

# Beyond phishing emails



# DISCLAIMER!

All the content of this presentation  
is based on my personal research  
and doesn't represent my  
employer's views.

# DISCLAIMER!

All the content of this presentation  
is based on real world phishing  
attacks. No 0days.

# whoami

- **Anastasios Pingios (@xorlgr)**
  - Principal Security Engineer @ Booking.com
  - Contributor at MITRE ATT&CK framework
  - xorl.wordpress.com (not very active lately)
  - Been around security since 2000s from both sides of the fence



# agenda

- Why phishing beyond emails?
- The story of Keeping Secrets Inc.
- Learnings for a red teamer
- Learnings for a blue teamer
- Q/A

# What is phishing?

*Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication*

# What is phishing?

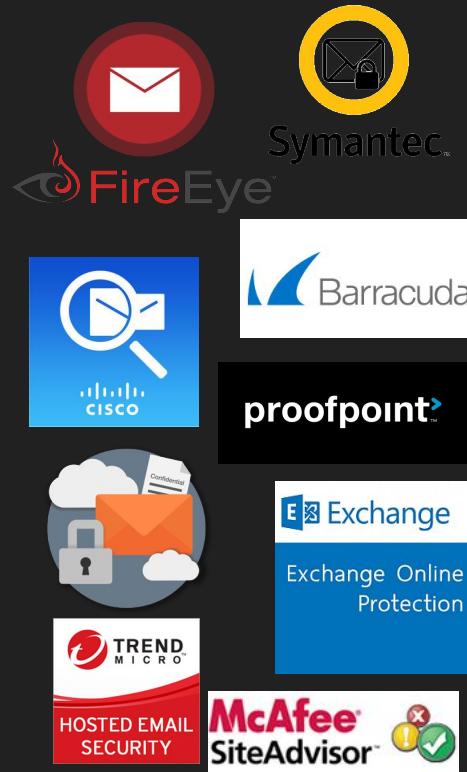
*Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication*

