TLP RED[[1]](#footnote-1)

**Отчет по модулю D**

|  |  |  |
| --- | --- | --- |
| **Название объекта исследования** | **Хэш сумма файла** | **Описание объекта исследования** |
| Cheskazal.ova | 298ек23щзаш2нпа209 | Образ виртуального диска машины Windows 10 |
| Toskazal.rar | 4298енпаршмщцуа2309 | Образ виртуального диска машины Linux (Debian) |

Хэш сумма файла снята до начала исследования. Файл открывался в режиме «Read Only»

Наименование исследуемого АРМ: Bochvar01

Системное время и часовой пояс: 18:00 UTC+3

Наименование пользователя-жертвы: djensen

Сетевые интерфейсы (можно пропустить если не успеваете, но в целом указать стоит)

***Описание методологии***

Для анализа образа диска были использованы следующие инструменты: EnCase для создания образа диска и FTK Imager для его анализа. Процесс анализа включал в себя несколько этапов:

1. Анализ файловой системы: Проведен анализ файловой системы для обнаружения нелегитимных (в т.ч. удаленных) файлов и папок.
2. Поиск вредоносного ПО: Использовались антивирусные сканеры для обнаружения следов вредоносного ПО.
3. Извлечение метаданных: Были извлечены метаданные для файлов на диске, включая даты создания, модификации и доступа.
4. Анализ журналов системных событий: Проведен анализ журналов системных событий для выявления подозрительной активности.

|  |  |  |
| --- | --- | --- |
| **Временные рамки инциденты** | | |
| **Дата и время события** | **Краткое описание события** | **Полное описание события** |
| 21.01.2024 09:34 | Пользователь АРМ djensen открывает вредоносную ссылку (рис. 1) | Пользователь djensen открыл ссылку http://большиебубы.рф/evil.sh, после чего была выполнена загрузка вредоносного ПО на хост |
| 21.01.2024 09:45 | Пользователь открывает вредоносный файл (рис. 2) | Бла-бла-бла |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

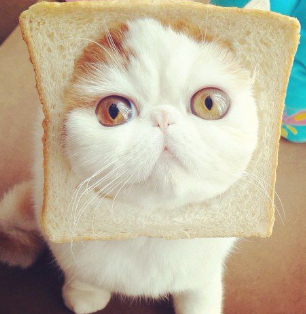
**Многоуровневое описание инцидента. Описание последовательности атак и подтверждающая информация.**

Анализ данных показал, что пользователь скачал подозрительный файл с веб-сайта, который позже был идентифицирован как Troyan.Syggen01. ВПО был создан создал туннель, позволяющий злоумышленнику получать удаленный доступ к системе (рис. 1).



(Рис. 1: Схема создания туннеля)

Во время анализа также были обнаружены следы удаления данных, что указывает на возможные попытки скрыть доказательства (рис. 2).



(Рис. 2: Сокрытие доказательств)

Были найдены следующие записи в журналах системных событий, которые подтверждают неавторизованный доступ к конфиденциальным данным (Рис. 3):

- ывопаиыдлфоафыа

- фапдлыалывдтажжфы

- ыоправдлпыв



(Рис. 3: Записи в журналах системных событий)

Были обнаружены следы вредоносного ПО, включая троянский конь и руткит. Схема распространения вредоносного ПО представлена на рисунке 4.



(Рис. 4: Схема распространения вредоносного ПО)

Анализ образа диска позволил выявить ключевые аспекты инцидента и собрать доказательства для дальнейшего расследования.

Рекомендации по предотвращению подобных инцидентов в будущем включают регулярные обновления антивирусного ПО, повышение безопасности сети и обучение пользователей безопасным практикам при работе с веб-ресурсами.

|  |  |  |
| --- | --- | --- |
| Индикаторы компрометации | | |
| Наименование индикатора | Хэш сумма (при наличии) | Описание индикатора |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Маркировка конфиденциальной информации, классифицирующая сведения в качестве крайне конфиденциальных, предназначенных только для конечного получателя [↑](#footnote-ref-1)