Trellix

There's no such thing as safe Email

How to secure collaboration

Nasir Shakour

Global Solutions Architect
Email and Network Security

Is email secure?

Is email security still a concern for you?

What are your email security challenges?

Do Messaging Platform Providers provide real security?

The Statistics

Email Security is still relevant

12:1

We see 12 malicious URLs for each one malicious attachment

91%

of cyberattacks begin with spear phishing

>25%

Detected filetypes are MS Office Docs

10%

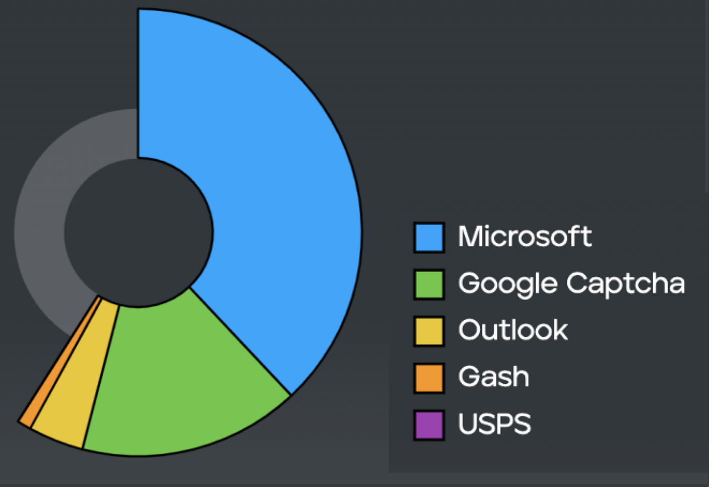
Emails remediated post delivery

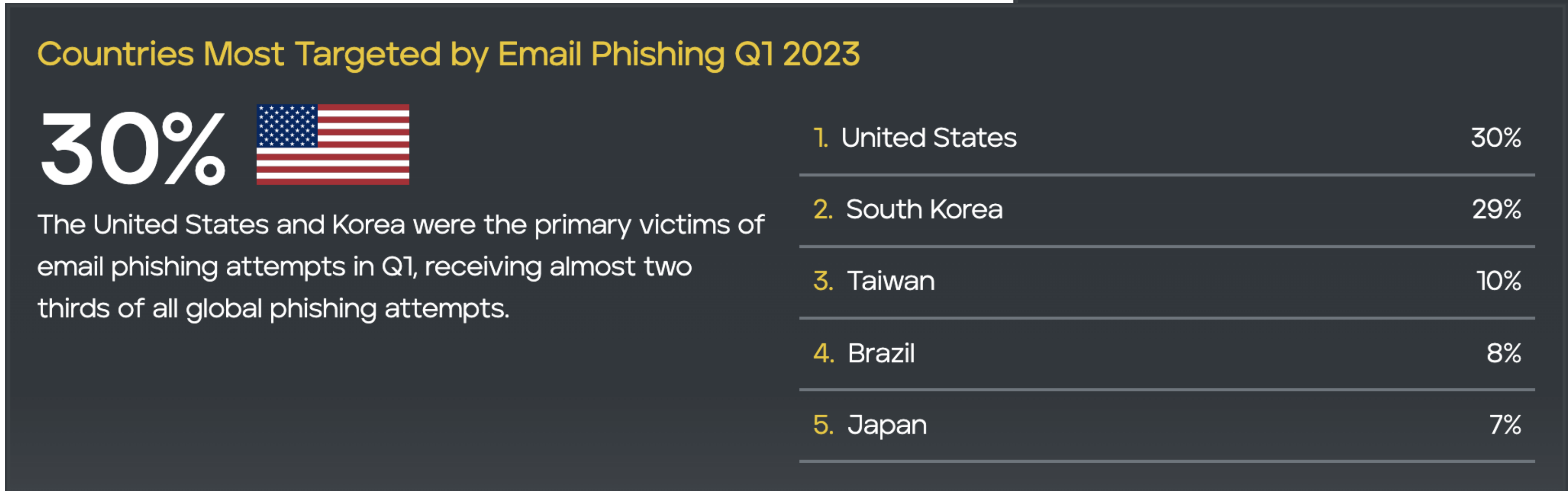
The Statistics

Email Security is still relevant

Products and Brands Most Targeted by Email Phishing Q1 2023

38% Though hundreds of brands were targeted, Microsoft products accounted for the most by a long shot in Q1 2023.



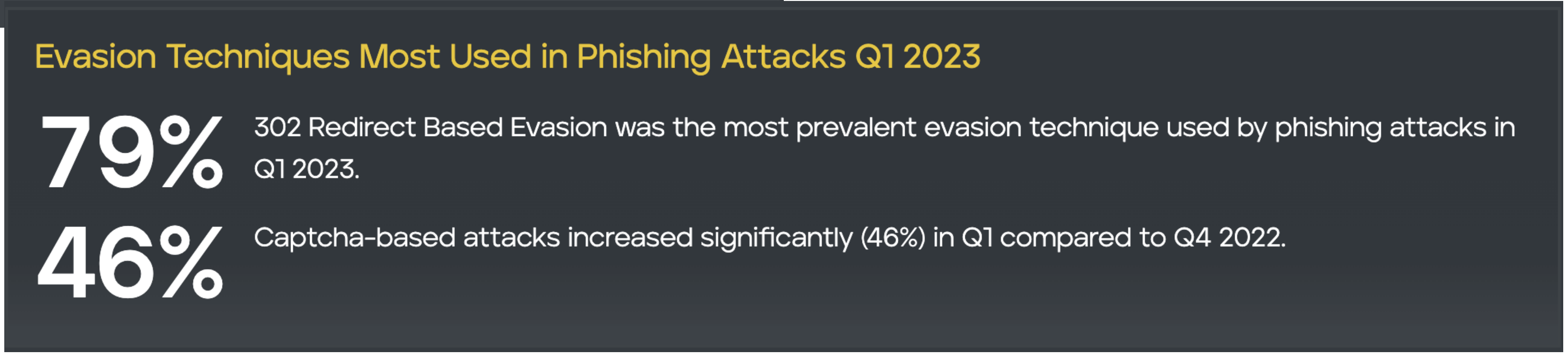


Countries Most Targeted by Email Phishing Q1 2023

30%

The United States and Korea were the primary victims of email phishing attempts in Q1, receiving almost two thirds of all global phishing attempts.

1. United States	30%
2. South Korea	29%
3. Taiwan	10%
4. Brazil	8%
5. Japan	7%



Evasion Techniques Most Used in Phishing Attacks Q1 2023

79% 302 Redirect Based Evasion was the most prevalent evasion technique used by phishing attacks in Q1 2023.

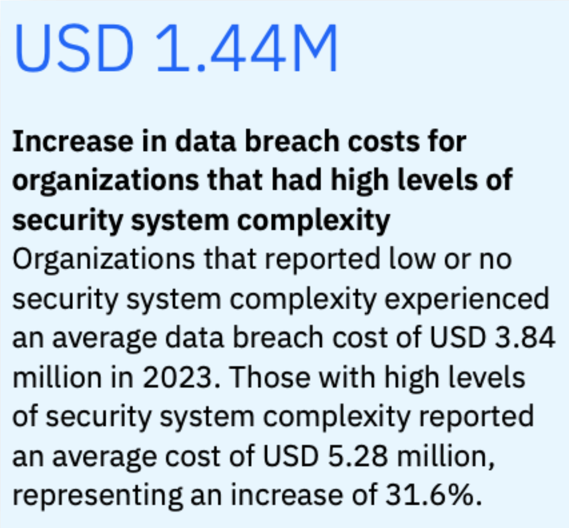
46% Captcha-based attacks increased significantly (46%) in Q1 compared to Q4 2022.

Trellix ADVANCED RESEARCH CENTER

Trellix

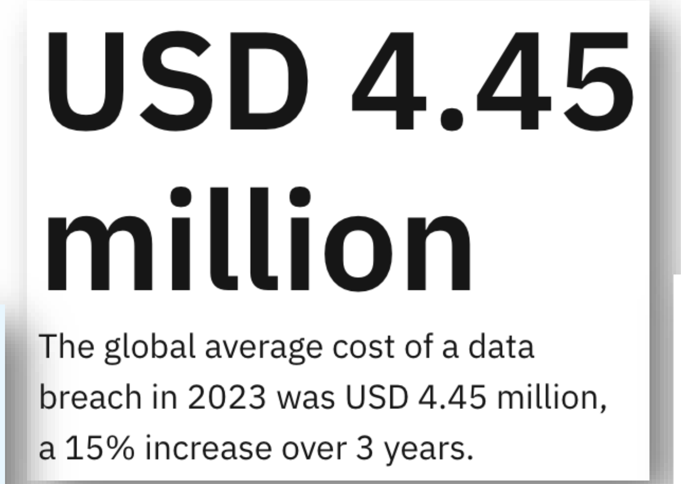
The Statistics

Email Security is still relevant



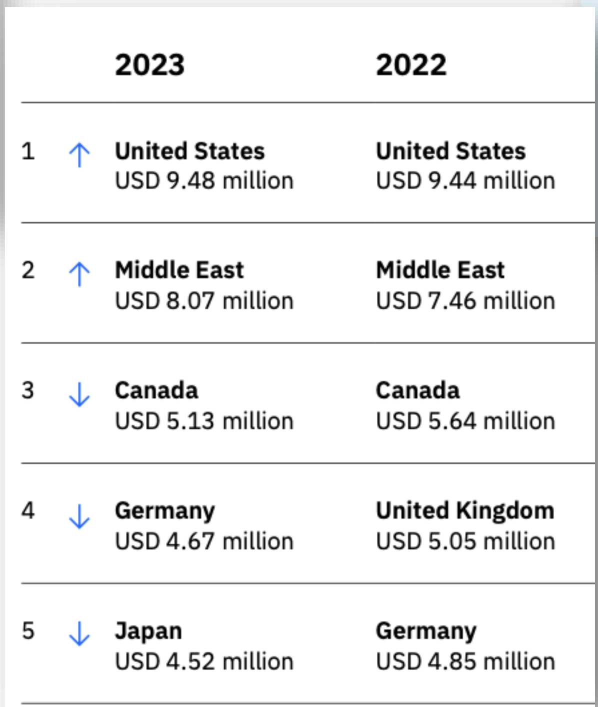
USD 1.44M

Increase in data breach costs for organizations that had high levels of security system complexity
Organizations that reported low or no security system complexity experienced an average data breach cost of USD 3.84 million in 2023. Those with high levels of security system complexity reported an average cost of USD 5.28 million, representing an increase of 31.6%.

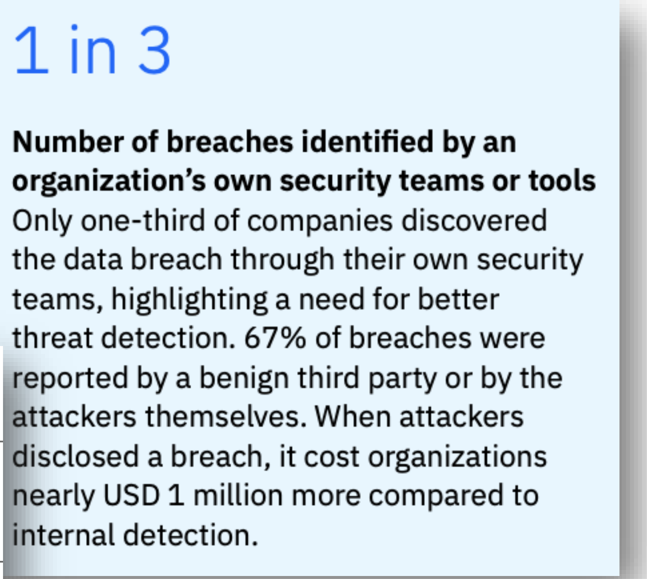


USD 4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.



		2023	2022
1	↑	**United States** USD 9.48 million	**United States** USD 9.44 million
2	↑	**Middle East** USD 8.07 million	**Middle East** USD 7.46 million
3	↓	**Canada** USD 5.13 million	**Canada** USD 5.64 million
4	↓	**Germany** USD 4.67 million	**United Kingdom** USD 5.05 million
5	↓	**Japan** USD 4.52 million	**Germany** USD 4.85 million

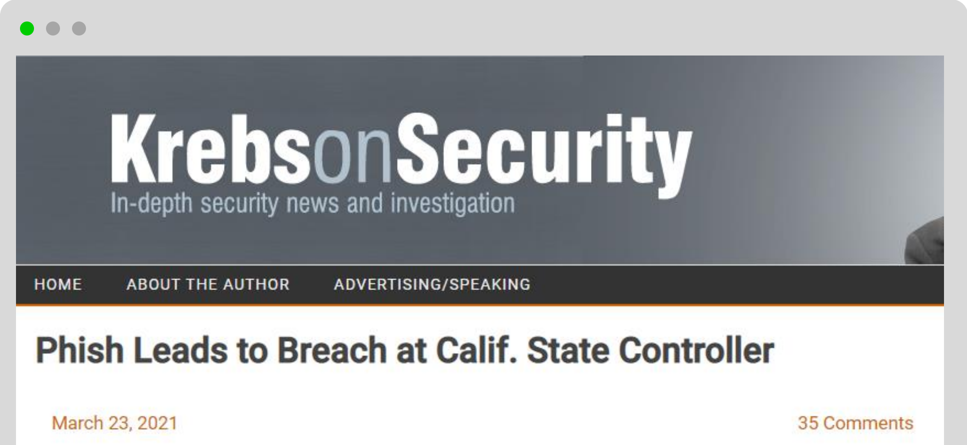


1 in 3

Number of breaches identified by an organization's own security teams or tools
Only one-third of companies discovered the data breach through their own security teams, highlighting a need for better threat detection. 67% of breaches were reported by a benign third party or by the attackers themselves. When attackers disclosed a breach, it cost organizations nearly USD 1 million more compared to internal detection.