# Why phishing beyond emails?

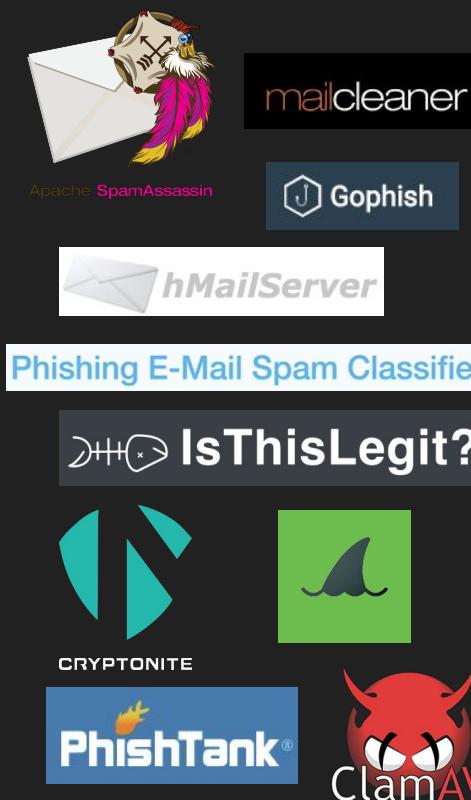
## Technologies

SPF	SPAM FILTER
DMARC	AV
DKIM	RESTRICTIONS
DLP	TLS
S/MIME	ML & NLP CLASSIFICATION
PGP	
POLICIES	

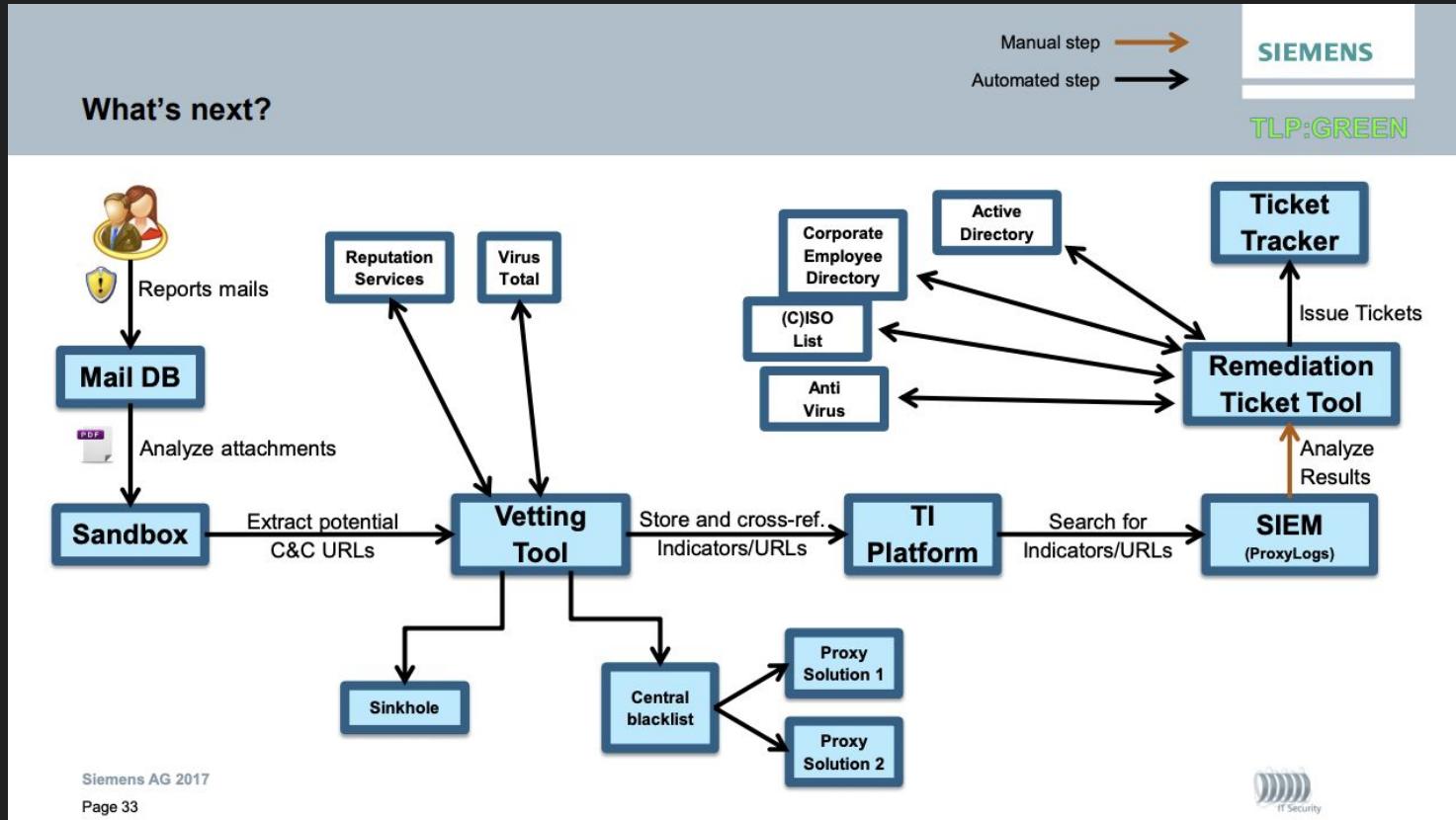
## Enterprise solutions



## Free/Open Source



# Why phishing beyond emails?



Source:

<https://www.first.org/resources/papers/conf2017/You-Dont-Need-a-Better-Car-You-Need-to-Learn-How-to-Drive-On-the-Importance-of-Cyber-Defense-Line-Automation.pdf>

# Why phishing beyond emails?

- Most defenders don't have incident response playbooks
- Catching people off guard
- Stealthy
- It's fun!

*Even the finest sword plunged into salt water will eventually rust*  
*Sun Tzu, The Art of War*



# The story of Keeping Secrets Inc.

A screenshot of a web browser displaying the homepage of Keeping Secrets Inc. The page has a dark header with a search bar containing 'keepingsecrets-inc'. Below the header is a navigation bar with links for 'Company', 'Products', and 'About'. To the right of the navigation are icons for a shopping cart, user profile, and a menu. The main content area features a large circular logo in the center. The logo contains a black key icon with intricate designs and the text 'KEEPING SECRETS INC.' below it. Below the logo is a grey button with the text 'Start now!'. To the left of the logo is a section labeled 'Contact us' with a graphic of a grid pattern. To the right of the logo are social media icons for Facebook and Twitter, along with a 'Best rated' badge featuring three blue stars.

keepingsecrets-inc

Keeping Secrets Inc.

