Впервые в Казахстане!
Только у нас!
Или анализ UEFI-трояна

Олег Биль,
главный архитектор-разработчик по исследованию вредоносного кода,
Лаборатория исследования вредоносного кода,
АО «Государственная техническая служба»

Обо мне

- Сфера интересов: исследование целевых атак, повышение эффективности использования сложных решений для выявления и анализа действий атакующих
- Основатель Лаборатории исследования вредоносного кода
- Читаю курсы по ИБ, от простых до экспертных
- Готовил студентов к участию в конференциях. Докладчики и призеры конференций Лаборатории Касперского и Positive Hack Days (Young School)
- Выступал на ряде конференций в Казахстане, а также — на Positive Hack Days (Москва, май 2018), BISSummit (Баку, июнь 2018), Security Analyst Summit (Сингапур, апрель, 2019), FIRST Conference (онлайн, в связи с эпидемией, ноябрь 2020).

Уточнение…

Мы концентрировались на анализе функциональной части вредоносного объекта. Некоторые детали процесса заражения и потока исполнения до выполнения реального вредоносного кода выходят за рамки данной презентации.

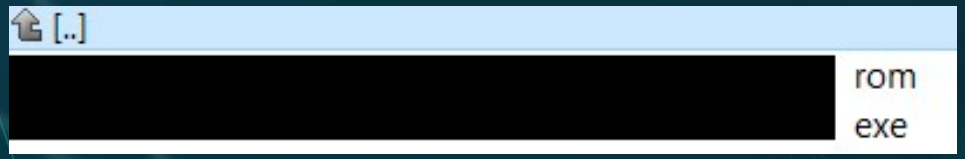
Что такое UEFI?

Универсальный интерфейс расширяемой прошивки (англ. Unified Extensible Firmware Interface)
Предназначен для замены BIOS
Поддерживает диски, размером более 2 Тб
Обеспечивает поддержку сети и имеет ряд других преимуществ, относительно BIOS

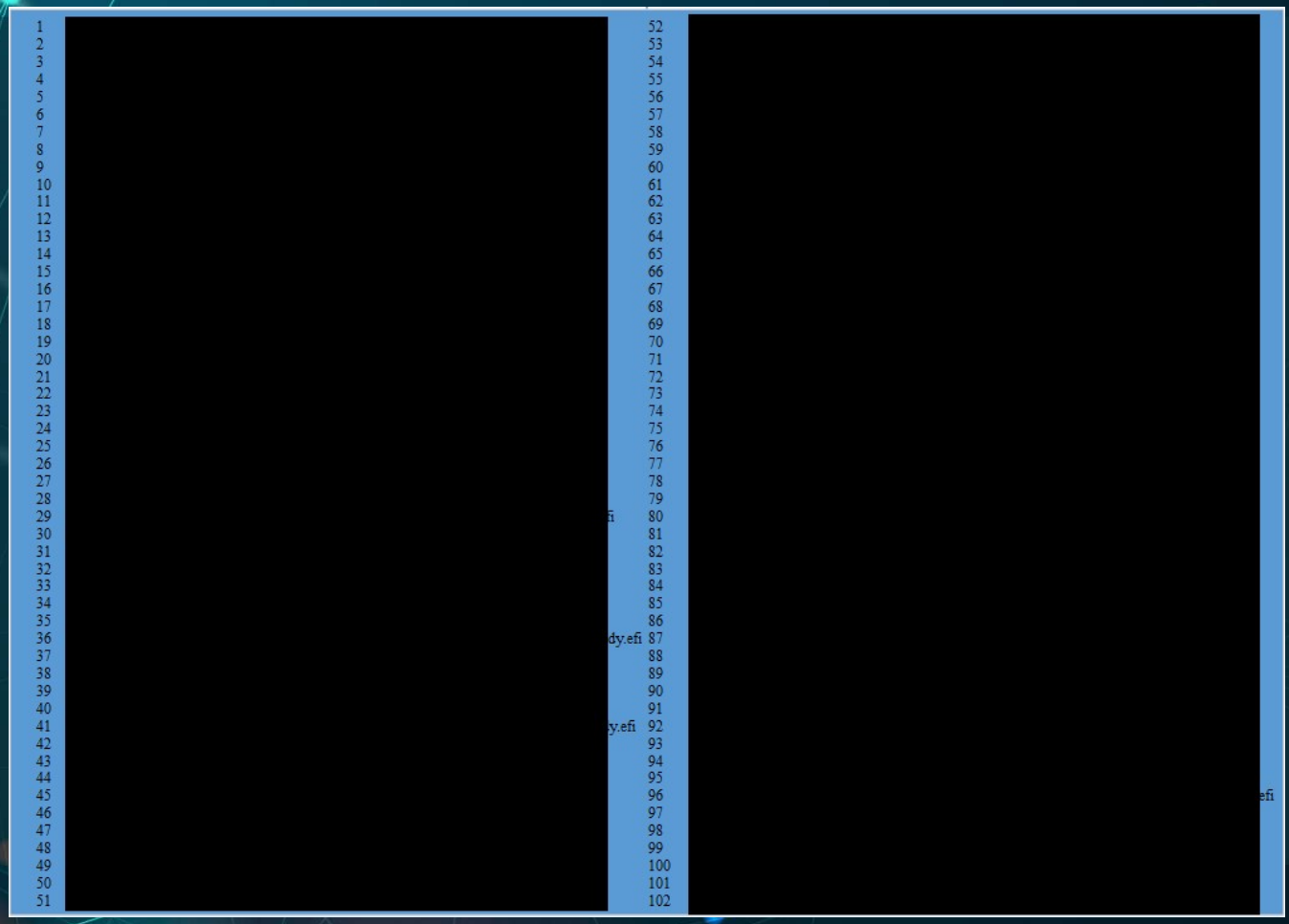
В чем проблема?

