REVERSINGLABS

SOLUTION BRIEF

How to Find High-Risk Phishing Attacks in SMTP Traffic and Abuse Boxes

Challenges

- **The email attack vector is the hardest to secure with malicious payloads well-hidden within volumes of data moving across networks every day.**
- **SOC Analysts are fatigued from monitoring and reacting to threat alerts in the abuse box and SIEM with no further data available for fast malware Y/N decision.**
- **Lack of security alert orchestration and integrated threat intelligence prevents businesses from rapidly responding to phishing attacks.**

A whopping 92% of cyberattacks gain unwelcomed entry into businesses via emails sent by attackers that deceive people into taking that unforgiving step, clicking on malicious email attachments and links. The result - attackers obtain full access to systems, sensitive documents and personal information. CEO impersonation, deeply hidden malicious payloads, and malicious links to malware sites create pervasive attacks across the enterprise, making phishing very difficult to prevent.

Organizations understand the problem and are allocating large portions of their security budgets to stop these attacks, but massive volumes of email and no visibility into embedded malware makes it very difficult to mitigate attacks that circumvent controls. In response, organizations have invested in layered web proxy, email gateway, EDR and abuse box security with varying degrees of success.

They are also investing in employee education and training including the simulation of phishing attacks to improve end user reporting as the last line of defense. Unfortunately 4% of people will always click, no matter how much training has taken place. Organizations also use advanced behavioral tools to identify high-risk communications between highly targeted individuals and roles.

But even with organizations investing heavily in security across the network, employee education and behavior analysis, malware infected files and objects are still getting through, resulting in 30% of phishing attacks being missed.

Benefits

- **Triage threats faster and more accurately with rapid classification directly in the SOC 'abuse email' inbox.**
- **Remove dependencies on A/V signatures and dynamic analysis by displaying malware indicators for proactive security without executing malware.**
- **Instantly send malware details to abuse box, SIEM, SOAR and triage tools, extending and optimizing existing capabilities for better ROI.**

Solution

The ReversingLabs Titanium Platform finds high-priority phishing attacks hidden across the network by analyzing emails and attachments, and comparing all files and objects against an authoritative global file reputation database. This analysis exposes threat indicators and crucial malware intelligence like classification, threat levels and related malware families. Results are filtered, grouped and instantly displayed in SOC analyst workflows for the fastest possible triage and response to phishing attacks.

The Titanium Platform integrates seamlessly through APIs and connectors to email gateways and SMTP relay points. This delivers real-time analysis of all email content and inbound traffic, increasing the breadth and depth of existing controls through destructive object visibility. Analysis results can be used to create YARA rules to update existing controls or for advanced search and threat hunting, to find unknown variants of malware lurking on networks.

Use Case | 1

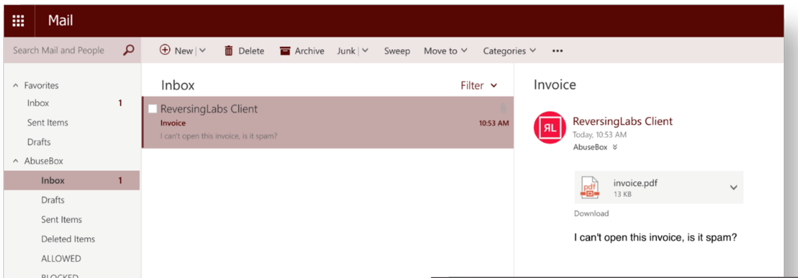
QUICKLY IDENTIFY HIGH-RISK PHISHING ATTACKS HIDDEN IN EMAIL ABUSE BOXES

Challenge: The high volume of phishing attacks reported to email abuse boxes makes it extremely difficult to determine legitimacy. Antivirus solutions are often the only tool SOC analysts have available to try to quickly identify malware, but they are unreliable against new or polymorphic malware because it usually takes at least 48 hours to weeks for vendors to create and distribute new signatures. The result is a large amount of false positives sitting in an email abuse box, waiting for manual analysis.

Solution: The ReversingLabs Titanium platform instantly analyzes all email attachments and links for malware infected files and objects armed to destroy business value. With a direct integration to Exchange, high risk and malicious emails are moved to a "BLOCKED" folder, speeding triage and response for SOC analysts.

Benefit: The automated movement of malicious emails to "BLOCKED" or "ALLOWED" folders allows analysts to triage faster without wasting time determining if malware is present in false positives. The prioritization of high risk malware, and rapid escalation to existing triage tools optimizes investigation and containment processes and increases the ROI of all existing security tools.

Phishing attacks forwarded by users to an abuse box are automatically scanned and comprehensively analyzed.



ReversingLabs Client
Invoice 10:53 AM
I can't open this invoice, is it spam?

