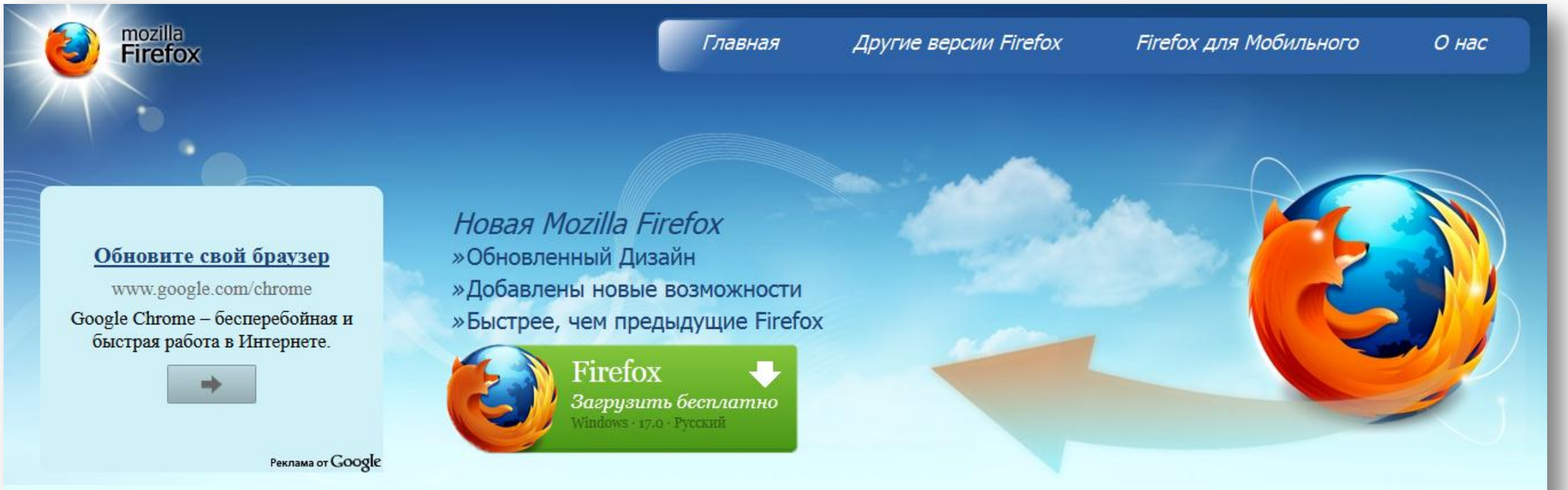
Yandex

Yandex

Graph-based Malware Distributors Detection

Andrei Venzhega
Web-search manager

http://firefox.mozil1a.ru/



О Браузере Мазила Фаерфокс

Скачать Мозилу бесплатно

Мазила фаерфокс является одним из самых популярных браузеров в мире. Фаерфокс – это быстрый и удобный браузер для современного человека, который не представляет свою жизнь без глобальной сети Интернет. Mozilla Firefox поддерживает все новые стандарты, которые позволяют полноценно пользоваться всеми возможностями Интернета. Браузер способен настроиться полностью под вас, с помощью стилей оформления и дополнений. Стили оформления можно создавать самому или же скачать уже имеющиеся стили, которые распределены на разные группы. Также Вы можете скачать нужные Вам дополнения, дополнения делают браузер еще совершеннее и удобнее. Скачать мозилу на русском языке бесплатно может любой человек. К примеру, самые популярные дополнения в России - это дополнения от Яндекса: Яндекс Бар, который делает браузер Mozilla Firefox еще удобнее. Мозила выпускает бэтта версии каждый месяц, чтобы тестировать новые доработки и изменения, а глобально обновляется раз в пол года, и уже немного осталось до выхода новой версии mozilla, за которым будущее. Уже скоро появятся бета версии Mozilla Firefox 18, которую можно будет скачать и попробовать новые функции и возможности, которые придумали и доработали программисты и простые пользователи. Ждем новых обновлений.

