Zeus Gameover

1. История появления и распространения.

**Gameover ZeuS появилась в 2014 году. Её создал российский хакер Евгений Михайлович Богачёв.**

**Программа была основана на оригинальном трояне ZeuS, чьи троянцы были впервые обнаружены в 2007 году. В 2011 году исходники ZeuS утекли в Сеть, в результате чего появились множественные подобия программы, в том числе Gameover.**

**Распространялась Gameover ZeuS через спам-письма, содержащие ссылки на веб-сайты, которые загружали вредоносное ПО на компьютер жертвы. Затем заражённый компьютер был интегрирован в ботнет, который на то время считался одним из самых сложных и безопасных в мире.**

**На пике своей активности в 2012 и 2013 годах от 500 000 до 1 миллиона компьютеров были заражены GameOver ZeuS.**

**В 2014 году оригинальный ботнет GameOver ZeuS был закрыт в результате сотрудничества правоохранительных органов нескольких стран и частных фирм по кибербезопасности под названием Operation Tovar.**

**2. Описание выполняемых действий, выявления, как лечить и какие меры защиты помогут в борьбе с ним.**

**Для выявления Zeus Gameover можно использовать следующий метод, разработанный компанией F-Secure. Нужно посетить тестовую страницу с заражённого компьютера. Это заставит вредоносный код внедрить себя в страницу. Затем страница проверит себя и обнаружит, если был добавлен код Gameover. Если строка «LoadInjectScript» найдена на странице, значит, браузер заражён Zeus Gameover.**

**Также для выявления этой угрозы можно использовать инструменты управления угрозами. Они позволяют обнаруживать подозрительную активность, как входящую в сеть, так и выходящую из неё, а также блокировать её и сообщать о ней.**

**Кроме того, для общей защиты от вредоносных программ рекомендуется использовать антивирусное программное обеспечение с быстрыми обновлениями и устанавливать последние патчи безопасности для всех приложений, включая браузеры и операционную систему Windows.**

**Для удаления вируса Zeus Gameover можно следовать таким рекомендациям:**

**- Показать скрытые файлы. Для этого нужно нажать Win+R, ввести «Панель управления» и нажать Enter. Затем кликнуть на ссылку «Внешний вид и персонализация» и выбрать «Параметры папок». В окне «Параметры папок» перейти на вкладку «Вид» и поставить галочку «Показывать скрытые файлы, папки и диски». Нажать «Применить» и «ОК» в нижней части окна «Параметры папок».**

**- Остановить вирусные процессы в диспетчере задач Windows. Для этого нужно нажать клавиши Ctrl+Alt+Del и выбрать «Дополнительные сведения».**

**- Удалить все вредоносные файлы и записи в реестре. Для этого нужно воспользоваться инструментом «Редактор реестра».**

**- Очистить вредоносные файлы cookie в браузерах. Например, в Google Chrome нужно нажать на меню «Инструменты», выбрать «Опции», перейти на вкладку «Под капотом», найти раздел «Приватность», нажать кнопку «Данные для просмотра» и «Удалить файлы cookie и другие данные сайтов». В Internet Explorer нужно нажать «Инструменты», выбрать «Безопасность», «Удалить историю просмотра», поставить галочку в поле «Файлы cookie» и нажать «Удалить». В Firefox нужно нажать «Инструменты», выбрать «Опции», перейти в раздел «Приватность» и нажать «Удалить отдельные файлы cookie».**

**Для защиты от вируса Zeus Gameover рекомендуется:**

**- Регулярно менять пароли. Эксперты советуют использовать сложные и сильные пароли, которые нужно регулярно менять.**

**- Обновлять устройство и программное обеспечение. Регулярные системные обновления помогают закрывать уязвимости.**

**- Использовать антивирусное программное обеспечение. Важно, чтобы программа автоматически обновлялась и применялись последние патчи безопасности.**

**- Не открывать вложения и ссылки в электронной почте из неизвестных и подозрительных источников.**