

{comments on}

В последнее время на адрес ряда корпоративных почт, в.т.ч. и на нашу почту приходят письма со следующим содержанием:

Здравствуйте.

ОАО Ростелеком расторгает договор с 30.09.2018г. в одностороннем порядке, в связи с вышедшими из строя линиями связи.

Все абоненты, автоматически переходят к нашим партнерам. Об изменениях в тарифных планах, и сроках подключения Вы можете узнать по телефону горячей линии и в таблице сроков подключения.

Часть статических IP адресов будет заблокированно в период с 15.10.2018г по 30.10.2018г.

Список адресов смотрите на странице 2 в приложении.

Менеджеры компании на которую Вы переводитесь свяжется с Вами для подписания договора в ближайшие дни.

С Уважением к Вам, ОАО Ростелеком

Теперь немного пояснений:

1) ОАО Ростелеком, давно уже стал ПАО «Ростелеком».

2) Кто, из здравомыслящих операторов, передаст своих абонентов своим партнерам (конкурентам)?

3) В теле письма есть ссылка (в плане информационной безопасности, она удалена), эта ссылка ведет на неопределенный файлообменник, где предлагается скачать zip-архив с файлом-заставкой внутри (компьютерный вирус).

Злоумышленники присылают спам-письма от имени Ростелеком

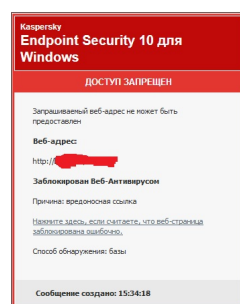
Автор: Administrator
04.09.2018 20:21

4) При проверке на сервисе www.virustotal.com выдаются следующие результаты:

The screenshot shows the VirusTotal interface. At the top, there is a search bar with the text "Search or scan a URL, IP address, domain, or file hash". Below this, a summary section indicates "3 engines detected this URL". The URL being analyzed is "http://bitly.com/[redacted]". Other details include the host "bitly.com", the downloaded file hash "5afe0d196ae922a233120f07f90962c3987c3f3765afcc414dee45d2322b820b", the last analysis date "2018-09-04 12:00:15 UTC", and a community score of "-12". A red circle with "3 / 67" is also visible. Below the summary, there are three tabs: "Detection", "Details", and "Community". The "Detection" tab is active, showing a table of engine results:

Engine	Result
Fortinet	Malware
Kaspersky	Malware
Sophos AV	Malicious
ADMINUSLabs	Clean
AegisLab WebGuard	Clean
AlienVault	Clean

5) Антивирус Касперский, так же блокирует переход по данной ссылке:



Запрашиваемый веб-адрес не может быть предоставлен

<http://bitly.com/XXXXXXXXXX>

Причина: опасный веб-адрес

Способ обнаружения: базы

[Нажмите здесь, если считаете, что веб-страница заблокирована ошибочно.](#)

Сообщение создано: 20:35:52