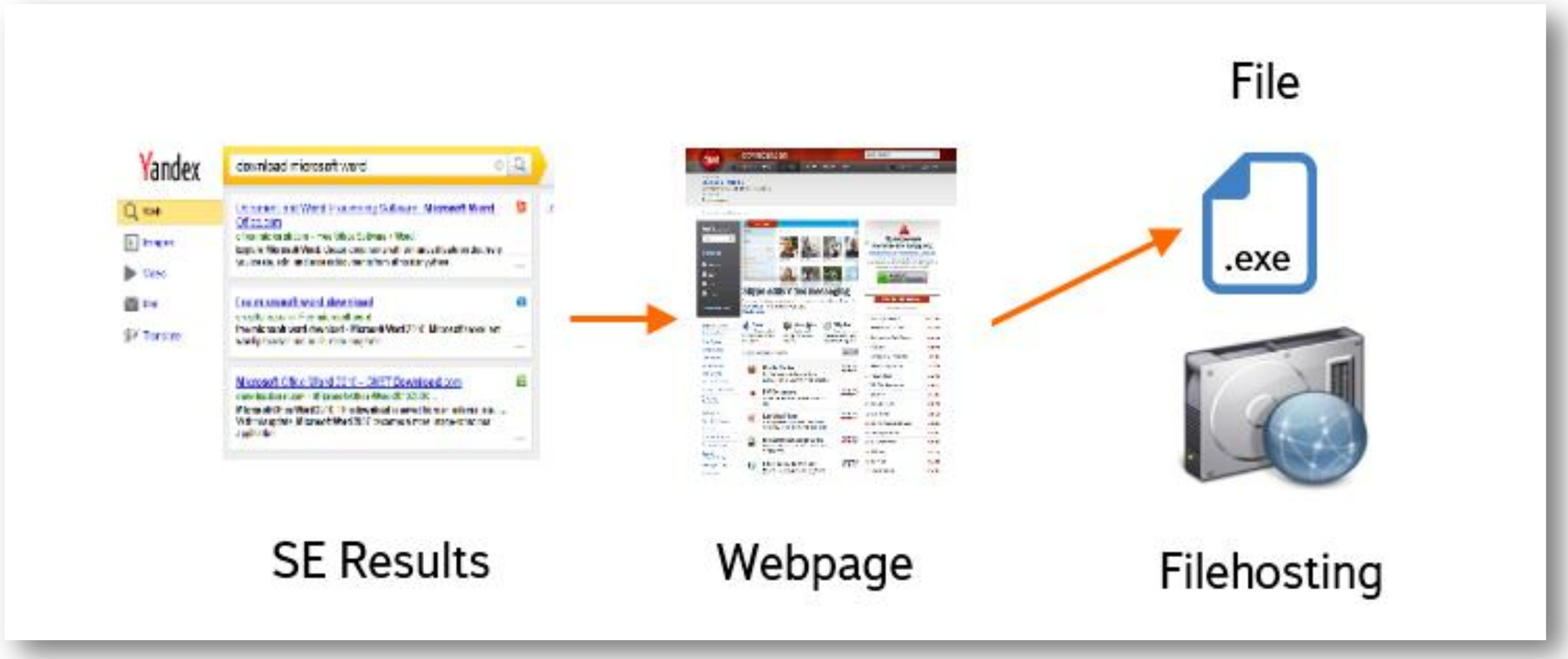
Mozilla Firefox с «Яндекс.Бар»

Что нового в полседней версии Mozilla Firefox ?

Скачать Мозилу последнюю версию

В новой версии мазила firefox появился новый и очень удобный интерфейс. Появилась кнопка « фаерфокс », она заменила все меню в верхней части браузера. Появилась кнопка « Домашняя страница » и кнопка « Визуальные закладки », что позволило значительно сэкономить место и увеличить функциональность браузера. Теперь нет строки состояния, она появляется в момент загрузки страницы или при наведении курсора на ссылки, позволяя сделать больше пространства для просмотра страницы. Появилась функциональная кнопка «Панорама» (группы вкладок), с помощью нее можно просматривать открытые сайты в виде небольших привью и делать легкую сортировку вкладок, создавать несколько отдельных групп вкладок и задавать им свое название. Переделана адресная строка, теперь она помогает вам перейти на те страницы, где вы были раньше, также можно вводить в нее поисковой запрос, не открывая сайт поисковой системы. Добавлена синхронизация, с помощью которой вы можете использовать ваши закладки, пароли и другие настройки на других компьютерах, и даже на вашем мобильном компьютере. Добавлена функция «Забыть о сайте», которая позволяет удалить из истории страницы ненужных для вас сайтов. Теперь каждый пользователь может Скачать или обновить бесплатно Mozilla Firefox rus с любой версии у нас на сайте. Mozilla Firefox подойдет для всех версий Windows включая Windows 7

Malware: search traffic



Search engines are the main source of traffic on malware distributors websites.

Malware: overview

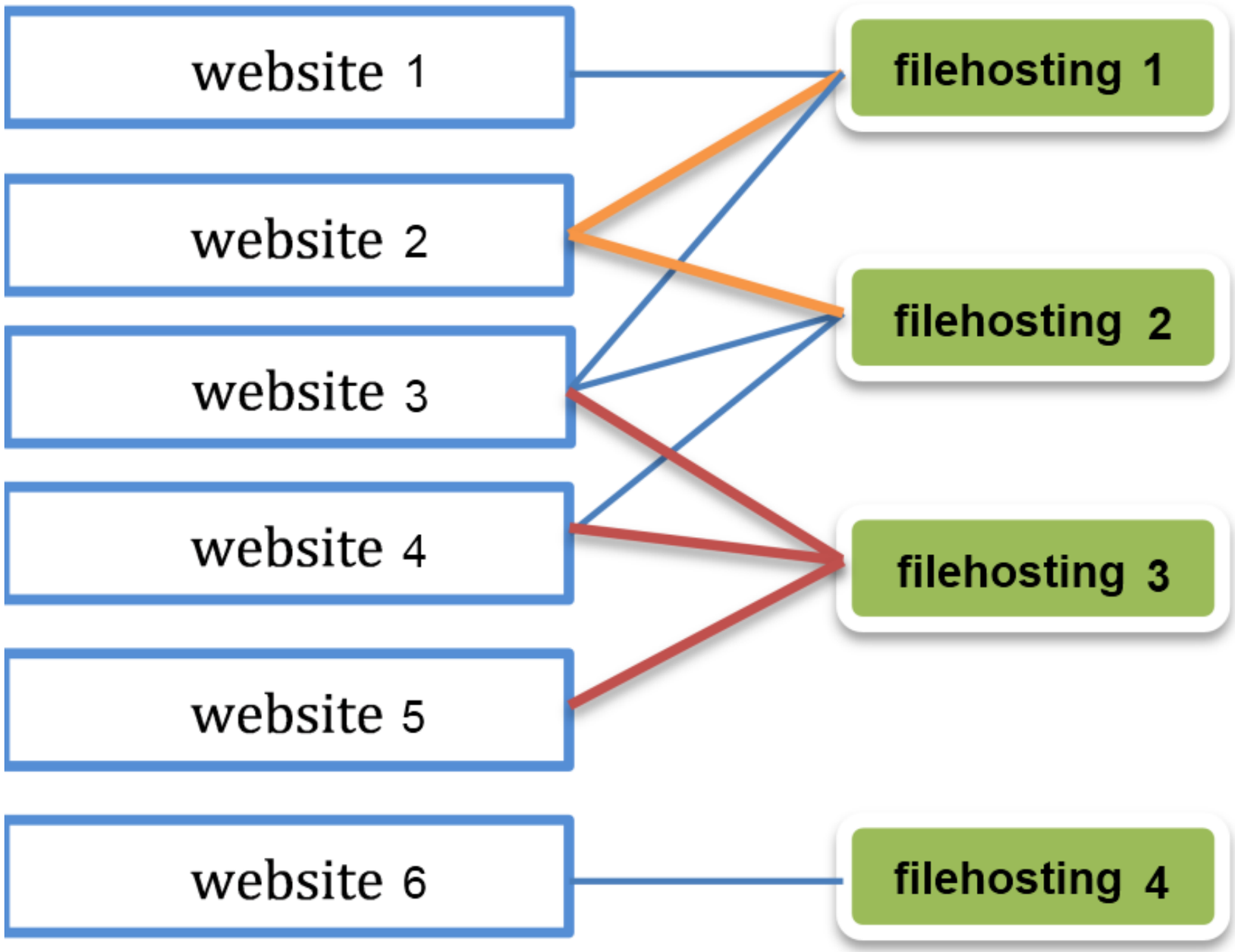
Symantec annual report 2011:

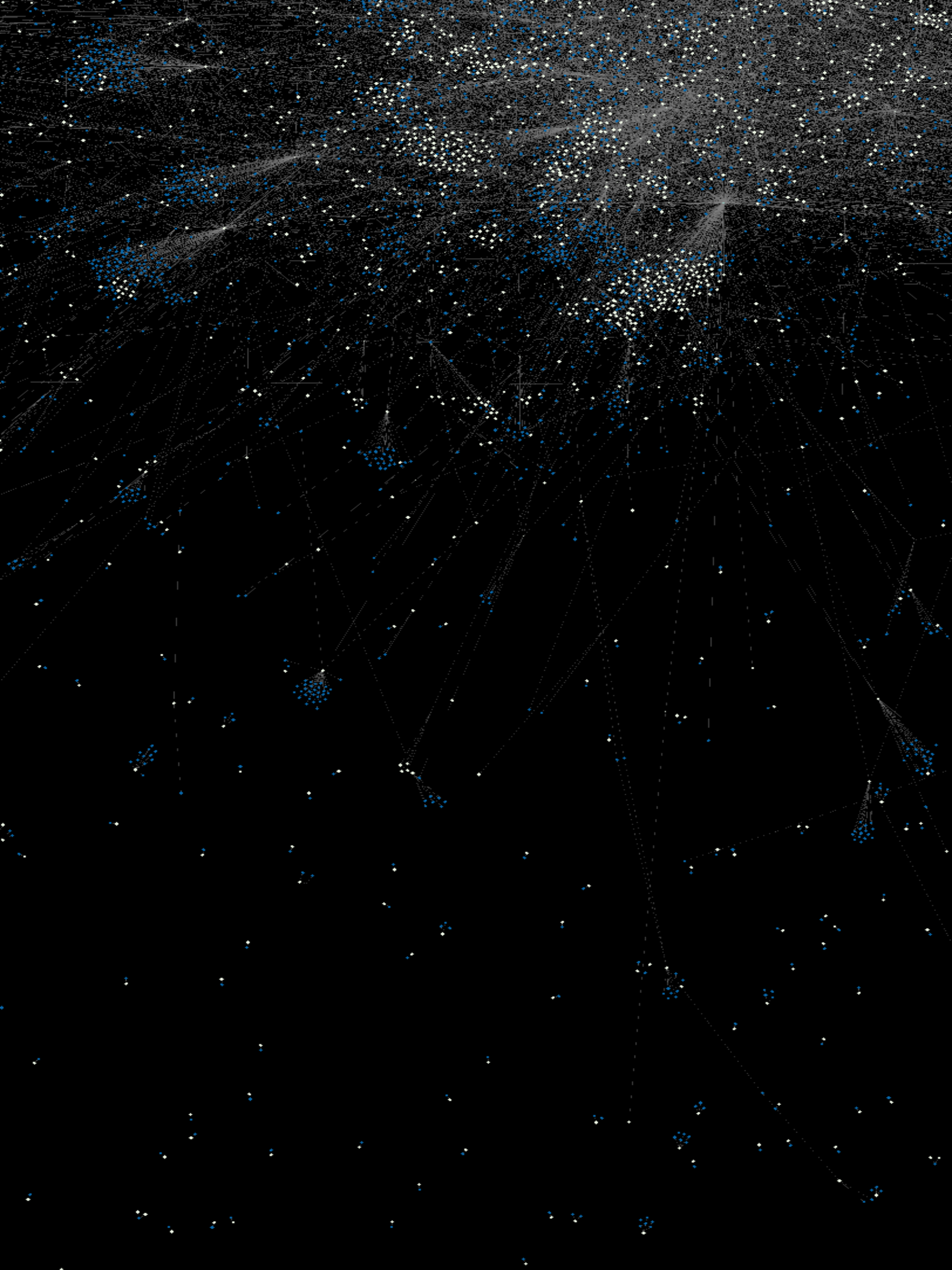
- About 403 millions new types of malicious software were detected in 2011 (41% more than 2010)

