Доклад

Эскалация привелегий. Shatter Attack

Серегин Д.А.

19 октября 2023

Российский университет дружбы народов, Москва, Россия

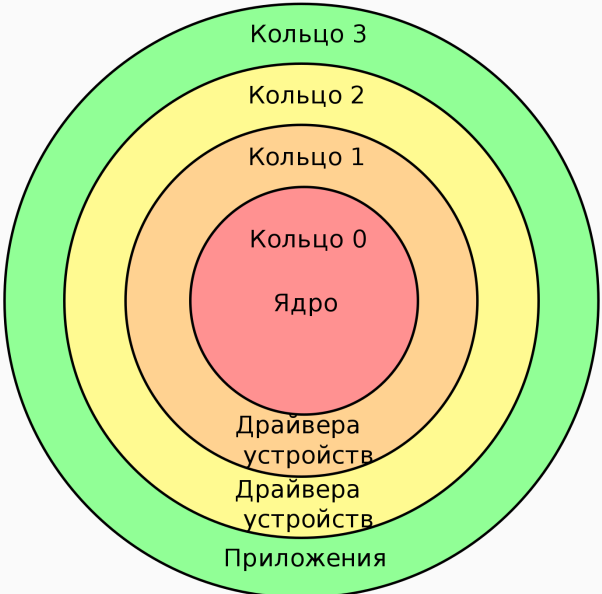
Эскалация (повышение) привилегий

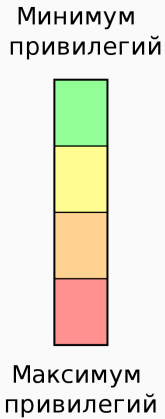
Повышение привилегий – это эксплуатация уязвимостей в операционной системе или программном приложении, которая позволяет получить доступ к ресурсам, которые обычно защищены от определенного пользователя. В результате пользователь получает большие привилегии, чем предполагалось разработчиком или системным администратором, и может выполнять несанкционированные действия на системе.

Цели атаки

1. Получение полного контроля над системой или сетью.
2. Доступ к конфиденциальной информации и возможность её модификации.
3. Запуск вредоносных программ.
4. Скрытое пребывание в системе, обходя средства мониторинга и обнаружения вторжений.
5. Продвижение вперёд в системе и достижение целей атаки.

Привелегии Windows





Повышение привелегий

1. *Горизонтальное повышение привилегий* – злоумышленник имитирует пользователя на том же уровне привилегий.
2. *Вертикальное повышение привилегий* – злоумышленник имитирует пользователя на высшем уровне привилегий
3. *Понижение привилегий* – злоумышленник имитирует пользователя с низким уровнем привилегий.

Недостаток передачи сообщений Windows

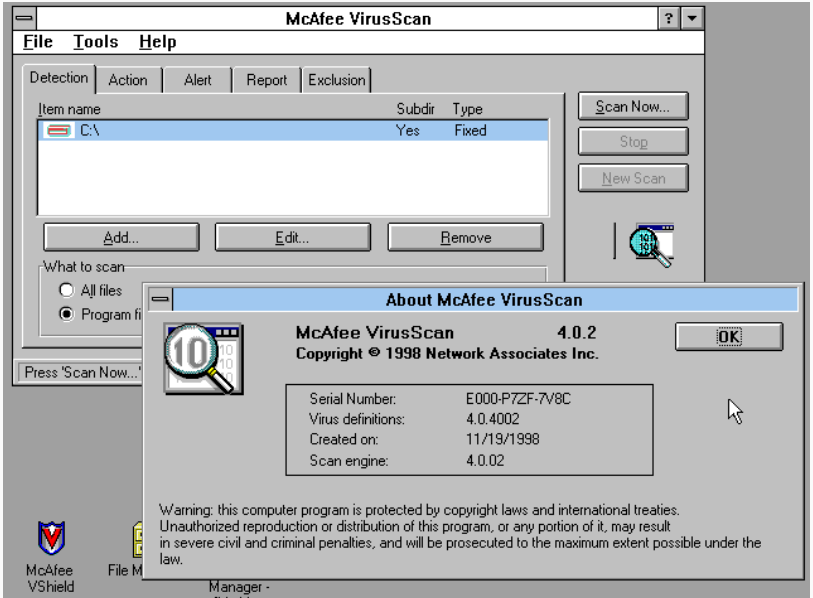
Принцип сообщений в Windows:

- При событиях, как нажатие клавиши или перерисовка окна, Windows отправляет соответствующее сообщение приложению.
- События обрабатываются в порядке очереди.

