WordPress под прицелом хакеров

Что нужно знать, и как избежать проблем

Коротко обо мне

Денис Синегубко - специалист по безопасности веб сайтов с 6-летним опытом работы в этой области.

Основатель и разработчик онлайн сервиса Unmask Parasites.

Блоггер, автор множества статей о взломах сайтов.

С 2013 г. работаю старшим исследователем в компании Sucuri, Inc., предоставляющей сервисы по мониторингу безопасности сайтов, их защите и восстановлению после взломов.

Каждый сайт попытаются взломать...

… и не раз ...

… независимо от тематики, размеров и платформы

Для чего взламывают сайты?

1. ДЕНЬГИ - чаще всего
2. политика / баловство / личные причины - значительно реже

В подавляющем большинстве случаев целью взлома является не сам сайт, а его посетители и ресурсы сервера.

Как же на взломах можно заработать?

- СПАМ - рассылка спама с сервера
- DDoS
- Black hat SEO
  - вставка скрытых ссылок в собственный контент сайта
  - дорвеи
- Phishing
- Похищение информации для перепродажи
- Перенаправление рекламы и платежей на свои эккаунты.
- Размещение вредоносного кода и атака посетителей сайта.
- Размещение мошеннических сайтов (например, “скачать бесплатно за СМС”) и противозаконного контента.
- Поиск уязвимостей и взлом других сайтов

Дополнительная информация: http://securelist.ru/analysis/1327/e-konomika-botnetov/

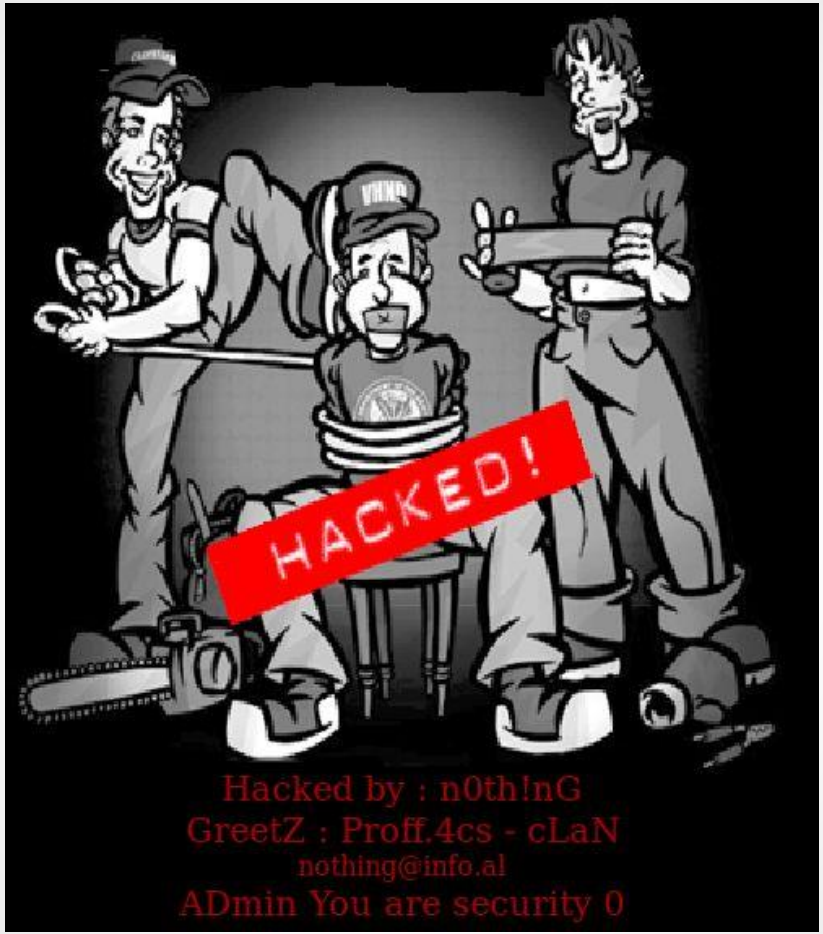
Defacements

Наиболее распространённый вид взломов, где больше хулиганства и политики, чем бизнеса.