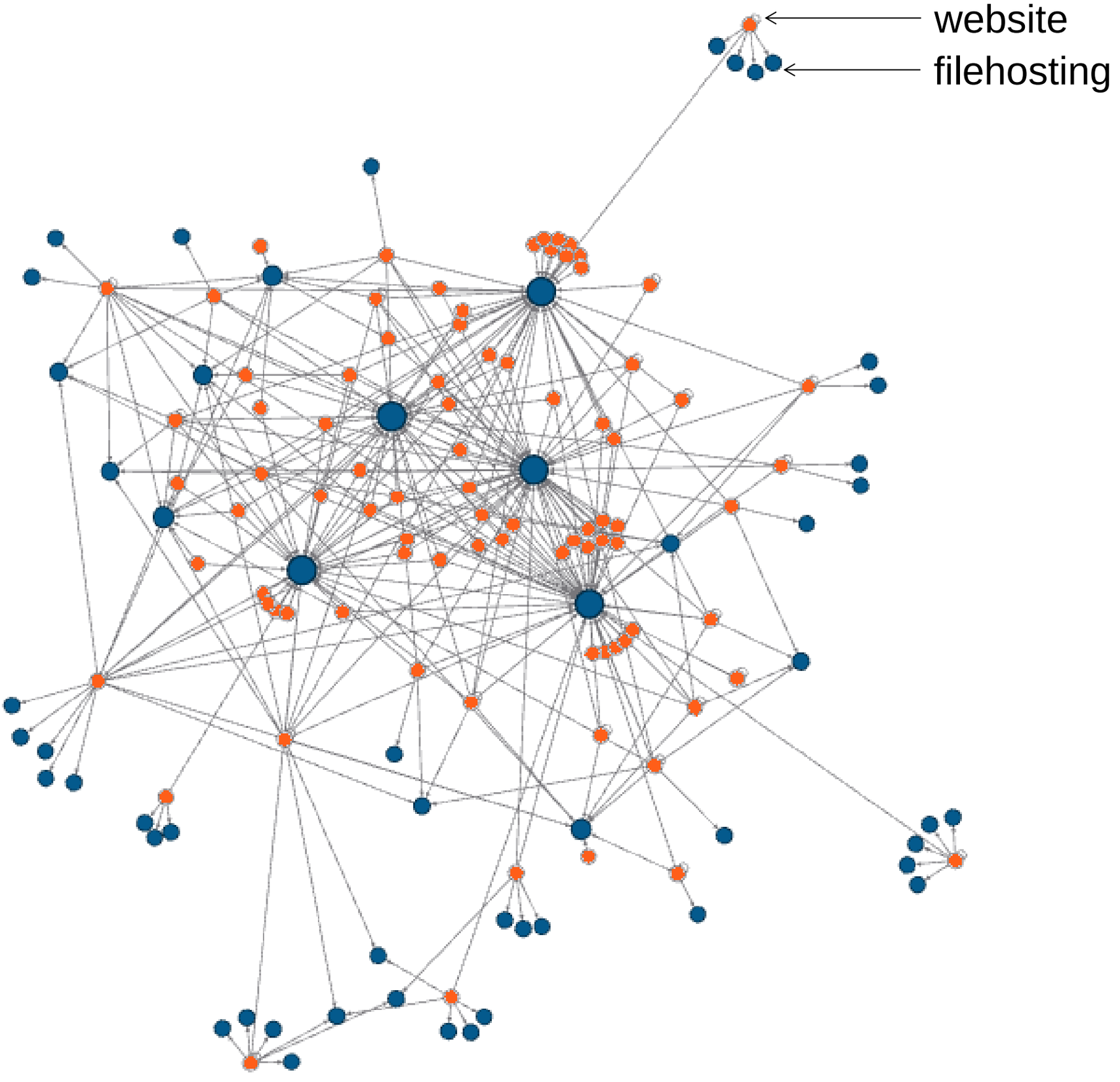
-.

- Signature-based methods can’t deal with unique signature malware.

