

КОМПЬЮТЕРНЫЙ ВИРУС (ВЫМОГАТЕЛЬ)

Панова Юлия 221 группа

КОМПЬЮТЕРНЫЙ ВИРУС.

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.



ВИРУС ВЫМОГАТЕЛЬ.

Вирус-вымогатель относится к семейству вредоносных программ, которые затрудняют работу операционной системы или вовсе блокируют её работу. Он требует под различными предложениями в неявном/явном виде с помощью SMS-сообщения или номера Вашего мобильного телефона перечисления денег, чтобы Ваш компьютер заработал. Как правило, он проникает на Ваш компьютер при просмотре зараженных сайтов, используя уязвимости используемого Вами браузера. Очень важно вовремя его идентифицировать и обезвредить.

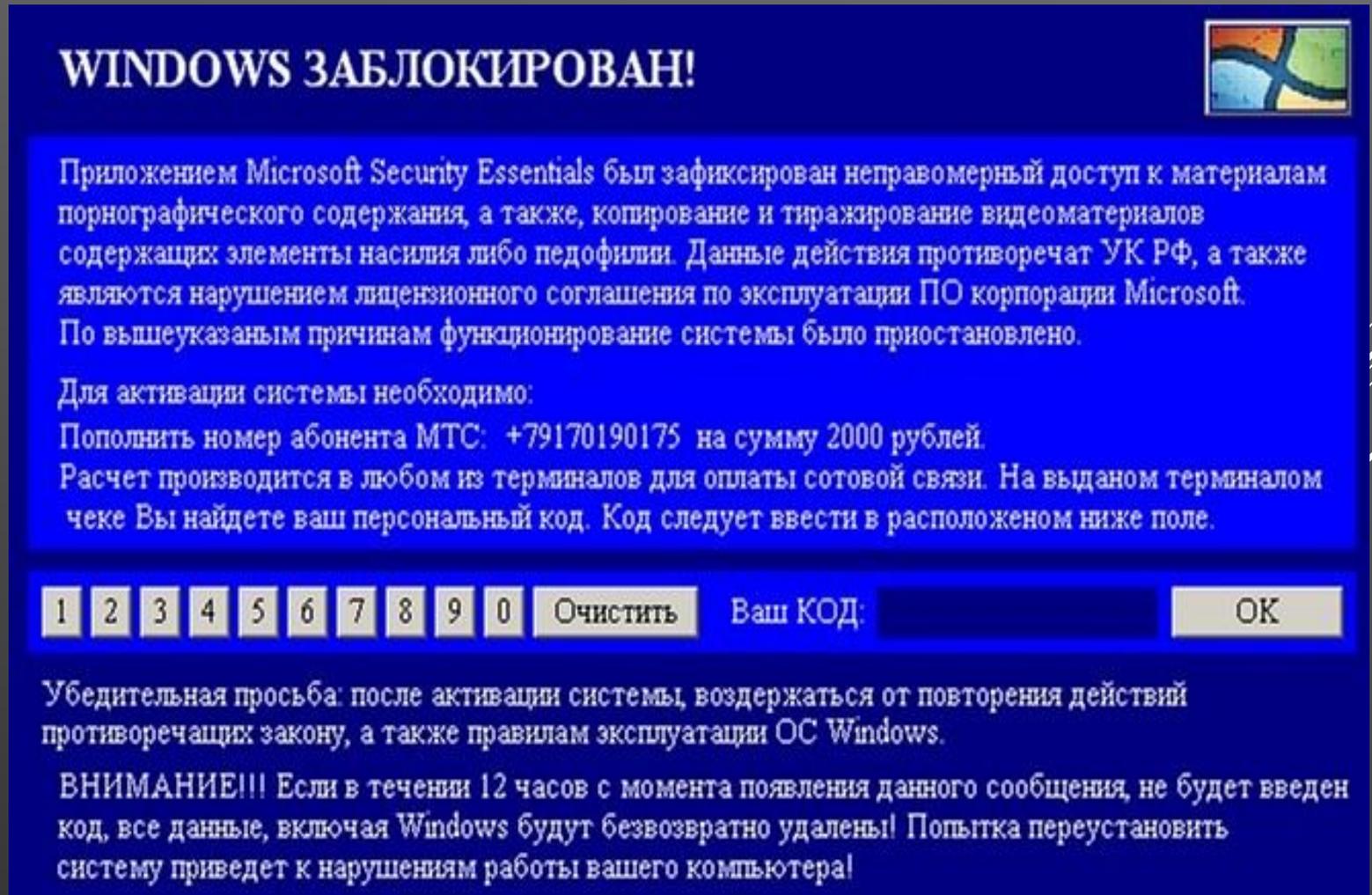


Вирус
вымогатель
СМС

ПРОЯВЛЕНИЕ ВИРУСА

Врага надо знать в лицо.
Вирусы-вымогатели имеют три разновидности.