IBM
Cost of a Data Breach
Report 2023

It only takes one...



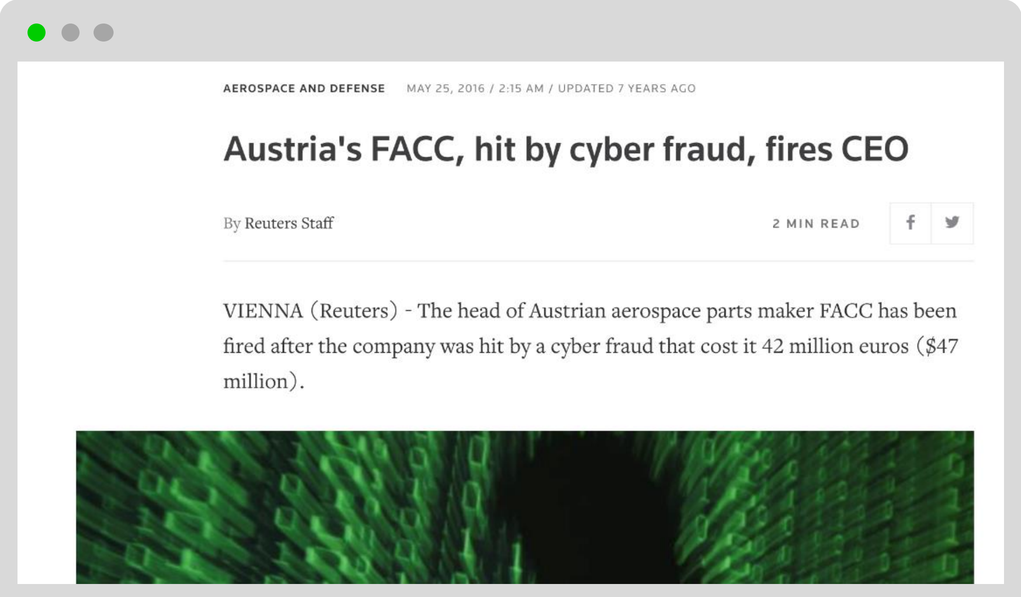
KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Phish Leads to Breach at Calif. State Controller

March 23, 2021 35 Comments

A phish
Office (
phishe
time to
targete

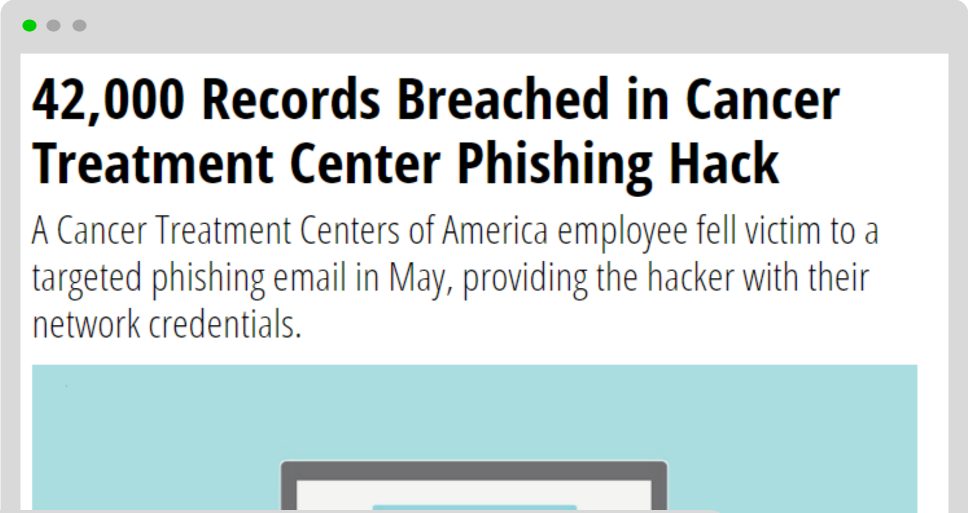


AEROSPACE AND DEFENSE MAY 25, 2016 / 2:15 AM / UPDATED 7 YEARS AGO

Austria's FACC, hit by cyber fraud, fires CEO

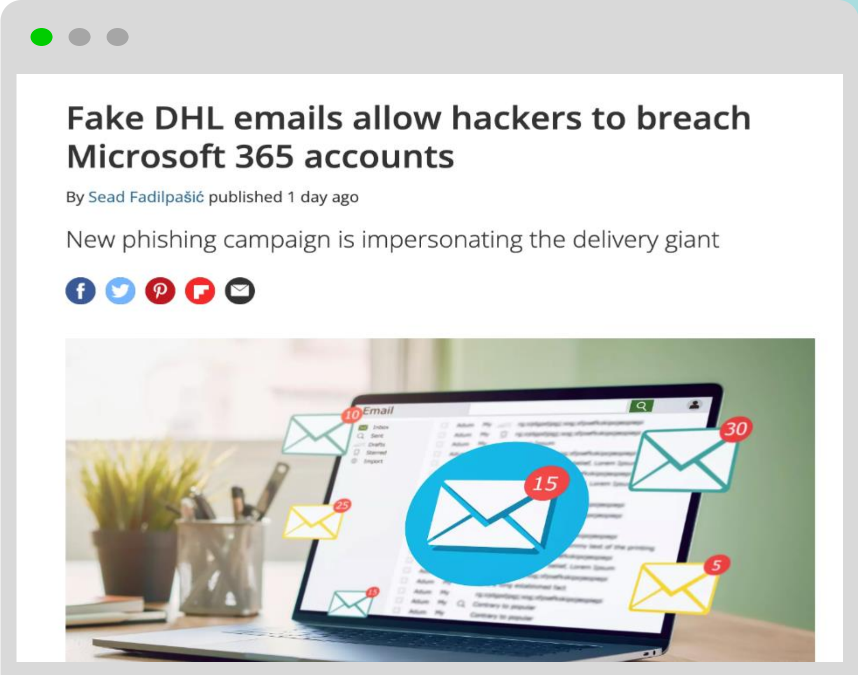
By Reuters Staff 2 MIN READ

VIENNA (Reuters) - The head of Austrian aerospace parts maker FACC has been fired after the company was hit by a cyber fraud that cost it 42 million euros ($47 million).



42,000 Records Breached in Cancer Treatment Center Phishing Hack

A Cancer Treatment Centers of America employee fell victim to a targeted phishing email in May, providing the hacker with their network credentials.



Fake DHL emails allow hackers to breach Microsoft 365 accounts

By Sead Fadilpašić published 1 day ago

New phishing campaign is impersonating the delivery giant

How can we secure email?

Trellix

Detection is the best defense

Despite extensive training, statistics show that human error remains a leading cause of successful phishing attacks

Threat Actors are constantly improving techniques

The volume of attacks has increased exponentially.

Trellix

Trellix Email Security

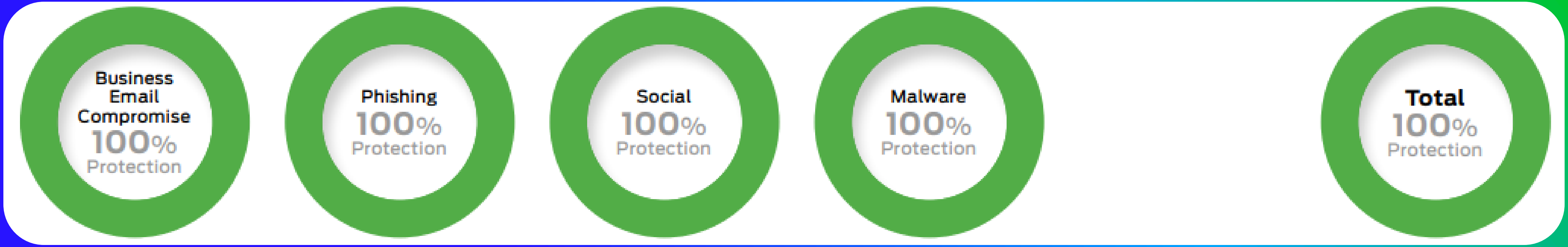
Trellix

We catch what others miss

Trellix identifies and blocks all email threat categories

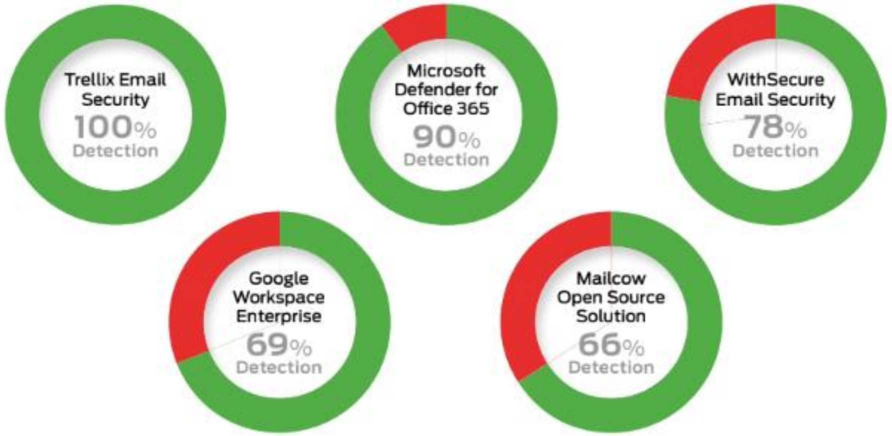
- ATTACHMENTS
- URLs
- POST-DELIVERY WEAPONIZATION
- SOCIAL MEDIA COVERAGE
- IMPERSONATION
- MULTI-STAGE DETECTION
- OUTBOUND DETECTION

