



PROSOL

---

AZERBAIJAN  
TECHNOLOGY  
POWER HOUSE

Banking in the new era, risks and mitigation

Rationale for Unified Cyber Posture

# Agenda

- Intro – Prosol
- The Burden of Cyber crime
- Can Banks combat it alone?
  - Learning from other countries : Japan, US, Nordic, Israel
  - What can we do?
- A sample of new attack vectors – real AZ data
- Summary

# Prosol – Baku's New Innovation Partner

- It's a pleasure to kick start Prosol in Baku
- Prosol is local - Offices in Baku (new @ Landmark) and Tel Aviv
- Technology innovation with strong roots in Israeli high tech
- We represent a large number of savvy products & companies:
  - Products – Cyber, Smart Buildings, AI, Scada, Fintech, Banking, Utilities, Cloud, Disaster Recovery, Telecom, ERP, and more
  - Outsourcing & Services – Wide range of on site services such as Tech Support, GDPR/CCPA, Cloud, IT Infrastructure etc.
  - Consulting and Know how transfer
  - Built to spec projects

# Banking in the new era is challenging.....





- Multiple new risk vectors – different type of attacks on banks
  - Hacktivist: 80% of the attacks but 1% success
  - Cybercriminals: 15%- 20% of the attacks 20% success
  - State Sponsored: 2% of attacks 98% success rate
  - Banks are successful preventing hacktivist, reasonably well with criminals and useless with State Sponsored
- Enormous damages
  - 2017 Banks lost \$17B to cyber criminals
  - The Equifax (Credit Bureau) breach cost the company over \$4 billion in total. (Time Magazine)
  - DDOS cost about \$1.8M on average per attacked bank (Kaspersky)
  - Highest spending per firm (\$18M Forbs)
  - Projected for 2021 - \$6 Trillion per annum in damages – bigger than illegal drugs

# Motivation for working together

- **Shortage of resources** *(The demand for cybersecurity professionals will increase to approximately 6 million globally by 2019, Palo Alto Networks Research Center)*
- **Lack of Training** - *More than 91% of hacking attacks today began with a phishing or spear phishing email and roughly 23% of phishing emails are open by employees even after they have received training to spot potential fraudulent messages. (Data Breach Investigations Report)*
- **Spiraling Costs** - *Worldwide spending on information security products and services reached more than \$114 billion (USD) in 2018 and will grow by 9% in 2019 (Gartner)*
- **Repetitive investments** - *A study of 400 global bank executives found that 71% focus digital investments on cybersecurity. (Forbes)*
- **Collaboration works** - *Payments firms Visa and Mastercard; large banks Citigroup, Morgan Stanley and Wells Fargo; all have fusion centers to help them better collect, analyze and share data on threats (Forbes)*



# Collaborate! (Some potential models)

-  FISC (The Center for Financial Industry Information Systems) - *FISC conducts research on threat/defense related to financial information systems,. The contributors are of wide range including financial institutions, insurance companies, securities firms, computer manufacturers and telecommunications companies.*
-  FS-ISAC - Financial Services Information Sharing and Analysis Center. *Members of the FS-ISAC worldwide receive timely notification and information specifically designed to help protect critical systems and assets from cyber and physical security threats. They share information anonymously. This information includes analysis and recommended solutions from leading industry experts. They also conduct training drills.*
-  The Israel National Cyber Directorate *is responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to operational defense in cyberspace. They provide incident handling services and guidance for all civilian entities as well as all critical infrastructures in the Israeli economy.*
-  Nordic Financial CERT - *an organization governed and paid for by its members in the Nordic financial industry. The purpose is to strengthen the resilience to cyber attacks, by enabling Nordic financial institutions to respond rapidly and efficiently to cyber security threats and online crime. As a collaborative initiative, it allows members to work together when handling cyber crime, sharing information and responding to threats in a coordinated manner.*

# Creating a unified defense posture -potential models.

There are different degrees of collaboration possible:

- Only Information Sharing
- Building a unified methodology and procedures
- Centralizing some of the resources (IR team, training, WAF, etc.)
- Distributing assets among partners.
- Outsourcing to a unified Siem/SOC.

