Lessons learned while PROTECTING GMAIL

Elie Bursztein, Nicolas Lidzborski, & Vijay Eranti
THE GMAIL SECURITY AND ANTI-ABUSE TEAM
LESSONS WE’VE LEARNED WHILE protecting Gmail users for over a decade
5 MAIN THREATS TO GMAIL
5 MAIN THREATS TO GMAIL

Malware

Account Hijacking
5 MAIN THREATS TO GMAIL

- Malware
- Account Hijacking
- Phishing
5 MAIN THREATS TO GMAIL

- Malware
- Account Hijacking
- XSS
- Web Attacks
- Phishing
5 MAIN THREATS TO GMAIL
900 MILLION+ USERS

hundreds of billions of messages per week
We launched login challenges in 2011.
Phishers updated their kits to ask for the challenge answers

NEVER STOP IMPROVING YOUR DEFENSES
THERE IS NO SILVER BULLET

99.9% accuracy detecting spammy email

91.7%
Large linear ML classifier

+4.7%
rule based system

+3.5%
deep learning

? Next gen

http://goo.gl/0jgK96 *incremental coverage measurement
TUNE YOUR CLASSIFIER

to match your product need

- False Negative: less than 0.1%
  - Spam classified as good

- False Positive: less than 0.05%
  - Good classified as Spam

[https://goo.gl/0jgK96](https://goo.gl/0jgK96)
You have missed mails meals

Google+Team <dcrosbie@trimac.com>

Jan 13 (9 days ago)

Be careful with this message. Many people marked similar messages as phishing scams, so this might contain unsafe content. Learn more

Google+

You have missed mail.

View mails.

Best regards
Google+ team

This mail was sent to [email protected] Don't want occasional updates about Google+ activity and friend suggestions? Change what mail Google+ sends you. Google Inc., 1600 Amphitheatre Pkwy, Mountain View, CA 94043 USA

IMPLEMENT CATCH-UP MECHANISMS
EMPOWER USERS
to take action through meaningful UI

USE OVERWHELMING FORCE

Deploy many countermeasures at once
EMAIL ATTACHMENT
ATTACKS COME IN BURSTS

plan for it
DON'T PROCESS TWICE

Whitelisting and blacklisting allows up to 50% reduction in computation
Gmail does not allow executable attachments.
USE ENSEMBLE LEARNING

multiple anti-viruses are combined

Caching
Policy
Multiple Engines

![Diagram showing the funnel process of Caching, Policy, and Multiple Engines leading to the use of ensemble learning for anti-virus detection.]

The diagram illustrates how multiple anti-virus engines are combined using ensemble learning techniques. The right side of the image includes a graph showing the F1 score across different numbers of anti-virus engines, with lines representing various strategies such as Union, Majority Voting, Logit, RF, and Bayes.

- **Caching**
- **Policy**
- **Multiple Engines**

The graph on the right shows the F1 score for different numbers of anti-virus engines, with lines indicating the performance of strategies like Logit, RF, and Bayes. The legend specifies different thresholds and engine configurations.

---

**Legend**
- **Union**
- **Majority Voting**
- **Logit_wo_family**
- **RF_wo_family**
- **Bayes_wo_family**
- **Logit_with_family**
- **RF_with_family**
- **Bayes_with_family**

**Thresholds**
- Threshold = 3
- Threshold = 5
USE DYNAMIC EXECUTION to catch undetected malwares (very rare)
Implement Emergency Blocking Systems

Unpredictable attacks and bugs happen. Get as ready as possible for it.
Encrypt everything in transit and at rest

INBOUND
62%
Messages from other providers to Gmail are encrypted

OUTBOUND
82%
Messages from Gmail to other providers are encrypted

https://goo.gl/iv2tlA * Gmail always tries to encrypt email communication. Encryption failures are due to other providers not supporting encryption
Closure Templates Strict Autoescaping

{template .page autoescape="strict"}
<a href="${profile.blogUrl}">

VS

Manual and Unsafe Escaping

{template .page}
<a href="${profile.blogUrl | sanitizeUrl}"
Number of XSS affecting Gmail webmail fixed per quarter

BE METRICS DRIVEN
PREVENT BUGS THROUGH GOOD SOFTWARE DESIGN
CSP blocks a lot of bad stuff

CSP helped us identify potential XSS

Smart labels potential XSS

```html
<! <img src=""> <img src=x onerror=alert(1)// >
```
IMPLEMENT DEFENSE IN DEPTH

- Deep Learning
- Encryption
- Linear Classifiers
- Antivirus
- Security audits
- Static Analyzers
- Auto-escaping
- Fuzzing
- DDOS prevention
- Dynamic Execution
- CSP
PAY FOR BUGS

it's worth it
KEY CHALLENGES IN 2016

Dynamic rendering
CSS, Javascript. E.g Media Queries

Hacked site
Good sites used in phishing attacks

Email security standards
Yet to be fully adopted

Advanced phishing attacks
E.g spear phishing
KEY TAKEAWAYS

Combine detection technologies in each layer
There is no silver bullet so diversification is key to lasting security.

Defense in depth
Add multiple layers of security because sooner or later an attacker will break one.

Have a strong team that keeps running
It takes all your efforts to keep the product clean. No rest for the brave.
Thank you!