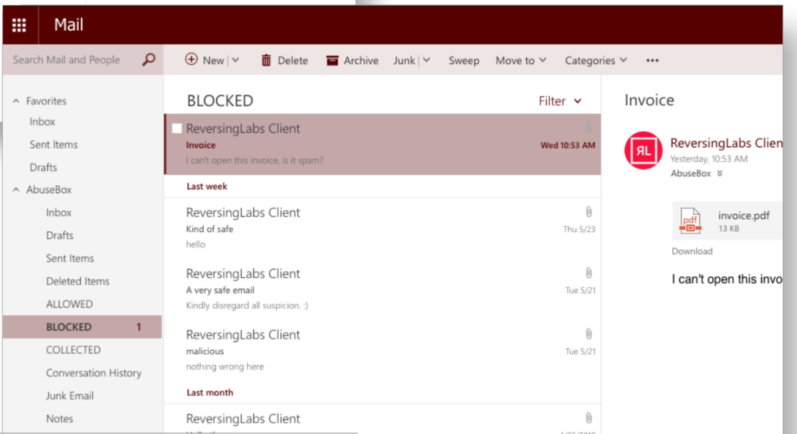
Invoice

ReversingLabs Client
Today, 10:53 AM
AbuseBox

invoice.pdf
13 KB

I can't open this invoice, is it spam?

If malware is found, the email is automatically moved to a "blocked" folder.



ReversingLabs Client
Invoice Wed 10:53 AM
I can't open this invoice, is it spam?

Last week

ReversingLabs Client
Kind of safe Thu 5/23
hello

ReversingLabs Client
A very safe email Tue 5/21
Kindly disregard all suspicion. :)

