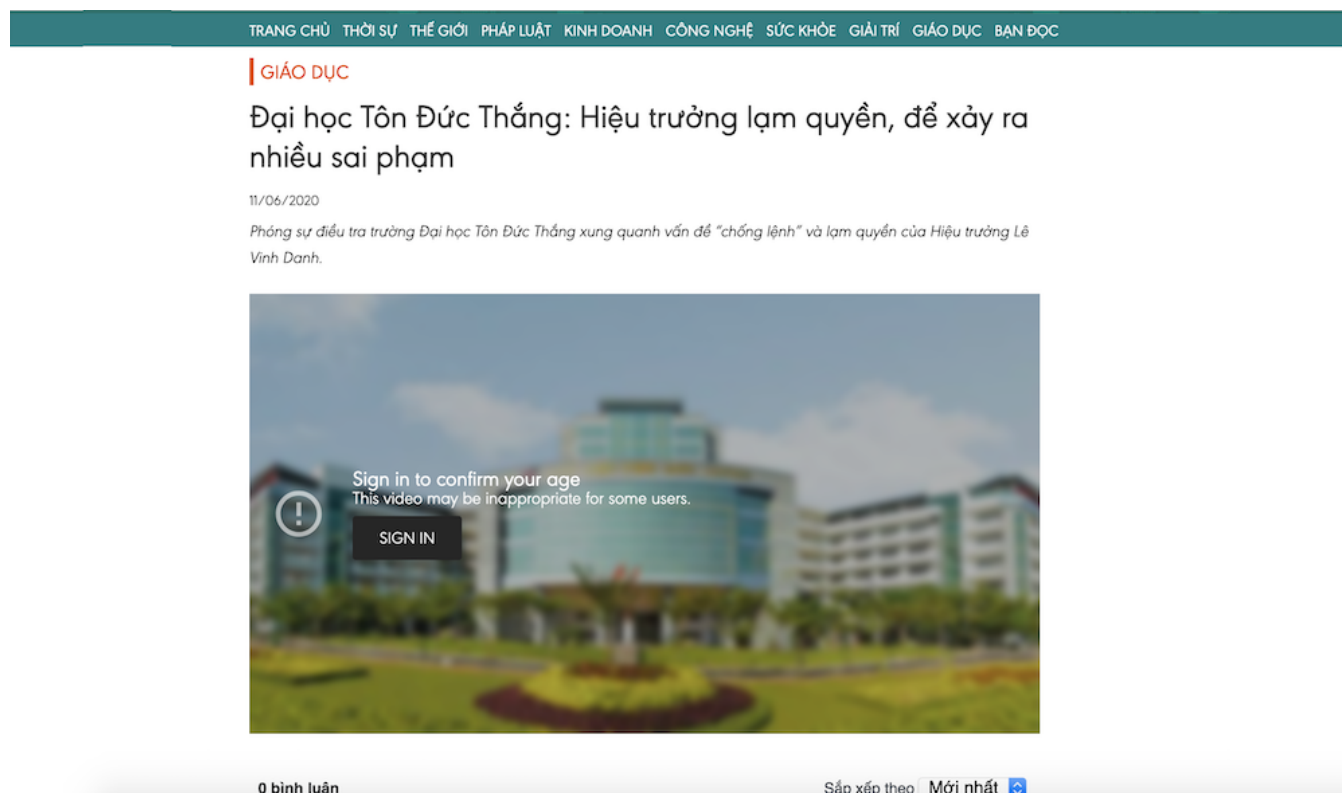
If the visitor is coming from a Windows system, after a few seconds the video will fail to load. A message will be displayed indicating that Flash Player is required, along with a button that can be clicked to immediately upgrade. An image of how this appears to the visitor is shown in Figure 2 below.



*Figure 2. Message displayed alerting the user to upgrade Flash Player*

The button would then lead to the download a RAR archive named *Adobe\_Flash\_Install.rar*. This archive was designed to fool the targeted user into infecting themselves with a Cobalt Strike implant. Details on the contents of this file are included later in this report.

