Автор: Иван Карташев © Комьпьюлента ИНТЕРНЕТ , МИР 2765 26.06.2004, 12:08 206

По интернету распространяется необычная инфекция

Эксперты по компьютерной безопасности предупреждают о новой опасности, угрожающей пользователям интернета. На этот раз поводом для беспокойства стал не совсем обычный компьютерный вирус, поражающий веб-серверы, а уже через них - клиентские компьютеры.

Источник необычной инфекции пока точно не установлен, но специалисты по безопасности предполагают, что происходящее - козни спамеров, пытающихся захватить компьютеры для проведения своих рассылок.

Согласно имеющимся данным, распространяется инфекция следующим образом. Злоумышленники взламывают веб-серверы, работающие под управлением Microsoft Internet Information Server 5, используя дыры в этом пакете. В результате атаки к станицам, размещенным на сайте, добавляется дополнительный код на javascript, эксплуатирующий одну из незаделанных дыр в браузере Internet Explorer, сообщается на специальном сайте, созданном Министерством внутренней безопасности США совместно с организацией CERT для оповещения о проблемах компьютерной безопасности.

Когда пользователь открывает пораженную страницу, срабатывает скрипт и на компьютер загружается троянская программа RAT, с помощью которой злоумышленники могут использовать пораженную машину в собственных целях. Как сообщает сайт eWeek со ссылкой на компанию NetSec, троян загружается с одного из двух серверов, причем наиболее часто используется сервер, расположенный в России, и несколько реже - сайт из США.

По данным NetSec и других компаний, работающих в сфере компьютерной безопасности, пораженными оказались веб-серверы достаточно крупных компаний и организаций, включая несколько банков и онлайновых магазинов. Ситуация усугубляется тем, что для успешного проведения атаки на клиентскую машину достаточно открыть веб-страницу в браузере, никаких дополнительных действий от пользователя не требуется. А поскольку патча для используемой дыры в Internet Explorer пока не существует, единственным средством защиты является отключение javascript с потерей части функциональности многих сайтов. Наиболее подходящим решением станет использование альтернативного браузера: ни Mozilla, ни Opera для атаки не уязвимы.

Данные "Лаборатории Касперского" о необычной атаке на Интернет

"Лаборатория Касперского" сообщила некоторые подробности относительно поразившей интернет новой массовой эпидемии. В ходе новой атаки используется целая комбинация вредоносных программ, которые применяются вместе с несанкционированным проникновением в компьютерные системы. Эпидемия затрагивает веб-серверы на базе Microsoft Internet Information Server 5 (IIS5) и пользовательские компьютеры, которые обращаются к пораженным веб-сайтам при помощи браузера Internet Explorer.

Особенно важно то, что злоумышленники применяют нестандартный механизм заражения пользовательских компьютеров. Сначала они взламывают веб-сервер, используя имеющиеся в IIS5 уязвимости, и заражают его написанной на Javascript троянской программой Trojan.JS.Scob.a. Затем, при посещении любой веб-страницы на зараженном сайте браузером Internet Explorer, скрипт-троян перехватывает управление и обращается к веб-сайту, на котором находится специальный PHP-скрипт. Этот скрипт, в свою очередь, использует неизвестную до сегодняшнего дня уязвимость в браузере Internet Explorer.

За счет использования этой уязвимости, на пользовательский компьютер устанавливается одна из версий программы-шпиона Backdoor.Padodor (модификаций w, x, y или z). Этот троян предоставляют злоумышленникам полный контроль над зараженной машиной. Авторами и инициаторами атаки, скорее всего, являются хакеры из России.

Специалисты "Лаборатории Касперского" не исключают, что в данном случае можно говорить о Zero-day

Exploit - то есть о бреши, еще никому неизвестной, для которой еще не выпущен соответствующий патч. Иными словами, возможно, что хакеры, обнаружив или выкупив брешь у автора, незаметно заразили IIS-серверы по всему миру для распространения программы-шпиона, утверждают в антивирусной компании.

Автор: Иван Карташев © Комньюлента ИНТЕРНЕТ , МИР 2765 26.06.2004, 12:08 206
URL: https://babr24.com/?ADE=13591 Bytes: 3955 / 3948 Версия для печати Скачать PDF

Автор текста: **Иван Карташев**.

эл.почта: babrmarket@gmail.com