



DUBLIN

IRELAND

34th ANNUAL FIRST CONFERENCE
JUNE 26 - JULY 1

2022

#FIRSTCON22

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

Daniel Lima (NTT, Brazil)

Advertisement

- 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](https://www.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

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

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.

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?



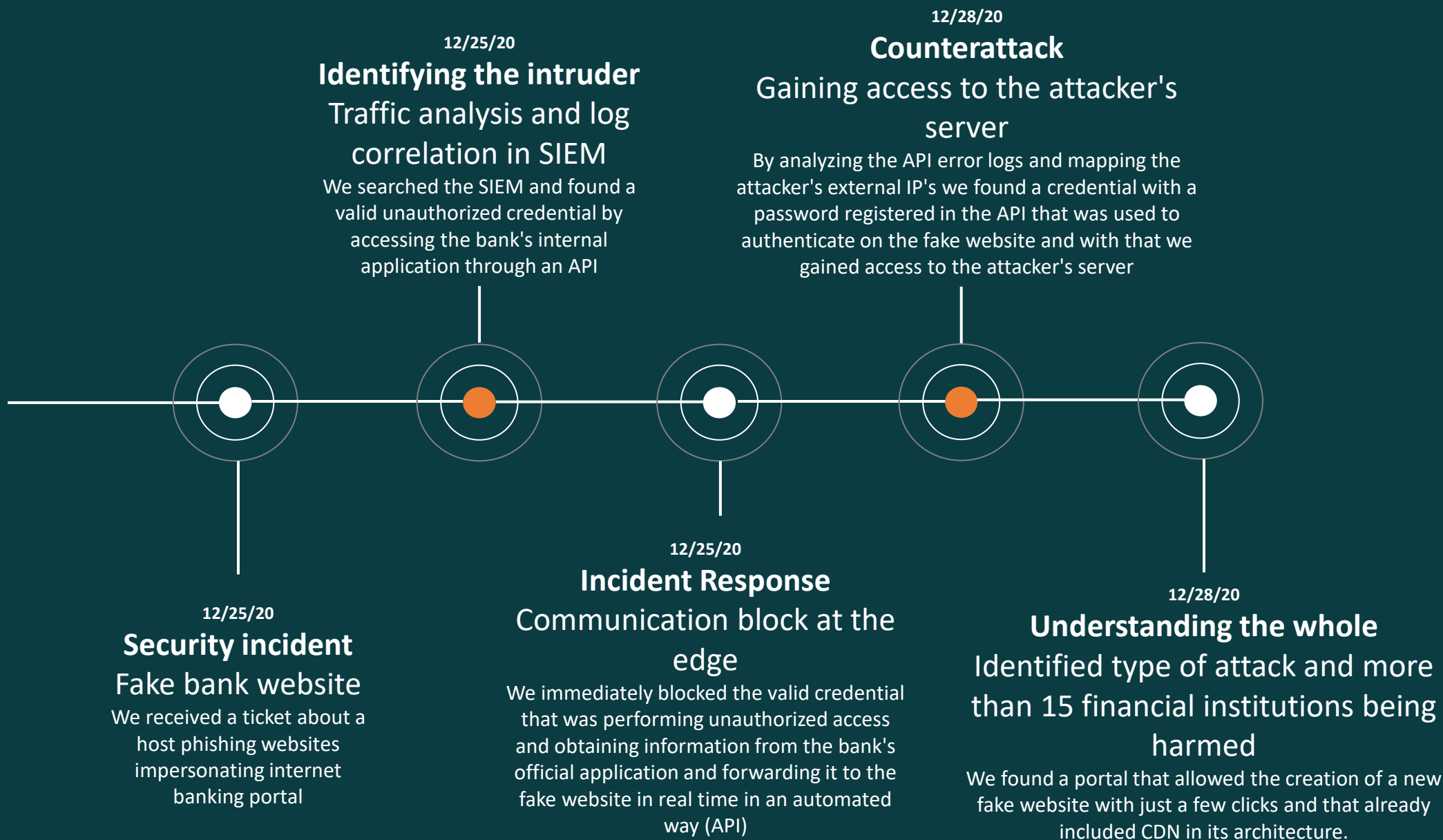
Daniel Lima

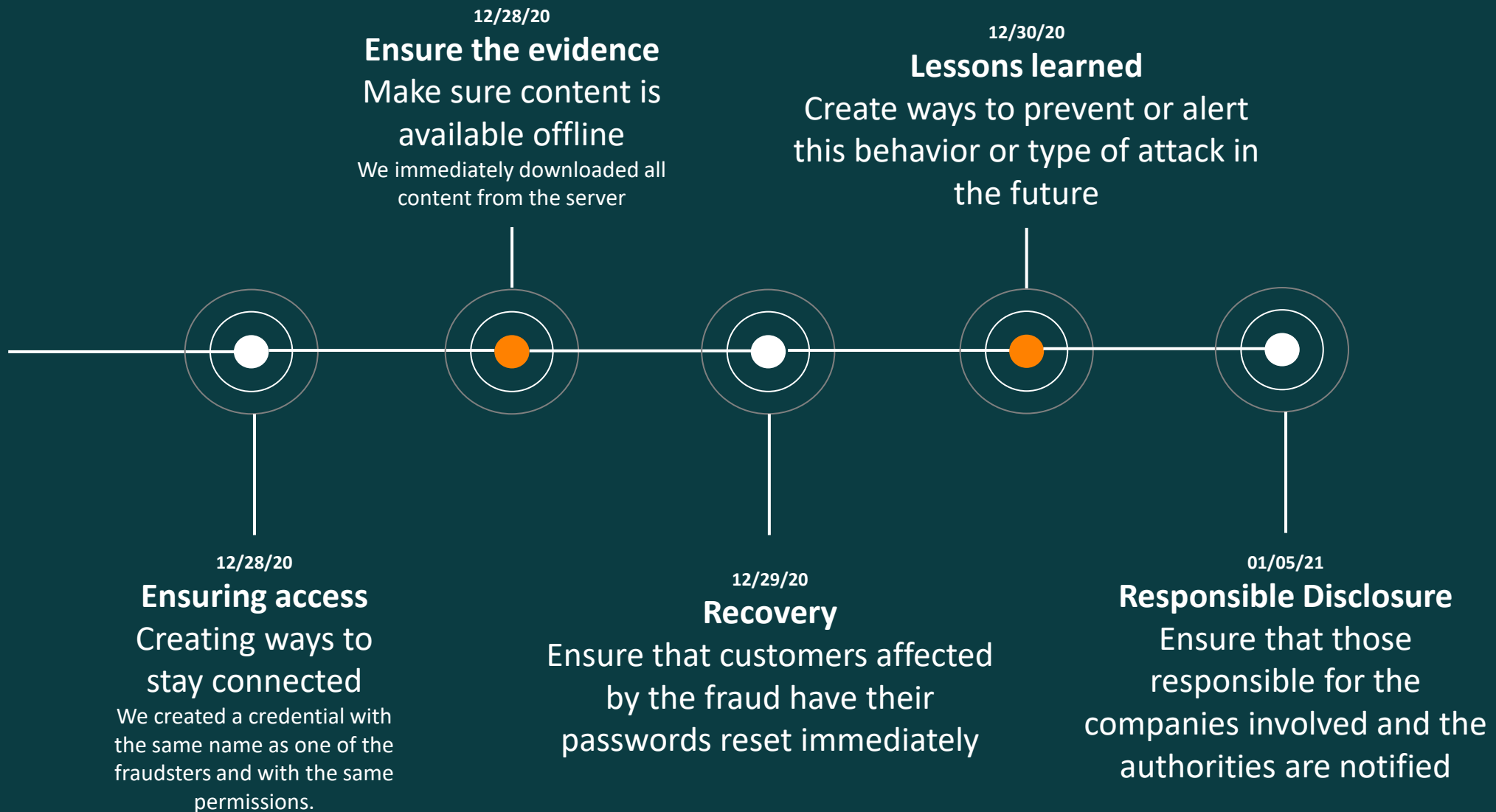
- [linkedin.com/in/danielolima](https://www.linkedin.com/in/danielolima)
- SOC Director  **NTT**
- + 9 years of cybersecurity experience

- Expert
 - Cryptography
 - Fraud and Risk Intelligence
 - Risk Management
 - CSIRT - Blue Team Operations
 - Advanced SOC Operations
 - CISA Certified ICS