ReversingLabs Client
malicious Tue 5/21
nothing wrong here

Last month

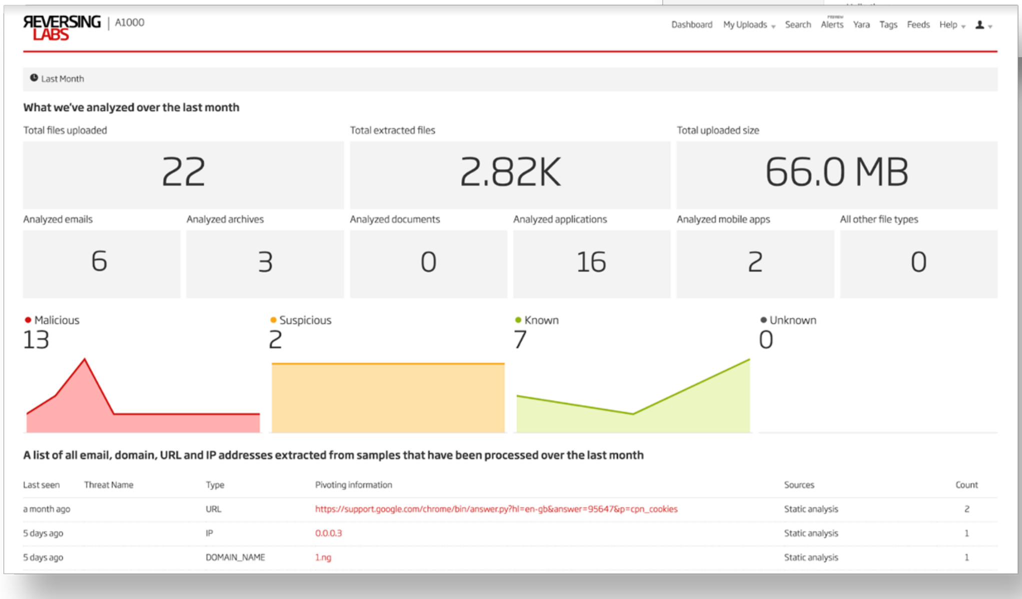
ReversingLabs Client 4/25/2019

Invoice

ReversingLabs Clien
Yesterday, 10:53 AM
AbuseBox

invoice.pdf
13 KB

I can't open this invo



What we've analyzed over the last month

Total files uploaded	Total extracted files	Total uploaded size
22	2.82K	66.0 MB

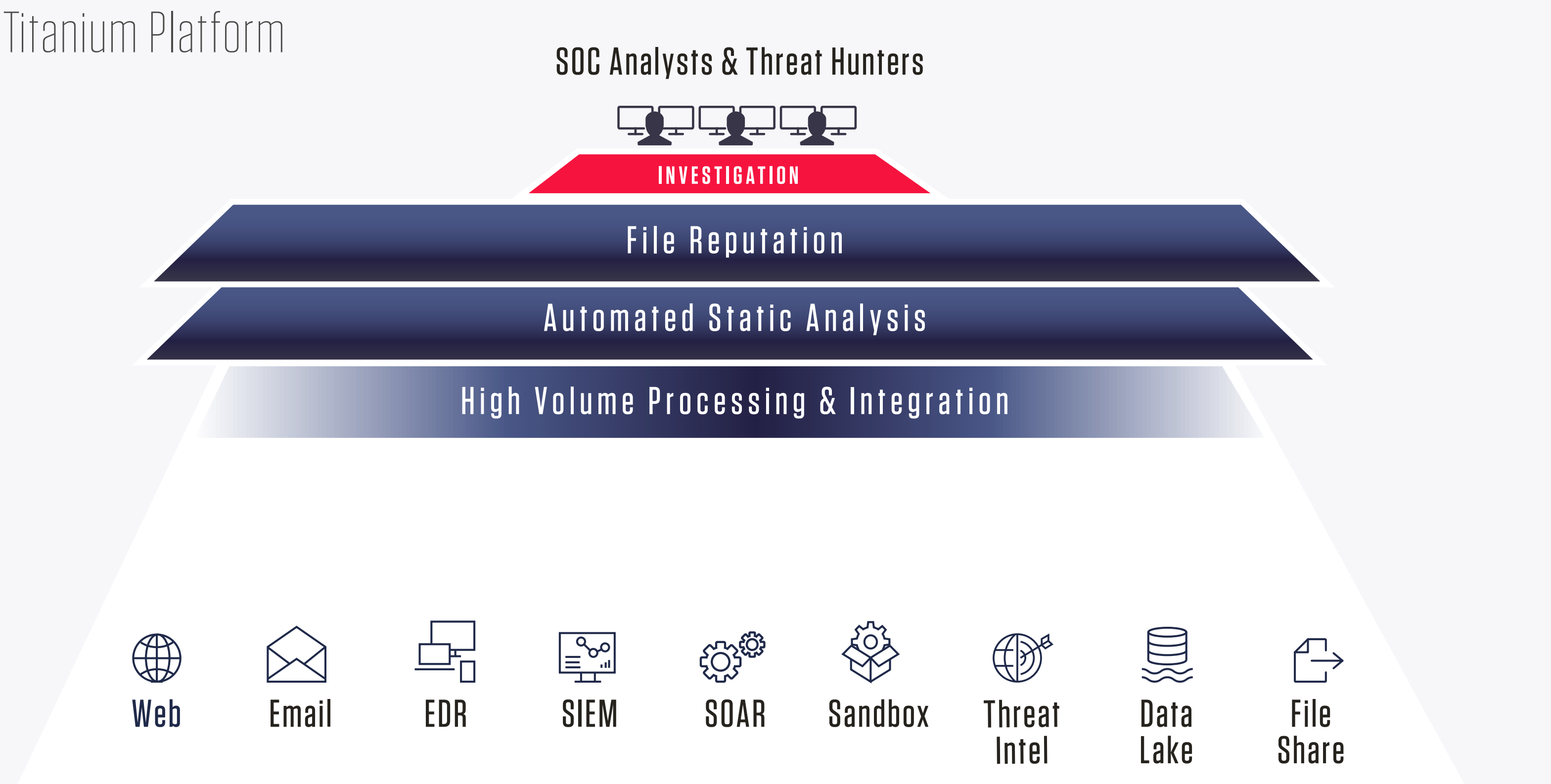
Analyzed emails	Analyzed archives	Analyzed documents	Analyzed applications	Analyzed mobile apps	All other file types
6	3	0	16	2	0

● Malicious	● Suspicious	● Known	● Unknown
13	2	7	0

A list of all email, domain, URL and IP addresses extracted from samples that have been processed over the last month

Last seen	Threat Name	Type	Pivoting information	Sources	Count
a month ago		URL	https://support.google.com/chrome/bin/answer.py?hl=en-gb&answer=95647&p=cpn_cookies	Static analysis	2
5 days ago		IP	0.0.0.3	Static analysis	1
5 days ago		DOMAIN_NAME	1.ng	Static analysis	1

Detailed email analysis results can be viewed in the ReversingLabs Advanced Malware Analysis Platform.



Use Case | 2

IDENTIFY HIDDEN EMAIL THREATS IN ALL INBOUND TRAFFIC

Challenge: Highly targeted ransomware and phishing attacks, emerging threats, encrypted documents, and malware embedded in large files often bypass existing layered security controls. This results in layered security controls still missing the high priority phishing attacks that impact businesses.

Solution: ReversingLabs SMTP service scans everything, rapidly identifying threats for complete coverage of all email and attachments in motion. Working alongside existing systems (Exchange Online Protection, ATP, ProofPoint, IronPort, Symantec Email Gateway, FireEye EX/AX), SOC analysts and threat hunters have instant insights into all inbound destructive objects, for the most advanced and actionable threat intelligence available.

Benefit: The instant identification, classification and prioritization of malware enriches all email security and phishing detection systems, improving email security efficiency with end-to-end visibility into hidden malware risks across the enterprise. Exposed malware indicators power highly optimized investigation and containment processes of true attacks in an email abuse box and across networks. Organizations can rapidly escalate suspicious and malicious email to existing triage tools, SOAR platforms and incident response teams, extending and optimizing existing capabilities for better ROI.

REVERSINGLABS

Worldwide Sales:
+1.617.250.7518
www.reversinglabs.com
Schedule Demo Here