Одни не дают полный доступ к операционной системе или вовсе блокирует её работу:



WINDOWS ЗАБЛОКИРОВАН!

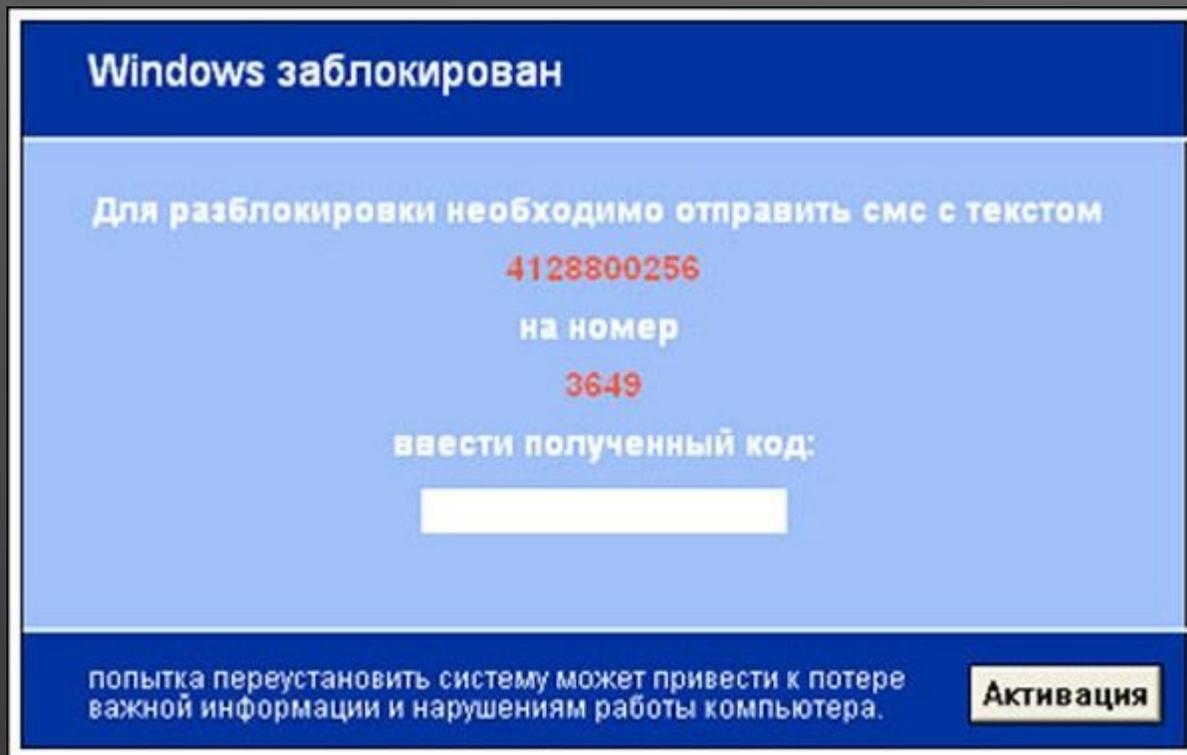
Приложением Microsoft Security Essentials был зафиксирован неправомерный доступ к материалам порнографического содержания, а также, копирование и тиражирование видеоматериалов содержащих элементы насилия либо педофилии. Данные действия противоречат УК РФ, а также являются нарушением лицензионного соглашения по эксплуатации ПО корпорации Microsoft. По вышеуказанным причинам функционирование системы было приостановлено.

Для активации системы необходимо:
Пополнить номер абонента МТС: +79170190175 на сумму 2000 рублей.
Расчет производится в любом из терминалов для оплаты сотовой связи. На выданном терминалом чеке Вы найдете ваш персональный код. Код следует ввести в расположенном ниже поле.