Company Products About

Start now!

Contact us

Best rated

KEEPING  
SECRETS INC.

Facebook Twitter

# The story of Keeping Secrets Inc.

A screenshot of a web browser window displaying the homepage of "Keeping Secrets Inc.". The browser interface includes standard controls (red, yellow, green buttons) and a search bar with the text "keepingsecrets-inc".

The website header features a stylized key icon followed by the company name "Keeping Secrets Inc.". Below the header is a navigation menu with links to "Company", "Products", and "About". On the right side of the header are icons for a shopping cart and user profile.

The main content area contains a large, red, cartoonish character with a grumpy expression and black spikes on its head. To the right of the character is a purple circular logo containing a black key and the text "KEEPING SECRETS INC.". Below the logo is a grey button labeled "Start now!".

At the bottom of the page, there is a "Contact us" section featuring a graphic of a grid with colored cells (white, grey, green, yellow). To the right of this graphic is a "Best rated" section with three blue star icons and social media links for Facebook and Twitter.

# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

# The story of Keeping Secrets Inc.

RECON

- Google dorks
- LinkedIn / company website
- OSINT

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

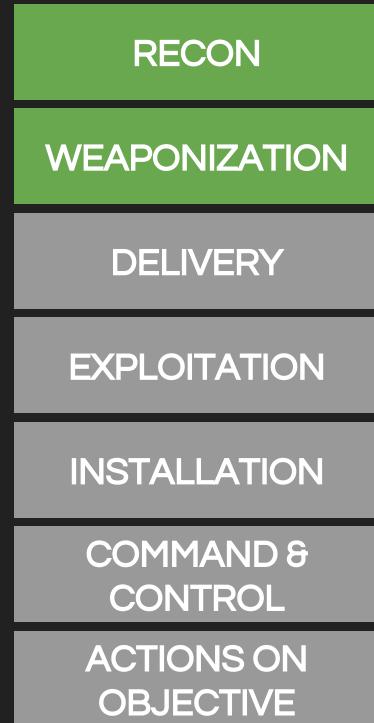
COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

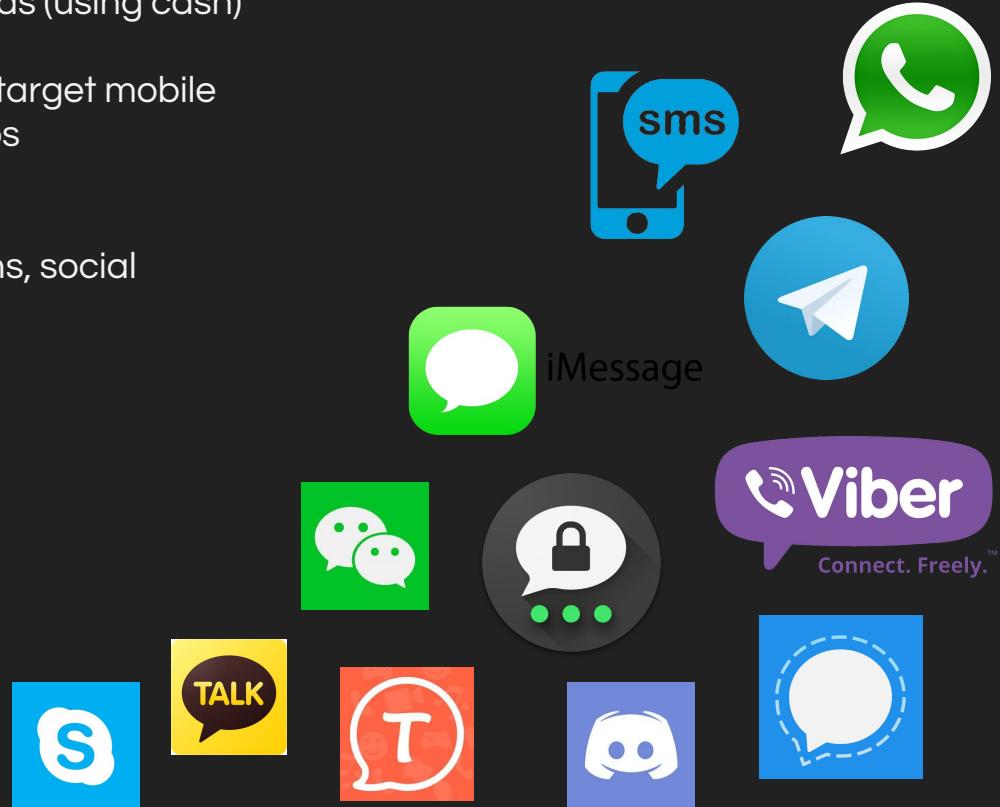
Targets:

- Usernames
- Phone numbers
- Email addresses
- Communication platforms
- Sample of messages

# The story of Keeping Secrets Inc.



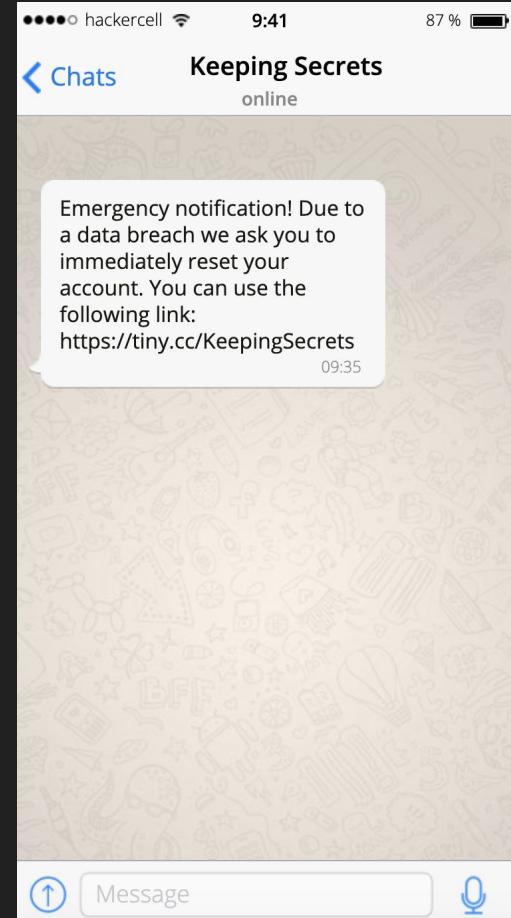
- Get prepaid SIM cards (using cash)
- Set up accounts on target mobile communication Apps
- Standard phishing preparation (domains, social engineering, etc.)



# The story of Keeping Secrets Inc.



- Standard phishing best practices
- Get advantage of preview functionality
- Additional capabilities
  - Ability to install mobile malware
  - Steal 2FA tokens
  - Turn the phone to a rogue AP
  - Pivot point for lateral movement



# The story of Keeping Secrets Inc.

RECON

Keeping Secrets Inc. was prepared for this!

WEAPONIZATION

- ✓ MDM on all mobile devices with access to corporate resources

DELIVERY

- ✓ Enterprise versions of communication platforms with centralized logging integrated to SIEM and threat detection platforms

EXPLOITATION

- ✓ Easy way for users to report suspicious activity

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE



# The story of Keeping Secrets Inc.

RECON

- Google dorks
- OSINT

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

Targets:

- Credentials
- Communication platforms
- Externally accessible platforms

# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

- Accessing platforms externally
- Credential stuffing attacks
- Standard phishing preparation (domains, social engineering, etc.)



# The story of Keeping Secrets Inc.

RECON

- Standard phishing best practices

WEAPONIZATION

- Get advantage of preview functionality

DELIVERY

- Additional capabilities

EXPLOITATION

- Collect insider information
- Use it to monitor activity in case of being discovered
- Ability to abuse to internal applications

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE



# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

Keeping Secrets Inc. was prepared for this too!