Trellix Ranks #1 in SE Labs Report

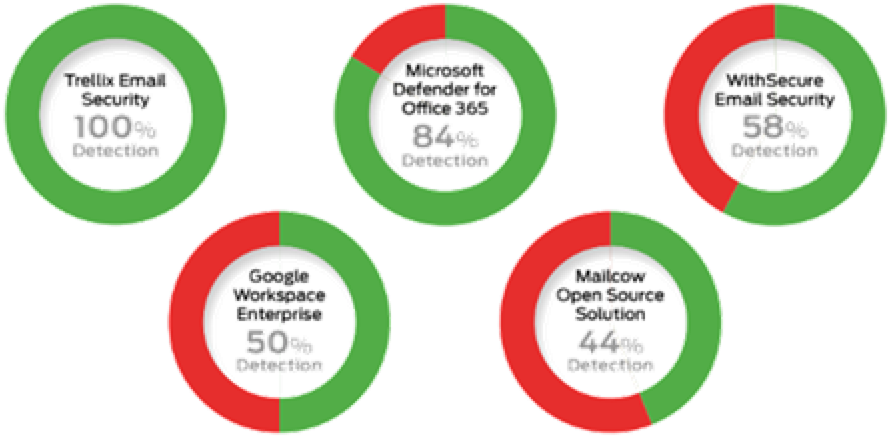


Overall Rankings

#1 in Detection



#1 in Accuracy

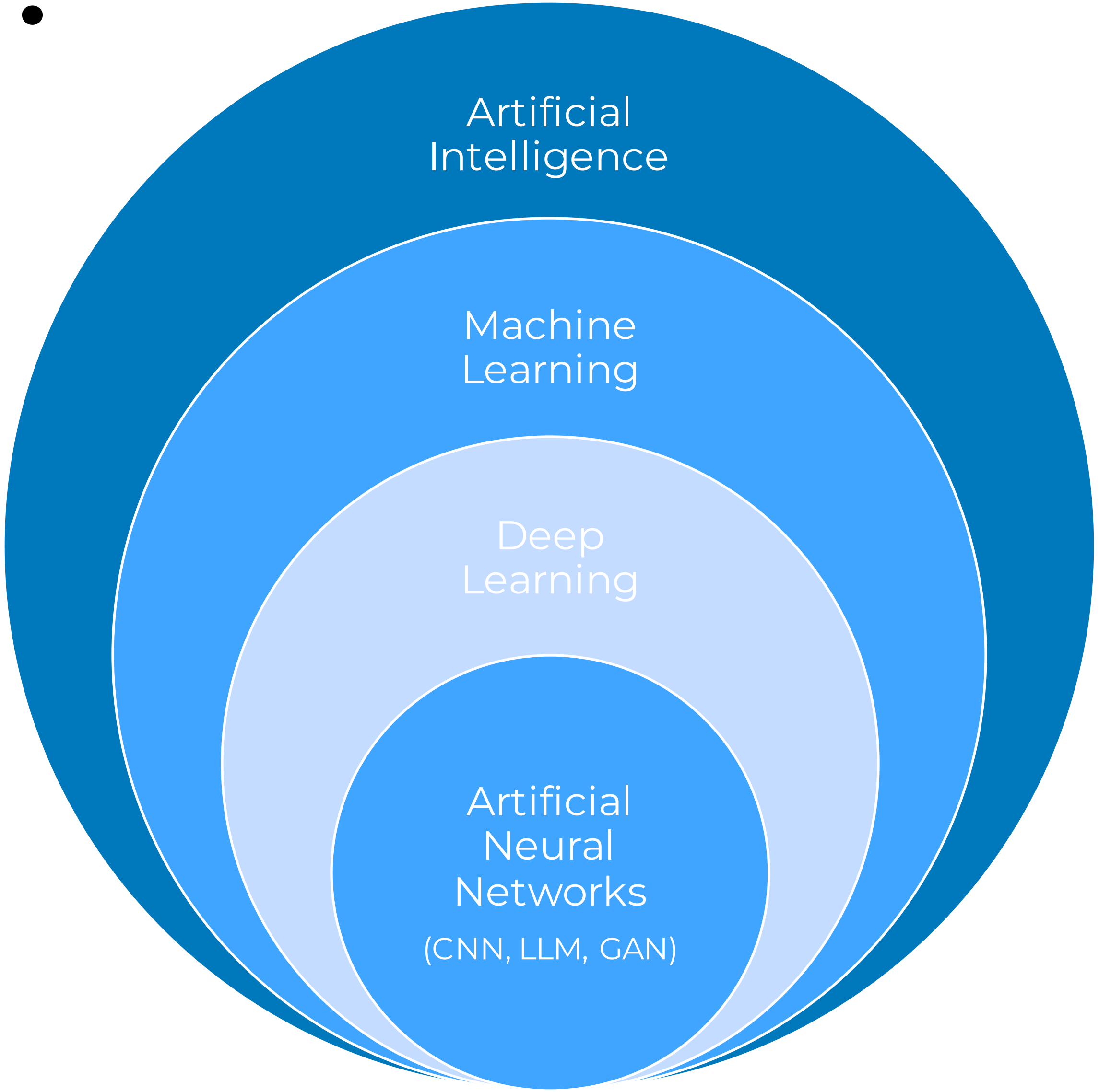


Source: SE Labs: Email Security Services (ESS): Enterprise 2023 Q1

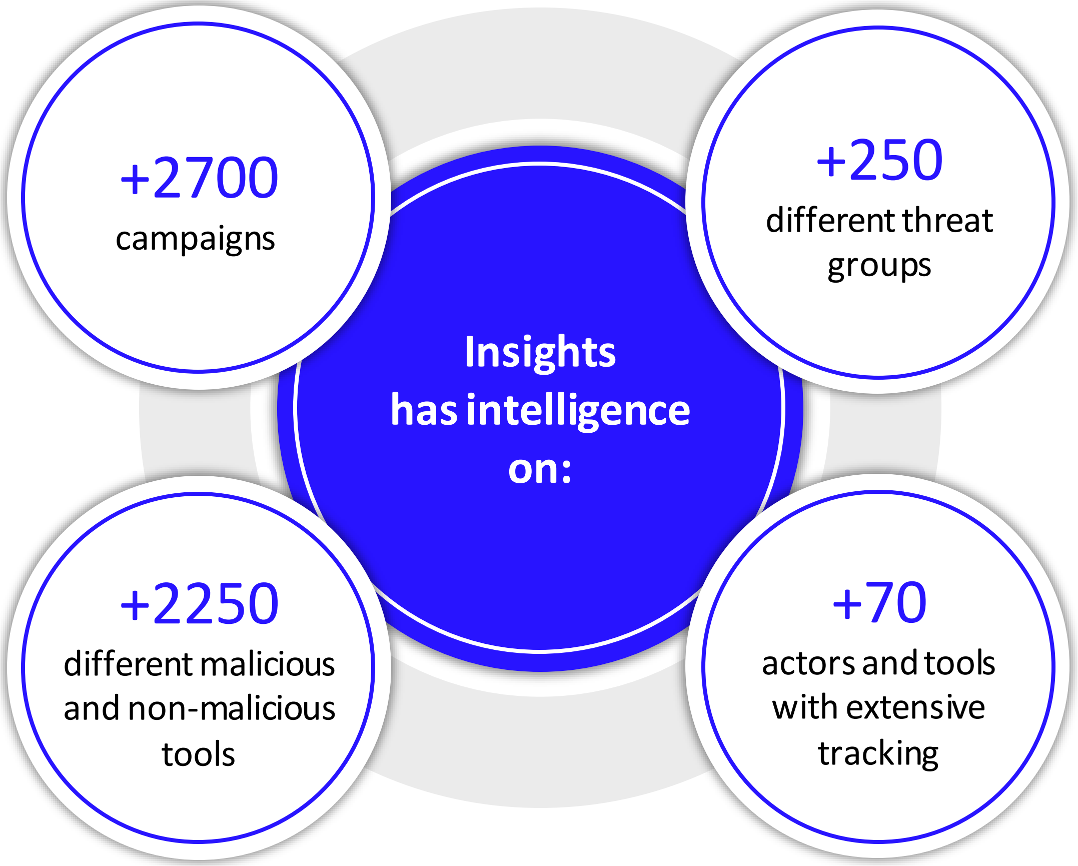
Artificial Intelligence

Trellix

What is AI?


Artificial Intelligence
Machine Learning
Deep Learning
Artificial Neural Networks
(CNN, LLM, GAN)

Intelligence-led detection



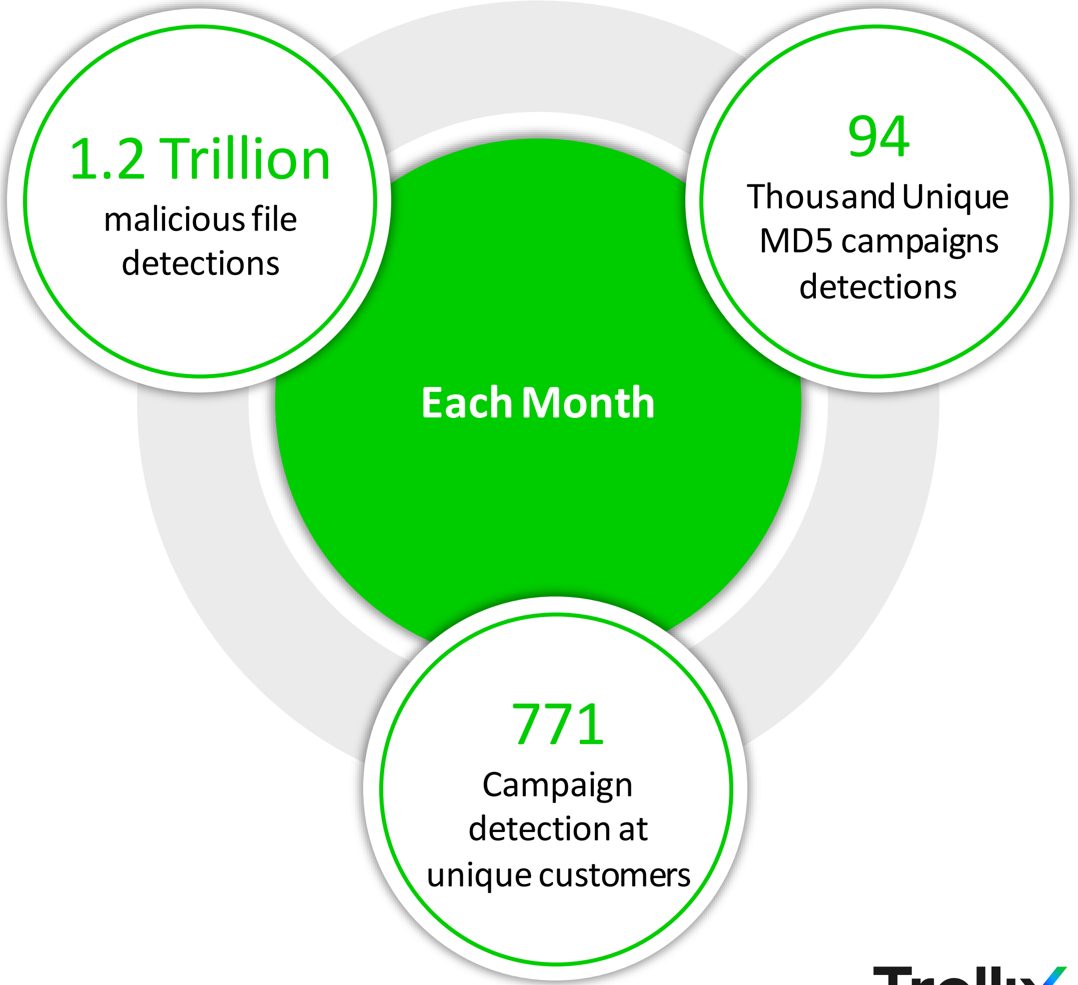
Insights has intelligence on:

+2700 campaigns

+250 different threat groups

+2250 different malicious and non-malicious tools

+70 actors and tools with extensive tracking



Each Month

1.2 Trillion malicious file detections

94 Thousand Unique MD5 campaigns detections

771 Campaign detection at unique customers

Advanced URL Defense for Email

Trellix Advanced URL Defense

Scalable URL detection using big data

Signature-based detections

Dynamic detections

Intelligence-led context and detection

Retroactive weaponization detections

Machine Learning

Advanced URL Defense

Deep learning phishing detection

Image classification

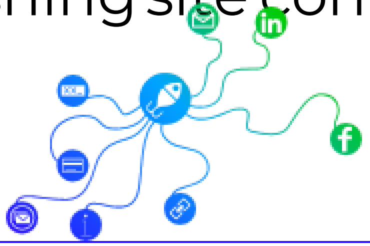
Credential phishing through application impersonation

HIDDEN LAYER 1
HIDDEN LAYER 2
HIDDEN LAYER 3
False brand website

Analytics-based phishing detection

Compares new page content against known phishing sites

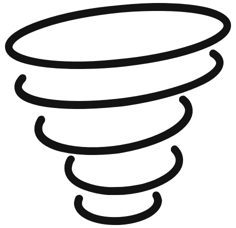
Inspects URL and phishing site content



Intelligence aggregation

Social media monitoring

C2 domains



Trellix

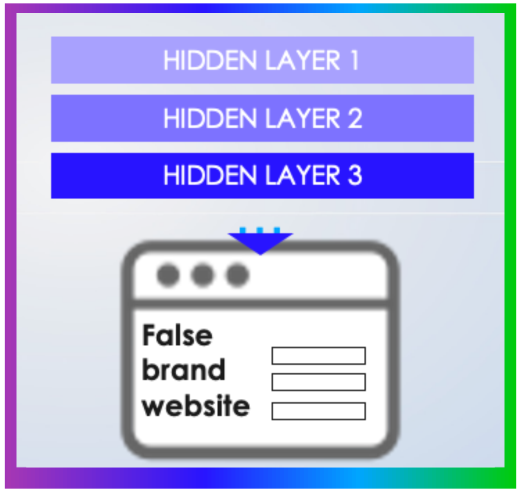
Multiple ML models detect Phishing

Visual Inspection

Advanced URL Defense plug in

Image classification engine
(Compiles/compares screenshots of commonly targeted brands against URLs in an email)