Bipartite graph






website
filehosting

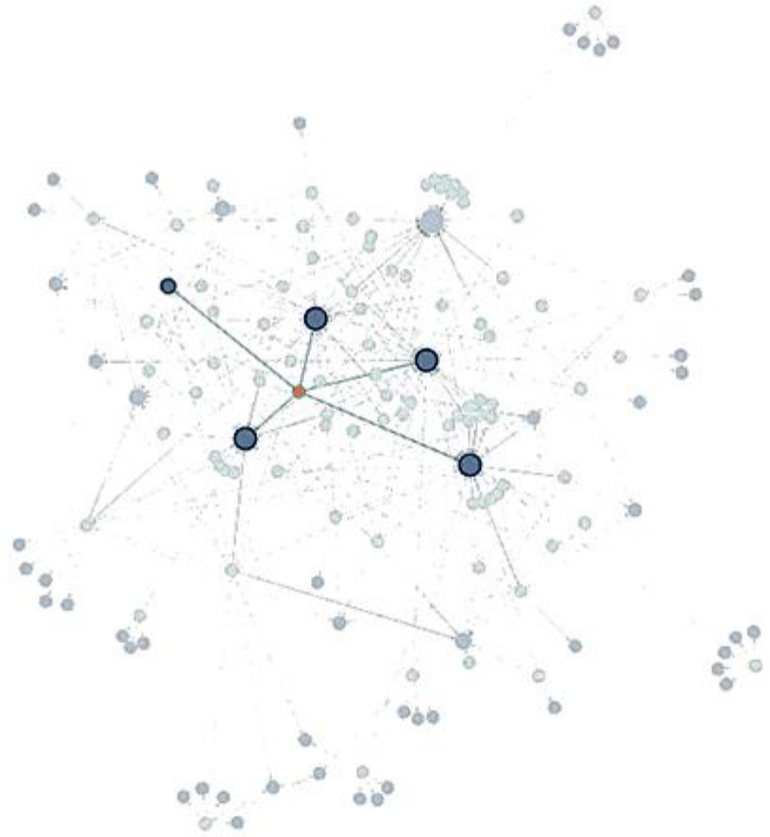
Graph initialization

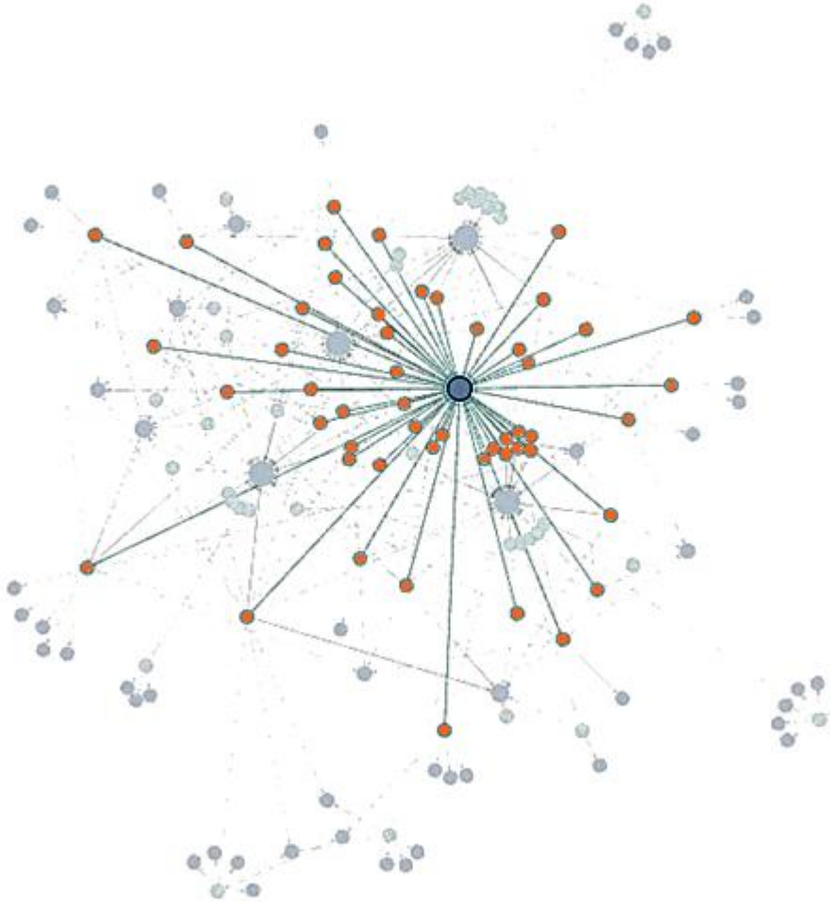
$$G = (V, E, W)$$

site: $S \subset V$; filehosting: $F \subset V$;

$$W : w(s, f) \in [0, 1];\ s \in S; f \in F;$$

$$M : m(v) = P(\text{v is bad}) \in [0, 1];\ v \in V.$$

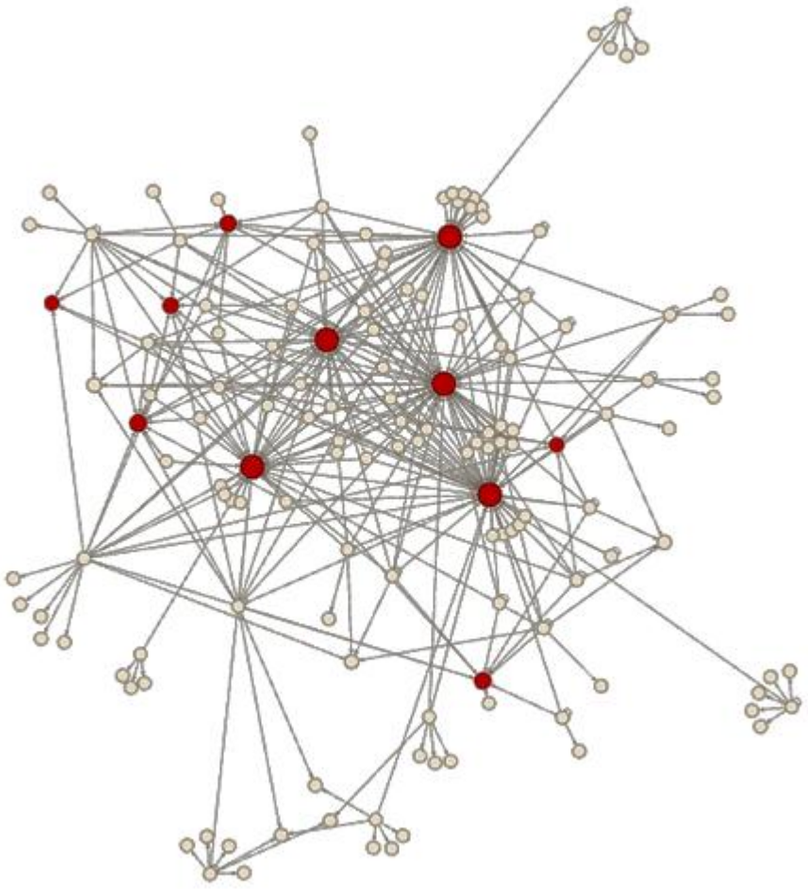




Malwarness rank

website rank: $$m_k(s_i) = \sum_{j \in N_i} \frac{w_s(s_i, f_j)\ m_{k-1}(f_j)}{W_s(s_i)};$$

filehosting rank: $$m_k(f_j) = \sum_{i \in N_j} \frac{w_f(s_i, f_j)\ m_{k-1}(s_i)}{W_f(f_i)};$$



