

Protección contra Amenazas Avanzadas y Sandboxing



It's in the news...

93% of phishing emails are now ransomware

May 20, 2016

Spoofting scam goes for the steal, scores Milwaukee Bucks' W-2 forms

FBI: \$2.3 Billion Lost to CEO Email Scams

FBI Report: Ransomware and Phishing Scams Increasing

Of course, the number one cause of data loss, according to the FBI report, continues to be social engineering and email compromises. The reported losses associated with business email compromises in 2015 was \$246,226,016.

Ottawa Hospital hit with ransomware, information on four computers locked down

Mark Zuckerberg's Twitter and Pinterest Accounts Hacked

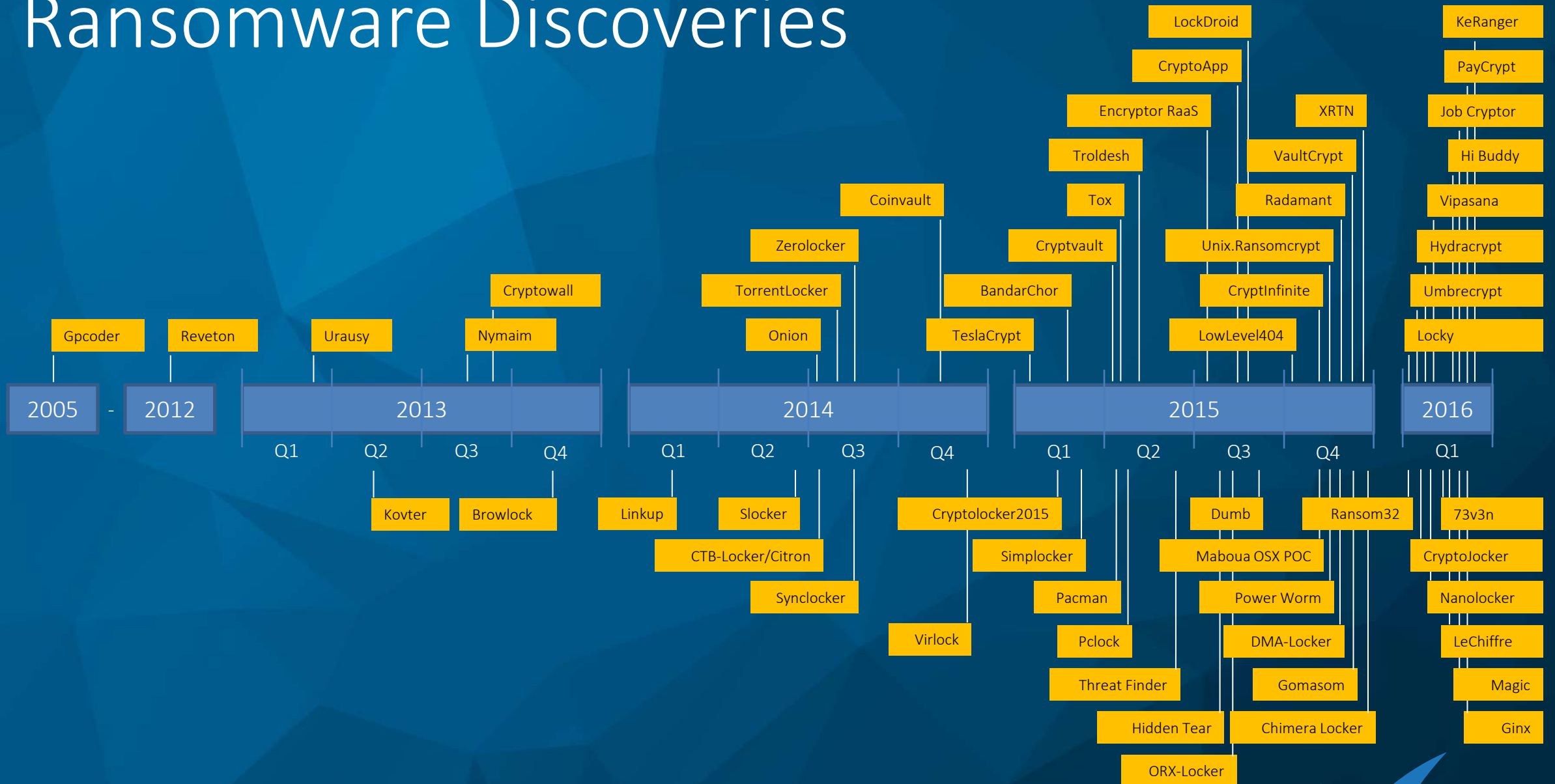
Facebook CEO had reused 'dadada' as password in accounts