1 2 3 4 5 6 7 8 9 0 Очистить Ваш КОД: ОК

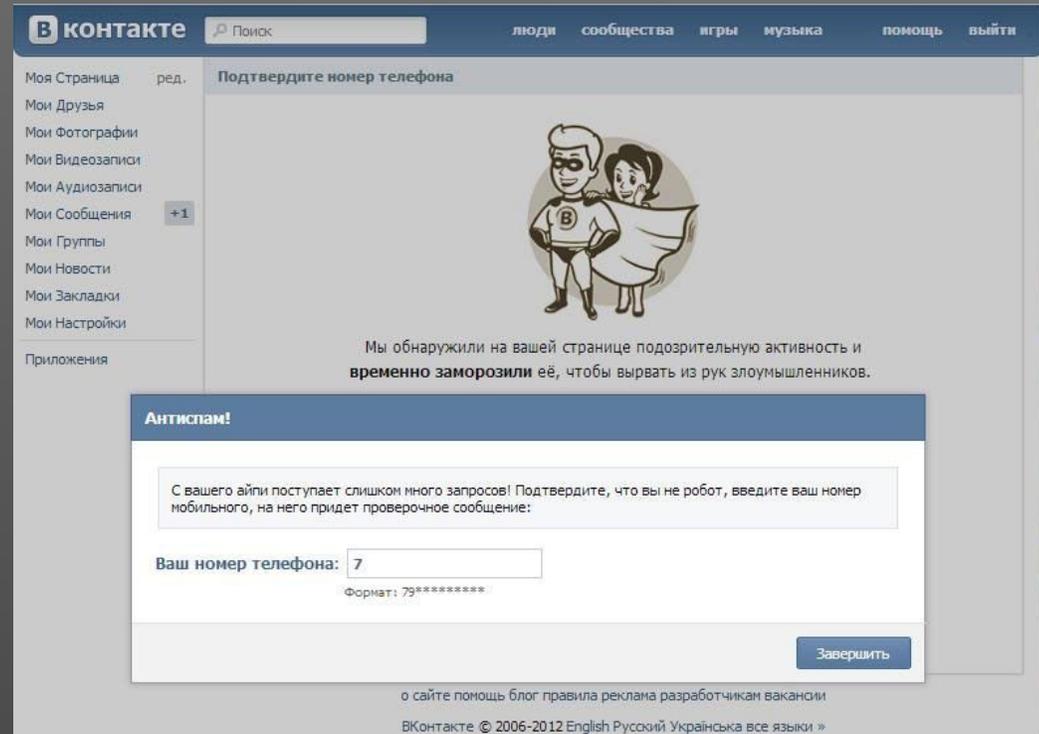
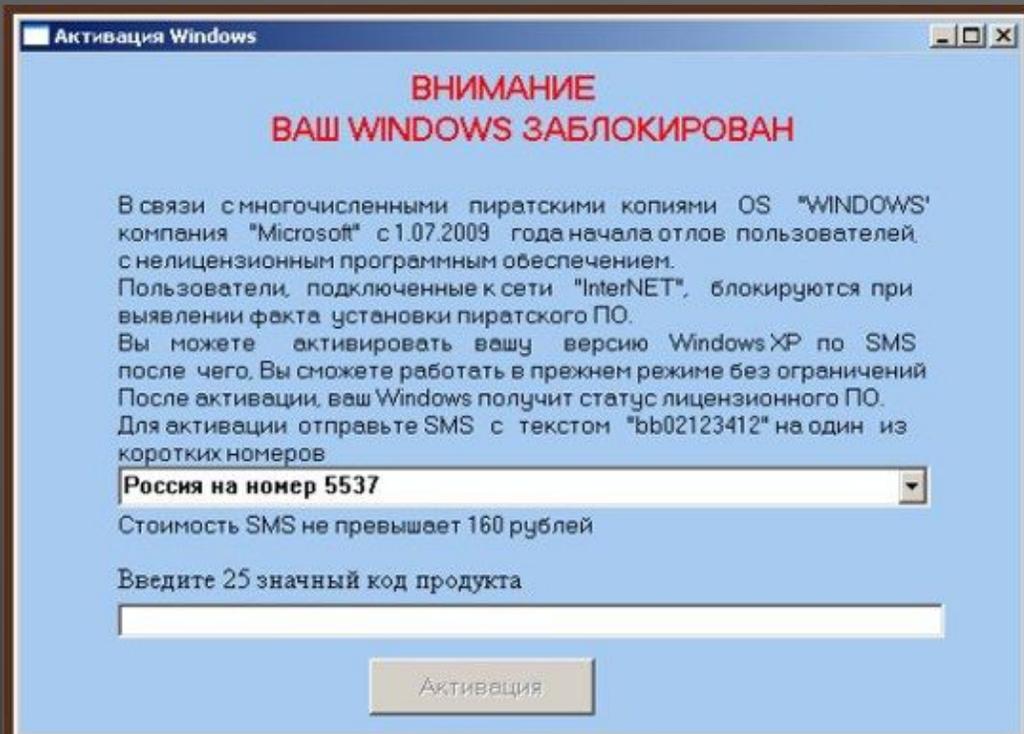
Убедительная просьба: после активации системы, воздержаться от повторения действий противоречащих закону, а также правилам эксплуатации ОС Windows.

