Артем Баранов
Ведущий вирусный аналитик ESET

Win32/Spy.Ranbyus нацелен на модификацию Java-кода систем удаленного банкинга Украины

Недавно мы обнаружили новую модификацию банковского трояна **Win32/Spy.Ranbyus**, который уже был предметом исследования наших аналитиков. Одна из его модификаций упоминалась Александром Матросовым в материале, посвященном эксплуатированию смарт-карт в банковских троянах.

Данная модификация обладает интересным функционалом, так как показывает возможность обхода операций аутентификации при осуществлении платежных транзакций с помощью устройств смарт-карт. В той же модификации был обнаружен код поиска активных смарт-карт или их ридеров, после нахождения которых бот отсылал информацию о них в командный центр C&C с описанием типа найденных устройств.

Аналитики ESET внимательно отслеживали последние модификации семейства этого трояна и выяснили, что Ranbyus начал специализироваться на модификации Java-кода в одной из самых популярных на Украине систем удаленного банкинга (remote banking systems), а именно, BIFIT *iBank 2*. Статистика на **ESET Virus Radar** показывает, что на Украине зафиксировано наибольшее количество инфекций Ranbyus.

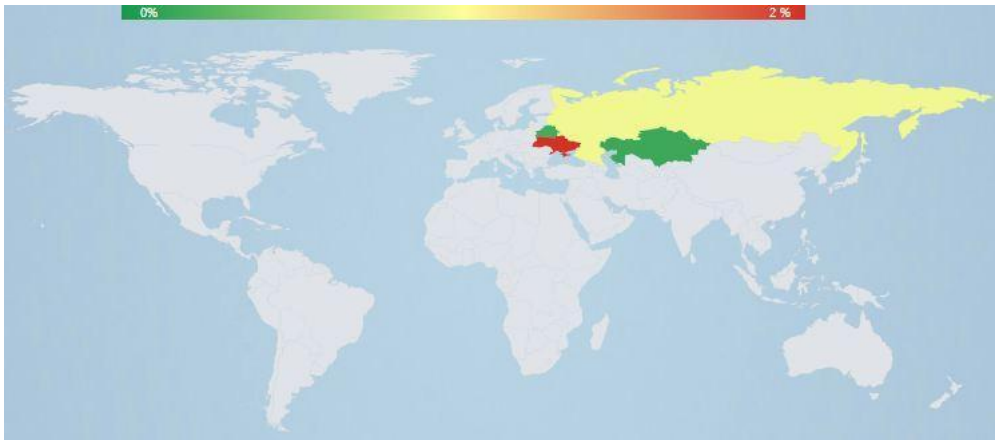

Рис. 1. Статистика распространения Ranbyus.

На рисунке 1 показана статистика распределения заражений Ranbyus по странам, на котором видно, что Украина является лидером по количеству заражений. Также очевидна нацеленность трояна на Россию и Украину.

Отличительной особенностью этого банковского трояна является отсутствие механизма web-инжектов, обычно применяемых в угрозах подобного рода (как, например, в небезызвестном Zeus). Вместо этого он реализует атаку на специфическое ПО, используемое при осуществлении различного рода платежей и других банковских операций.

Win32/Spy.Ranbyus собирает информацию о зараженной системе (активные процессы, версию ОС и т. д.) и отправляет ее на командный сервер (C&C). Основной функционал по краже денег основан на наборе различных форм-грабберов, нацеленных на пресловутое банковское ПО. Например, грабберы для разработанных под Java-платформу программ выглядят так (рис. 2):

```
int __cdecl inject_java()
{
  int v0; // eax@3
  char v2; // [sp+0h] [bp-10h]@1

  init(&v2);
  create_process_mutex(&v2);
  if ( get_config_value_96() )
    get_import(&v2);
  mem_alloc();
  delete_iBank_files();
  init_java_hooks(&v2);
  init_browser_and_java_grabber();
  init_java_javaw_browser_grabber();
  create_thread_ex(sub_4074B9, 0, 0);
  v0 = get_imports_table();
  (*(v0 + kernel32_Sleep))(-1);
  exit_process(&v2);
  return 0;
}
```

Рис. 2. Код инжекции Java-граббера.

Наш коллега Александр Матросов уже описывал схожий функционал в другом семействе банковских вредоносных программ – Carberp. Эти программы обладают специальным функционалом по модификации виртуальной Java-машины (Java Virtual Machine, JVM) и отслеживанию активности ПО, предназначенного для осуществления платежей.