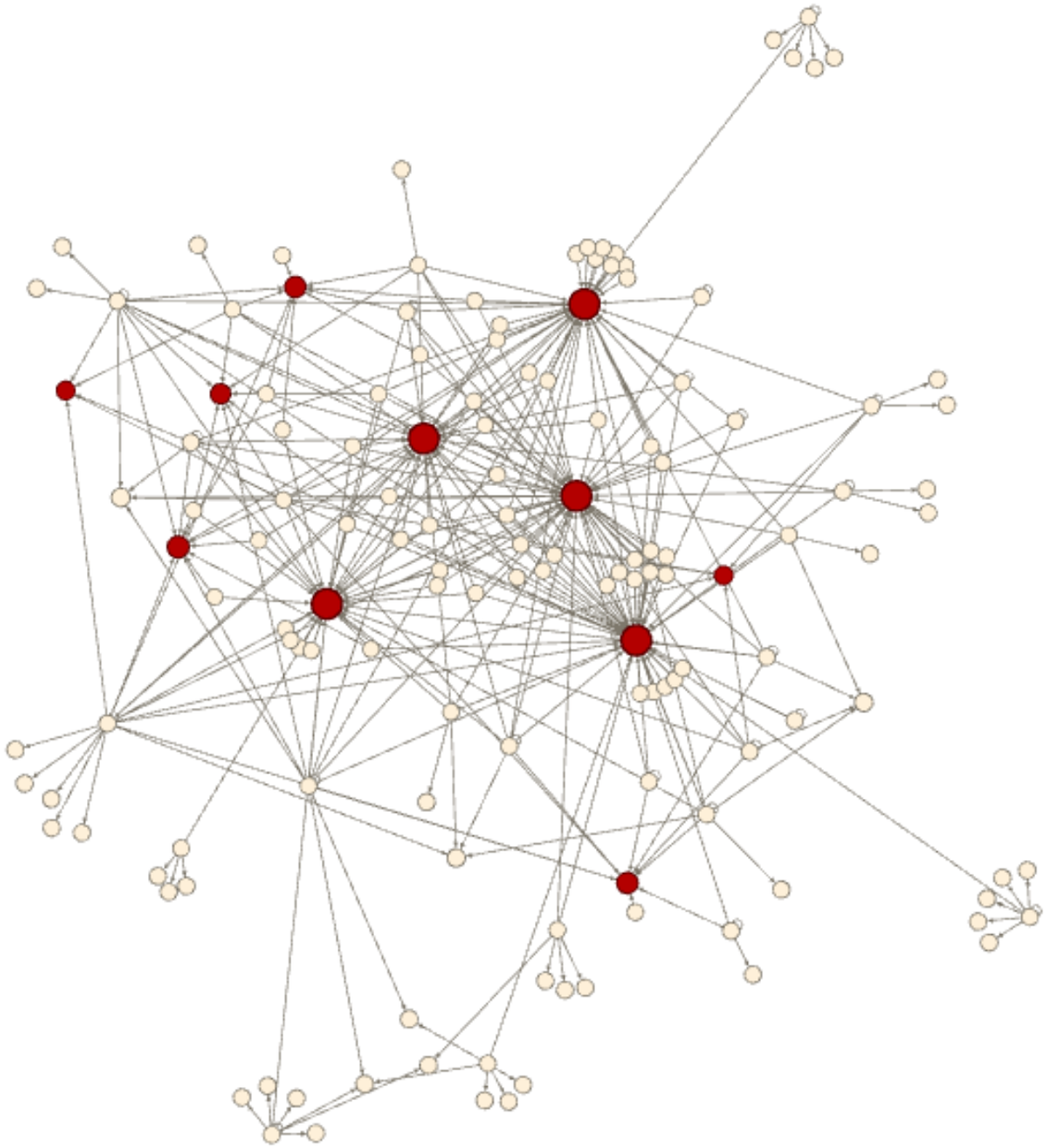
sum of edges weights:

$$W_s(s_i) = \sum_{j \in N_i} w_s(s_i, f_j); \quad W_f(f_j) = \sum_{i \in N_j} w_f(s_i, f_j);$$