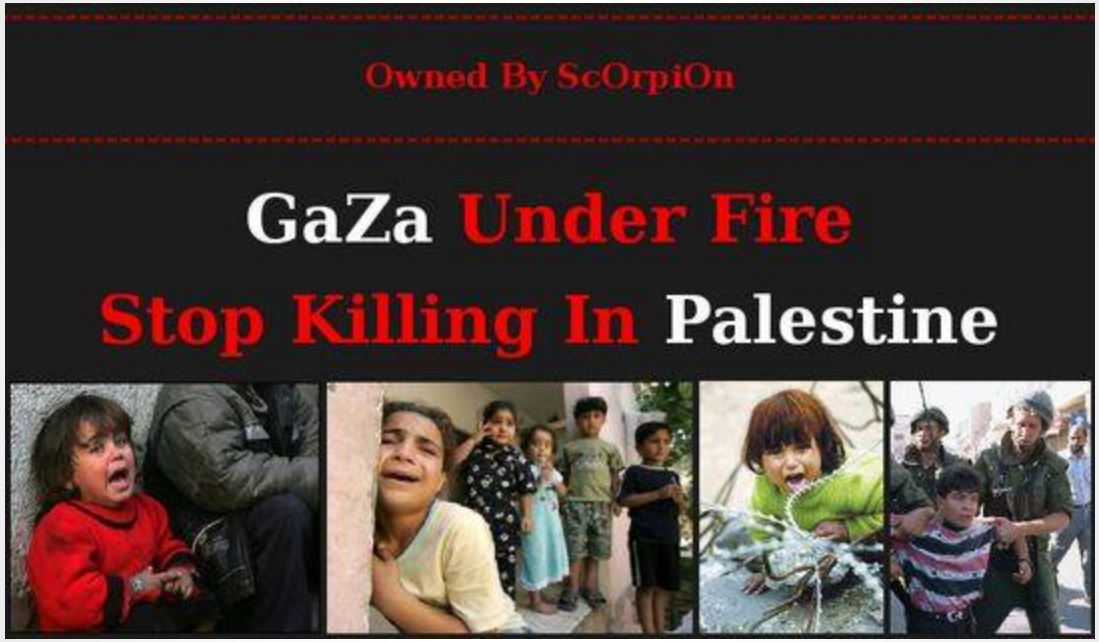
Сайты массово взламывают, чтоб доказать свою “крутизну” и чтоб оставить миру какое-то послание.

Отчёты о таких взломах можно найти на Zone-h.org, где различные хакерские группировки соревнуются друг с другом и выставляют доказательства своих “достижений”.

Примеры: http://blog.sucuri.net/2013/12/friday-the-13th-a-gallery-of-webmaster-nightmares.html



Пример политического послания на взломанной веб странице



Массовый автоматический взлом

Как для “бизнесменов” так и для “активистов” справедливы следующие принципы:

- чем больше сайтов взломать, тем лучше
- каждый взломанный сайт хоть для чего-то сгодится.

Поэтому взлом сайтов автоматизирован и поставлен на поток. За день один человек может взломать тысячи сайтов.

Именно поэтому хакеры любят сайты, построенные на единой платформе и использующие одинаковые компоненты. Они не требуют индивидуального подхода, и их взлом можно автоматизировать, что даёт большую эффективность.

WordPress - самый популярный в мире блог-движок

а значит и самая лакомая цель для хакеров

>60 миллионов сайтов, ~60% в сегменте CMS

Most popular content management systems

© W3Techs.com	usage	change since 1 July 2014	market share	change since 1 July 2014
1. WordPress	22.8%	+0.2%	60.5%	+0.2%
2. Joomla	3.0%	-0.1%	8.1%	-0.1%
3. Drupal	2.0%		5.2%	
4. Blogger	1.1%		2.9%	-0.1%
5. Magento	1.0%		2.7%	

percentages of sites

Fastest growing content management systems since 1 July 2014

© W3Techs.com	sites
1. WordPress	598
2. Magento	47
3. Shopify	37

daily number of additional sites

Данные с http://w3techs.com/

Какие последствия может иметь взлом для сайта?

- **подмоченная репутация (предупреждения поисковиков и антивирусов, defacement, автоматические перенаправления на порно сайты)**
- **риск заразить компьютеры посетителей и свои собственный компьютер**
- **проблемы с ранжированием в поисковиках**
- **потеря траффика, продаж, показов рекламы, отключение рекламных кампаний**
- **повреждение файлов/базы или уничтожение сайта**
- **время, деньги и усилия на восстановление сайта**

chrome

Веб-сайт, на который вы хотите перейти, содержит вредоносное ПО!