- ✓ 2FA for all externally accessible platforms
- ✓ Proxy with threat detection for all comms
- ✓ Preview with suspicious site detection
- ✓ Separation of duties/access control on different channels based on role definitions



# The story of Keeping Secrets Inc.



# The story of Keeping Secrets Inc.

RECON

Initial recon discovered various social media platforms and other communities used:

WEAPONIZATION

- Social media
- Forums
- Blogs
- News websites

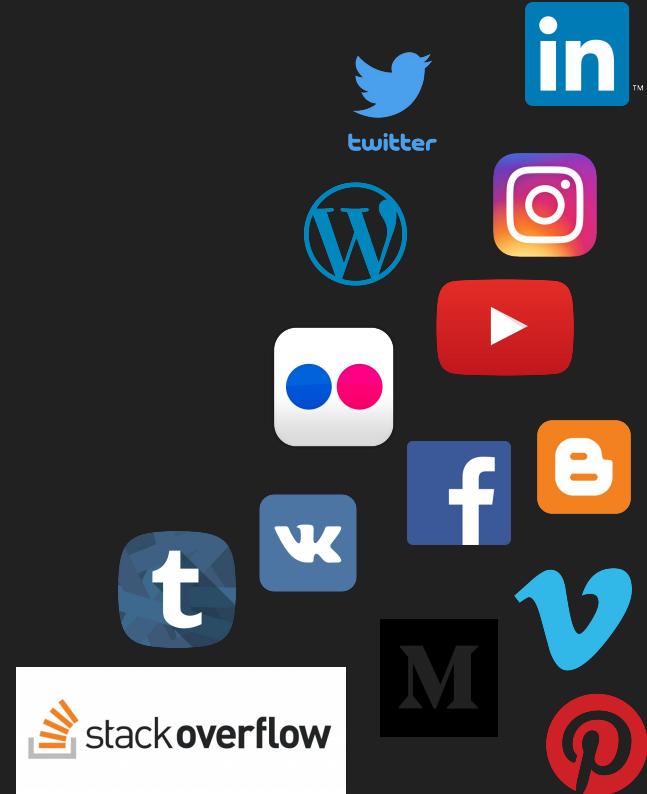
DELIVERY

EXPLOITATION

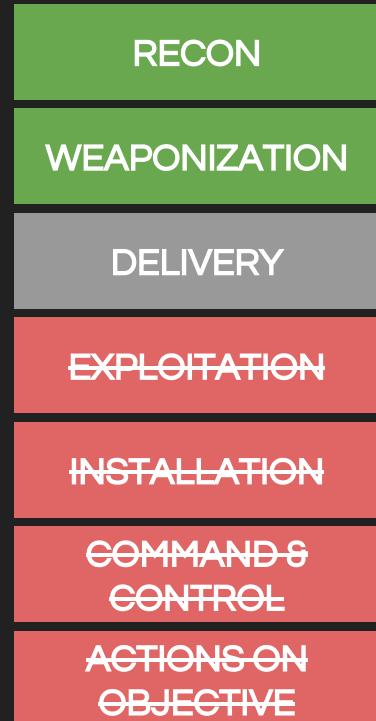
INSTALLATION

COMMAND &  
CONTROL

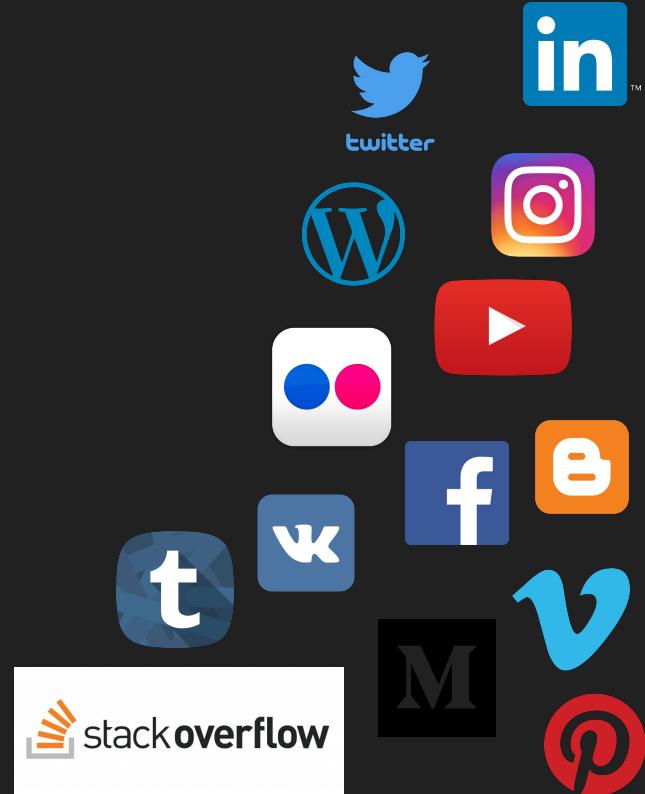
ACTIONS ON  
OBJECTIVE



# The story of Keeping Secrets Inc.



- Create anonymous accounts/personas
- Standard phishing preparation (domains, social engineering, etc.)



# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

- Standard phishing best practices
- Additional capabilities
  - Easier for social engineering
  - Rich text editors make hiding links easier
  - Many social media, forums, blogs, etc.  
Allow users to modify or delete their comments and posts.

Message:



Today, 05:51

money  
Junior Member

Join Date: Dec 2018

Posts: 21

Reputation: 0 [+/-]

Balance: 0.00\$

Hi all,

This is pretty simple to do, here are some steps to make it happen:

1. First login to this [mistakenly exposed page](#)
2. Go to the menu
3. Download secrets!

# The story of Keeping Secrets Inc.

*But ...*

# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

The attack was thwarted once again.

- ✓ Enterprise browsers
- ✓ Next generation web gateway
- ✓ Secure application gateways

**GREAT SUCCESS!**



# The story of Keeping Secrets Inc.



G Suite

*Please note: GSuite is only an example, the same also applies to other providers of similar services*

# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

- Create GMail accounts/personas
- Standard phishing preparation (domains, social engineering, etc.)

# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

- Standard phishing best practices
- Additional capabilities