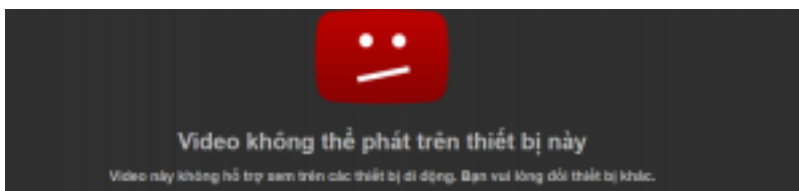
If a visiting user is on a mobile device that was detected as running iOS or Android, an image is displayed, indicating that the requested video contains age-restricted content. The visitor is supposed to “Sign in” to view the content as shown in Figure 3.



*Figure 3. Mobile users presented with “Sign in” message*

The SIGN IN button contained a hyperlink to a page on the hostname **accounts.gservice[.]reviews**. This page was down did not return interesting content in any of Volexity’s tests. Volexity believes this page is likely intended to be used for phishing credentials.

Finally, if users attempt to access the page using a device for which there is no configured payload, they are advised to access the content using a different device. The error this is displayed is shown in Figure 4.



*Figure 4. Message displayed to users not on Windows, Android, or iOS devices.*



The appearance of the overlay and the URL for the various buttons shown above are generated according to the visitor's browser data. A closer look at the payload delivery component of the JavaScript is shown below. It shows the malware download URLs hosted on Dropbox for Windows users, and the identical phishing links for Android and iOS visitors.

```
var os_url_mapping = {
  'windows_x86': 'https://www.dropbox[.]com/s/puhwqhjcvn2xuum/Adobe_Flash_Install.rar?dl=1',
  'windows_x64': 'https://www.dropbox[.]com/s/puhwqhjcvn2xuum/Adobe_Flash_Install.rar?dl=1',
  'linux_x86': '',
  'linux_x64': '',
  'mac_os': '',
  'android': 'https://accounts.gservice[.]reviews/?
  ancf_=36562273654a289e0cc0418f1c9d4b&_hhobt=5b878805dc643d7e66d81b45797a3d323baa7def&edobt=5edf2e13',
  'ios': 'https://accounts.gservice[.]reviews/?
  ancf_=36562273654a289e0cc0418f1c9d4b&_hhobt=5b878805dc643d7e66d81b45797a3d323baa7def&edobt=5edf2e13'
};
```

On other websites, different cloud storage solutions such as Amazon S3 or Google Drive were used to host Windows, OSX, and Android malware payloads. The OSX and Android implants will be detailed in a future blog.

### Cobalt Strike: For Red Teams and Nation State Actors

The Adobe\_Flash\_install.rar archive that was returned from the baomoivietnam[.]com website contained the files **Flash\_Adobe\_Install.exe** and **goopdate.dll**. The table below provides some basic information on all three of these files.

Filename	SHA256	Notes
Adobe_Flash_Install.rar	230ac0808fde525306d6e55d389849f67fc328968c433a5053d676d688032e6f	RAR file containing Adobe_Flash_Install.exe and goopdate.dll
Flash_Adobe_Install.exe	69061e33acb7587d773d05000390f9101f71dfd6eed7973b551594eaf3f04193	A legitimate copy of Google's Update utility

Filename	SHA256	Notes
goop-date.dll	7fd58fa4c9f24114c08b3265d30be5aa8f6519ebd2310cc6956eda6c6e6f56f0	A malicious DLL crafted by the attacker

The file **goopdate.dll** has the hidden file attribute set and will not show in Windows Explorer on systems using default settings. This results in the user seeing only the **Flash\_Adobe\_Install.exe** file to execute in order to install what they believe to be an update to Flash Player. When run, it will automatically load goopdate.dll due to search order hijacking. Goopdate.dll is a highly obfuscated loader whose ultimate purpose is to load a Cobalt Strike stager into memory and then execute it. The Cobalt Strike stager will simply try to download and execute a shellcode from a remote server, in this case using the following URL:

```
| summerevent.webhop[.]net/QuUA
```

The table below has the details for the returned file from the Cobalt Strike staging server at the time of analysis.

