

# Barracuda Networks

Sep 05, 2019

## Table of Contents

Your scan summary .....	Page 1
A look at your employees .....	Page 2
Threats to your security .....	Page 3
DMARC protection status of your domains .....	Page 4
Sources of attacks .....	Page 5

# Your scan summary

Scan completed on  
**Sep 05, 2019 at 11:19 AM**

Duration  
**2 minutes**

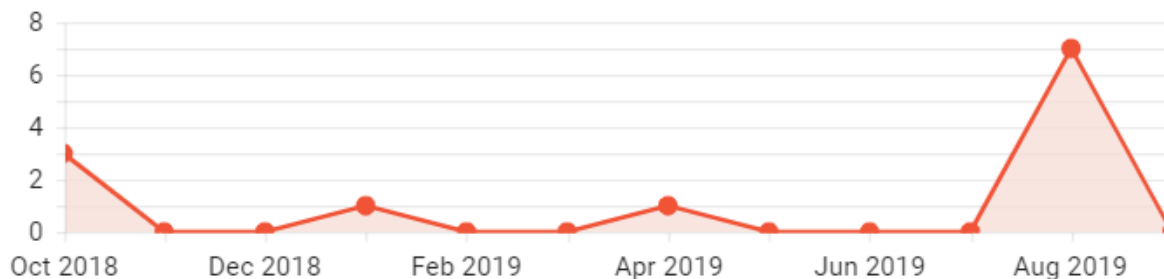
Emails scanned  
**2,085**

Threats detected  
**18**

## Total Threats Found

18

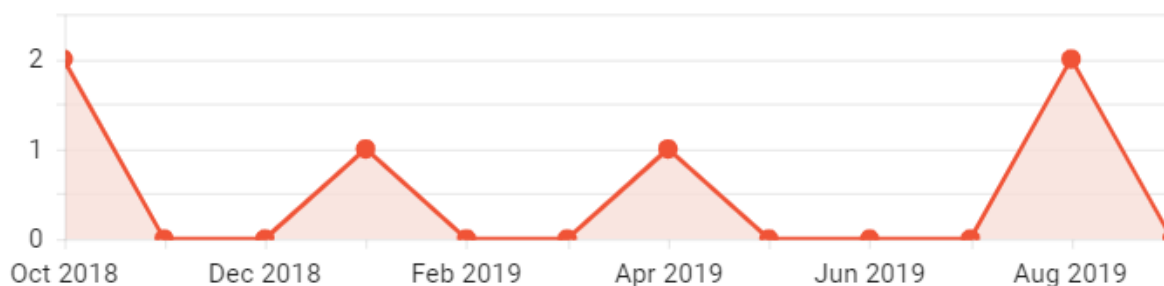
Total threat emails found across all of your employees' inboxes in the past 12 months.



## Employees with Threats

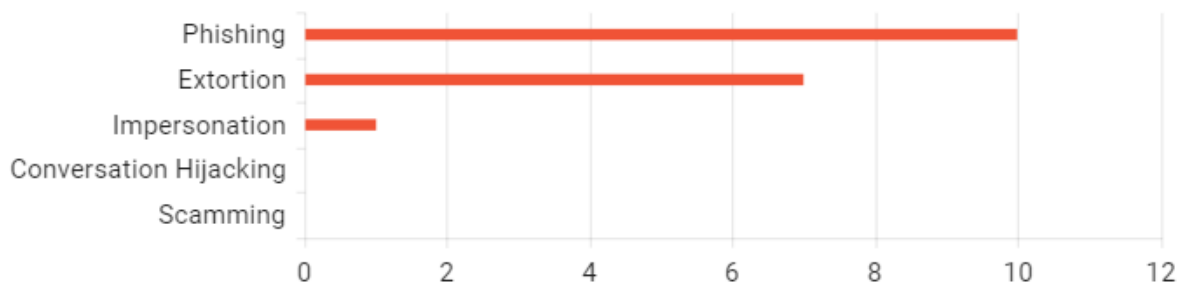
5

Number of employees who have threat emails found in their inboxes in the past 12 months.



## Threat Types Found

Total email threat types found in the past 12 months.



**Conversation Hijacking** - An attack where cybercriminals insert themselves into existing business conversations, or initiate new ones, to steal money or personal information.

**Extortion** - An attempt to obtain money or something of value by threatening to release embarrassing personal information, like images or videos.

**Impersonation** - An attack where the malicious actor pretends to be a person, organization, or service to entice the victim to wire money, buy gift cards, or disclose business information.

**Phishing** - An attempt to trick victims into believing a message is from a trusted organization to get them to disclose sensitive information, like credentials or banking information.

**Scamming** - Emails used by cybercriminals to defraud victims or steal their identity by tricking them into disclosing personal information.

## Domain DMARC Status

DMARC is an email authentication protocol that enables domain owners to protect their domains from unauthorized use, also known as email spoofing.