Google Chrome заблокировал доступ к www.[redacted]

Даже если в прошлом вы посещали этот веб-сайт без последствий, в этот раз ваш компьютер может заразиться вредоносным ПО.

Вредоносное ПО – это программное обеспечение, специально созданное для совершения преступных действий, например хищения идентификационных данных, кражи денег или безвозвратного удаления файлов.

Подробнее...

Назад Дополнительно

Помогать Google в улучшении системы обнаружения вредоносного ПО (при появлении подобных предупреждений в Google будут отправляться дополнительные сведения). "Политика конфиденциальности"

Какие последствия может иметь взлом для сайта?

- подмоченная репутация (предупреждения поисковиков и антивирусов, defacement, автоматические перенаправления на порно сайты)
- **риск заразить компьютеры посетителей и свои собственный компьютер**
- проблемы с ранжированием в поисковиках
- потеря траффика, продаж, показов рекламы, отключение рекламных кампаний
- повреждение файлов/базы или уничтожение сайта
- время, деньги и усилия на восстановление сайта

Какие последствия может иметь взлом для сайта?

- подмоченная репутация (предупреждения поисковиков и антивирусов, defacement, автоматические перенаправления на порно сайты)
- риск заразить компьютеры посетителей и свои собственный компьютер
- **проблемы с ранжированием в поисковиках**
- потеря траффика, продаж, показов рекламы, отключение рекламных кампаний
- повреждение файлов/базы или уничтожение сайта
- время, деньги и усилия на восстановление сайта

Какие последствия может иметь взлом для сайта?

- подмоченная репутация (предупреждения поисковиков и антивирусов, defacement, автоматические перенаправления на порно сайты)
- риск заразить компьютеры посетителей и свои собственный компьютер
- проблемы с ранжированием в поисковиках
- **потеря траффика, продаж, показов рекламы, отключение рекламных кампаний**
- повреждение файлов/базы или уничтожение сайта
- время, деньги и усилия на восстановление сайта

Какие последствия может иметь взлом для сайта?

- подмоченная репутация (предупреждения поисковиков и антивирусов, defacement, автоматические перенаправления на порно сайты)
- риск заразить компьютеры посетителей и свои собственный компьютер
- проблемы с ранжированием в поисковиках
- потеря траффика, продаж, показов рекламы, отключение рекламных кампаний
- **повреждение файлов/базы или уничтожение сайта**
- время, деньги и усилия на восстановление сайта

Какие последствия может иметь взлом для сайта?

- подмоченная репутация (предупреждения поисковиков и антивирусов, defacement, автоматические перенаправления на порно сайты)
- риск заразить компьютеры посетителей и свои собственный компьютер
- проблемы с ранжированием в поисковиках
- потеря траффика, продаж, показов рекламы, отключение рекламных кампаний
- повреждение файлов/базы или уничтожение сайта
- **время, деньги и усилия на восстановление сайта**

Как взламывают?

Сайты на WordPress в первую очередь сайты - а значит для их взлома можно использовать те же способы, что и для взлома любого другого сайта, независимо от его платформы

- похищение и подбор паролей FTP/ CPanel, etc.
- недостаточно строгая изоляция эккаутнов на общем хостинге.
- вредоносная реклама / виджеты

Атаки, специфичные для WordPress

Как взламывают WordPress сайты?

- Автоматизированный подбор паролей.
- Древние версии WordPress
- Дыры в плагинах и темах.
- Плагины и темы из непроверенных источников.
- Доступ к wp--config.php с соседних эккаунтов сервера
- Доступ к базе данных.

Атаки, специфичные для WordPress

Как взламывают WordPress сайты?

- Автоматизированный подбор паролей.
- Древние версии WordPress
- Дыры в плагинах и темах.
- Плагины и темы из непроверенных источников.
- Доступ к wp--config.php с соседних эккаунтов сервера
- Доступ к базе данных.

Атаки, специфичные для WordPress

Как взламывают WordPress сайты?

- Автоматизированный подбор паролей.
- Древние версии WordPress
- Дыры в плагинах и темах

  например TimThumb.php (включён во множество тем) и MailPoet (1,7 миллионов скачиваний)
- Плагины и темы из непроверенных источников.
- Доступ к wp--config.php с соседних эккаунтов сервера
- Доступ к базе данных.