Bogus CNN Breaking News Spam Emails Spread Massive Malware Attacks

LinkedIn Breach Results In Phishing Scams



Ransomware Discoveries



Barracuda ATP Review

Volume of Data

- Volume of data critical for machine learning
- Barracuda processes ~1 Billion emails per day
- Machine learning farms process and learn



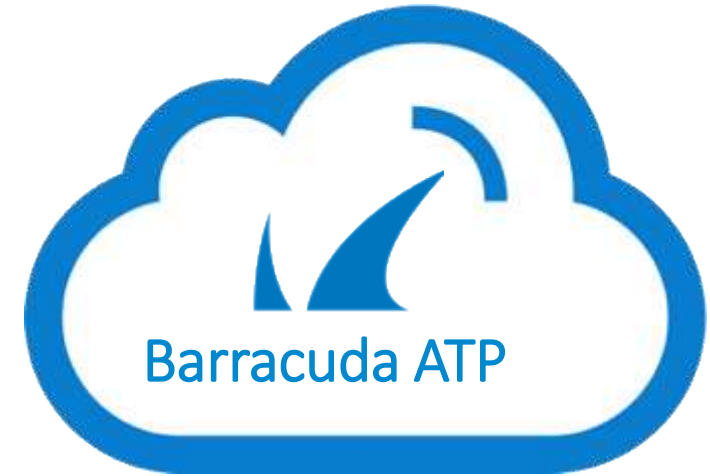
Barracuda ATP Review

Volume of Data

- Volume of data critical for machine learning
- Barracuda processes ~1 Billion emails per day
- Machine learning farms process and learn

Diversity of Data

- Process threat info across all vectors
- Real-time threat info from network, email, web, etc.
- Global customers of all shapes and sizes



Barracuda ATP Review

Volume of Data

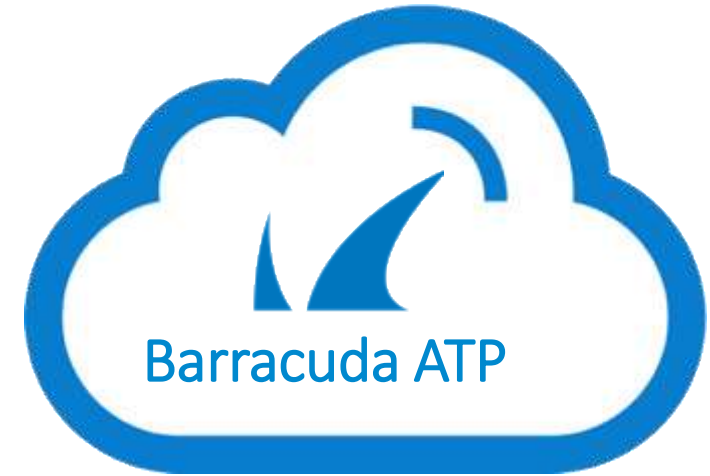
- Volume of data critical for machine learning
- Barracuda processes ~1 Billion emails per day
- Machine learning farms process and learn