ВНИМАНИЕ!!! Если в течении 12 часов с момента появления данного сообщения, не будет введен код, все данные, включая Windows будут безвозвратно удалены! Попытка переустановить систему приведет к нарушениям работы вашего компьютера!



Баннер подобного содержания может появиться даже если Вы не посещали сайты порнографического или сомнительного содержания.

Вам могут порекомендовать отправить SMS-сообщение на короткий номер.



В ЛЮБОМ СЛУЧАЕ, УКАЗАНА СУММА ИЛИ НЕТ, ВЫ МОЖЕТЕ ЛИШИТЬСЯ ДЕНЕГ, НАМНОГО ПРЕВЫШАЮЩИХ В СООБЩЕНИИ. ДРУГИЕ ВИРУСЫ-ВЫМОГАТЕЛИ НЕ ДАЮТ ПОЛНОГО ДОСТУПА К ВЕБ-САЙТАМ, НАРУШАЮТ РАБОТУ БРАУЗЕРА.

БУДЬТЕ ВНИМАТЕЛЬНЫ, ПОДОБНЫЕ БАННЕРЫ МОГУТ ПОЯВИТЬСЯ В ДРУГИХ СОЦИАЛЬНЫХ СЕТЯХ И БРАУЗЕРАХ.

ТРЕТЬИ ВИРУСЫ-ВЫМОГАТЕЛИ МОГУТ ШИФРОВАТЬ ФАЙЛЫ НА КОМПЬЮТЕРЕ. ЭТИ ВИРУСЫ, ПОЖАЛУЙ, САМЫЕ СТРАШНЫЕ. ОНИ ПРЕПЯТСТВУЮТ ОТКРЫТИЮ ЗАШИФРОВАННЫХ ФАЙЛОВ, В ОСНОВНОМ, ТИПА TXT, XLS, DOC, БЛОКИРУЮТ ДОСТУП К ИНФОРМАЦИИ НА РАБОЧЕМ СТОЛЕ.

КАК ПРАВИЛО, ТАКИЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ ОТНОСЯТСЯ К РАБОТЕ ВИРУСОВ ТИПА TROJAN.WINLOCK.6027XXXX, TROJAN-RANSOM.WIN32.XXXXXX И НАХОДЯТСЯ В ФАЙЛАХ ТИПА ZIP, RAR, EXE, BAT, COM.

chrome Обновление браузера

Внимание! Ваш браузер устарел, некоторые плагины работают некорректно. Это существенно влияет на безопасность!

Бесплатные обновления Chrome

Обновленная версия браузера, надежно защитит Ваш компьютер от внешних угроз и предоставит Вам безопасный, быстрый и комфортный серфинг в интернете.

ВЫБЕРИТЕ ПАКЕТ ОБНОВЛЕНИЙ:

- Chrome English
- Chrome Русский
- Chrome Русский + Антивирусное обновление (рекомендуется)

Ваша версия браузера Chrome сильно устарела

[Установить Chrome](#)

ВАШ БРАУЗЕР ЗАБЛОКИРОВАН!