Provides brand targeting insight

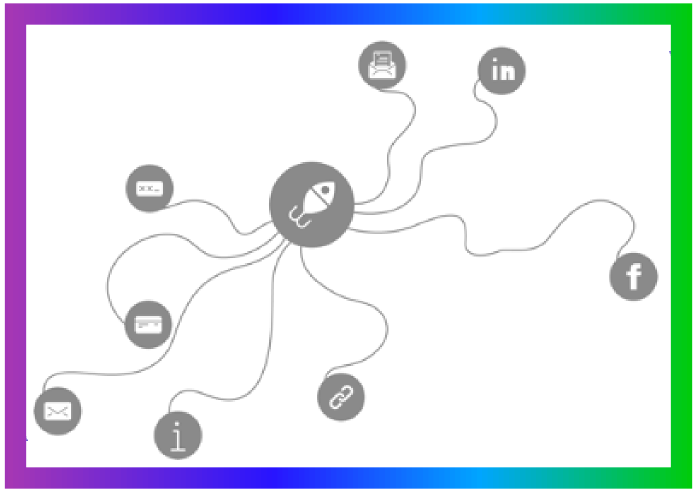


Site Inspection

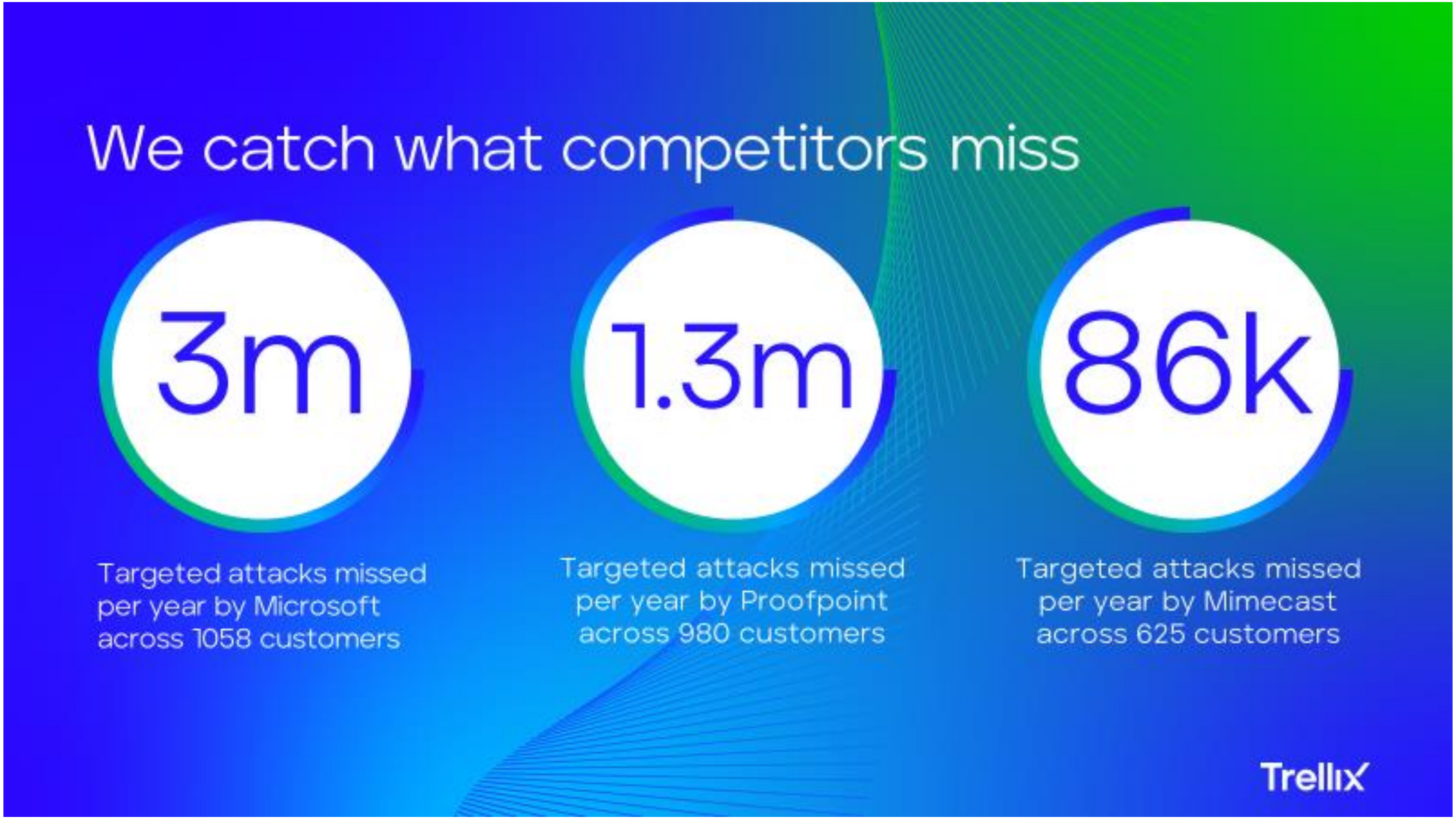
Compares new page content against known phishing sites

Inspects URL and phishing site content

Crawls and inspects content links



Trellix



We catch what competitors miss

3m

Targeted attacks missed per year by Microsoft across 1058 customers

1.3m

Targeted attacks missed per year by Proofpoint across 980 customers

86k

Targeted attacks missed per year by Mimecast across 625 customers

Trellix

Impersonation Detection

Trellix

Technique: Impersonation

- **CEO fraud or “whaling”** – impersonate senior executive asking for urgent wire transfer payment
- **Supplier impersonation** - sending false invoices requesting fund transfers to fraudulent accts
- **Email spoofing** - Display name, Legitimate domains, Lookalike domains
- **Account takeovers** – attackers compromise an employe’s account then ask for payment or sensitive data

Impersonation Detection

Techniques Used to Stop Evolving Inline Attacks

New Domains & Name Servers

Looks-Like & Sounds-Like Domains

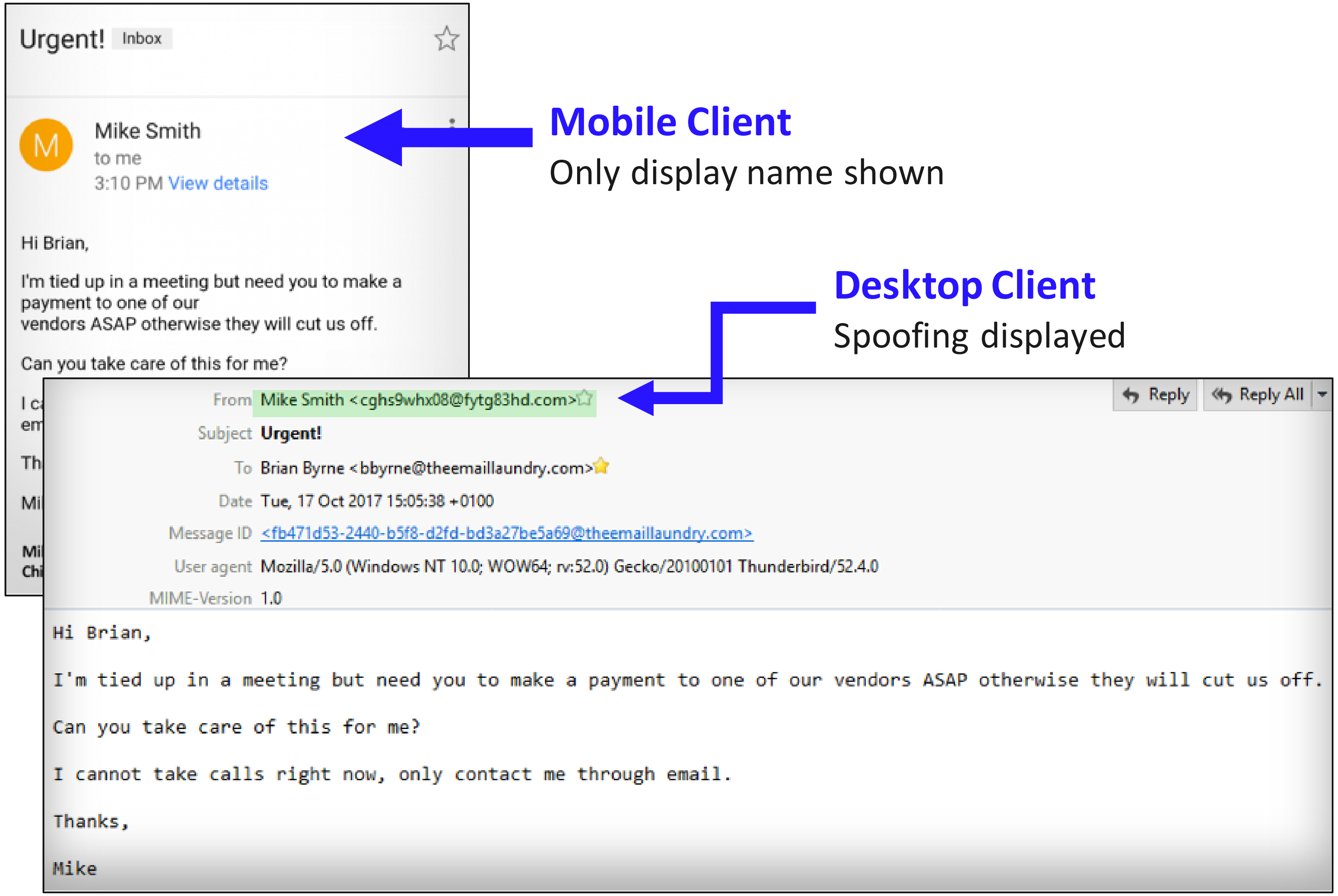
Reply-to Address & Message Header Analysis

Friendly Display Name & Username Matching

CEO Fraud Algorithms

Trellix

Display name impersonates a trusted source



Urgent! Inbox

Mike Smith

to me

3:10 PM View details

Hi Brian,

I'm tied up in a meeting but need you to make a payment to one of our vendors ASAP otherwise they will cut us off.

Can you take care of this for me?

I c
em

Th

Mi

Mi
Chi

Mobile Client

Only display name shown

Desktop Client

Spoofing displayed

From Mike Smith <cghs9whx08@fytg83hd.com>

Subject **Urgent!**

To Brian Byrne <bbyrne@theemaillaundry.com>

Date Tue, 17 Oct 2017 15:05:38 +0100

Message ID <fb471d53-2440-b5f8-d2fd-bd3a27be5a69@theemaillaundry.com>

User agent Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Thunderbird/52.4.0

MIME-Version 1.0

```
Hi Brian,

I'm tied up in a meeting but need you to make a payment to one of our vendors ASAP otherwise they will cut us off.

Can you take care of this for me?

I cannot take calls right now, only contact me through email.

Thanks,

Mike
```

Detecting Brand Impersonation

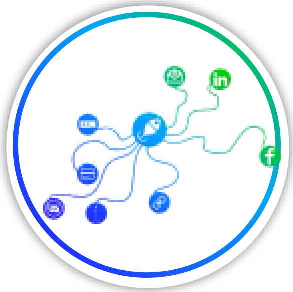
Visual comparison with known brands

Image classification & inspection

Compares screenshots of commonly targeted brands with web pages referenced by suspicious URLs

(PhishVision)

Identify content coming from known phishing sites



Deep content inspection

Crawls and analyzes new domain and page content to identify reuse from known phishing sites

(Kraken)

Trellix

Antispam Content Engine

Categories of Rules:

CEO Fraud Rules

Phishing (Financial, Email Accounts, Social Networks etc)

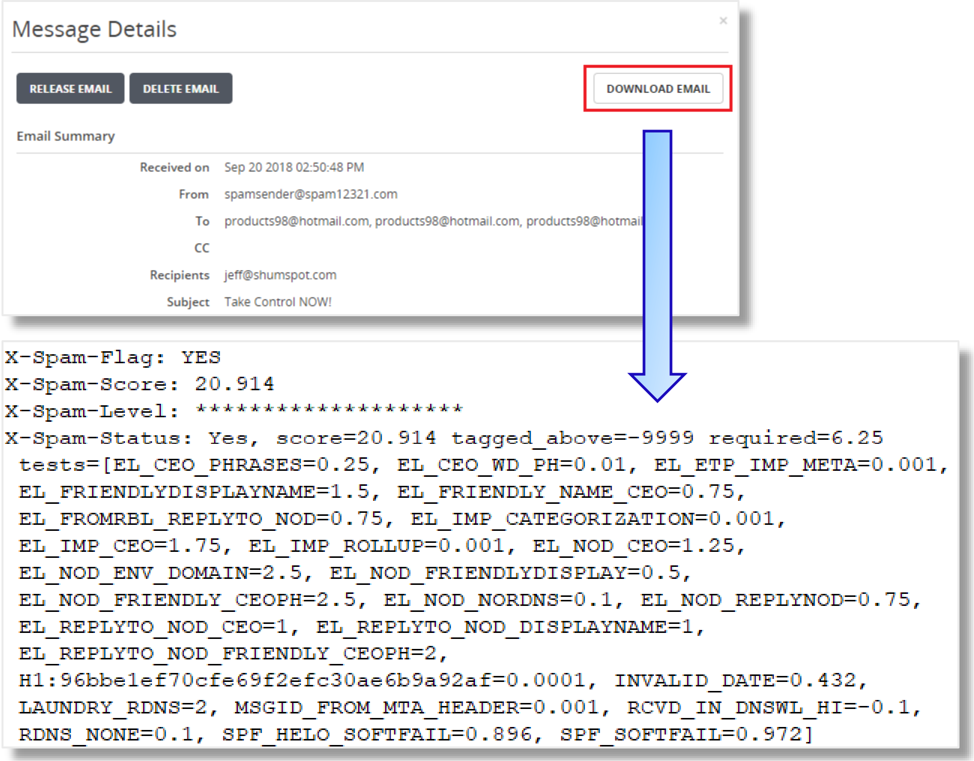
Snowshoe Spam

Explicit Content

Header Rule Checks

Hashes

GeoDist / Machine Learning



Message Details

Email Summary

Received on Sep 20 2018 02:50:48 PM
From spamsender@spam12321.com
To products98@hotmail.com, products98@hotmail.com, products98@hotmail
CC
Recipients jeff@shumspot.com
Subject Take Control NOW!

```
X-Spam-Flag: YES
X-Spam-Score: 20.914
X-Spam-Level: ********************
X-Spam-Status: Yes, score=20.914 tagged_above=-9999 required=6.25
 tests=[EL_CEO_PHRASES=0.25, EL_CEO_WD_PH=0.01, EL_ETP_IMP_META=0.001,
 EL_FRIENDLYDISPLAYNAME=1.5, EL_FRIENDLY_NAME_CEO=0.75,
 EL_FROMRBL_REPLYTO_NOD=0.75, EL_IMP_CATEGORIZATION=0.001,
 EL_IMP_CEO=1.75, EL_IMP_ROLLUP=0.001, EL_NOD_CEO=1.25,
 EL_NOD_ENV_DOMAIN=2.5, EL_NOD_FRIENDLYDISPLAY=0.5,
 EL_NOD_FRIENDLY_CEOPH=2.5, EL_NOD_NORDNS=0.1, EL_NOD_REPLYNOD=0.75,
 EL_REPLYTO_NOD_CEO=1, EL_REPLYTO_NOD_DISPLAYNAME=1,
 EL_REPLYTO_NOD_FRIENDLY_CEOPH=2,
 H1:96bbe1ef70cfe69f2efc30ae6b9a92af=0.0001, INVALID_DATE=0.432,
 LAUNDRY_RDNS=2, MSGID_FROM_MTA_HEADER=0.001, RCVD_IN_DNSWL_HI=-0.1,
 RDNS_NONE=0.1, SPF_HELO_SOFTFAIL=0.896, SPF_SOFTFAIL=0.972]
```

Results

Phishing

	Protection
Trellix Email Security	100
Microsoft Defender	100
WithSecure Email Security	100
Google Workspace Enterprise	98
Mailcow Open Source Solution	94

Business Email Compromise

	Protection
Trellix Email Security	100
Microsoft Defender	100
WithSecure Email Security	15
Google Workspace Enterprise	19
Mailcow Open Source Solution	15