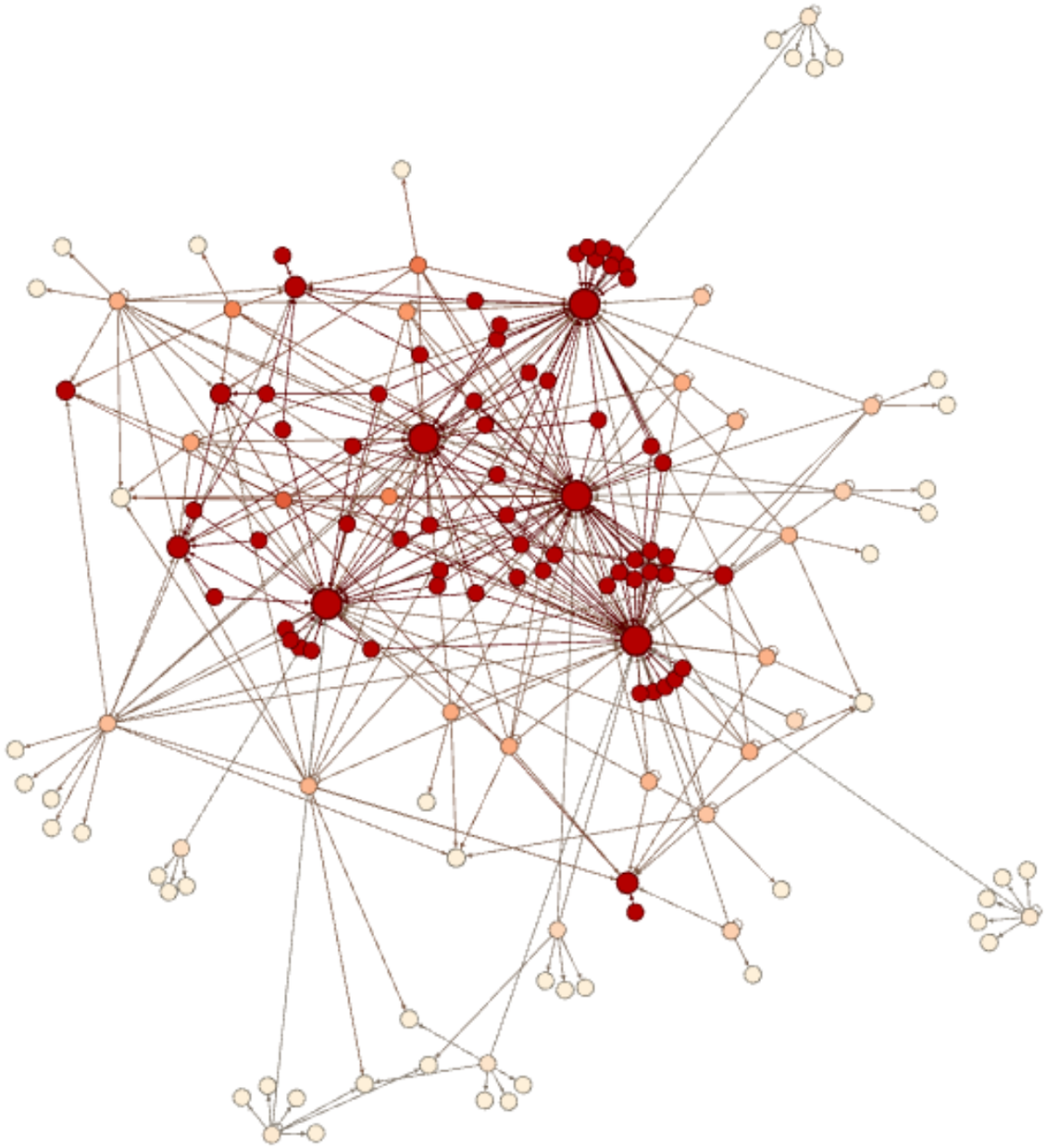
N_i – set of all neightbors of vertice v_i;

the stop condition on *k* iteration : $\|m_k(v) - m_{(k+1)}(v)\| < \varepsilon;\ \forall v \in V;$

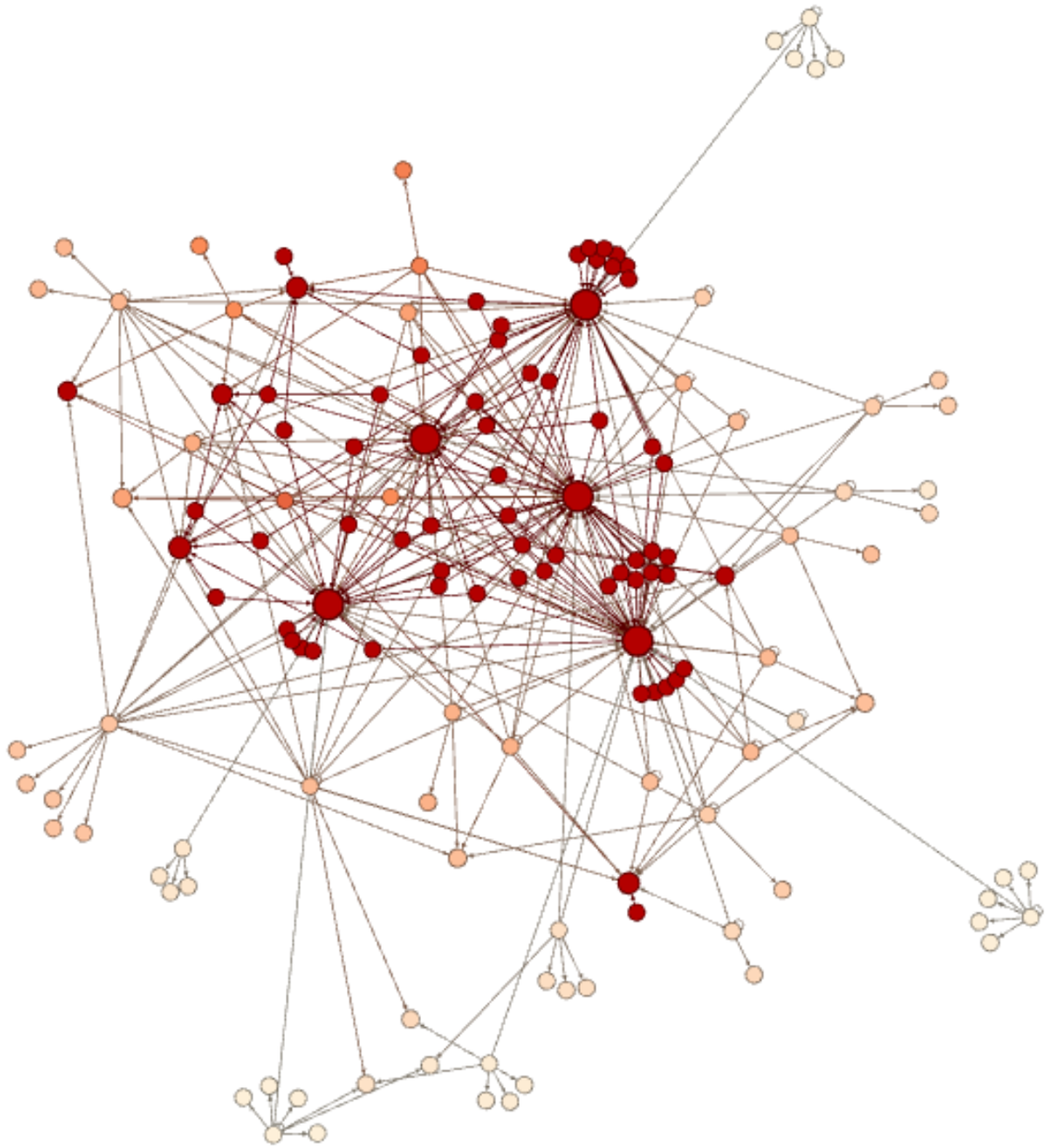
Method visualization. Prior set. Step 1-1