Атаки, специфичные для WordPress

Как взламывают WordPress сайты?

- Автоматизированный подбор паролей.
- Древние версии WordPress
- Дыры в плагинах и темах.
- Плагины и темы из непроверенных источников.
- Доступ к wp--config.php с соседних эккаунтов сервера
- Доступ к базе данных.

Атаки, специфичные для WordPress

Как взламывают WordPress сайты?

- Автоматизированный подбор паролей.
- Древние версии WordPress
- Дыры в плагинах и темах.
- Плагины и темы из непроверенных источников.
- Доступ к wp--config.php с соседних эккаунтов сервера
- Доступ к базе данных.

Атаки, специфичные для WordPress

Как взламывают WordPress сайты?

- Автоматизированный подбор паролей.
- Древние версии WordPress
- Дыры в плагинах и темах.
- Плагины и темы из непроверенных источников.
- Доступ к wp--config.php с соседних эккаунтов сервера
- Доступ к базе данных.

Атаки, специфичные для WordPress

Что делают после взлома?

- вставка вредоносного кода в файлы тем и плагинов (header.php, footer.php, 404.php)
- вставка вредоносного кода в основные файлы WP
- несанкционированная установка плагинов.
- добавление администраторов (в том числе невидимых в админке).
- добавление виджетов с вредоносным кодом.
- добавление статей и модификация существующих статей
- Вредоносный код в базе (wp_options)
- Саморазмножающийся вредоносный код
- DDoS используя pingback

Пример вредоносного кода в footer.php

```
<?php eval(gzinflate(base64_decode('pRn9c9o49ufczP0PKuPGuHHAGAihiZN223R3Z67bHk1v5iZpGWE
</div>
                    <?php get_sidebar(); ?>
                </div>
            </div>
        </div><footer class="art-footer"><?php get_sidebar('footer'); ?></footer>

    </div>
</div>



<div id="wp-footer">
    <?php wp_footer(); ?>
</div>
</body>
</html>
```

Базовые решения влияющие на безопасность

- Пароли и имена пользователей (FTP, WP -admin)!
- Безопасность локальной машины вебмастера.
- SFTP/SSH безопаснее, чем FTP
- Не сохраняйте пароли в FTP- клиентах - используйте менеджеры паролей.
- Хостинг нескольких сайтов на одном эккаунте - плохая идея.
- Регулярно делайте резервные копии.
- Не экономьте на логах.

Обновления, темы и плагины

- Своевременное обновление WordPress, тем и плагинов.
- Где вы берёте темы и плагины? Никогда не доверяйте “неофициальным” источникам.
- Нужны ли вам все установленные темы и плагины?

Имейте представление об архитектуре WordPress

- **wp-admin/** и **wp-includes/** - только базовые файлы.
  - Ничего постороннего там не должно появляться.
  - Взломы обнаруживаются сравнением, лечатся удалением и переустановкой.

- **wp-config.php** - содержит пароли и не должен читаться никем кроме владельца
  - 400 - идеальные права для него

- **wp-content/** - единственное место, куда могут добавляться файлы.
  - требует пристального внимания
  - в идеале можно запретить прямой доступ к .php файлам в этом каталоге, так как всё должно выполняться чере API WordPress.
  - но в реальной жизни некоторые плагины пренебрегают этим требованием
  - поэтому желательно ограничить каталоги загрузок типа wp-content/uploads/

```
<Files *.php>
deny from all
</Files>
```

Элементы продвинутой безопасности

- Мониторинг целостности файлов!
- SVN update.
- Плагины для безопасности
- Файрволл сайта

  (на уровне плагина или внешний вроде CloudPoxy)
- Внешний мониторинг сайта

Дополнительное чтение

Экономика ботнетов
http://securelist.ru/analysis/1327/e-konomika-botnetov/

Настройка WordPress против взломов
http://codex.wordpress.org/Hardening_WordPress

Использование Subversion для установки, обновления WordPress и обнаружения изменений
http://codex.wordpress.org/Using_Subversion
http://codex.wordpress.org/Installing/Updating_WordPress_with_Subversion

Блог Sucuri о безопасности WordPress
http://blog.sucuri.net/category/wordpress

Уже готовы обеспечивать безопасность своих сайтов?

Или ещё есть вопросы?

;-)

Форма для контактов: http://blog.unmaskparasites.com/contact/