SECURITY NEED-TO-KNOWS

FOR THE FINANCIAL SECTOR
INTRODUCTION

STATE OF THE FINANCIAL SECTOR
- Attacks against customers
- Attacks against institutions

REGULATIONS ON THE HORIZON
- GDPR on data protection
- PSD2 on open banking

CONFRONTING THE CHALLENGES
- Response capabilities
- Your part of the puzzle
Let’s get acquainted

Diederik.perk@fox-it.com
Threat intelligence advisor
Author/speaker/trainer
Weak spot for cartoons & memes
FROM PAYMENT SYSTEMS TO SURGERY ROOMS

KNOW THE RISK BEFORE IT IMPACTS YOU
PHYSICAL WORLD NOT SAFE FROM HARM
Security’s job is to inspire trust

Cannot be done in isolation
ISSUES IN AND AROUND THE OFFICE

What do you see?
TWO SIDES OF THE SAME COIN

Blue Team
Vulnerability-centric
‘Cyber Hygiene’

Red Team
Threat-centric
‘Active Defense’
State of the financial sector

Attacks as a daily routine
Portrait of a Master Thief

WANTED BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

EVGENIY MIKHAILOVICH BOGACHEV

Date(s) of Birth Used:
Height: Approximately 5'9"
Weight: Approximately 180 pounds
NCIC: W50089595
Occupation: Bogachev works in the Information Technology field

Hair: Brown (usually shaves his head)
Eyes: Brown
Sex: Male
Race: White

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.
A Fraud Operation

Businessclub

Leaders
- Alex/Bentley
- Slavik

Support
- xMan
- Dey
- Chingiz
- Kykypyky

Third party suppliers
- Paurch
- (Blackhole, Andreas, Czeslaw, ...)

23 backend instances (including debug)
- mem1, mem2, mem3, mem4, mem5, mem6, mem7, mem8, mem9, mem10, mem11, mem12, mem13, mem14, mem15, mem16, mem17, mem18, mem19, mem20, mem21, mem22, mem23, debug, default, dev, prod, test

Team leader (2/2)
- Alex
- Dear

Technical support (3/3)
- chingiz
- ded
- kykypyky

Crypter's (2/3)
- c4y_2
- crypt4you
- mrlapis

spam (4/4)
- dot
- j.p.morgan
- roach
- uho

at0m
- zeus_at0m@businessclub.so
Value may be perceived differently

Nice graphics processing unit (GPU) you have there...
Multi stage Fraud attack by Banking Trojan
Conditions and Countermeasures

- Volume
- Velocity
- Veracity

Value

All infected devices

- Browser based online banking
- Customer of targeted bank
- Sufficient funds
- Successful transaction

Hardening
Sinkhole C&C
Malware Analysis
Retroactive Hunting
Anomaly Detection
GOING AFTER BIG FISH

TRANSFER FUNDS OUT FROM WITHIN
Bank of Bangladesh
Carbanak

How the Carbanak cybergang stole $1bn
A targeted attack on a bank

1. Infection
   - Carbanak backdoor sent as an attachment
   - Bank employee
   - Emails with exploits
   - Credentials stolen
   - 100s of machines infected in search of the admin PC

2. Harvesting Intelligence
   - Intercepting the clerks’ screens
   - Cash transfer systems

3. Mimicking the staff
   - How the money was stolen
   - Online-banking: Money was transferred to fraudsters’ accounts
   - E-payment systems: Money was transferred to banks in China and the US
   - Inflating account balances: The extra funds were pocketed via a fraudulent transaction
   - Controlling ATMs: Orders to dispense cash at a pre-determined time
Developments in regulation

Blame the victim?
Legislation, Guidance, authorities and initiatives....

- NCBs
- NCAs
- ORPs
- European Commission
- ECB
- EBA
- FS-ISAC
- GDPR
- NIS Directive
- TIBER
- CBEST
- CPMI-IOSCO
- G7 fundamental elements
- Oversight framework
- Eurosystenm
- PSD2
- Guidance
- SIPS
- SSM
- CERT-EU
- ESCB
- Regulation
- PIRPS
- ESMA
- National CERTs
- Etc., etc.
How open is open banking in terms of security?

Exposure vs. exploitation
<table>
<thead>
<tr>
<th>Threat Actor</th>
<th>Method</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organised Crime Groups</td>
<td>MITM</td>
<td>Extortion</td>
</tr>
<tr>
<td></td>
<td>Supply-Chain Attack</td>
<td>Identity Theft</td>
</tr>
<tr>
<td></td>
<td>Trojan App</td>
<td>Fraud</td>
</tr>
<tr>
<td>Nation States</td>
<td>Credential Theft</td>
<td>Espionage</td>
</tr>
<tr>
<td>Insider Threats</td>
<td>Traffic Analysis</td>
<td>Disruption</td>
</tr>
<tr>
<td>Competitor Organisations</td>
<td>Data Manipulation</td>
<td></td>
</tr>
<tr>
<td>Hacktivists</td>
<td>DDOS/SQL Injection</td>
<td></td>
</tr>
</tbody>
</table>
Adoption Rate

SCENARIOS AND SIGNPOSTS

Extortion
GDPR fine

Commodity Fraud
Scalable vulnerability

Rogue TPP spyware
Business model without ROI
Countering the adversary

Where they reside
INTELLIGENCE DRIVEN SECURITY

Campaigns
= Bad guys' intentions

Tools, techniques & procedures
= Attack types

Incidents
= Events where things went wrong

Indicators
= Fingerprint for detection

Proactive
intel research

Threat actors
= Bad guys

Exploit targets
= Vulnerabilities / CVEs

Reactive
SOC analysis

Observables
= Anything you see in the cyber domain
A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents.
“Every soldier a sensor”
Q & A