Diversity of Data

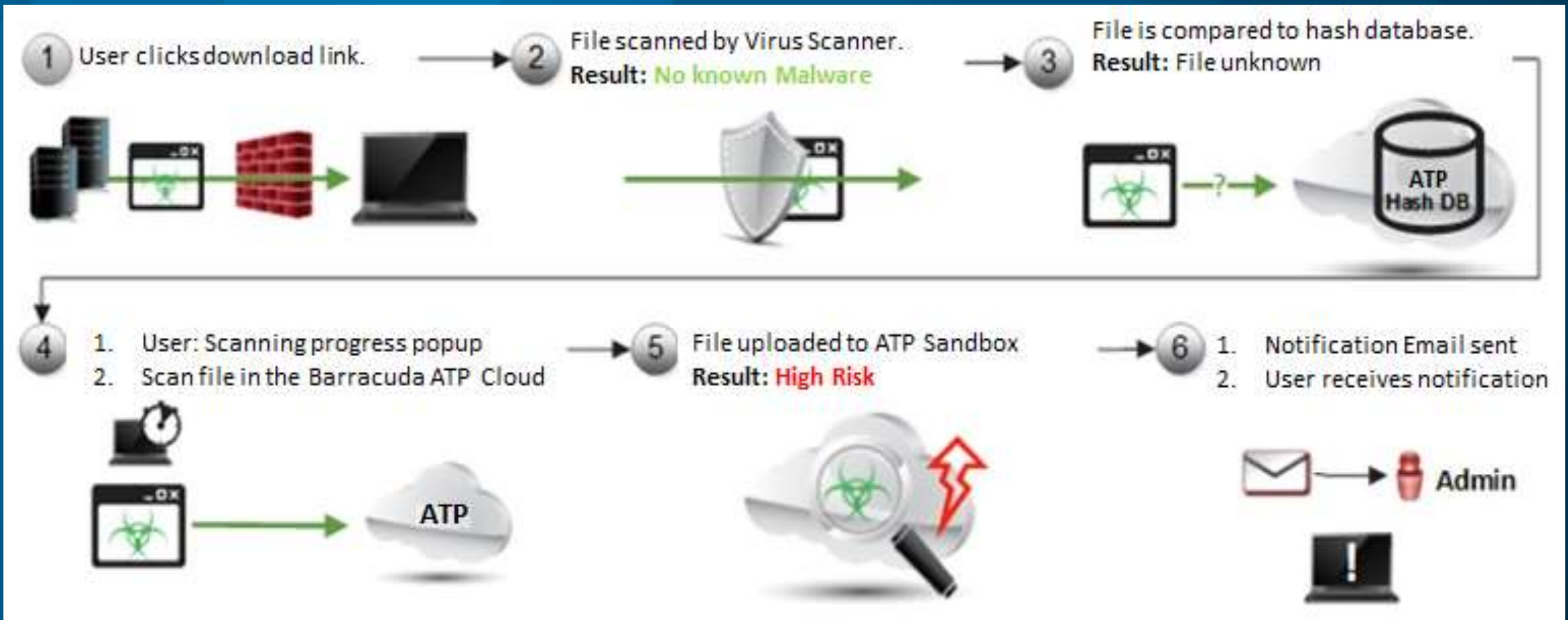
- Process threat info across all vectors
- Real-time threat info from network, email, web, etc.
- Global customers of all shapes and sizes

Micro-Service is Key

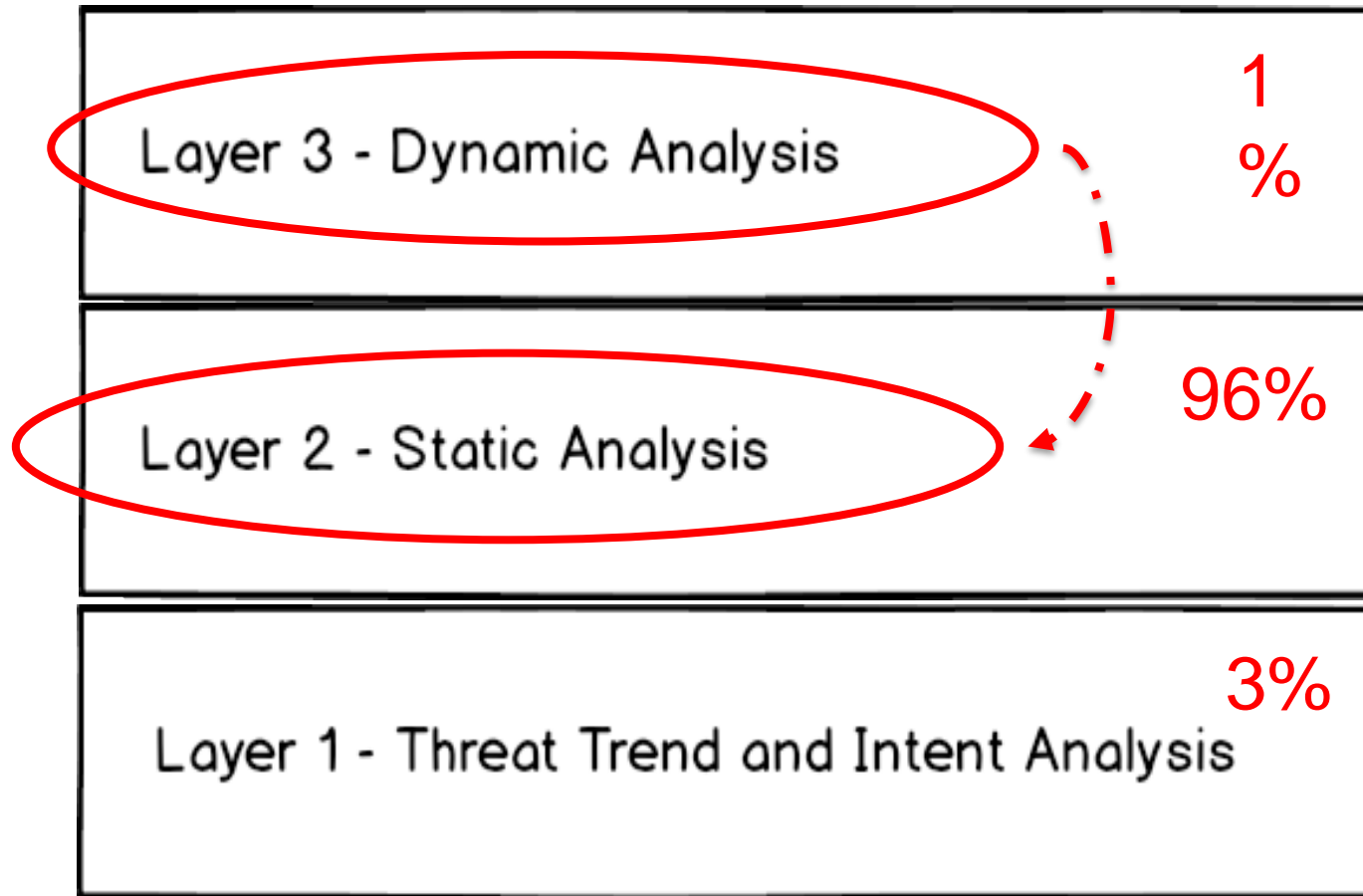
- 3 scan layers (AV/Static/Dynamic)
- Reduces scan/decision time
- Shares database across products