**4** Not Configured  
Domain can be spoofed or used for fraud

**1** Reporting Mode  
Domain fraud is reported, but is not enforced

**0** Enforcement Mode  
Domains protected with DMARC enforcement

# A look at your employees

All Employees  
**10**

High-Risk Employees  
**0**

Medium-Risk Employees  
**3**

Low-Risk Employees  
**7**

## Top at-risk employees

	EMPLOYEE NAME	EMPLOYEE EMAIL	JOB TITLE	RISK LEVEL	HIGH-RISK FACTORS	THREATS FOUND
1	<b>Lior Gavish</b>	lior@sookasa.onmi...	CTO	<b>Medium</b>	Holds executive position	<b>9</b>
2	<b>Alexey Tsitkin</b>	alexey@sookasa.onmi...		Low		<b>5</b>
3	<b>Marco Schweighauser</b>	marco@sookasa.onmi...	Software Engineer	Low		<b>2</b>
4	<b>Nadia Korshun</b>	nadia@sookasa.onmi...		Low		<b>1</b>
5	<b>Itay Bleier</b>	itay@sookasa.onmi...	CFO	<b>Medium</b>	Holds executive position	<b>1</b>

# Threats to your security






## Top 10 threats received

	RECEIVED	RECIPIENTS	SAMPLE RECIPIENT	EMAIL	ATTACK TYPE
1	Marco Schweighauser	6	<b>Marco Schweighauser</b> Software Engineer marco@sookasa.onmicrosoft.com	<b>(13) incoming mails failed Sync</b> Lior Gavish lior.gavish@gmail.com	<b>Phishing</b>
2	Marco Schweighauser	2	<b>Marco Schweighauser</b> Software Engineer marco@sookasa.onmicrosoft.com	<b>marco@sookasa.onmicrosoft.com : 031012</b> Jeffery Cuevas 497778@cudapost.com	<b>Extortion</b>
3	Lior Gavish	1	<b>Lior Gavish</b> CTO lior@sookasa.onmicrosoft.com	<b>lior@sookasa.onmicrosoft.com : 031012</b> Jeffery Cuevas 116034@cudapost.com	<b>Extortion</b>
4	Lior Gavish	1	<b>Lior Gavish</b> CTO lior@sookasa.onmicrosoft.com	<b>lior@sookasa.onmicrosoft.com : 031012</b> Jeffery Cuevas 649847@cudapost.com	<b>Extortion</b>
5	Lior Gavish	1	<b>Lior Gavish</b> CTO lior@sookasa.onmicrosoft.com	<b>lior@sookasa.onmicrosoft.com : 031012</b> Jeffery Cuevas 690172@cudapost.com	<b>Extortion</b>
6	Lior Gavish	1	<b>Lior Gavish</b> CTO lior@sookasa.onmicrosoft.com	<b>lior@sookasa.onmicrosoft.com : 031012</b> Jeffery Cuevas 869208@cudapost.com	<b>Extortion</b>
7	Lior Gavish	1	<b>Lior Gavish</b> CTO lior@sookasa.onmicrosoft.com	<b>High level of danger. Your account was under attack.</b> Cortez Schmitt 502621@cudapost.com	<b>Extortion</b>
8	Alexey Tsitkin	1	<b>Alexey Tsitkin</b> alexey@sookasa.onmicrosoft.com	<b>Notification</b> Microsoft Outlook 687936@cudapost.com	<b>Phishing</b>
9	Alexey Tsitkin	1	<b>Alexey Tsitkin</b> alexey@sookasa.onmicrosoft.com	<b>Morning</b> Nadia Korshun nadia.169524@cudapost.com	<b>Imperson...</b>
10	Lior Gavish	1	<b>Lior Gavish</b> CTO lior@sookasa.onmicrosoft.com	<b>Please update your payment information</b> Netflix 924496@cudapost.com	<b>Phishing</b>

# DMARC protection status of your domains

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email-validation system designed to detect and prevent email spoofing. It can be used to defend against certain types of emails attacks, including phishing and email spam. In these types of attacks, the email sender's address is forged, but the email itself appears to be legitimate. DMARC attempts to counter the illegitimate usage of the exact domain name in the From field of email message headers. If you have DMARC enabled and other organizations are recognizing DMARC, then your domain cannot be spoofed in phishing attempts to those recipients, thereby protecting the reputation of your domain.

## Top domains

DOMAIN	DMARC STATUS
1 cudafir.com	 <b>Not Configured</b> Domains can be spoofed or used for fraud. Consider protecting your domains.
2 cudadmarctest.net	 <b>Not Configured</b> Domains can be spoofed or used for fraud. Consider protecting your domains.
3 scan.barracudanetworks.com	 <b>Not Configured</b> Domains can be spoofed or used for fraud. Consider protecting your domains.
4 sookasa.co	 <b>Not Configured</b> Domains can be spoofed or used for fraud. Consider protecting your domains.
5 sookasa.com	 <b>Reporting Mode</b> Domain fraud is reported, but it's not enforced. Consider changing to Enforcement Mode to actively protect your domains.

# Sources of Attacks

## Top attacking domains

	ATTACKING DOMAIN	EMAILS WITH THREATS
1	cudapost.com	12
2	gmail.com	6