Attachment Inspection

Trellix

Technique: Malicious Attachments

- Password-protected .zip files containing ransomware

- Microsoft Office documents using macros to deploy malicious payloads

- Google docs containing an embedded .pdf doc to be downloaded to view, which then leads to a malicious executable

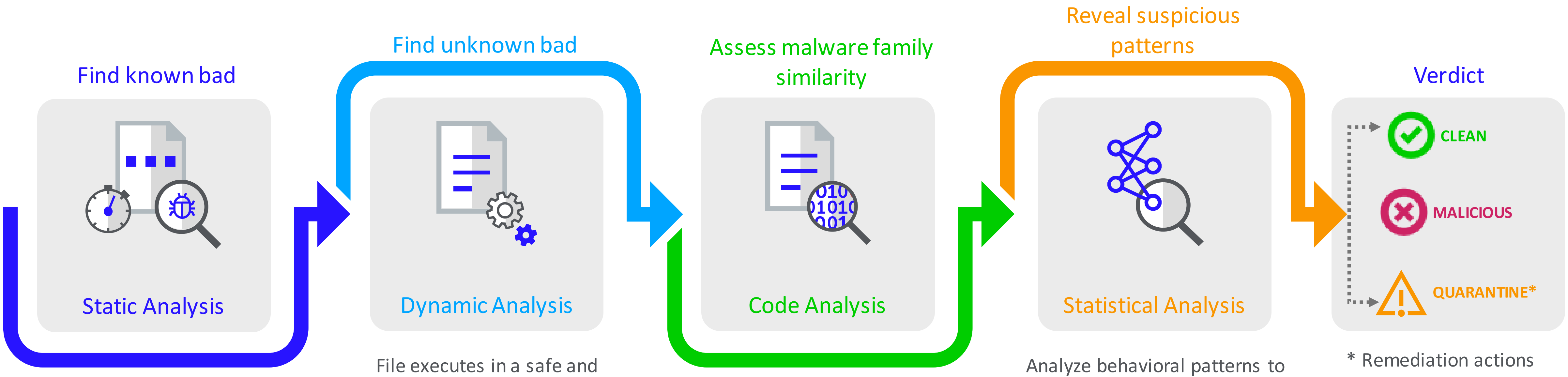
- Dropbox, Slack, and GitHub are all used as phishing lures

Technique: Malicious URLs

- Often disguised with alternate text or graphics
- Shortened using services like bit.ly
- Can lead to malicious sites for credential harvesting
- Used to download a payload such as ransomware

Multi-stage inspection process

More than just a sandbox



Find known bad

Static Analysis

Find unknown bad

Dynamic Analysis

Assess malware family similarity

Code Analysis

Reveal suspicious patterns

Statistical Analysis

Verdict

CLEAN

MALICIOUS

QUARANTINE*

Lower intensity analytical methods: signatures, reputation, and emulations

Performs high speed analysis at scale

File executes in a safe and instrumented environment.

Observe file execution and look for malicious behavior.

Remove obfuscation to expose original executable code.

Analyze attributes and instruction sets to identify characteristics similar to known bad behaviors

Analyze behavioral patterns to identify maliciousness.

Uncover patterns in code to identify emerging threats.

* Remediation actions configurable by integration

Trellix

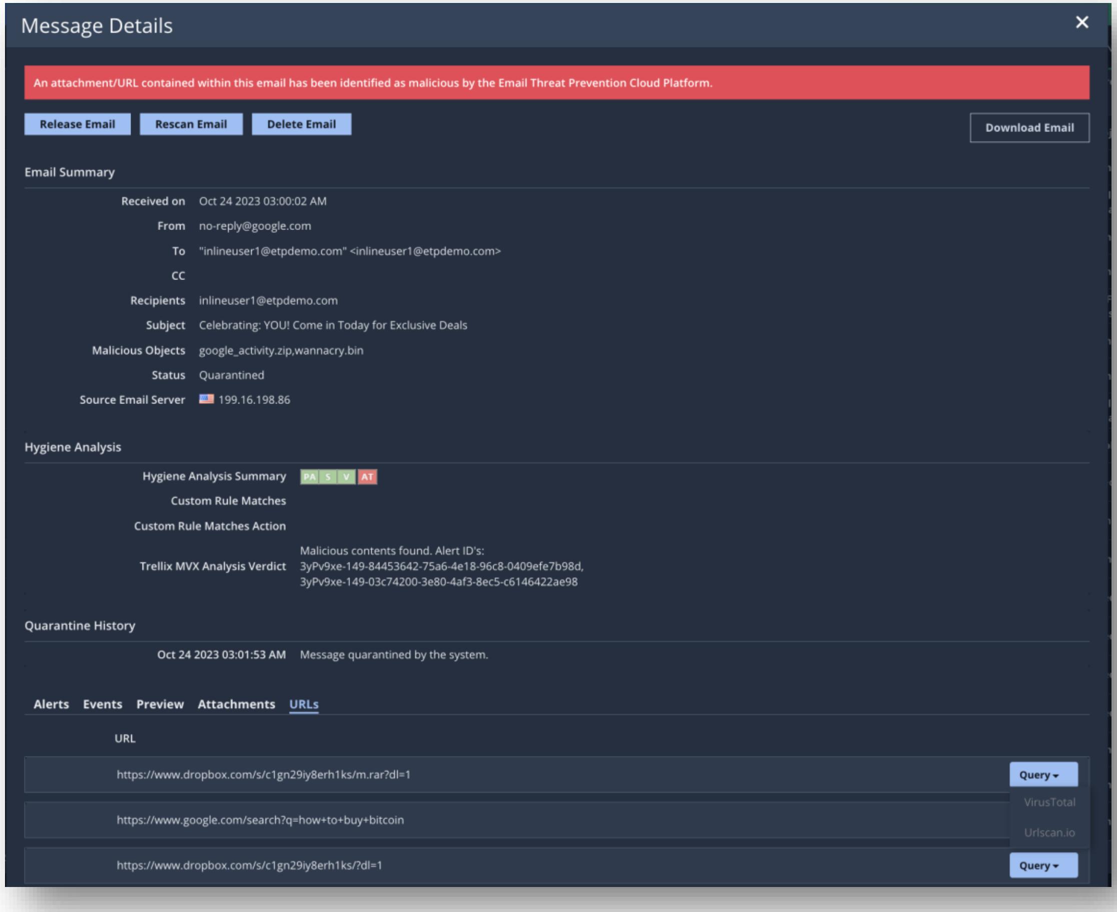
Results

Malware
100%
Protection

Malicious Attachments

	Protection
Trellix Email Security	100%
Microsoft Defender	91%
WithSecure Email Security	76%
Google Workspace Enterprise	43%
Mailcow Open-Source Solution	41%

Email Security – Cloud Portal



An attachment/URL contained within this email has been identified as malicious by the Email Threat Prevention Cloud Platform.

Email Summary

Received on	Oct 24 2023 03:00:02 AM
From	no-reply@google.com
To	"inlineuser1@etpdemo.com" <inlineuser1@etpdemo.com>
CC	
Recipients	inlineuser1@etpdemo.com
Subject	Celebrating: YOU! Come in Today for Exclusive Deals
Malicious Objects	google_activity.zip,wannacry.bin
Status	Quarantined
Source Email Server	199.16.198.86

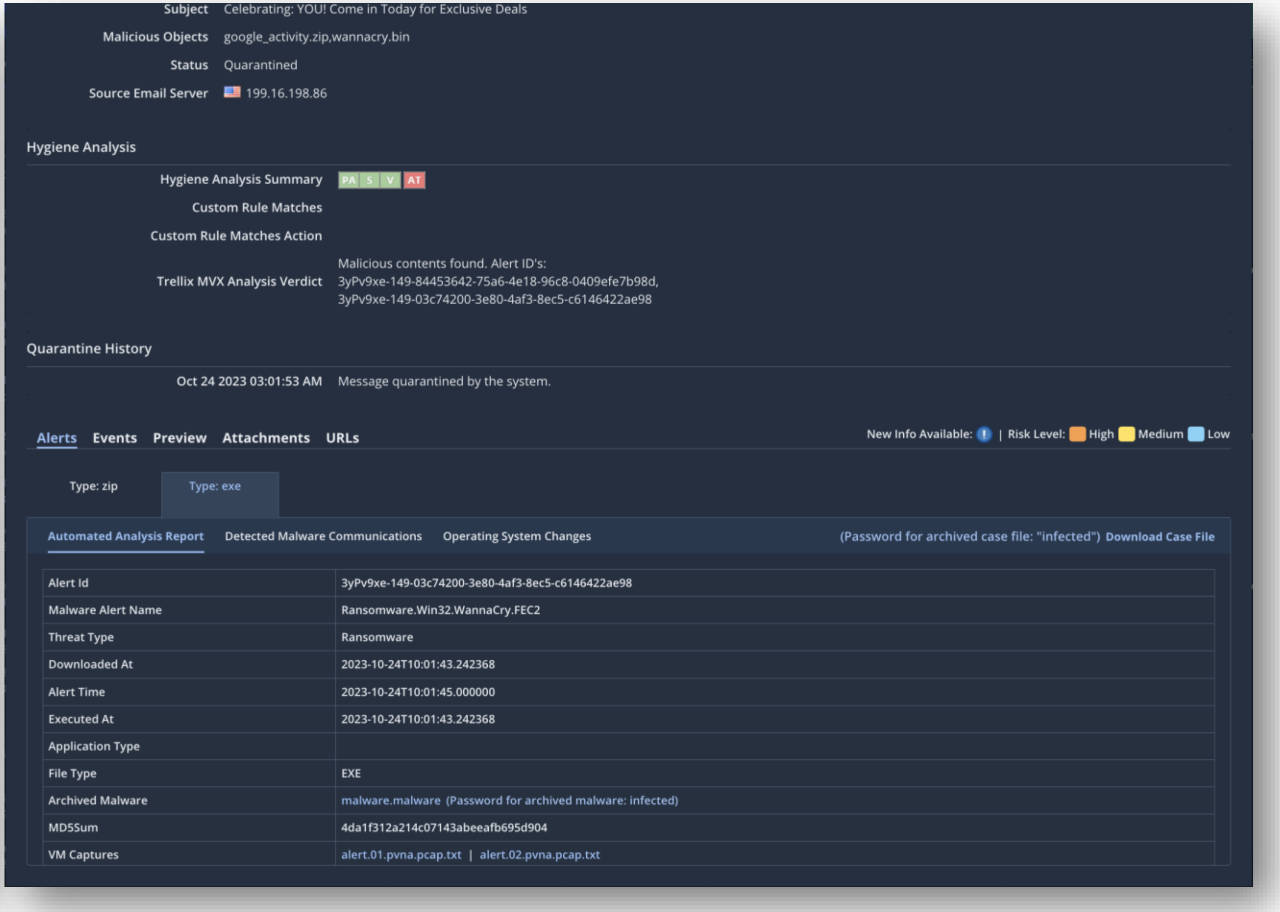
Hygiene Analysis

Hygiene Analysis Summary	PA S V AT
Custom Rule Matches	
Custom Rule Matches Action	
Trellix MVX Analysis Verdict	Malicious contents found. Alert ID's: 3yPv9xe-149-84453642-75a6-4e18-96c8-0409efe7b98d, 3yPv9xe-149-03c74200-3e80-4af3-8ec5-c6146422ae98

Quarantine History

Oct 24 2023 03:01:53 AM	Message quarantined by the system.

URL
https://www.dropbox.com/s/c1gn29iy8erh1ks/m.rar?dl=1
https://www.google.com/search?q=how+to+buy+bitcoin
https://www.dropbox.com/s/c1gn29iy8erh1ks/?dl=1



Subject	Celebrating: YOU! Come in Today for Exclusive Deals
Malicious Objects	google_activity.zip,wannacry.bin
Status	Quarantined
Source Email Server	199.16.198.86

Hygiene Analysis

Hygiene Analysis Summary	PA S V AT
Custom Rule Matches	
Custom Rule Matches Action	
Trellix MVX Analysis Verdict	Malicious contents found. Alert ID's: 3yPv9xe-149-84453642-75a6-4e18-96c8-0409efe7b98d, 3yPv9xe-149-03c74200-3e80-4af3-8ec5-c6146422ae98

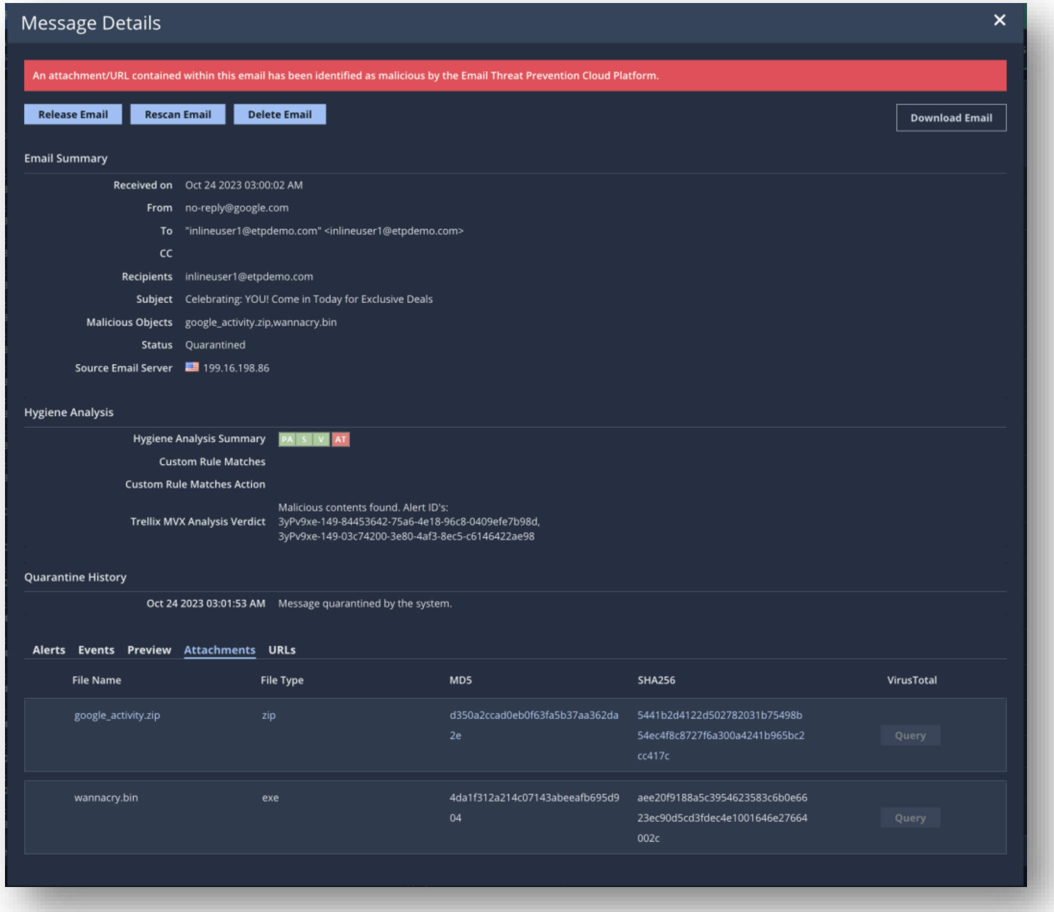
Quarantine History

Oct 24 2023 03:01:53 AM	Message quarantined by the system.