HTTP and HTTPS



Barracuda Advanced Threat Protection



- Analysis and detonation of advanced threats
- Scans 900+ attributes in less than 1 second

- Machine learning farm
- Behavioral and heuristic analysis

- Multi-opined A/V engines
- Blocks spam, viruses, phishing, and other malware



What Exactly Does the Sandbox Find?



form_8460560.doc

Threat

application/msword

198,144 bytes

✓ Detected by observing the file's behavior in a **sandbox**

EXHIBITS 27 MALICIOUS ACTIVITIES

Network: Command&Control traffic observed

Network: Hide network activity through code injection

Packer: Loading an embedded PE image (potential unpacking)

Search: Enumerates running processes

Steal: Reading user's mail server credentials

Stealth: Creating executables masquerading system files



Detect: The Barracuda Email Threat Scanner

Cloud service that scans O365 mailboxes

Find advanced sleeping threats

Identifies owners of said threats


Provides detailed reports and recommendations

Free



**Barracuda
Essentials**
for Office 365

TOP THREATS



Lashandra Mulero has a threat in their inbox

Folder:	Inbox
Date:	Apr 25, 2016
From:	Maryann Mccann
Subject:	Csp Inc. Bill e-invoice (006269502)
Read:	Yes
Threat:	Csp Inc..doc

[?](#) [...](#)



3 Step Process

1) Scan

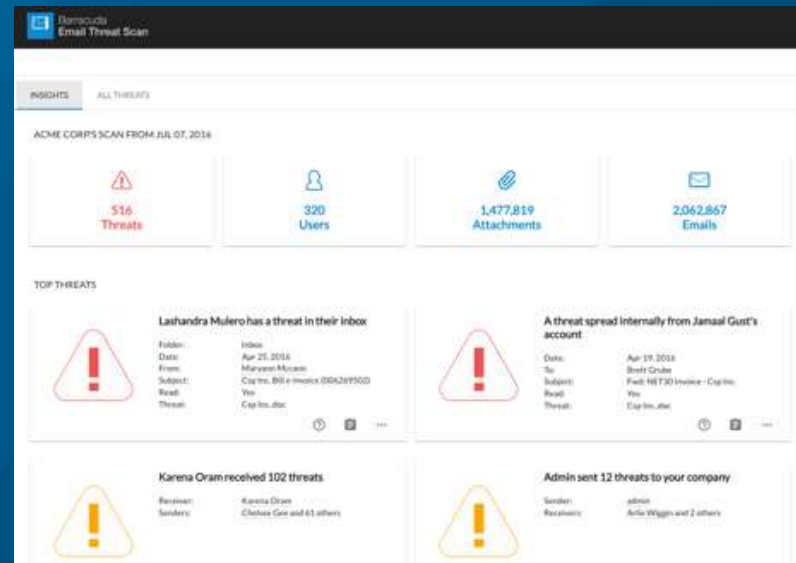
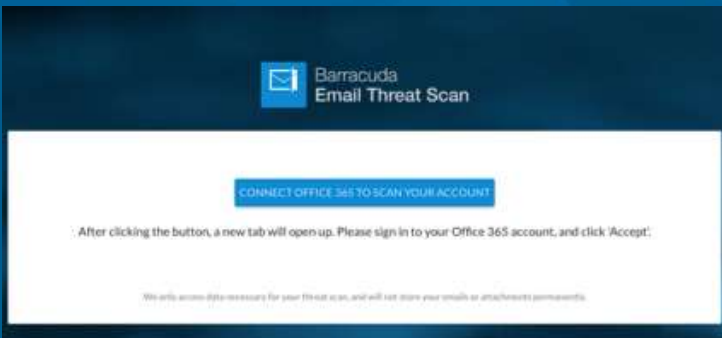
Send customer link to scan.barracuda.com/signup

