How I handled one of the biggest banking fraud incidents of 2020

Daniel Lima (NTT, Brazil)
• All information contained in this presentation is based on real events occurred in 2020. All sensitive information was removed in order to protect the institutions and people involved in the case.

• This lecture is informative and aims to assist in identifying and responding to threats.

• Using it wisely and for good, is part of the principles of an Ethical Hacker.
Thales Cyrino

- linkedin.com/in/thalescyrino
- Cybersecurity Sales Director  NTT
- + 20 years of IT and cybersecurity experience

- Develop Cybersecurity business in LATAM
- Member of Cisco Secure Partner Advisory Council
- Cybersecurity Go-To-Market Strategy
- Data Protection Officer
- SABSA Framework practice
**Scenario and Challenges**

**Increasing Fintech presence**
More than 1289 fintech's in Brazil, between 2016 and 2022 was created 513 new finance startups.

**Huge Increase of frauds attempts**
In 2021 there were almost 4 digital fraud attempts per minute in Brazil.
- Growth of 445% of robot attempts
- Growth of 138% of Human attempts in second half of 2021

**2020 Brazil launched PIX**
Central bank in Brazil launched the electronic payment system
- More than 110 million of Brazilian use PIX
- 1.4 Billions of transaction are made daily

**Pandemic accelerate criminal changes**
During pandemic, the poverty increased in Brazil.
The main criminal factions changed their criminal behavior to digital crimes.
- Today 89% of the crimes are digital in Brazil.

**Digital and Physical world**
The criminal are doing kidnaping and forcing people to transfer money using electronic payment system, the biometrics and continuous authentication is becoming a necessity

**Skills and expertise**
There is a gap of 4 million around the world – and the demand for cybersecurity professionals is only growing.
- In Brazil the gap is around 441K
Who Am I?

Daniel Lima
- linkedin.com/in/danielolima
- SOC Director • NTT
- + 9 years of cybersecurity experience

- Expert
  - Cryptography
  - Fraud and Risk Intelligence
  - Risk Management
  - CSIRT - Blue Team Operations
  - Advanced SOC Operations
  - CISA Certified ICS
Timeline of Incident
12/25/20
**Identifying the intruder**
Traffic analysis and log correlation in SIEM
We searched the SIEM and found a valid unauthorized credential by accessing the bank's internal application through an API.

12/25/20
**Incident Response**
Communication block at the edge
We immediately blocked the valid credential that was performing unauthorized access and obtaining information from the bank's official application and forwarding it to the fake website in real time in an automated way (API).

12/28/20
**Counterattack**
Gaining access to the attacker's server
By analyzing the API error logs and mapping the attacker's external IP's we found a credential with a password registered in the API that was used to authenticate on the fake website and with that we gained access to the attacker's server.

12/28/20
**Understanding the whole**
Identified type of attack and more than 15 financial institutions being harmed
We found a portal that allowed the creation of a new fake website with just a few clicks and that already included CDN in its architecture.

12/25/20
**Security incident**
Fake bank website
We received a ticket about a host phishing websites impersonating internet banking portal.
Ensure the evidence
Make sure content is available offline
We immediately downloaded all content from the server.

Lessons learned
Create ways to prevent or alert this behavior or type of attack in the future.

Ensuring access
Creating ways to stay connected
We created a credential with the same name as one of the fraudsters and with the same permissions.

Recovery
Ensure that customers affected by the fraud have their passwords reset immediately.

Responsible Disclosure
Ensure that those responsible for the companies involved and the authorities are notified.
Understanding the Attack
Entry #1
E-mail Phishing + Fake Site

Returns the actual account information to the user, Account Balance and Transactions, which makes it difficult to identify Fraud.