**Organizations can start in a simple model and evolve with time in collaboration with world class expertise**



# Regulators Role as an Enabler

Financial institutions need the regulators support when it comes to Cyber crime:


- Creating a joint framework for all of the financial community
- Removing regulatory hurdles
- Working with relevant government agencies and industry experts

Just to make a point on evolving new attack  
vectors – a live example

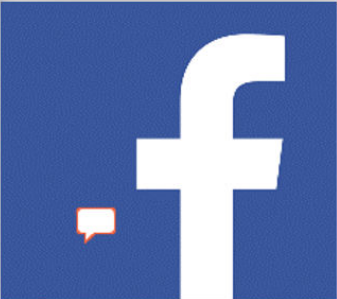
(Telco Ransomware Op Jerusalem)

# Time for 1 example- what is 3<sup>rd</sup> party risk

3







## IT HURTS!

Third-Party Breach Examples

### 01

#### British Airways

September 2018

Scope	380K Credit card details	Cause	MageCart gang	Result	£1 Billion cost
-------	--------------------------	-------	---------------	--------	-----------------

### 02.

#### Ticketmaster

April 2018

Scope	40k Client records	Cause	Hacked vendor	Result	~\$1M lost
-------	--------------------	-------	---------------	--------	------------

### 03.

#### Facebook

September 2018

Scope	50 Million login details & private data	Cause	Bug, hacked	Result	\$ Billions
-------	---	-------	-------------	--------	-------------


# Investigate - fully automated

**reflectiz**


My Websites


BANKOFAMERICA


Group By Channel: All Channels


 15


Signed in as Shai Schiller 0.12.9


 Dashboard


 Inventory


 Domains


 Privacy


 Performance












 Waterfall

 Alerts

 Control

 My Websites

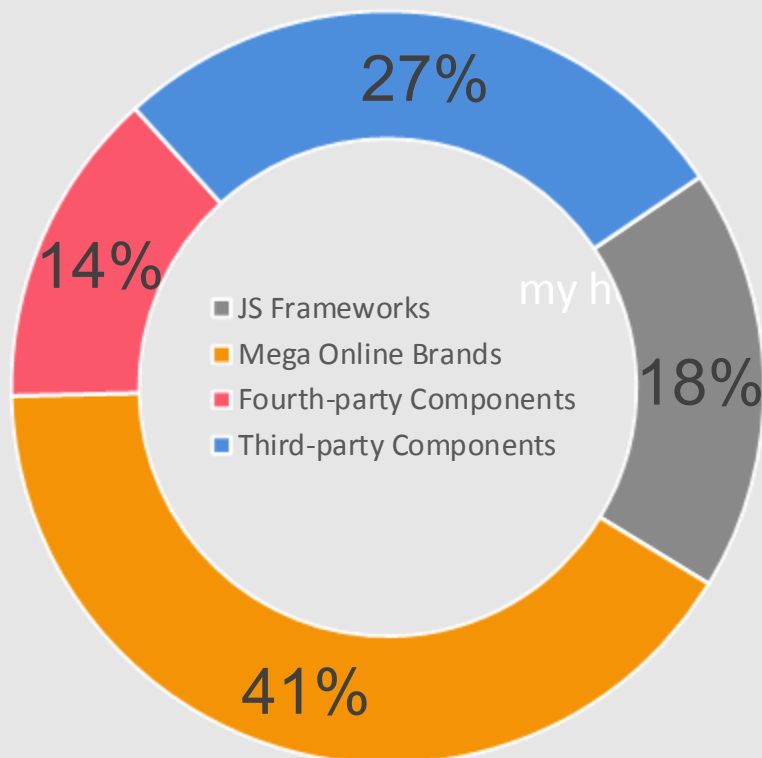
 Sign out

236		bankofamerica.com	Daily Scan	12/05/2019 11 PM	Ready	<a href="#">REFLECT</a>
6202		ibar.az	Daily Scan	12/05/2019 08 PM	Not Ready	
6203		pashabank.az	Daily Scan	13/05/2019 02 AM	Ready	<a href="#">REFLECT</a>
6206		kapitalbank.az	Daily Scan	13/05/2019 01 AM	Ready	<a href="#">REFLECT</a>
6208		xalqbank.az	Daily Scan	13/05/2019 08 AM	Not Ready	
6209		asb.az	Daily Scan	13/05/2019 01 AM	Ready	<a href="#">REFLECT</a>
6210		bankrespublika.az	Daily Scan	12/05/2019 11 PM	Ready	<a href="#">REFLECT</a>
6211		accessbank.az	Daily Scan	13/05/2019 12 AM	Ready	<a href="#">REFLECT</a>
6212		unibank.az	Daily Scan	13/05/2019 12 AM	Ready	<a href="#">REFLECT</a>
6213		rabitabank.com	Daily Scan	13/05/2019 01 AM	Ready	<a href="#">REFLECT</a>
6214		premiumbank.az	Daily Scan	13/05/2019 01 AM	Ready	<a href="#">REFLECT</a>