2) Educate

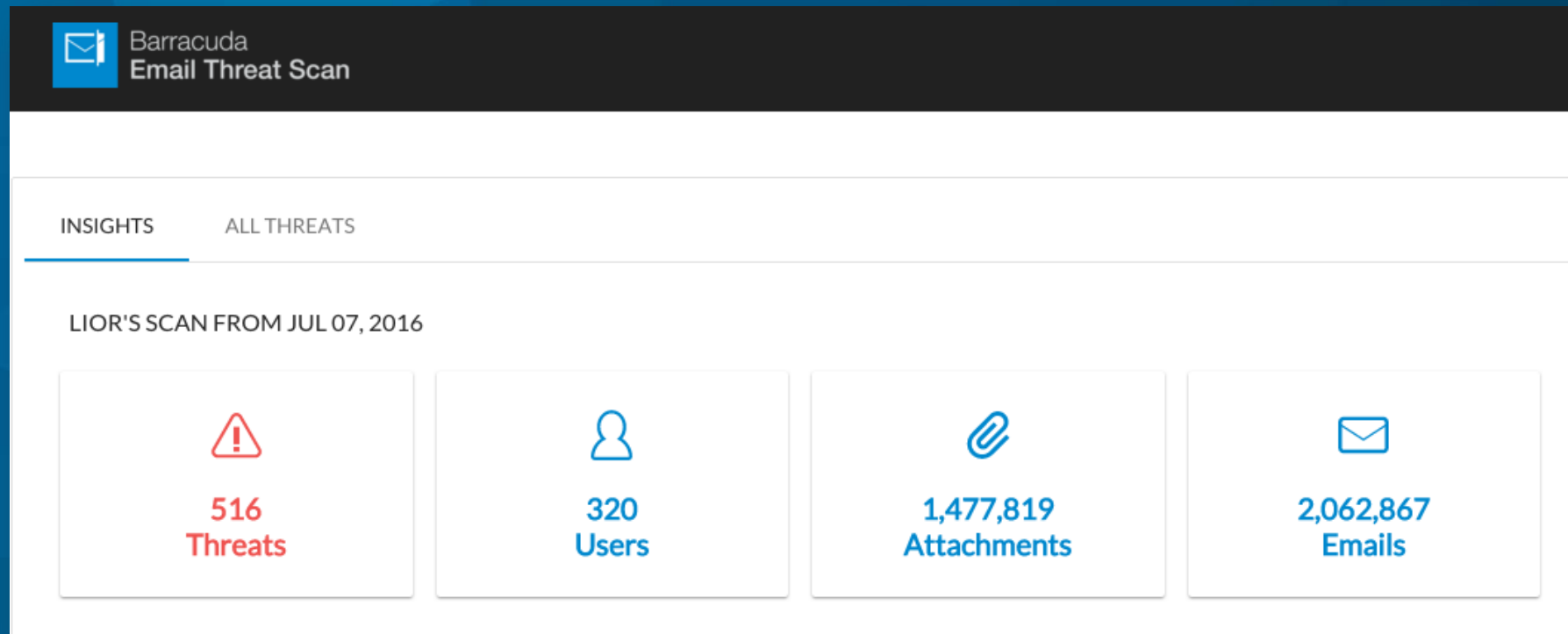
Educate customer on their top risks

3) Remediate

Provide remediation checklist & sign up for Essentials



Educate: Present Overall Risk Level



Thank You