Entry #2
Malware Executable

STOLEN DATA
- Identity
- Account
- Password
- Credit Card
- Security Key Card

Real-time Database Sync

MySQL

Automated API

Attacking User Panel
Real Time Fraud Panel
Add New Domains
Deploy CDN

Access to the bank's internal system
<table>
<thead>
<tr>
<th>COMPARISON</th>
<th>Normal Phishing</th>
<th>Automated Phishing + Combined Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steals user credentials</td>
<td>✔ OK</td>
<td>✔ OK</td>
</tr>
<tr>
<td>Performs fraud with stolen customer data</td>
<td>✔ OK</td>
<td>✔ OK</td>
</tr>
<tr>
<td>Steals Company credentials</td>
<td>✗</td>
<td>✔ OK</td>
</tr>
<tr>
<td>Create fake banking system program</td>
<td>✗</td>
<td>✔ OK</td>
</tr>
<tr>
<td>Online Fraud Information Dashboard</td>
<td>✗</td>
<td>✔ OK</td>
</tr>
<tr>
<td>Online authentication API on the internal systems of some banks</td>
<td>✗</td>
<td>✔ OK</td>
</tr>
<tr>
<td>Returns the real information of the client through the fake website, making the attack invisible.</td>
<td>✗</td>
<td>✔ OK</td>
</tr>
</tbody>
</table>
## Online Fraud Dashboard

<table>
<thead>
<tr>
<th>Description</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digitando senha da internet</td>
<td>12 hrs 51 min 57 s</td>
</tr>
<tr>
<td>Senha errada, solicitando novamente.</td>
<td>5 hrs 46 min 33 s</td>
</tr>
<tr>
<td>R$ 221.98 D</td>
<td>Cliente expulsado</td>
</tr>
<tr>
<td>R$ 0,00 C</td>
<td>Aguardando comando silenciado</td>
</tr>
<tr>
<td>R$ 2,000,00 D</td>
<td>Aguardando cliente digitar o SMS</td>
</tr>
<tr>
<td>R$ 0,89</td>
<td>Cliente expulsado</td>
</tr>
<tr>
<td>R$ 4,74 C</td>
<td>Digitando assinatura eletrônica silenciado</td>
</tr>
</tbody>
</table>
The combination of different attacks makes them more effective

- Niche-targeted Phishing, not a single company
- Theft of customer credentials
- Theft of company credentials
- Access to the company's internal and official environment (Internet Bank)
- Attackers use Content Delivery Network (CDN) to mask the original IP addresses and provide a valid and trusted digital certificate.
The time between the registration of a new domain and the start of the campaign is very short, which makes it difficult to identify.

- More than 15 financial institutions, including banks and acquirers
- More than 10,000 customers affected
- More than 14 email domains between leaked emails
- Malware artifact found

Unmeasurable loss of customer confidence in using digital means of payment or account management
Malware Analysis
# Sandbox Analysis

## Behavioral Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Severity</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific Set Of Indicators Signalling High Likelihood of Maliciousness Detected</td>
<td>95</td>
<td>100</td>
</tr>
<tr>
<td>Process Deleted an Executable in a System Directory</td>
<td>90</td>
<td>100</td>
</tr>
<tr>
<td>Process Modified a File in a System Directory</td>
<td>60</td>
<td>100</td>
</tr>
<tr>
<td>Process Opens a Listening Port</td>
<td>80</td>
<td>90</td>
</tr>
<tr>
<td>Process Deleted an Executable in the Program Files Directory</td>
<td>80</td>
<td>90</td>
</tr>
<tr>
<td>Alternate Data Stream File Creation Detected</td>
<td>80</td>
<td>90</td>
</tr>
<tr>
<td>Process Modified a File in the Program Files Directory</td>
<td>80</td>
<td>90</td>
</tr>
<tr>
<td>Process Modified Firefox Certificate Database</td>
<td>75</td>
<td>85</td>
</tr>
<tr>
<td>Sample Launched Copy Of Itself</td>
<td>60</td>
<td>100</td>
</tr>
<tr>
<td>Process Attempted to Access the FireFox Password Manager Local Database</td>
<td>95</td>
<td>75</td>
</tr>
<tr>
<td>Process Modified an Executable File</td>
<td>70</td>
<td>80</td>
</tr>
<tr>
<td>Process Modified File in a User Directory</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recent Digital Signature

Malware Installation Log

Artifact 12: "\TEMP\Instalação do Módulo Adicional de Segurança\Log"

- **Src. disk**: 0
- **Imports**: 0
- **Type**: ISO-8859 text, with CRLF line terminators
- **Size**: 2050
- **Exports**: 0
- **AV Sigs**: 0
- **Path**: "\TEMP\Instalação do Módulo Adicional de Segurança\Log"
- **Mime Type**: text/plain; charset=binary
- **Magic Type**: ISO-8859 text, with CRLF line terminators