  - Trick the users by injecting calendar events without email notifications
  - Use document sharing modifications for your phishing message
  - Modify users' GSuite settings to get access to all of their resources
  - Use shared docs as pivot points for phishing links
  - Forms, Spreadsheet, Slides, etc.

Would you like to send invitation emails to Google Calendar guests?



Dismiss

Don't send

Send

URGENT: Important announcement  
Saturday, October 5 · 3:00 – 4:00pm

2 guests  
1 yes, 1 awaiting

Organizer: [REDACTED]@gmail.com  
[REDACTED]@gmail.com

Please check out the meeting agenda before joining the meeting.  
Meeting agenda: <https://tiny.cc/KeepingSecretsAgenda>

30 minutes before  
[REDACTED]@gmail.com

Going? Yes No Maybe

[REDACTED]@gmail.com has invited you to view the following document:

KeepingSecrets 2020 plan

Please sign up at <https://tiny.cc/KeepingSecrets2020> before the end of the day to get full access to the 2020 plan.

Open in Docs

Google Docs: Create and edit documents online.  
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA  
You have received this email because someone shared a document with you from Google Docs.

Google

# The story of Keeping Secrets Inc.



# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

Keeping Secrets Inc. nailed it!

- ✓ GSuite policies
- ✓ Only allowing authorized applications
- ✓ Not automatically added events to calendars
- ✓ Google is in fact working to permanently fix this!

459,024 views | Sep 9, 2019, 04:38am

## Google To Fix Malicious Invites Issue For 1 Billion Calendar Users



Davey Winder Senior Contributor @  
Cybersecurity

I report and analyse breaking cybersecurity and privacy stories



Google is finally working on a fix for a security problem that leaves more than a billion Calendar users exposed to attack. VISUAL CHINA GROUP VIA GETTY IMAGES

Source:

<https://www.forbes.com/sites/daveywinder/2019/09/09/google-finally-confirms-security-problem-for-15-billion-gmail-and-calendar-users/#5b7dc319279f>

# The story of Keeping Secrets Inc.

Keeping Secrets Inc. party is coming ...



# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

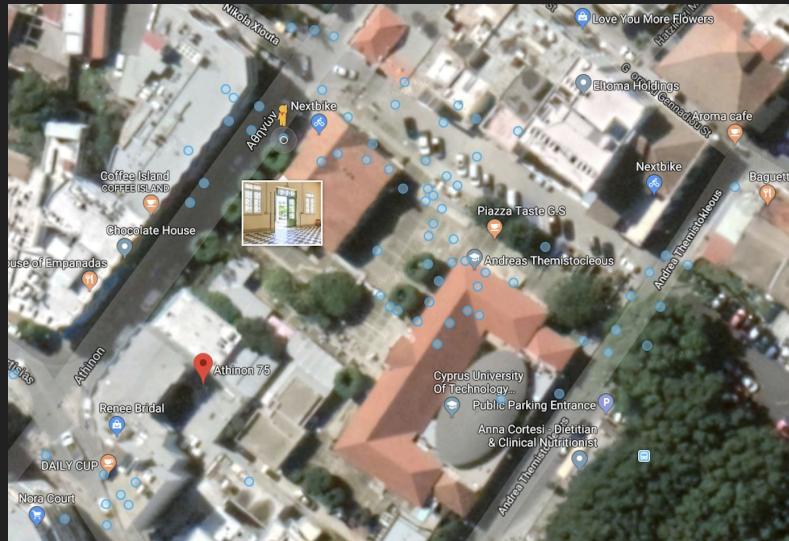
EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

- Event announcements
- Office addresses
- Using online street view services to
- Assess the physical security of the location



# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

- Generate QR codes, shortened links, etc.
- Print out stickers or identical flyers
- Plan out the intrusion (if necessary)
- Standard phishing preparation (domains, social engineering, etc.)



# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

- Standard phishing best practices
- Additional capabilities
  - You can do it remotely if printers are exposed over the internet
  - Most people trust QR codes more than clicking on links



# The story of Keeping Secrets Inc.

*Who thinks that this worked?*

# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

Keeping Secrets Inc. is better than this.

- ✓ Physical security controls
- ✓ No links/QR codes on flyers policy



# The story of Keeping Secrets Inc.



# The story of Keeping Secrets Inc.

RECON

- Social media platforms used
- Names and/or accounts of employees
- Brand details (names, logos, office locations,etc.)

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

# The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE

- Create anonymous accounts/personas
- Get gift cards (pay cash) to buy online advertisements
- Tweak ad settings to target Keeping Secrets Inc.
- Standard phishing preparation (domains, social engineering, etc.)

The screenshot shows a targeting configuration page with the following sections:

- Ad group details > Targeting > Creatives**
- Your audiences**:
  - Tailored and flexible audiences
  - All Search
  - Target similar people to those in your chosen audiences.
- Demographics**:
  - Gender: Any gender  Male  Female
  - Age: All ages  Age range
  - Locations, languages, technology
  - All Search   
Bulk upload
  - No location, device, or platform targeting selected
  - Target people who first used Twitter on a new device or carrier

# The story of Keeping Secrets Inc.

RECON

- Standard phishing best practices
- Take advantage of the preview functionality

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &  
CONTROL

ACTIONS ON  
OBJECTIVE



Keeping Secrets Inc.

Sponsored

Like Page

Are you already working for Keeping Secrets Inc.? Want to join our new office?



JOIN OUR NEW OFFICE TODAY

Join our new office today!

Be a member of one of the most exciting teams!

[HTTPS://TINY.CC/KEEPINGSECRETSOFFICE](https://tiny.cc/keepingsecretsoffice)



20

0 Comments 2 Shares



Like



Comment



Share

# The story of Keeping Secrets Inc.



# What did we learn?

- Phishing can be delivered via various channels. For example:
  - Messaging platforms
  - Social media
  - Cloud applications
  - Physical world
  - Online advertisements
- There is no single off-the-shelf solution to protect you against all of them

# Learnings for a red teamer

- Think outside the box
- Any method your target is using for electronic communications is a potential phishing delivery channel
- Adapt. Improvise. Overcome
- *“Advanced” methods makes you look better to your customers*

# Learnings for a **blue** teamer

- You cannot buy security
- It's not your users' fault
- Identify your ingress and egress points
- Use defense in depth
- Work towards a “Zero Trust” model

# Questions?

