T&T Security

#CODEIB

Как скрыть атаки ВПО от обнаружения песочницей и как этому противодействовать?

Тохтабаев Арнур, T&T Security

Background:

- Учился и работал в США с 2005 по 2013 год
- Получил степень доктора PhD в государственном университете штата Нью-Йорк (State University of New York at Binghamton)
- Работал Профессором-Исследователем в Центре Безопасных Информационных Систем при университете Джорджа-Мейсена (Center for Secure Information Systems at George Mason University)*

База

9 лет исследования в США

11 публикаций в США и Европе**, 81** цитата

Результат – Новая антивирусная технология

Большая перспектива в коммерциализации

** Данный центр входит в десятку лучших научных центров по кибербезопасности в США*

Угрозы

Доступность инструментов "ВПО"

Cobalt (Strike), Metasploit (Anti-AV), leaked packs

Скрытые атаки

Sandbox Evasion, Endpoint evasion

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

DOCUMENTATION

Artifact Kit

Cobalt Strike uses the Artifact Kit to generate its executables and DLLs. The Artifact Kit is a source code framework to build executables and DLLs that evade some anti-virus products.

Легальные каналы

RDP, DLL-side loading, Powershell

BLOG

« Cobalt Strike 3.10 – Хакер vs. 肉雞

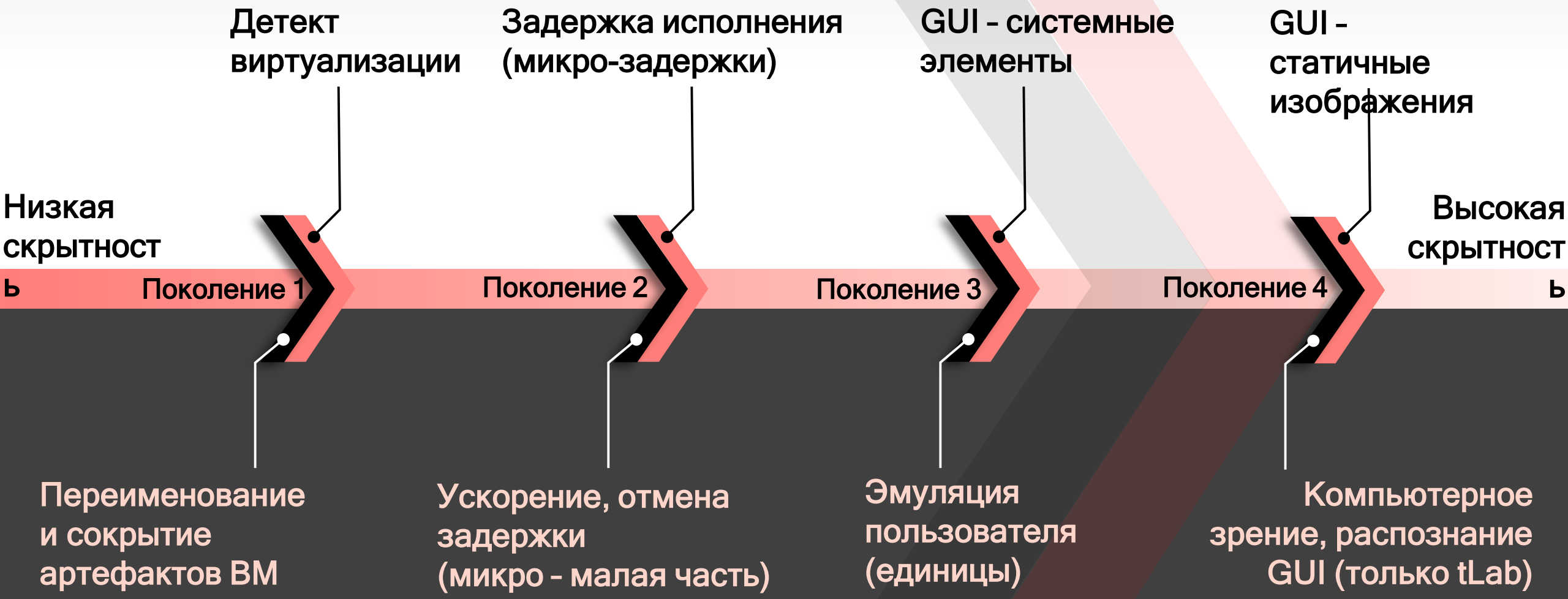
In-Memory Evasion

February 8, 2018

Безфайловые атаки

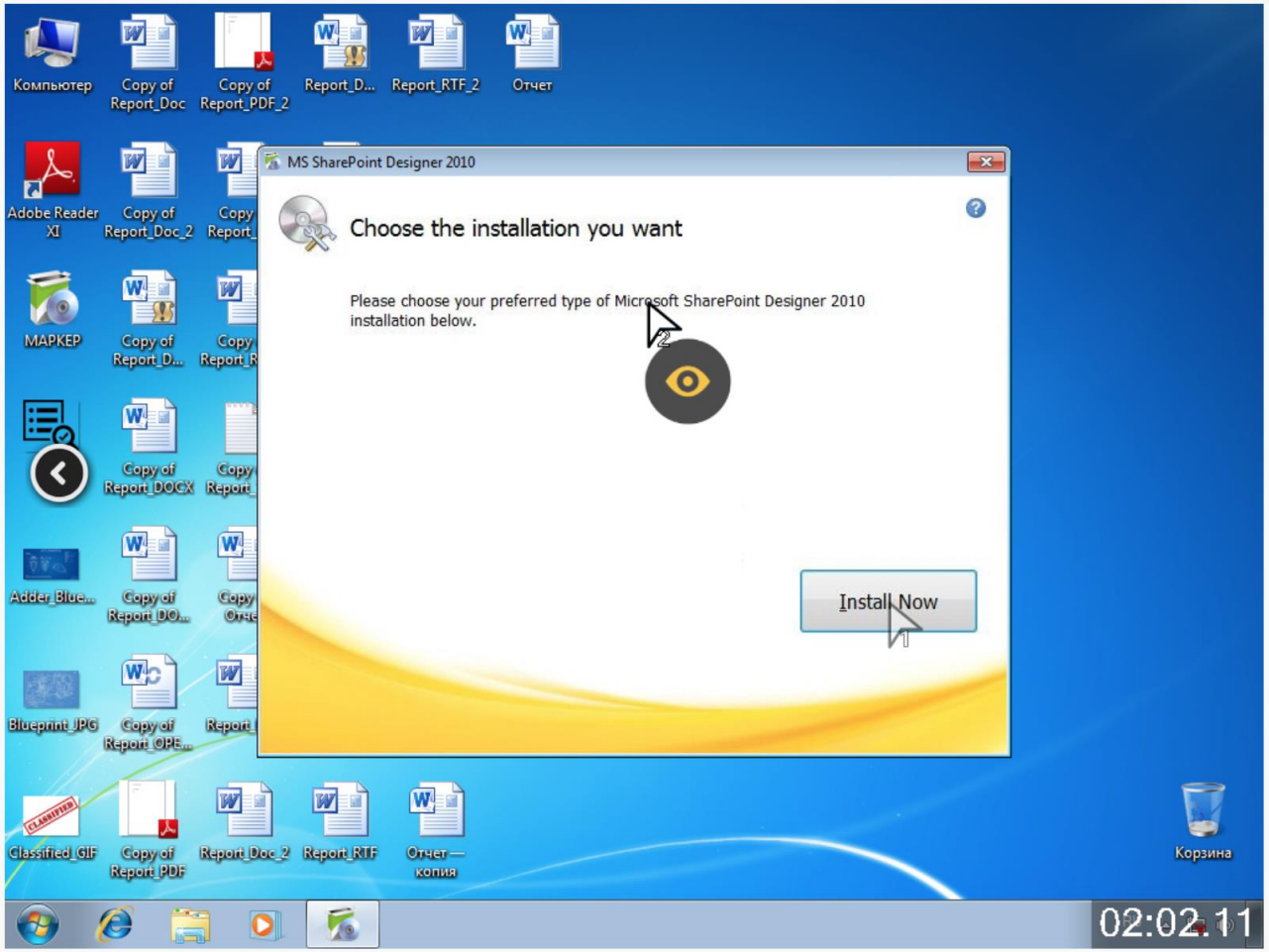
Reflective DLL (виртуальный загрузчик) - стелс