Timeline of Incident





Understanding the Attack

Entry #1 E-mail Phishing + Fake Site



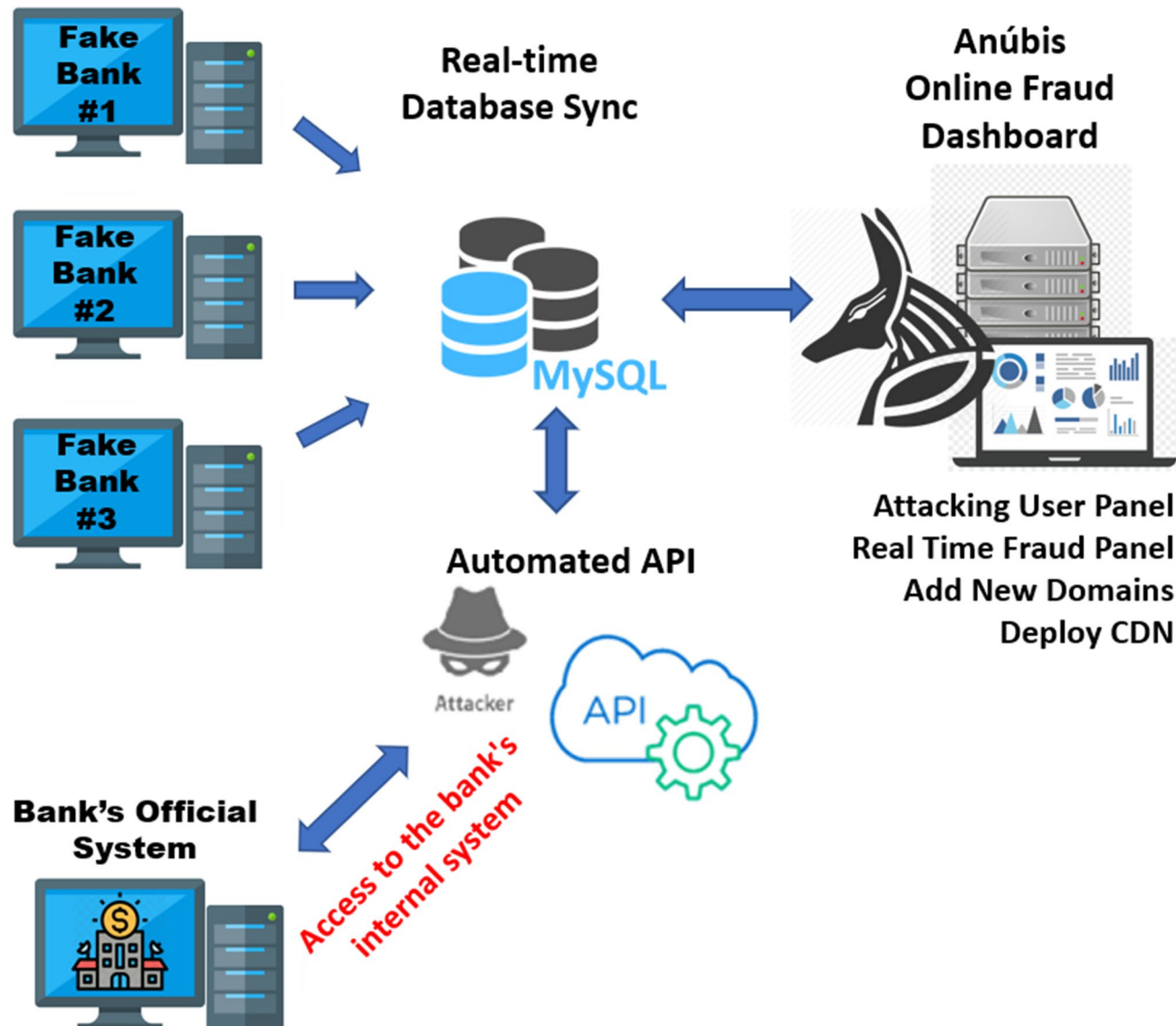
INTERNET

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



COMPARISON	Normal Phishing	Automated Phishing + Combined Attack
Steals user credentials	✓ OK	✓ OK
Performs fraud with stolen customer data	✓ OK	✓ OK
Steals Company credentials	X	✓ OK
Create fake banking system program	X	✓ OK
Online Fraud Information Dashboard	X	✓ OK
Online authentication API on the internal systems of some banks	X	✓ OK
Returns the real information of the client through the fake website, making the attack invisible.	X	✓ OK