(Password for archived case file: "infected")

Alert Id	3yPv9xe-149-03c74200-3e80-4af3-8ec5-c6146422ae98
Malware Alert Name	Ransomware.Win32.WannaCry.FEC2
Threat Type	Ransomware
Downloaded At	2023-10-24T10:01:43.242368
Alert Time	2023-10-24T10:01:45.000000
Executed At	2023-10-24T10:01:43.242368
Application Type	
File Type	EXE
Archived Malware	malware.malware (Password for archived malware: infected)
MD5Sum	4da1f312a214c07143abeeafb695d904
VM Captures	alert.01.pvna.pcap.txt | alert.02.pvna.pcap.txt

Email Security – Cloud Portal



An attachment/URL contained within this email has been identified as malicious by the Email Threat Prevention Cloud Platform.

Email Summary

Received on	Oct 24 2023 03:00:02 AM
From	no-reply@google.com
To	"inlineuser1@etpdemo.com" <inlineuser1@etpdemo.com>
CC	
Recipients	inlineuser1@etpdemo.com
Subject	Celebrating: YOU! Come in Today for Exclusive Deals
Malicious Objects	google_activity.zip,wannacry.bin
Status	Quarantined
Source Email Server	199.16.198.86

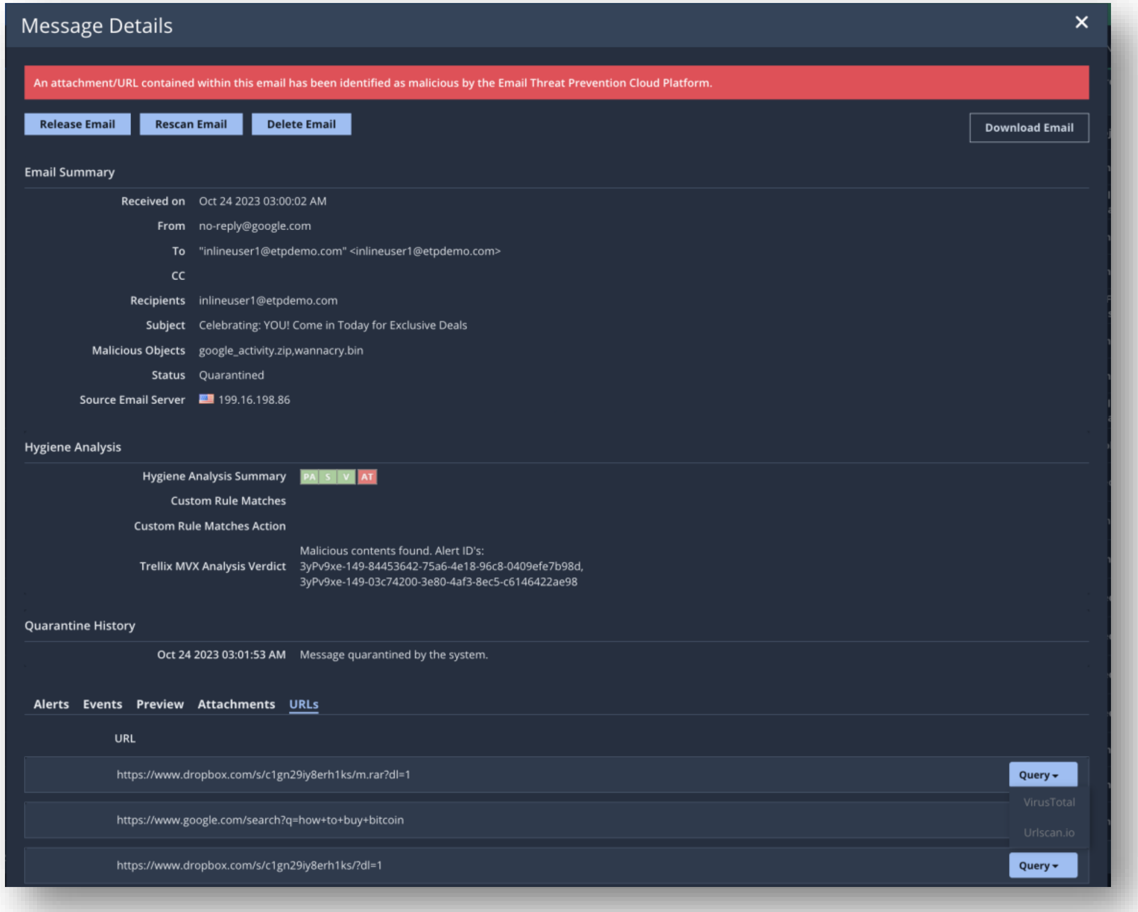
Hygiene Analysis

Hygiene Analysis Summary	🟩 PA 🟩 S 🟩 V 🟥 AT
Custom Rule Matches	
Custom Rule Matches Action	
Trellix MVX Analysis Verdict	Malicious contents found. Alert ID's: 3yPv9xe-149-84453642-75a6-4e18-96c8-0409efe7b98d, 3yPv9xe-149-03c74200-3e80-4af3-8ec5-c6146422ae98

Quarantine History

Oct 24 2023 03:01:53 AM	Message quarantined by the system.

File Name	File Type	MD5	SHA256	VirusTotal
google_activity.zip	zip	d350a2ccad0eb0f63fa5b37aa362da2e	5441b2d4122d502782031b75498b54ec4f8c8727f6a300a4241b965bc2cc417c	Query
wannacry.bin	exe	4da1f312a214c07143abeeafb695d904	aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c	Query



An attachment/URL contained within this email has been identified as malicious by the Email Threat Prevention Cloud Platform.

Email Summary

Received on	Oct 24 2023 03:00:02 AM
From	no-reply@google.com
To	"inlineuser1@etpdemo.com" <inlineuser1@etpdemo.com>
CC	
Recipients	inlineuser1@etpdemo.com
Subject	Celebrating: YOU! Come in Today for Exclusive Deals
Malicious Objects	google_activity.zip,wannacry.bin
Status	Quarantined
Source Email Server	199.16.198.86

Hygiene Analysis

Hygiene Analysis Summary	🟩 PA 🟩 S 🟩 V 🟥 AT
Custom Rule Matches	
Custom Rule Matches Action	
Trellix MVX Analysis Verdict	Malicious contents found. Alert ID's: 3yPv9xe-149-84453642-75a6-4e18-96c8-0409efe7b98d, 3yPv9xe-149-03c74200-3e80-4af3-8ec5-c6146422ae98

Quarantine History

Oct 24 2023 03:01:53 AM	Message quarantined by the system.

URL	
https://www.dropbox.com/s/c1gn29iy8erh1ks/m.rar?dl=1	Query ▾
https://www.google.com/search?q=how+to+buy+bitcoin	
https://www.dropbox.com/s/c1gn29iy8erh1ks/?dl=1	Query ▾

Results

Social Engineering

	Protection
Trellix Email Security	100%
Microsoft Defender	56%
WithSecure Email Security	0%
Google Workspace Enterprise	2%
Mailcow Open-Source Solution	1%

Moving beyond email to protect employee collaboration

Digital transformation has introduced a new threat vector

Extended Enterprise

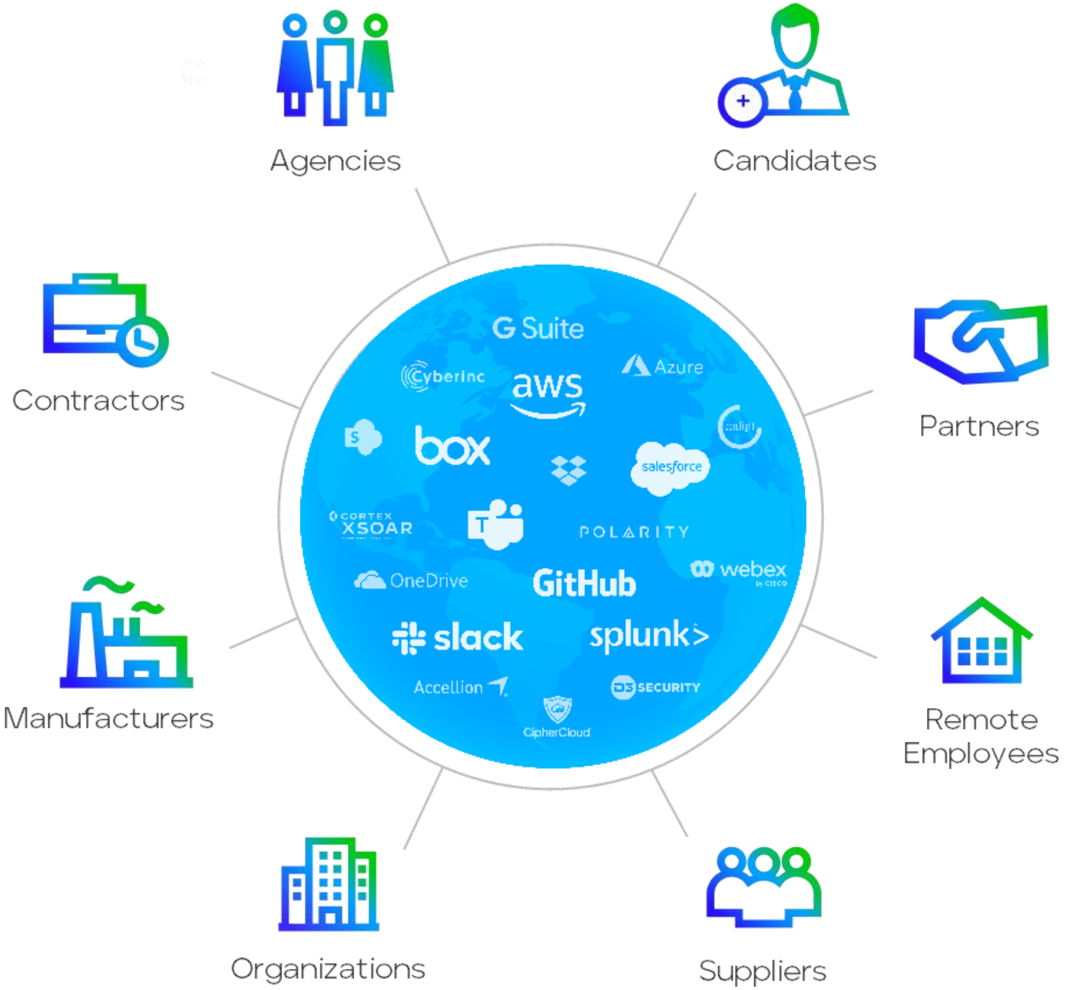
Business agility and innovation require third-party relationships to extend enterprise capabilities

Digital Transformation

Digitally-enabled partner ecosystem creates significant risk exposure

SaaS Insecurity

Vendors secure their platform but don't worry that they provide an open door to your environment



The Staistics

Digital transformation

82%

Reported a breach as a result of digital transformation[1]

Third party exposure

55%

At least one breach occurred through a third party[1]

