**ОТЧЕТ ОБ ИССЛЕДОВАНИИ**

|  |  |  |
| --- | --- | --- |
| Информация об исследуемой ОС |  | Ubuntu 16.04.6 LTS |
|  |  |  |
| Время начала инцидента |  | 2019-09-04 11:53:34 |
|  |  |  |
| Время окончания инцидента |  | 2019-09-04 12:08:51 |
|  |  |  |
| Пользователь пострадавший в инциденте |  | Test |
|  |  |  |
| Классификация злоумышленника |  | File encryptor |
|  |  |  |
| IP адрес злоумышленника |  | 192.168.1.38 |
|  |  |  |
| Схема заражения ОС |  | Port sweeping, ssh bruteforce, encrypter download, file encrypt |
|  |  |  |
| Слабости в информационной системе используемые злоумышленником |  | Ssh на стандартном порту, слабый пароль ssh, возможность исполнения скриптов python из браузера. |
|  |  |  |
| Индикаторы компрометации и пути до вредоносного ПО или инструментов злоумышленника |  | Индикаторы компрометации — множественные записи в auth.log об отказе аутентификации по ssh, с последующей успешной аутентификацией |
|  |  |  |
| Логика работы вредоносного ПО (операции, выполняющиеся на заражаемой системе, взаимодействие с сервером злоумышленника, результат работы) |  | В папке home жертвы единственным случайно сгенерированным ключем шифруются файлы '.doc','.txt','.rc','.ini','.dat','.conf','\_history'.   Затем ключ отправляется на сервер на хост злоумышленника на порту 9999  К именам зашифрованных файлов добавляется расширение .enc, исходные файлы удаляются. |
|  |  |  |
| Алгоритм восстановления системы от действий вредоносного ПО |  | Из дампа dump.pcap извлекается криптор и отправленный на сервер злоумышленника ключ. На основе информации из криптора пишется декриптор. Расшифровываются файлы. |
|  |  |  |
| Восстановленная информация пользователя |  | Расшифрованный файл secrets.txt |
|  |  |  |
| Рекомендации по настройке ОС для избегания повторения инцидента в будущем |  | Изменить политики паролей пользователей для уменьшения вероятности подбора паролей.  Запретить исполнение скриптов python из браузера. |

Исполнитель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_Д.Д.Сутягин\_

**ЛИСТ ДЛЯ ЗАМЕТОК**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_