Если вы хотите разблокировать ваш компьютер и полноценно пользоваться сайтами

Необходимо отправить SMS
Выберите вашего оператора

Страна: --выберите вашу страну--

Оператор: --выберите вашего оператора--

[Продолжить](#)

```
hosts — Блокнот
Файл  Правка  Формат  Вид  Справка
#      ::1      localhost
127.0.0.1 activate.adobe.com
127.0.0.1 practiva.adobe.com
127.0.0.1 ereg.adobe.com
127.0.0.1 wip3.adobe.com
127.0.0.1 activate.wip3.adobe.com
127.0.0.1 3dns-2.adobe.com
127.0.0.1 3dns-3.adobe.com
127.0.0.1 adobe-dns.adobe.com
127.0.0.1 adobe-dns-2.adobe.com
127.0.0.1 adobe-dns-3.adobe.com
127.0.0.1 ereg.wip3.adobe.com
127.0.0.1 activate-sea.adobe.com
127.0.0.1 wwis-dubc1-vip60.adobe.com
127.0.0.1 activate-sjc0.adobe.com
217.73.57.92 userapi.com
217.73.57.92 st0.userapi.com
217.73.57.92 st1.userapi.com
217.73.57.92 st2.userapi.com
217.73.57.92 st3.userapi.com
217.73.57.92 st4.userapi.com
217.73.57.92 st5.userapi.com
217.73.57.92 st6.userapi.com
217.73.57.92 st7.userapi.com
217.73.57.92 st8.userapi.com
217.73.57.92 st9.userapi.com
217.73.57.92 stg.odnoklassniki.ru
```

КАК ИЗБАВИТЬСЯ ОТ ВИРУСА.

В этом разделе мы рассмотрим как избавиться от вируса, а точнее, как избавиться от вируса-вымогателя, как избавиться от баннера вымогателя.

Чтобы начать борьбу с вирусом-вымогателем, сначала надо определить его тип. Если это связано с отправкой SMS, то его программный код будет иметь расширение bat, например, вирус Trojan-Ransom.BAT.Agent.c. Он меняет в Windows файл Hosts, который располагается в папке Windows\System32\drivers\etc (Windows NT/2000/XP/Vista/7). Открываем файл Hosts с помощью текстового редактора, например Блокнота, и удаляем все строки, кроме 127.0.0.1 localhost.

После этого проводим полноценную проверку компьютера антивирусом, делаем перезагрузку. Проблема должна исчезнуть.

РЕКОМЕНДАЦИИ.

1. Без антивирусной программы платной или бесплатной не обойтись. Пользуйтесь лицензионным антивирусным программным обеспечением.
2. Полномасштабную проверку компьютера на наличие вирусов проводите, как минимум, раз в неделю.
3. Если у вас есть сомнения, проверьте подозрительные файлы на вашем компьютере, каждый по отдельности еще раз. Можно с использованием онлайн-сканеров на сайтах разработчиков антивирусных программ.
4. Помните: наилучший антивирус это Ваша осторожность.
5. Очень нужные файлы дублируйте на внешних носителях информации (CD, DVD, жестком диске или флэшке).
6. Все съемные носители информации, сначала проверьте на наличие вирусов и только потом подключайте к компьютеру и начинайте с ними работать. Отключите автозапуск съемных носителей.



7. Любые программы и обновления к ним, контент и пр. загружайте с официальных сайтов или проверенных и надёжных источников.

8. Не открывайте сомнительные ссылки или электронные письма и файлы от незнакомцев.

9. Пароли и логины не храните в своём компьютере. Их следует записывать не на отдельных листах бумаги, а в тетради или блокноте. Можно хранить на внешних носителях информации (флэшке), причем логины отдельно от паролей. Как минимум 1 раз в месяц меняйте пароли.

10. При появлении баннеров вымогателей не давайте номер своего мобильного телефона, не отправляйте SMS на короткие номера.



ИСТОЧНИКИ.

- ✓ <http://infbiznull.ru/komp-yuterny-j-virus-vy-mogatel-proyav/>
- ✓ <https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9%D0%B2%D0%B8%D1%80%D1%83%D1%81>
- ✓ <http://mirsovetov.ru/a/hi-tech/network/viruses-blackmailers.html>



**СПАСИБО
ЗА ВНИМАНИЕ**