**SHA256**: cc541ca97c11f49313320cd8d1a8897515050016b97d68c387245b8c1015b8d1
**MD5**: 380b2ec85267878315c8c385f42568998

**SHA1**: 3442c46e5d874e1f7e08d64732d388c4265c9
**Created At**: +758.0s
**Modified By**: 5 (GBPCEF_falso.exe)
**Created By**: 5 (GBPCEF_falso.exe)
Warsaw Registry modified

<table>
<thead>
<tr>
<th>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL[20E60725-16C8-4FB9-8BC2-AF92C5F8D06D]_IS1</th>
<th>26</th>
<th>(gbpcefwr64.tmp)</th>
<th>DisplayIcon</th>
<th>C:\Program Files\ Warsaw\</th>
</tr>
</thead>
<tbody>
<tr>
<td>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>Warsaw Setup</td>
<td></td>
</tr>
<tr>
<td>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL[20E60725-16C8-4FB9-8BC2-AF92C5F8D06D]_IS1</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>Publisher</td>
<td></td>
</tr>
<tr>
<td>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL[20E60725-16C8-4FB9-8BC2-AF92C5F8D06D]_IS1</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>DisplayName</td>
<td>Warsaw 2.15.1.1 64 bits</td>
</tr>
<tr>
<td>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL[20E60725-16C8-4FB9-8BC2-AF92C5F8D06D]_IS1</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>Inno Setup: Language</td>
<td>en</td>
</tr>
<tr>
<td>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL[20E60725-16C8-4FB9-8BC2-AF92C5F8D06D]_IS1</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>EstimatedSize</td>
<td>68389</td>
</tr>
<tr>
<td>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL[20E60725-16C8-4FB9-8BC2-AF92C5F8D06D]_IS1</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>Inno Setup: User</td>
<td>SYSTEM</td>
</tr>
<tr>
<td>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL[20E60725-16C8-4FB9-8BC2-AF92C5F8D06D]_IS1</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>MinorVersion</td>
<td>15</td>
</tr>
<tr>
<td>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL[20E60725-16C8-4FB9-8BC2-AF92C5F8D06D]_IS1</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>UninstallString</td>
<td>&quot;C:\Program Files \Warsaw&quot;</td>
</tr>
<tr>
<td>MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL[20E60725-16C8-4FB9-8BC2-AF92C5F8D06D]_IS1</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>Inno Setup: Setup Version</td>
<td>5.5.9 (u)</td>
</tr>
<tr>
<td>USER\S-1-5-19\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS</td>
<td>26</td>
<td>(gbpcefwr64.tmp)</td>
<td>ProxyOverride</td>
<td>&lt;local&gt;</td>
</tr>
</tbody>
</table>
4 Steps to work on Incident
Preparation

• Know and Monitor your customers...

• Critical servers, networks, applications and endpoints

• Level of importance and priority

• Create baseline of standards to be used in future comparisons

• Determine the Security events and set the thresholds

• Create a communication plan
Detection and Analysis

• Identification...

• Do the analysis

• Determine the entry point

• Determine the extent of the breach

• Do your homework
Containment
Eradication and Recovery

• Work to do...
• Stop the bleeding
• Fix the threat entry point
• Remove the Threat
• Resume operation and services
Post-Incident Activity

• Take a breath and carry on...

• Lessons learned

• Continuous improvement cycle – PDCA

• Use your efforts and results to raise funds

• Prepare for the next attacks
Counter-Attack Tips
If you know
the enemy and
you know
yourself, you
need not fear
the outcome
of a hundred
battles – Sun
Tzu

- Identify attackers / threats
- Search inside the internet, and in public or paid intelligence feeds
- List correlations
- Understand the structure of the attacker's environment (CDN, DNS, IP's)
- Analyze data traffic and URL code

- Identify code calls (API's) and the credentials used
- If credentials are not encrypted, use base64 decode or URL decode to obtain credentials in clear text
- Try to inject commands and code
- Always see the logs and their errors!
- Always remember to use VPN with IP masking to perform any tests or analyzes.
Screen with the profile of the attackers obtained through access to the main fraud server
Final Considerations
Responsible Disclosure is killing the 0-day industry
Together

WE

Achieve

More

• Value people and teamwork
• Have a multidisciplinary team
• Autonomy and trust are important
• Do what you love, it takes a lot less work
• Always share your knowledge
Thank You
For your attention