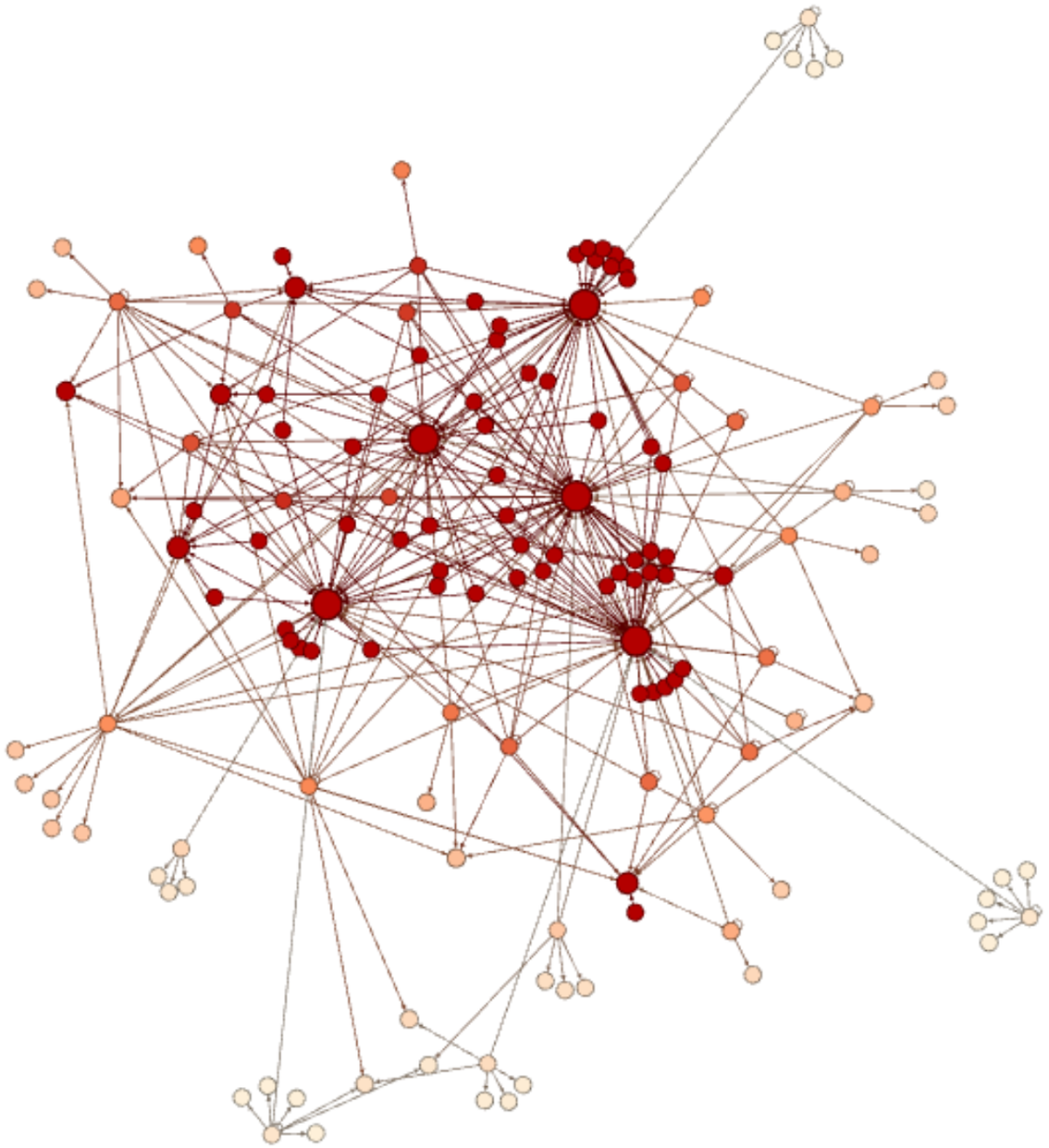
Method visualization. Step 1-2



Method visualization. Step 2-1



Method visualization. Step 2-2



Results

Method detected filehostings (FH) distributing maleware (MD) files with:
97% - precision
60% - recall (strongly depends from the initialization set)

2.1 times decrease of the of malware distributers in top10 search results

Only **9%** of files from malware FH at the moment of their detection were in anti-virus signature bases.

More than 90% of files from these FH were in anti-virus signature bases after 2 weeks.

1 week is the minimum lifetime of FH, an average lifetime of MD websites is much longer.

Yandex

Andrei Venzhega

web-search manager

a.venzhega@ya.ru