Uncertainty

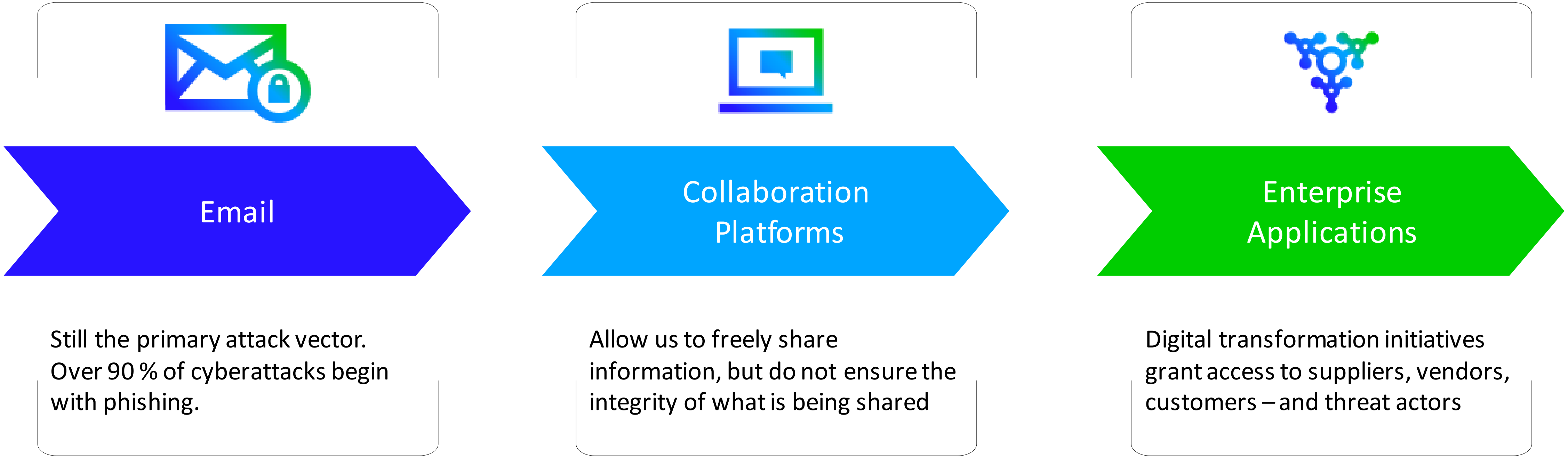
53%

Security readiness untested in their digital transformation[2]

[1] Ponemon, “Digital Transformation is Increasing Cyber Risk”
[2] Gartner, “IT Roadmap for Digital Business Transformation”

The nature and velocity of collaboration has changed

Creating three main fronts to defend



Email

Still the primary attack vector. Over 90 % of cyberattacks begin with phishing.

Collaboration Platforms

Allow us to freely share information, but do not ensure the integrity of what is being shared

Enterprise Applications

Digital transformation initiatives grant access to suppliers, vendors, customers – and threat actors

And our adversaries adapt

Attackers compromised employee accounts by tricking them into downloading a malicious file, disguised as a legitimate Excel document

Attackers created a google drive document with malicious links and tagged victims, asking them to login to provide feedback.

Attackers gained access to the GitHub repositories of several companies by sharing a malicious file on the platform.

How can we secure collaboration platforms?

Trellix Collaboration Security

Trellix

What is Trellix IVX for Collaboration Security?

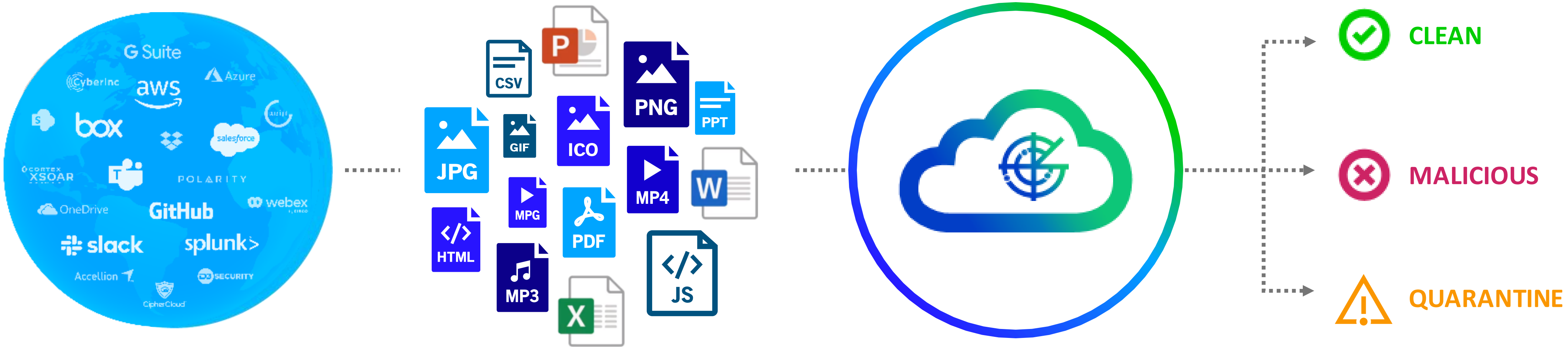
Cloud-based threat detection that pinpoints known and unknown malware

Applications supported

File types supported

Comprehensive, multi-layered detection

Verdict



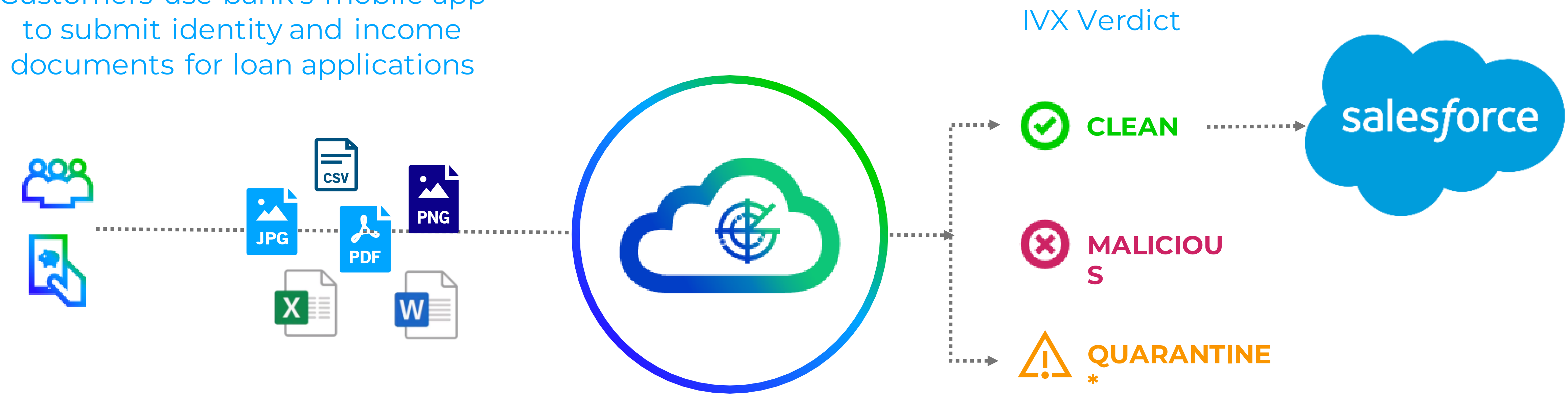
CLEAN

MALICIOUS

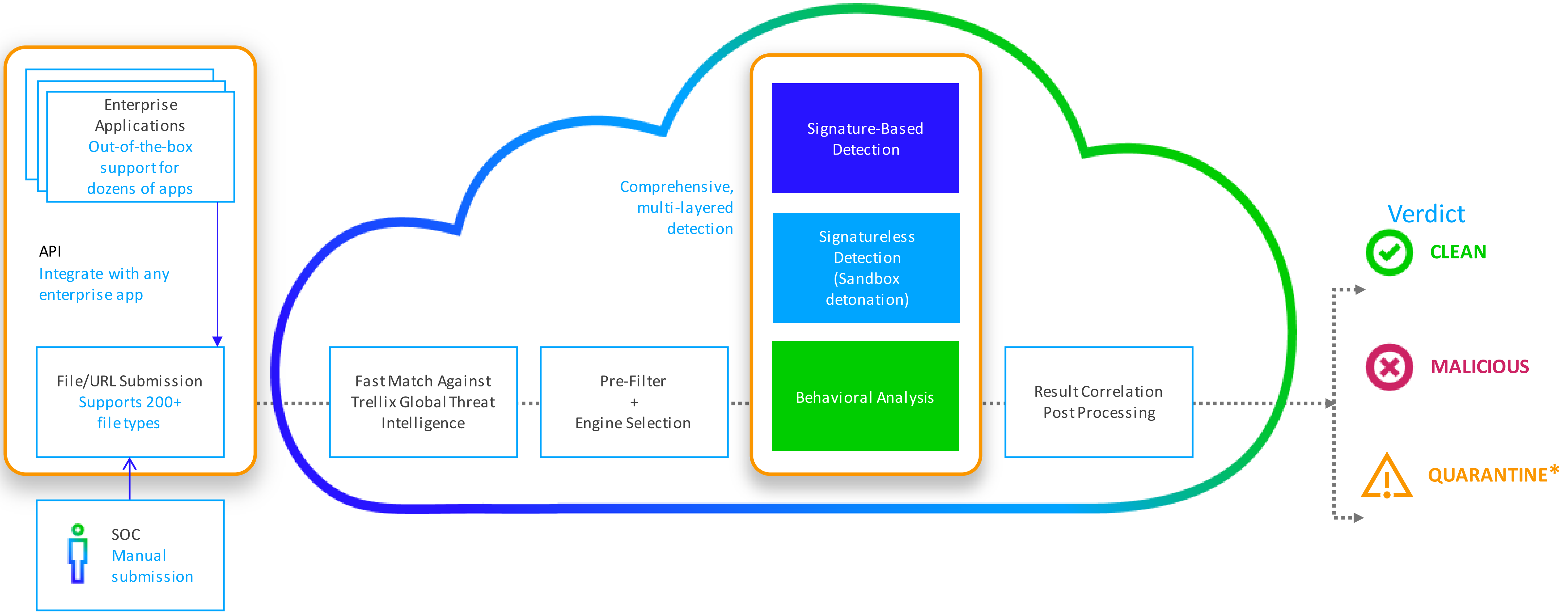
QUARANTINE

IVX blends into existing workflows

Customers use bank’s mobile app to submit identity and income documents for loan applications



Trellix IVX - How it works



Enterprise Applications
Out-of-the-box support for dozens of apps

API
Integrate with any enterprise app

File/URL Submission
Supports 200+ file types

SOC
Manual submission

Comprehensive, multi-layered detection

Fast Match Against Trellix Global Threat Intelligence

Pre-Filter
+
Engine Selection

Signature-Based Detection

Signatureless Detection (Sandbox detonation)

Behavioral Analysis

Result Correlation Post Processing

Verdict

CLEAN

MALICIOUS

QUARANTINE*

Custom-built for malware analysis at speed and scale

Hardened Hypervisor

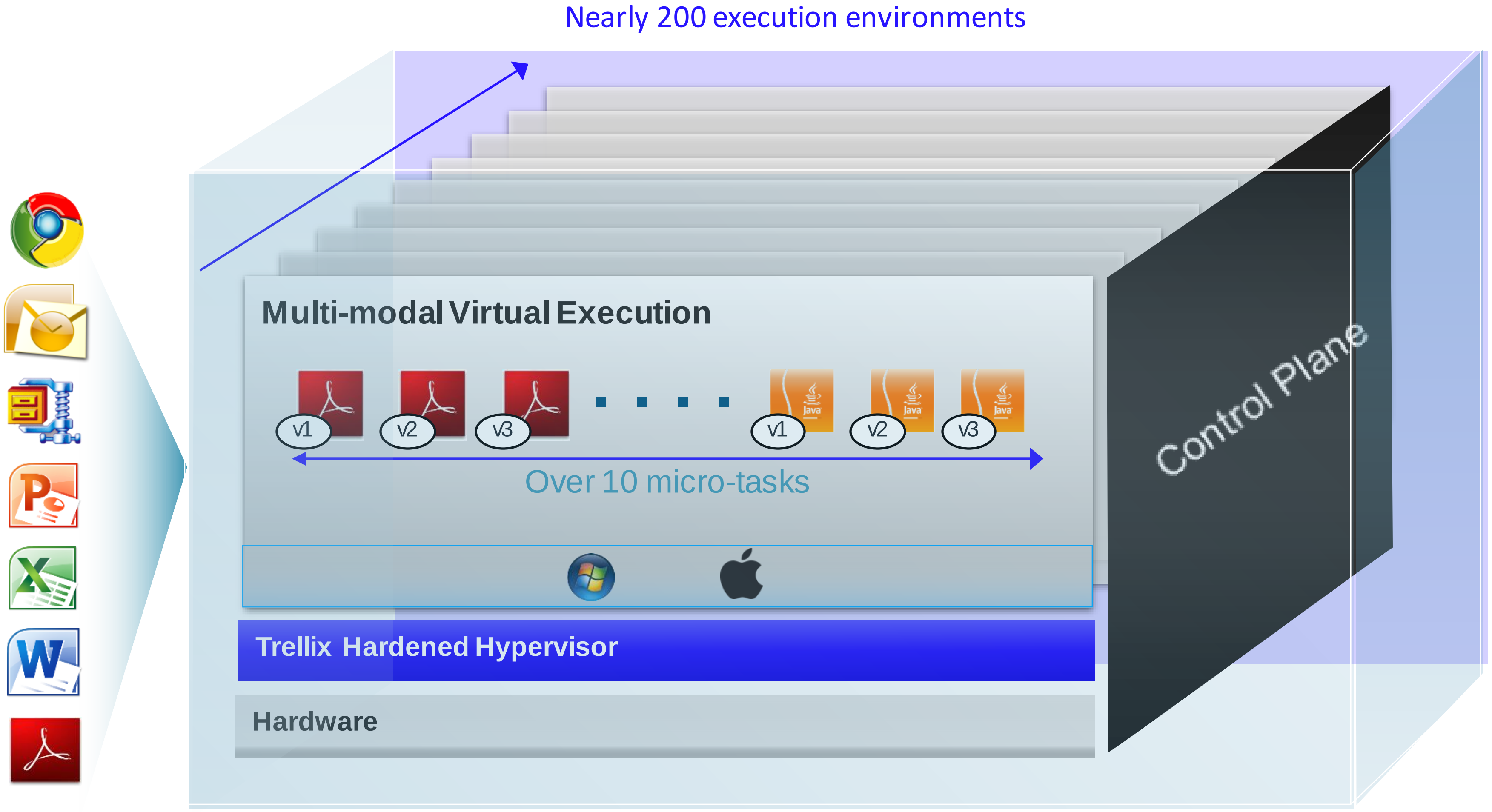
- Designed for large scale threat analysis
- Custom hypervisor with built-in countermeasures
- Detect sandbox-aware and evasion tactics

