

# ThreatMark

# Threat Mark Threat Detection Solution

Cyber-threat detection solution based on deep behavioral profiling supported by the latest advancements in machine learning.

The growth in the number of online and mobile users and transactions brings more cyber threats. Hackers continually look for new attack vectors and come up with new techniques and malware. The rise of mobile banking means more attacks on mobile devices and more cross-channel attacks that are difficult to detect by traditional means.

#### About ThreatMark

• An experienced team of fraud-prevention specialists, cyber security professionals, and AI/ML experts

# Instead of a reactive approach, we strive to identify attacks as they happen for the first time.

By monitoring device and session information in the context of each individual user, we identify cyber threats with outstanding precision!

• A global company with main offices in the UK and the Czech Republic

### ThreatMark Provides Protection Against:



Banking malware



Phishing



Social engineering



BOT access/scraping



#### Higher detection rate<sup>1</sup>

ThreatMark TDS is sensitive to modern techniques of online fraud, including social engineering, phishing, and zero-day attacks.

compared to traditional FDS alone <sup>2</sup> estimated SMS cost savings



Account takeovers



Mobile banking threats



#### Fewer false positives<sup>1</sup>

Deep behavioral profiling and a holistic approach make ThreatMark TDS adaptive and precise in analyzing potential fraud.



Endpoint attacks



Cross-channel attacks



#### Deeper knowledge of users<sup>2</sup>

ThreatMark TDS can verify digital identities with high accuracy, allowing banks to save money on two-factor authentication in 90% of cases.

Contact us at sales@threatmark.com — in linkedin.com/company/ThreatMark — 🖖

@ThreatMark

## Multi-Layered Approach to Threat and Fraud Detection

Big Data Analytics										
Device aware Layer 1	Session aware Layer 2	User aware Layer 3	Transaction aware Layer 4							
Access	Logon	Navigation	Transactions							
<ul> <li>Connection check (TOR, anon proxy)</li> <li>Browser and OS security check</li> <li>Malware, phishing</li> <li>Device fingerprint</li> </ul>	<ul> <li>GeoIP check</li> <li>Login time check</li> <li>Logon biometrics</li> <li>Velocity checks</li> <li>Action context</li> </ul>	<ul> <li>Clickstream profiling</li> <li>Scripted access and automation detection</li> <li>Session hijacking</li> <li>Behavior and app interaction biometrics</li> </ul>	<ul><li>Money mule blacklist</li><li>Anomalous transactions</li><li>Behavioral profiling</li></ul>							
\$→□			<b>□</b> → (\$							

#### Deep behavioral profiling

We monitor users throughout their online journeys and evaluate them according to hundreds of parameters, including their behavioral patterns, session parameters, transaction details, biometrics, and their interaction with web and mobile applications. Deep knowledge of users allows us to increase the detection rate and decrease the number of false positives.

#### Machine learning

The latest advancements in machine learning and artificial intelligence are used to analyze user behavior and hundreds of technical and financial parameters. As a result, we are able to detect suspicious activities on a user's profile and prevent fraud, even in the preparation phase, which was previously impossible.

#### Our Threat Detection Solution

can be implemented either as a part of the complete Fraud Detection Solution along with Mobile Fraud Detection—ThreatMark FDS 2.0—or to complement a third-party Fraud Detection Solution. Integration with internal applications or an authentication system allows banks to provide fast and automated processing.



ThreatMark FDS 2.0 Full-Stack Threat Detection and Fraud Prevention



Complements Transaction Monitoring by Third-Parties

#### Deployment

- Easy and fast: in weeks instead of months
- Flexible: fully managed on premise or in the cloud, no software licenses, no new components to manage
- Rich analytical web interface: for security teams and fraud analysts
- Support from our fraud analyst: to get the most of our system

IVINI		Ait	farms .							
Detections overview			11107		· INTERNAL CALIF	NEW CASE				
💤 Malware	14		A Time T	A 1014 W	Detection type	Alerts of detection	Section	Persistent session	User	IP
ed Phinhing	14	۹	01124/2018 11 48 00 AM	162	Theorem Industry		۹.	۹.	7283725618	<b>b</b> 194.212.57.229
C+ Account Takeover		٩	11124-2018 11:30 35 AM	719	Rearcial endware		9	Q.	4458035413	<b>b</b> 31.30.140.43
Suspicious transactions	14	۹	01124/2018 11:00:54 AM	130	<b>Georgial malware</b>		٩	Q	4458035413	<b>b</b> 194.212.197.116
A Webbacking	14	۹	0112402018-00-00-02-AM	176	Transiel melware	S10	۵.	α,	0581334357	<b>194.212.75.77</b>
Insecure Configuration	14	٩	01745018.08.08.52.84	183	Saspicious transaction	THE THEA IST	۹,	۹.	7283725618	<b>b</b> 194.212.68.119
U Simila		٩	DATE VOLUME OF DRIVE WAS	179	Account Takeover	IPC LOC OM MUE	Q.	٩	7283725618	<b>b</b> 194.212.68.119
• officer.		9	0102402010-00-40:01-AM	1.22.	Phisbing withins	PLG HOV	۹.	Q.	6142054034	<b>b</b> 194.212.4.138
IDVITTY:		٩	01124/2018 04:38 17 464	500	Phishing victim	PON	۹.	۵,	521250	<b>=</b> 100.183.116.133
& Climite		۹	01242018.0638-17 MM	500	Phisbing sectors	POV	NW.	9	047740	<b>15.246.167.30</b>
1 Arrounds		۹,	0112412010 00:38 17 AM	500	Phistolog wictim	101	۹.	а,	441378	≖ 105.80.120.51
# Transactions		٩	01/24/2018 00:38:17 AM	808	Phisbing shemain	10	NA.	RUN.	N/A	<b>28.63.137.155</b>
Devices		a,	010342010-0638-57.864	909	Phisting domain	10	344	104	N/A	<b>=</b> 188,103,139,99
A Perdistent sessions		٩	12112412010 (XL38-17 AM	500	Phásháng victim	#0V	۹,	9	266223	197.8.65.11
		4	D1124/2018-06-25-38-AM	611	Automatical Information	that has them be the	۹.	9	4707034414	<b>b</b> 31.30.77.76
al services		9	01242010 12-15-55 AM	154	Phisking victors	PUE POV	۹.	9	4458035413	<b>b</b> 31.30.150.87
COM100		9	01222010-06122-10-PM	122	Tinuncial matware	w.	۹.	9	6142054034	<b>b</b> 31.30.152.41

Ш

www.threatmark.com

**.**