# Summary – Around 22 per Site

3 Fourth-  
party  
components

9  
components  
from mega  
online  
brands



6 Third-party  
vendors  
components

4 JS  
Frameworks  
and open-  
source apps

## 10 Main Banks

- [www.pashabank.az](http://www.pashabank.az)
- [www.kapitalbank.az](http://www.kapitalbank.az)
- [www.ibar.az](http://www.ibar.az)
- [www.xalqbank.az](http://www.xalqbank.az)
- [www.asb.az](http://www.asb.az)
- [www.bankrespublika.az](http://www.bankrespublika.az)
- [www.accessbank.az](http://www.accessbank.az)
- [www.unibank.az](http://www.unibank.az)
- [www.rabitabank.com](http://www.rabitabank.com)
- [www.premiumbank.az](http://www.premiumbank.az)

# Summary – Real live

## 45459 - The app `Google reCaptcha` is Keylogging User Password

First Seen: 5/2/2019 Last Seen: 5/6/2019

### Description:

Google reCaptcha has started to Keylogging User Password. 3rd-parties can request access to various activities, some might have play-scripts might cause severe sensitive data leaks, usually as part of keylogging. Known issues include identity thefts, financial Script:

[www.gstatic.com/recaptcha/api2/v1555968629716/recaptcha\\_\\_az.js](http://www.gstatic.com/recaptcha/api2/v1555968629716/recaptcha__az.js)

Affected Page:

Item Examples:

login, password

### Recommendation:

Verify this 3rd-party is authorized to issue the noted suspicious activity and confirm with the vendor why this activity is required.

## 45464 - The app `jQuery` needs further examination

First Seen: 5/2/2019 Last Seen: 5/6/2019

### Description:

The app `jQuery` needs further examination. A vulnerability was found in jQuery up to 3.3.x. this vulnerability.

Example page that are using the app:

<https://.az/?hl=ru>

<https://.az/?hl=en>

<https://.az/loans/manat?hl=az>

<https://.az/loans?hl=az>

[.az/?hl=ru](https://.az/?hl=ru)

[.az/?hl=en](https://.az/?hl=en)

[.az/loans/manat?hl=az](https://.az/loans/manat?hl=az)

[.az/loans?hl=az](https://.az/loans?hl=az)

## 45554 - The app `E-pul.az` is Monitoring User Inputs

First Seen: 5/2/2019 Last Seen: 5/6/2019

### Description:

E-pul.az has started to Monitoring User Inputs. 3rd-parties can request might cause severe sensitive data leaks, usually as part of keylogging. K Script:

Affected Page:

[www.az/en/private/utility-payments](http://www.az/en/private/utility-payments)

Item Examples:

amount

## 45833 - `turn.com` domain certificate has expired

First Seen: 5/7/2019 Last Seen: 5/11/2019

### Description:

turn.com domain certificate has expired. The web-communications do not comply with SSL/TLS demands. The `AddThis` send requests to the unsecured domain.

### Recommendation:

Confirm that using this domain matches your site's activity and policies. If approved, verify the domain owner

# Summary – Everyone has been breached...

- Cyber-attacks on critical financial infrastructure are a major threat, creating significant damage and disruption to the business
- Financial institutions are inherently lucrative targets. The complexity of the industry, connectivity between institutions and introduction of new systems and technologies create a broad attack surface.
- Breaches and breakdowns are inevitable ,assume you have been breached, focus on resilience.
- ***Collaboration is key, no organization can do everything by themselves***
- Regulators should take an active part.





PROSOL

Thank you!

E-mail: [info@prosol.az](mailto:info@prosol.az)

Tel: (012) 404 12 21