Multi-modal Virtual Execution

- Multiple operating systems
- Multiple service packs
- Multiple applications
- Multiple file-types

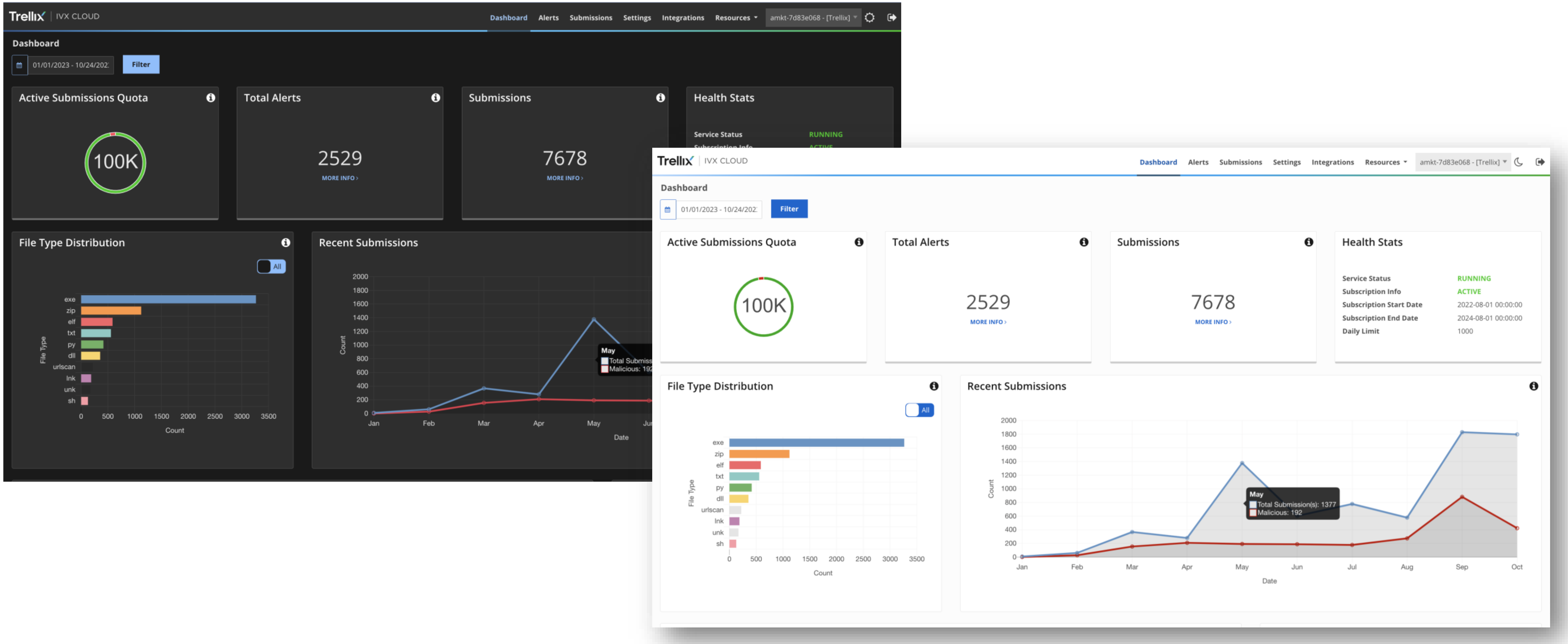
Threat Protection at Scale

- Multi-stage analysis
- Over 2000 simultaneous executions


Nearly 200 execution environments
Multi-modal Virtual Execution
v1
v2
v3
v1
v2
v3
Over 10 micro-tasks
Trellix Hardened Hypervisor
Hardware
Control Plane

Trellix

IVX Cloud Portal



Dashboard

01/01/2023 - 10/24/202

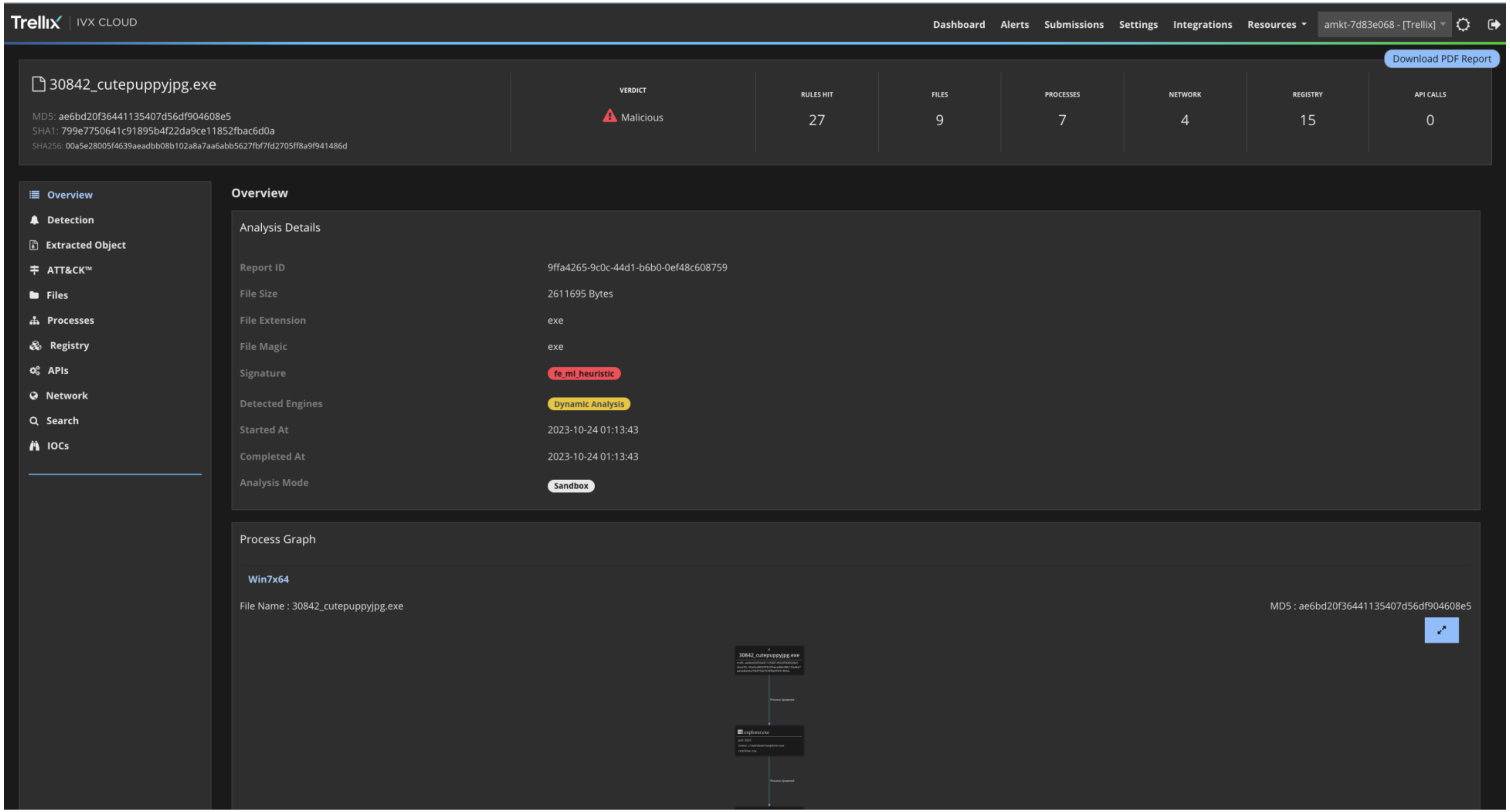
Total Alerts: 2529

Submissions: 7678

Service Status	RUNNING
Subscription Info	ACTIVE
Subscription Start Date	2022-08-01 00:00:00
Subscription End Date	2024-08-01 00:00:00
Daily Limit	1000

May
Total Submission(s): 1377
Malicious: 192

IVX Cloud Portal



30842_cutepuppyjpg.exe

MD5: ae6bd20f36441135407d56df904608e5
SHA1: 799e7750641c91895b4f22da9ce11852fbac6d0a
SHA256: 00a5e28005f4639aeadbb08b102a8a7aa6abb5627fbf7fd2705ff8a9f941486d

VERDICT	RULES HIT	FILES	PROCESSES	NETWORK	REGISTRY	API CALLS
Malicious	27	9	7	4	15	0

Overview

Analysis Details

Report ID	9ffa4265-9c0c-44d1-b6b0-0ef48c608759
File Size	2611695 Bytes
File Extension	exe
File Magic	exe
Signature	fe_ml_heuristic
Detected Engines	Dynamic Analysis
Started At	2023-10-24 01:13:43
Completed At	2023-10-24 01:13:43
Analysis Mode	Sandbox

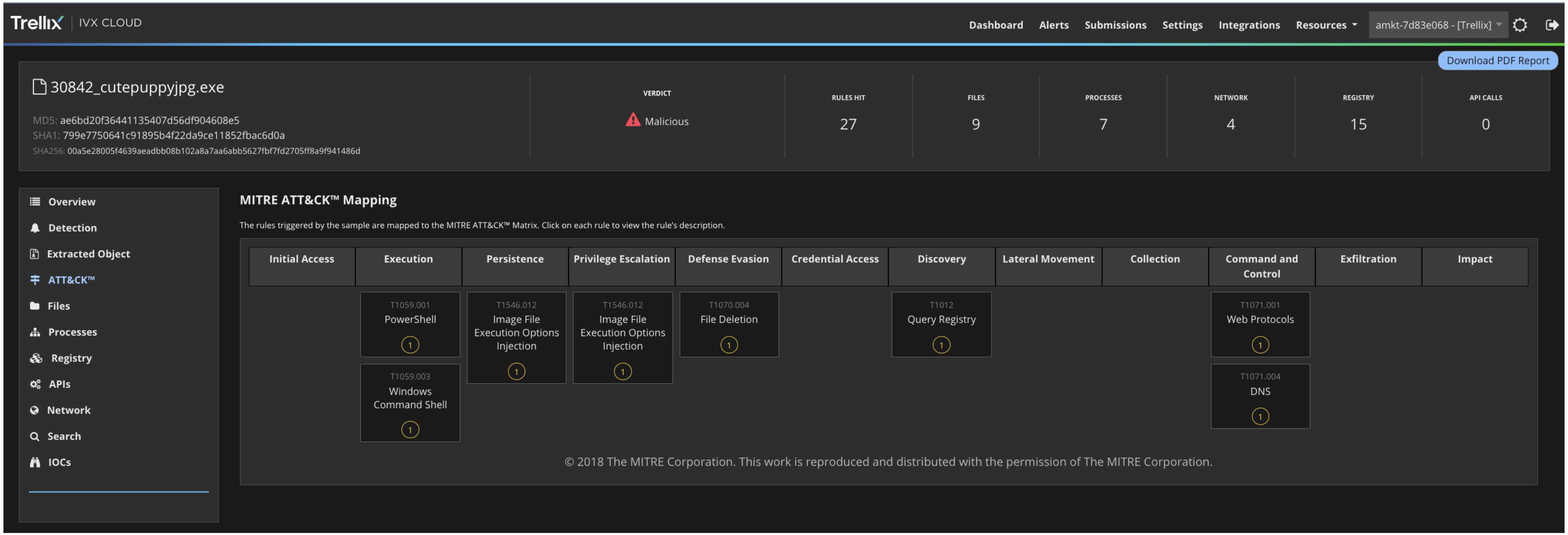
Process Graph

Win7x64

File Name : 30842_cutepuppyjpg.exe

MD5 : ae6bd20f36441135407d56df904608e5

IVX Cloud Portal



30842_cutepuppyjpg.exe

MD5: ae6bd20f36441135407d56df904608e5
SHA1: 799e7750641c91895b4f22da9ce11852fbac6d0a
SHA256: 00a5e28005f4639aeadbb08b102a8a7aa6abb5627fbf7fd2705ff8a9f941486d

VERDICT	RULES HIT	FILES	PROCESSES	NETWORK	REGISTRY	API CALLS
⚠ Malicious	27	9	7	4	15	0

MITRE ATT&CK™ Mapping

The rules triggered by the sample are mapped to the MITRE ATT&CK™ Matrix. Click on each rule to view the rule's description.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	T1059.001 PowerShell 1	T1546.012 Image File Execution Options Injection 1	T1546.012 Image File Execution Options Injection 1	T1070.004 File Deletion 1		T1012 Query Registry 1			T1071.001 Web Protocols 1		
	T1059.003 Windows Command Shell 1								T1071.004 DNS 1		

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Trellix

Thank You!

Grazie! ¡Gracias!