- Это – буткит! Код, получающий управление на очень ранней стадии загрузки компьютера, когда еще не работают многие защитные механизмы (в том числе – реализованные в ОС и антивирусах).
- Заражает UEFI прошивку! Это позволяет вредоносному коду «выживать» на компьютере после переустановки ОС, форматирования или замены жесткого диска (т.к. вредонос находится в энергонезависимой памяти на материнской плате).
- Относительно новый вектор угроз. В статье https://www.ptsecurity.com/ru-ru/research/analytics/bootkits-evolution-and-methods-of-detection/ говорится об изучении 39 семейств буткитов. Заражающих прошивку – единицы.
- Трудно искать, многие специалисты не знают про данный вектор.

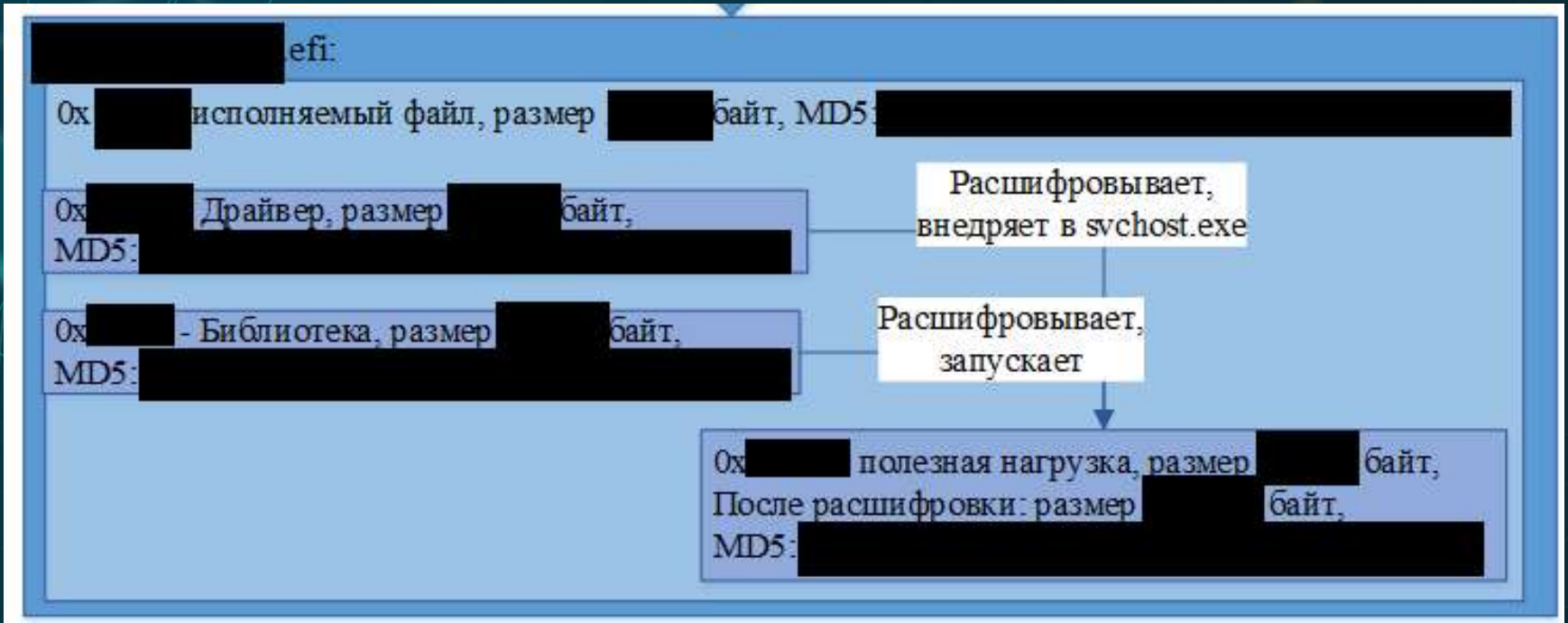
С чего всё началось?



С чего всё началось?



Что получилось?



Что он может делать?

- Файловый шпион (отправка локальных файлов на сервер, создание листинга каталогов, перемещение файла, удаление файлов)
- Загрузчик файлов с сервера (создание нового файла и запись в него)
- Запуск произвольного исполняемого файла
- Удаленный шелл
- Профилирование зараженного компьютера
- Работает без конкретного сервера управления (прослушивает порт).

Как с этим жить?

- Secure Boot, Intel Boot Guard (существуют уязвимости, например, статья: Researchers discovered a flaw in three signed third-party UEFI boot loaders that allow bypass of the UEFI Secure Boot feature)
- Современные антивирусы (нет гарантий в случае целевых атак)
- Экспертное исследование.

Спасибо!
Вопросы?

info@sts.kz

www.sts.kz