MAIN PAGE

SfyLabs

Products | Blog | Partners | Contact

Manage cyber risk and protect your online assets

[picture1: relation threats + services]

Providing executives and managers with a strategic advantage, while allowing operational teams to remediate in real-time.

Since 2013 we have been actively helping the financial industry to be cyber-threat-aware and minimize risk exposure. With use of our custom analysis and detection capabilities, response to complex cyber threats has become simple and efficient.

PRODUCT PAGE

[picture2: TF + CSD]

ThreatFabric

ThreatFabric Cyber Threat Intelligence service gives you real-time visibility on the mobile threat landscape.

[picture3: Android Malware families]

ThreatFabric is the perfect combination of dark-web investigations and malware analysis to empower and support you to:

- Have a complete overview of the threat landscape
- Be aware of your current risk exposure
- Know how to handle attacks and fraud
- Protect your brand and reputation
- Constantly improve your security strategy
- Educate your users and customers

[link] want to know more

ClientSideDetection

ClientSideDetection service provides the tools to assess risk, detect and stop fraud in real-time.

[picture4: CSD Ecosystem]

ClientSideDetection is the balanced combination between behavior analysis and malware detection to allow you to:

- Ensure your fraud team and their tools are ahead
- Detect and identify new threats
- Strengthen your security, remaining agentless
- Visualize real-time risk via a central dashboard
- Detect fraud before it can be performed
- Reduce costs due to successful fraud

[link] want to know more

THREATFABRIC PAGE

ThreatFabric

Know the threats, asses the risk and react

Although cyber-criminal motivations are numerous, the prominent one remains money. Threat actors motivated by financial gain have noticed the shift of bank customers from desktop to mobile based online banking.
The dominant market share and the flexibility offered by the Android operating system, combined with the shift towards mobile banking has resulted in the surge in Android malware visible since early 2014.

Since their early stage, mobile based threats haven't ceased evolving and regularly offering new features or improvements, allowing criminals to remain undetected and reach their goals. Due to their nature, mobile malware capabilities are nowadays surpassing their desktop-based ancestors.

[picture6: growth of mobile threats]

Part of the service:

- Real-time alerting
- Total visibility on threat landscape
- Direct expert access
- C-level reporting
- API + feeds for real-time operations

Key points of the service:

Easy to use	Structured dissemination through simple interfaces
Relevant	Information that does apply to your context
Proactive	Close to real-time, enabling efficient risk deflection
Reliable	Decision making without false-positives or noise
Actionable	The information is structured to be used straight away

CSD PAGE

ClientSideDetection

Being aware of threats is important, detecting them is even better

One of the challenges of financial institutions is to be able to keep an eye on the numerous attack vectors used by criminals. Financially motivated threat actors broadening their scope towards mobile attacks results in additional vectors to worry about.
The end-users remain the weak link in the security chain, therefore visibility on the endpoints used to interact with online services is of utmost importance.

Criminals are abusing the convenience of online services. Most of the time it’s with the use of both malware and social-engineering that threat actors manage to gather information necessary to perform fraud.

CSD Web

- Integrates in website
- Invisible to end-user
- Highly obfuscated
- End to end encryption
- Tempering detection
- Behavior analysis
- Device finger-printing

CSD Portal

- Manageable via central interface
- Risk based score visualization
- Real-time stakeholder alerting
- Connects to your fraud engine

CSD Mobile

- Integrates in mobile app
- Invisible to end-user
- Fail safe environment
- Highly obfuscated
- End to end encryption
- Behavior analysis
- Root detection
- Device finger-printing

[picture5: relation threats + services]

▪ Automatically detects new inject attacks ▪ Browser fingerprinting to detect RAT sessions ▪ Detects page tampering attempts		▪ Automatically detects new overlay attacks ▪ Detects abnormal behavior and tempering attempts ▪ Automated app upload for additional analysis
[link] want to know more		

CONTACT PAGE

SfyLabs

Products | Blog | Partners | Contact

Address
SfyLabs B.V.
Naritaweg 106C
1043CA Amsterdam

Contact information
Tel: +31 X XXXX XXXX
Mail: info@sfylabs.com

Request a demo or whitepaper [form]
Name:
Email:
Company:
Message:
[Send]

DON’T USE THE INFORMATION BELOW

https://www.group-ib.com/secure_bank.html

ThreatFabric:
https://www.group-ib.com/intelligence.html
https://www.crowdstrike.com/solutions/threat-intelligence-solutions/