Недостаток в Win32:

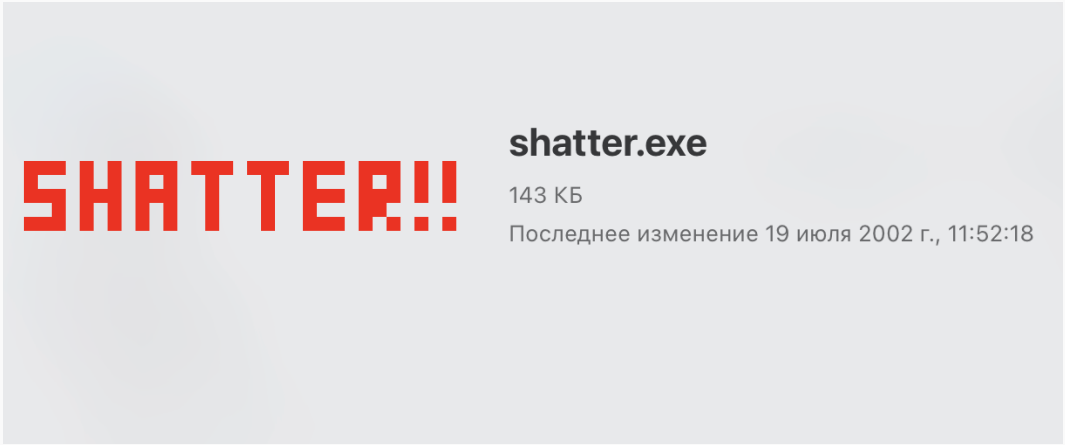
- Любое приложение на текущем рабочем столе может отправлять сообщения любому окну, без аутентификации.

VirusScan

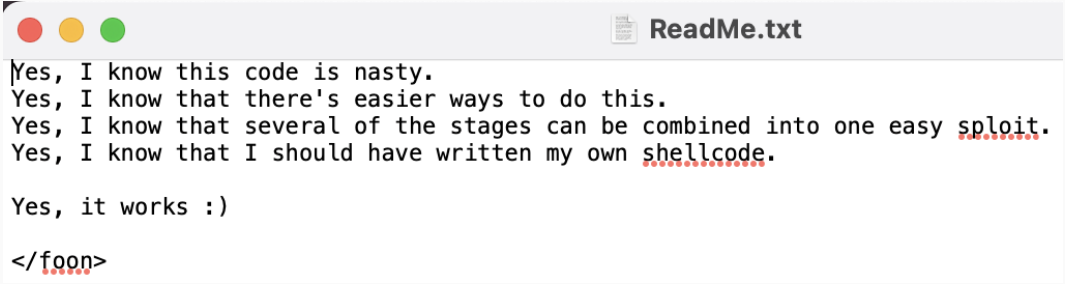

McAfee VirusScan
File Tools Help
Detection Action Alert Report Exclusion
Item name Subdir Type
C:\ Yes Fixed
Scan Now...
Stop
New Scan
Add... Edit... Remove
What to scan
All files
Program fi
Press 'Scan Now...'
About McAfee VirusScan
McAfee VirusScan 4.0.2
Copyright © 1998 Network Associates Inc.
OK
Serial Number: E000-P7ZF-7V8C
Virus definitions: 4.0.4002
Created on: 11/19/1998
Scan engine: 4.0.02
Warning: this computer program is protected by copyright laws and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result
in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the
law.
McAfee VShield
Manager -

Этапы атаки

1. Поиск окна
2. Устранение ограничений
3. Внедрение Shellcode
4. Выполнение кода


SHATTER!!
shatter.exe
143 КБ
Последнее изменение 19 июля 2002 г., 11:52:18

ReadMe


ReadMe.txt
Yes, I know this code is nasty.
Yes, I know that there's easier ways to do this.
Yes, I know that several of the stages can be combined into one easy sploit.
Yes, I know that I should have written my own shellcode.
Yes, it works :)
</foon>