SHA256	Notes
cbca9a92a6aa067ff4cab8f1d34ec49ffc9a06c90881f48-da369c973182ce06d	BEACON binary returned by C2 server

This payload is configured to talk to the same domain (summerevent.webhop[.]net) using a malleable command-and-control (C2) profile for Cobalt Strike that impersonates Google's Safe Browsing service. This malleable C2 profile is used by a wide variety of red team and real-world attackers. It is readily available on GitHub and has been used by OceanLotus as far back as 2017. The payload contained several configuration strings encoded with the single-byte XOR key 0x69. Interesting and relevant decoded strings are listed below:

```
summerevent.webhop.net,/safebrowsing/rd/tnOztRgLx1ugKt8uumGcreRFm5CqXD9ge-zzz5sA6WzhC
Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0
@/safebrowsing/rd/r8l4jO3947jVxa5wBhEijGc0y77iX4oFy
GAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
PREF=ID=
Cookie
GAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
U=sRv85UHijBrrWiHz
PREF=ID=
```

## Conclusion

---

OceanLotus has continued to evolve the ways in which it seeks to target individuals outside of spear phishing and leveraging compromised websites. The creation and maintenance of several websites, for the purpose of creating a larger online presence in which the attack chain against visitors can be fully controlled, is not an attack method commonly identified. This level of effort shows that OceanLotus will go to great lengths to extend its reach and find new ways to compromise individuals and organizations it has set its focus on.

Individuals that are at high risk and likely to be targeted by OceanLotus should be particularly careful with respect to websites they are visiting, especially if the websites are suggested or otherwise linked to via e-mail, chat, messaging services, or even SMS. Further, regardless of the websites, Volexity recommends these individuals use extreme caution if a website presents a file for download or requests that they sign in. OceanLotus has used techniques to fool users into revealing their credentials, authorizing malicious OAuth access, or downloading malware onto their systems for several years.

## Indicators of Compromise

---

Value	Type	Notes
thamcungbisu[.]org	Domain	Fake site set up by OceanLotus
baomoivietnam[.]com	Domain	Fake site set up by OceanLotus
baodachieu[.]com	Domain	Fake site set up by OceanLotus
nhansudaihoi13[.]org	Domain	Fake site set up by OceanLotus
tinmoivietnam[.]com	Domain	Fake site set up by OceanLotus
laostimenews[.]com	Domain	Fake site set up by OceanLotus

malaynews[.]org	Domain	Fake site set up by OceanLotus
kmernews[.]com	Domain	Fake site set up by OceanLotus
philiippinesnews[.]net	Domain	Fake site set up by OceanLotus
ledanvietnam[.]org	Domain	Fake site set up by OceanLotus
khmerleaks[.]com	Domain	Fake site set up by OceanLotus
khmer-livenews[.]com	Domain	Fake site set up by OceanLotus
hypepodscase[.]com	Domain	Used to host OceanLotus profiling kit and malware delivery JS
arbenha[.]com	Host-name	Used to host OceanLotus profiling kit and malware delivery JS
gservice[.]reviews	Domain	Likely used in Android phishing in SWC context

summerevent.webhop[.]net	Domain	Cobalt Strike C2 address
dance-til-dawn.podzone[.]net	Domain	Cobalt Strike C2 address
andreagahuvrauvin[.]com	Domain	OceanLotus DNS malware C2 address
theme.blogwix[.]com	Host-name	Used to host OceanLotus profiling kit and malware delivery JS
outlook-client[.]com	Domain	Likely used in phishing in SWC context
gusercontent[.]com	Domain	Likely used in phishing in SWC context
service[.]net	Domain	Likely used in phishing in SWC context
yhsetting[.]com	Domain	Likely used in phishing in SWC context
hmacount[.]com	Domain	Likely used in phishing in SWC context

---

fontloading[.]com	Domain	Likely used in phishing in SWC context
viewerservice[.]com	Domain	Likely used in phishing in SWC context
cbca9a92a6aa067ff4cab8f1d34ec49ffc9a06c90881f48da369c973182ce06d	SHA256	Cobalt-Strike Beacon file
230ac0808fde525306d6e55d389849f67fc328968c433a5053d676d688032e6f	SHA256	RAR delivery file
7fd58fa4c9f24114c08b3265d30be5aa8f6519ebd2310cc6956eda6c6e6f56f0	SHA256	Loader DLL

---