Online Fraud Dashboard

Digitando senha da internet [Redacted] Livre Bauru-Sao Paulo	12 hrs 51 min 57 s
Senha errada, solicitando novamente. [Redacted] Livre Não localizado	5 hrs 46 min 23 s
R\$ 221,98 D Cliente expulso [Redacted] Fugitivo Não localizado	13 hrs 25 min 33 s
Digitando senha da internet [Redacted] Livre Não localizado	13 hrs 44 min 40 s
R\$ 0,00 C Aguardando comando silenciado [Redacted] Fugitivo Sao Paulo-Sao Paulo	16 hrs 38 min 5 s
Digitando senha da internet [Redacted] Livre Não localizado	18 hrs 15 min 30 s
R\$ 2.000,00 D Aguardando cliente digitar o SMS [Redacted] Fugitivo Sao Paulo-Sao Paulo	19 hrs 30 min 17 s
R\$ 0,89 Cliente expulso [Redacted] Fugitivo Não localizado	20 hrs 57 min 53 s
R\$ 4,74 C Digitando assinatura eletrônica silenciado [Redacted] Fugitivo Tome Acu-Para	20 hrs 16 min 24 s

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

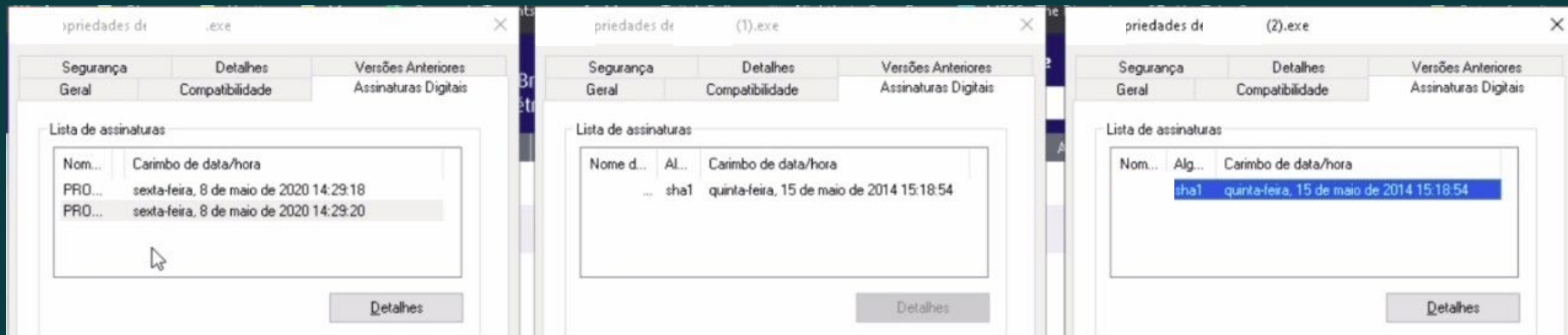
Malware Analysis

Sandbox Analysis

Behavioral Indicators

+ Specific Set Of Indicators Signalling High Likelihood of Maliciousness Detected	Severity: 95	Confidence: 100
+ Process Deleted an Executable in a System Directory	Severity: 90	Confidence: 100
+ Process Modified a File in a System Directory	Severity: 90	Confidence: 100
+ Process Opens a Listening Port	Severity: 80	Confidence: 90
+ Process Deleted an Executable in the Program Files Directory	Severity: 80	Confidence: 90
+ Alternate Data Stream File Creation Detected	Severity: 80	Confidence: 90
+ Process Modified a File in the Program Files Directory	Severity: 80	Confidence: 90
+ Process Modified Firefox Certificate Database	Severity: 95	Confidence: 75
+ Sample Launched Copy Of Itself	Severity: 75	Confidence: 95
+ Process Attempted to Access the FireFox Password Manager Local Database	Severity: 95	Confidence: 75
+ Process Modified an Executable File	Severity: 60	Confidence: 100
+ Process Modified File in a User Directory	Severity: 70	Confidence: 80

Recent Digital Signature



Malware Installation Log

Artifact 12: \TEMP\Instalação do Módulo Adicional de Segurança .log Created by: 5 (falso.exe)