Скрытые атаки и анти-уклонение (sandbox evasion)



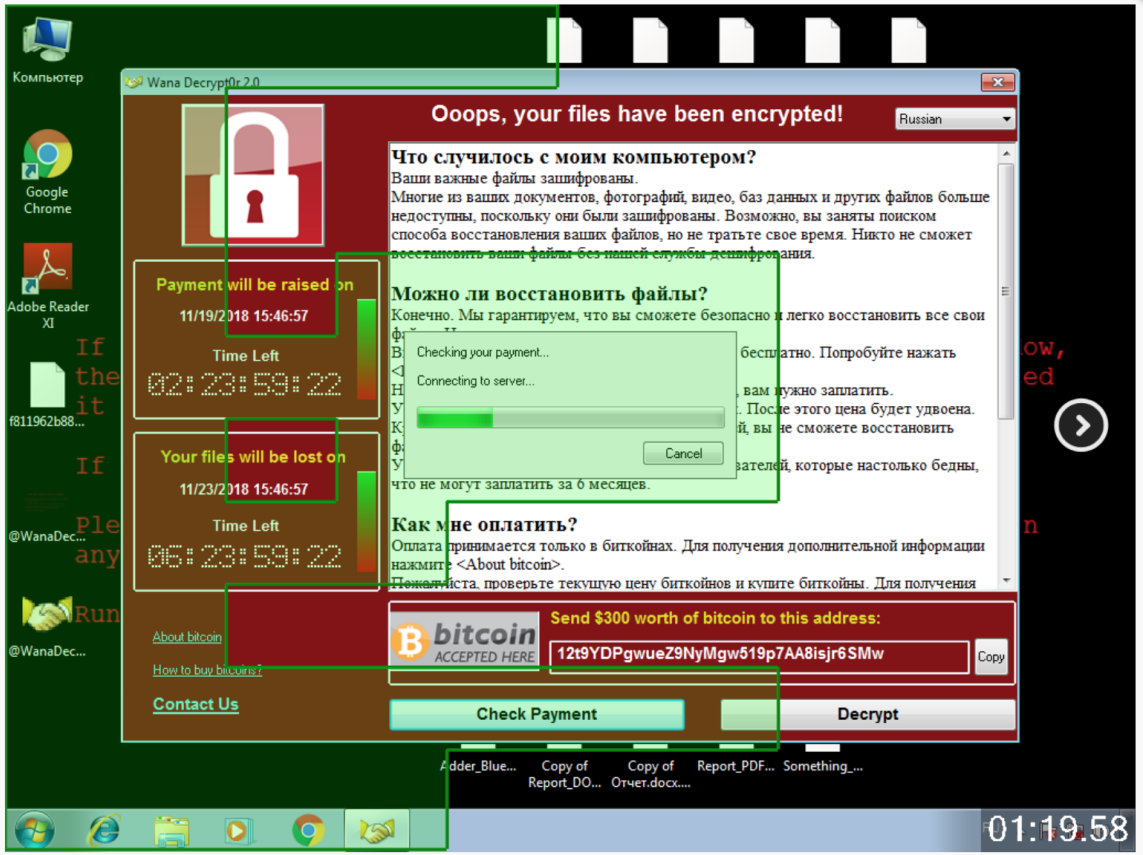
Результат: Некоторые виды угроз может обнаружить только tLab

Противодействие: ВПО на статичных изображений



- Сложные фильтры
- Идентификация многоугольников
- Используются только фигуры не содержащие другие фигуры
- Сигнал клика отправляется на координаты центров найденных фигур.

Пример (мульти-клик)



Обнаружено визуальное изменение: **11,0085864%** экрана

Иерархия критериев для Sandbox-систем

Адаптация решения под задачи заказчика, оперативное реагирование при смене модели угроз (в том числе ядро)

2 в 1 – Обнаружение угроз в потоке и исследование угроз. Максимально развернутая аналитика по образцу ВПО для эффективного реагирования.

0-day ВПО, таргетированные угрозы, технология уклонения от обнаружения (evasive malware)

Отчеты (экспорт), аналитика, локализация, кастомизация

Коннекторы (Web/Mail), SIEM

T&T Security

Q/A Session