Ranbyus использует другой подход – он модифицирует Java-код только для определенного приложения, не прибегая к модификации JVM. Например, Ranbyus может модифицировать расположение форм, чтобы скрыть информацию о поддельных транзакциях, реализованных через троян (рис. 3).

```
removeNodeFromParent•
(Ljavax/swing/tree/MutableTreeNode;)V•
getText•
getUserObject•
getChild•
(Ljava/lang/Object;I)Ljava/lang/Object;•
getChildCount•
(Ljava/lang/Object;)I•
getRoot•
getModel•
()Ljavax/swing/tree/TreeModel;•
class com.bifit.swing.tree.XTree•
getComponent•
(I)Ljava/awt/Component;•
()Ljava/lang/Object;•
getComponentCount•
()I•
javax/swing/text/JTextComponent•
javax/swing/JLabel•
prepareRenderer•
(Ljavax/swing/table/TableCellRenderer;II)Ljava/awt/Component;•
getCellRenderer•
(II)Ljavax/swing/table/TableCellRenderer;•
getContentPane•
()Ljava/awt/Container;•
SUM•
(I)Ljava/lang/String;•
%.02f•
repaint•
setText•
(Ljava/lang/String;)V•
class javax.swing.JLabel•
fireTableDataChanged•
(I)Ljava/lang/Object;•
getRowCount•
getColumnCount•
()Ljavax/swing/table/TableModel;•
class com.bifit.swing.table.Table•
```

Рис. 3. Методы Java, отслеживаемые Ranbyus.

Кроме того, **Win32/Spy.Ranbyus** может блокировать действия системы удаленного банкинга и показывать такое сообщение (рис. 4):

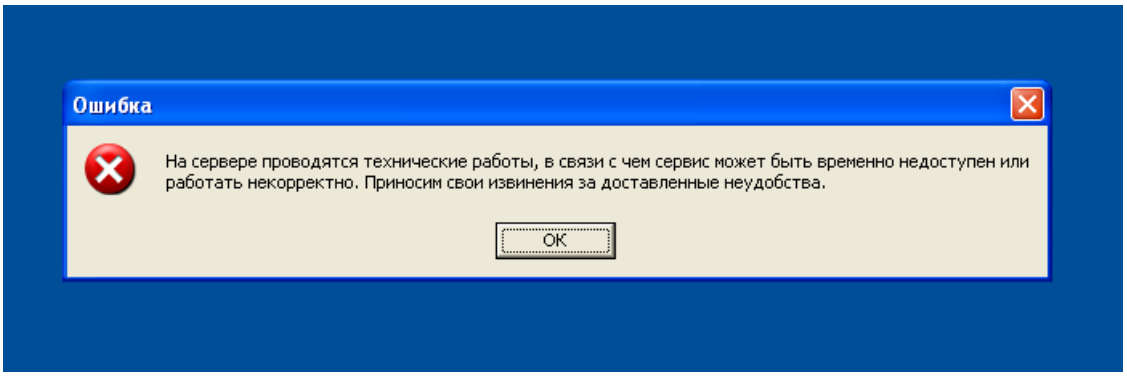

Рис. 4.

Пока Ranbyus нацелен только на украинские и российские банки, атаки в других регионах замечены не были. К слову, русифицирована даже панель управляющего центра ботнета **Win32/Spy.Ranbyus** (рис. 5):

Главная | Боты | Слежение | Акки | Поиск | Загрузки | Демон | Граббер | Обновление | Настройки | Выйти ([redacted]

I-bank bifit | PC-bank bifit | Промсвязь | I-bank BSS | Alfa | Неизвестные

supported RBS

Ботнеты: Все | install | general | qd

#	ID	Date	Country	Comments	Links
1	lenovo-060d72e5_c9045a14_8a7b2ead	[redacted]	-	ключ 5,8кк	Подробнее Комментарий Удалить
2	elena-pc_b663f28c_ed5b292	[redacted]	-	токен, две подписи	Подробнее Комментарий Удалить
3	fz0RIKEm_c6b211e3_499e218c	[redacted]	-	токен 508	Подробнее Комментарий Удалить
4	xp_1ac0bc70_3c7b458	[redacted]	-	2,7кк токен	Подробнее Комментарий Удалить
5	RGN-EKAT-WS01_9f480b46_771fa102	[redacted]	-		Подробнее Комментарий Удалить
6	lHrsNuxk7M_a80c2f7_5d938b13	[redacted]	-	bss	Подробнее Комментарий Удалить
7	user1_ca5689b2_ed207fd7	[redacted]	-	токен	Подробнее Комментарий Удалить
8	bos_dde6cd8f_935812d0	[redacted]	-		Подробнее Комментарий Удалить
9	516c2954c5ac410_9755e5a9_68c47b8e	[redacted]	-		Подробнее Комментарий Удалить
10	microsof-02e5d0_b8b24a9_33d125d0	[redacted]	-	ИСПОЛЬЗОВАН. 500к	Подробнее Комментарий Удалить
11	GlavBux_4d519b63_6728dafe	[redacted]	-	токен	Подробнее Комментарий Удалить

Рис. 5.

На данный момент группа Carberp является лидером на киберпреступном рынке в России, обеспечив себе присутствие в двадцатке наиболее активных российских угроз за весь год. При этом Ranbyus занимает лидирующую позицию среди банковских вредоносных программ и на Украине.