Src: disk	Imports: 0	Type: ISO-8859 text, with CRLF line terminators	SHA256: cc542ca87c31f14313328cd8d2a4888752599916dbfd0be30724858c1015bd51
Size: 2050	Exports: 0	AV Sigs: 0	MD5: 380bc8528678331fc0c300f425689093
Path	\TEMP\Instalação do Módulo Adicional de Segurança .log		
Mime Type	text/plain; charset=binary		
Magic Type	ISO-8859 text, with CRLF line terminators		
SHA1	3442c4ba5d6874e1f7ea0866d78e2d088c4205c9		
Created At	+758.0s		
Modified By	5 (GBPCEF_falso.exe)		
Created By	5 (GBPCEF_falso.exe)		

Warsaw Registry modified

MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{20E60725-16C8-4FB9-8BC2-AF92C5F8D06D}_IS1	26 (gbpcefwr64.tmp)	DisplayIcon	C:\Program Files\ Warsaw\
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE	26 (gbpcefwr64.tmp)	Warsaw Setup	
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{20E60725-16C8-4FB9-8BC2-AF92C5F8D06D}_IS1	26 (gbpcefwr64.tmp)	Publisher	
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{20E60725-16C8-4FB9-8BC2-AF92C5F8D06D}_IS1	26 (gbpcefwr64.tmp)	DisplayName	Warsaw 2.15.1.1 64 bits
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{20E60725-16C8-4FB9-8BC2-AF92C5F8D06D}_IS1	26 (gbpcefwr64.tmp)	Inno Setup: Language	en
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{20E60725-16C8-4FB9-8BC2-AF92C5F8D06D}_IS1	26 (gbpcefwr64.tmp)	EstimatedSize	68389
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{20E60725-16C8-4FB9-8BC2-AF92C5F8D06D}_IS1	26 (gbpcefwr64.tmp)	Inno Setup: User	SYSTEM
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{20E60725-16C8-4FB9-8BC2-AF92C5F8D06D}_IS1	26 (gbpcefwr64.tmp)	MinorVersion	15
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{20E60725-16C8-4FB9-8BC2-AF92C5F8D06D}_IS1	26 (gbpcefwr64.tmp)	UninstallString	"C:\Program Files\ Warsaw\
MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{20E60725-16C8-4FB9-8BC2-AF92C5F8D06D}_IS1	26 (gbpcefwr64.tmp)	Inno Setup: Setup Version	5.5.9 (u)
USER\S-1-5-19\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS	26 (gbpcefwr64.tmp)	ProxyOverride	<local>

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.**

Dashboard **Usuários** Domínios Cloudflare

Dashboard #ANUBIS-171 Novo usuário

 Anubis Nível 1 Key: 5f8c7f1ad3158 Email: anubisdns@gmail.com Phone: (91) 8181-1111 Último acesso: 25/12/20 00:21:30 BLOQUEAR	 Rushador Nível 2 Key: 5f8b9ed40c562 Email: rushador@anubis.host Phone: (88) 1771-7171 Último acesso: 22/12/20 09:56:10 BLOQUEAR	 Malware Nível 1 Key: 5f8c9f3c047c Email: sysmalware@gmail.com Phone: Último acesso: 25/12/20 07:55:40 BLOQUEAR	 Mirror Nível 3 Key: 5f8f95c585f6a Email: mirror@anubis.host Phone: Não informado Último acesso: 20/12/20 20:43:51 BLOQUEAR
 Xinxá Nível 3 Key: 5fa41334866a4 Email: xinx@anubis171.com Phone: Não informado Último acesso: 20/12/20 13:57:06 BLOQUEAR	 Batman Nível 3 Key: 5f8b9902d4c37 Email: batman@anubis171.com Phone: Último acesso: 22/12/20 08:02:11 BLOQUEAR	 Skull Monster Nível 2 Key: 5fb7c37276099 Email: skull@anubis171.com.br Phone: Não informado Último acesso: 21/12/20 10:25:11 BLOQUEAR	 SKULL NU Nível 3 Key: 5f8eba094bfe Email: skullnubank@anubis171.com.br Phone: Não informado Último acesso: 04/12/20 15:42:58 BLOQUEAR

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

