Результаты расследования инцидента в ООО “Acme Corp”

# Executive Summary

Высокоуровневое описание инцидента. Здесь представлена информация, которая представляет наибольшую важность для исполнительных руководителей компании без указания конкретных технических подробностей. Данный раздел должен содержать:

1. Временные рамки инцидента
2. Вектор(а) атаки
3. Высокоуровневое описание последовательности атаки
4. ВПО и инструменты, которые были использованы в процессе атаки (без конкретного описания технических деталей)
5. Какие цели были поставлены злоумышленниками и какие результаты были достигнуты при атаке

|  |  |
| --- | --- |
| Название объекта исследования | Описание объекта исследования |
| traffic.pcapng | Сетевой трафик атакованной машины |

# Результаты исследования

Обнаружение открытого порта 36402

 **116.203.251.161:** IP-адрес клиента, который отправил запрос. – внешний командный сервер

 **172.16.216.130:** IP-адрес DNS-сервера, к которому отправлен запрос. – атакованная машина Linux

Много рекламы в трафике

Тело скрипта передается в TXT-записи в DNS

Начало аномалии 69.552113068



## Временные рамки инцидента

В таблице данного раздела участникам необходимо привести конкретные события на скомпрометированных системах.

|  |  |  |
| --- | --- | --- |
| Дата и время события | Краткое описание | Полное описание (необязательно) |
| 06.11.2022 13:51:54 | ocsp ответ |  |

## Вектор(а) атак и подтверждающая информация

В данном разделе участникам необходимо описать конкретные векторы атак, используемые злоумышленниками. Информация о каждом векторе должна содержать проверяемое доказательство.

## Описание последовательности атаки и подтверждающая информация

В данном разделе участникам необходимо описать последовательность атаки и привести доказательства своих суждений (скриншоты, перечисление использованных артефактов форензики). В текущем разделе необходимо привести данные (доказательства) о причастности/непричастности подозреваемого. Предпочтительным представлением является разбиение данного раздела на подразделы с заголовками третьего уровня.

## Перечень секретной информации, находящейся на компьютере

|  |  |
| --- | --- |
| Имя файла | Описание |
| - | - |

## ВПО и инструменты, которые злоумышленники использовали в процессе атаки

В данном разделе участникам необходимо привести перечень используемых злоумышленниками инструментов в данной форме:

|  |  |
| --- | --- |
| Название ВПО/инструмента | Цель использования |
| Ubuntu Firefox Modifications | Аддон к Firefox, adware/spyware |

## Используемые C&C сервером команды

|  |  |
| --- | --- |
| Название команды | Описание команды |
|  |  |

## Справка о восстановлении файлов

В данном разделе необходимо привести информацию о восстановленных файлах. Также в данном разделе нужно в кратком виде привести информацию об алгоритме шифрования файлов.

|  |  |  |
| --- | --- | --- |
| Имя файла | Описание файла | Содержимое файла |
|  |  |  |

# 

# Индикаторы компрометации (IOC)

## Файловые индикаторы компрометации (sha1sum файлов, связанных с атакой; пути закрепления ВПО)

Информация в данном разделе приведена маркированным списком.

## Сетевые индикаторы компрометации (IP адрес(а) злоумышленника)

**116.203.251.161** внешний командный сервер