

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?

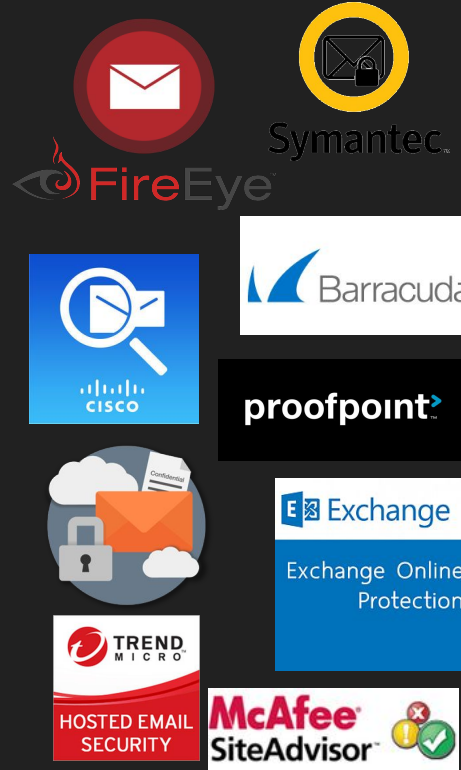
Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication

Why phishing beyond emails?

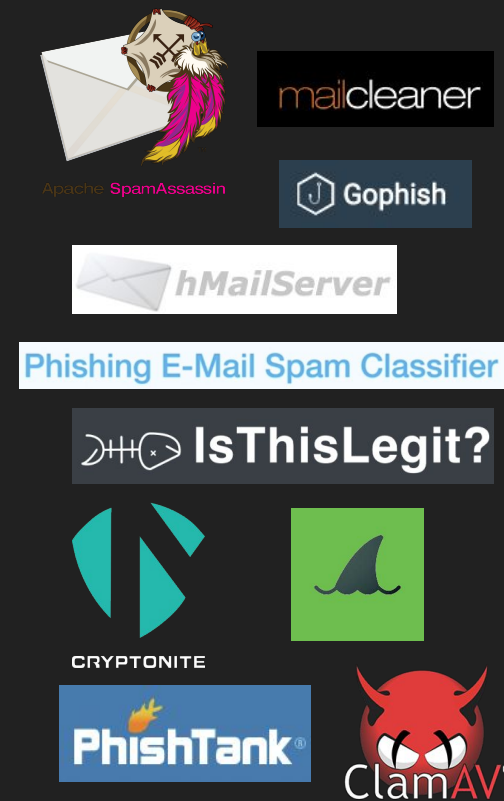
Technologies

SPF	SPAM FILTER
DMARC	
DKIM	AV
DLP	RESTR- ICTIONS
S/MIME	TLS
PGP	ML & NLP CLASSIF- ICATION
POLICIES	

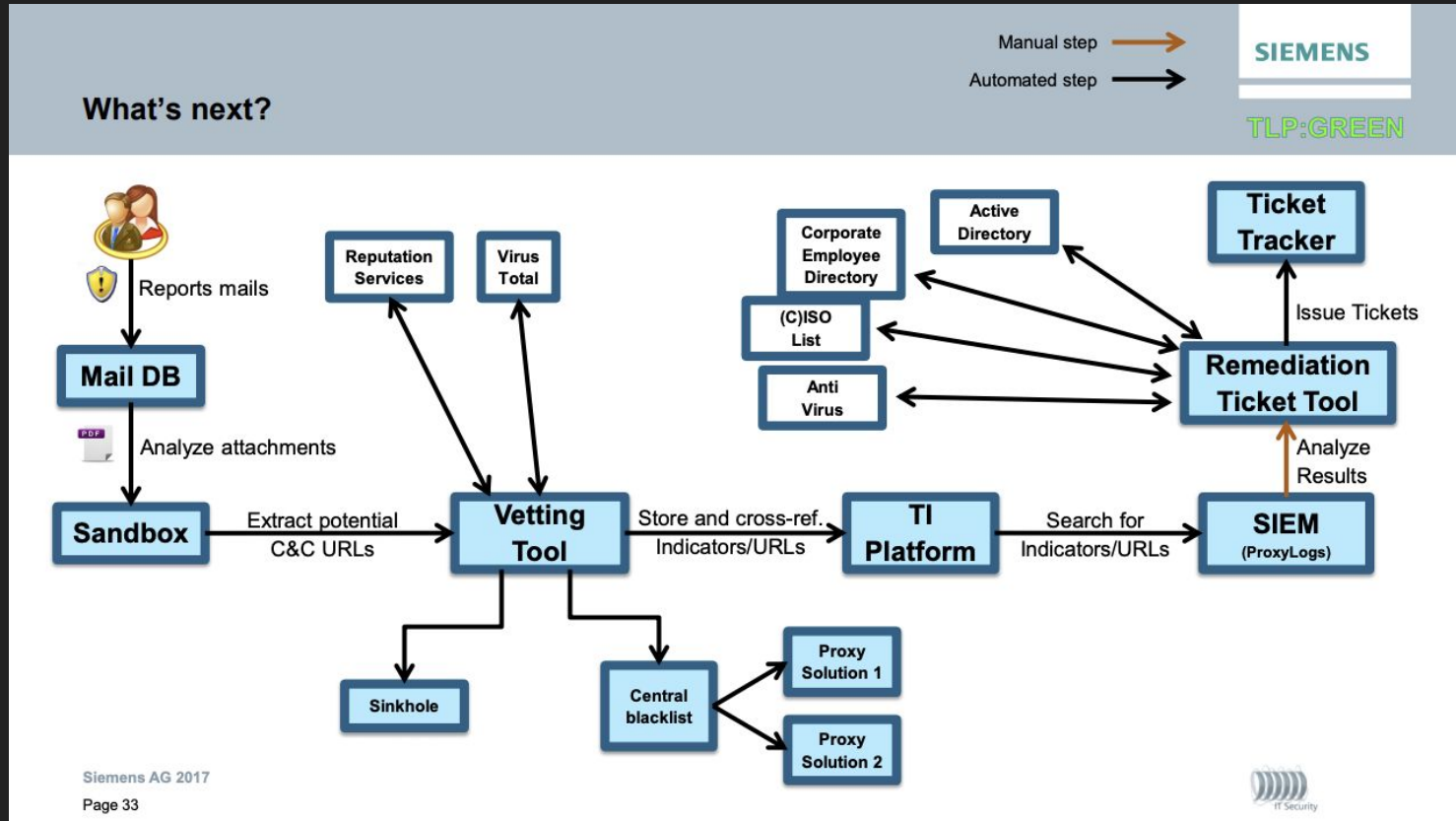
Enterprise solutions



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>

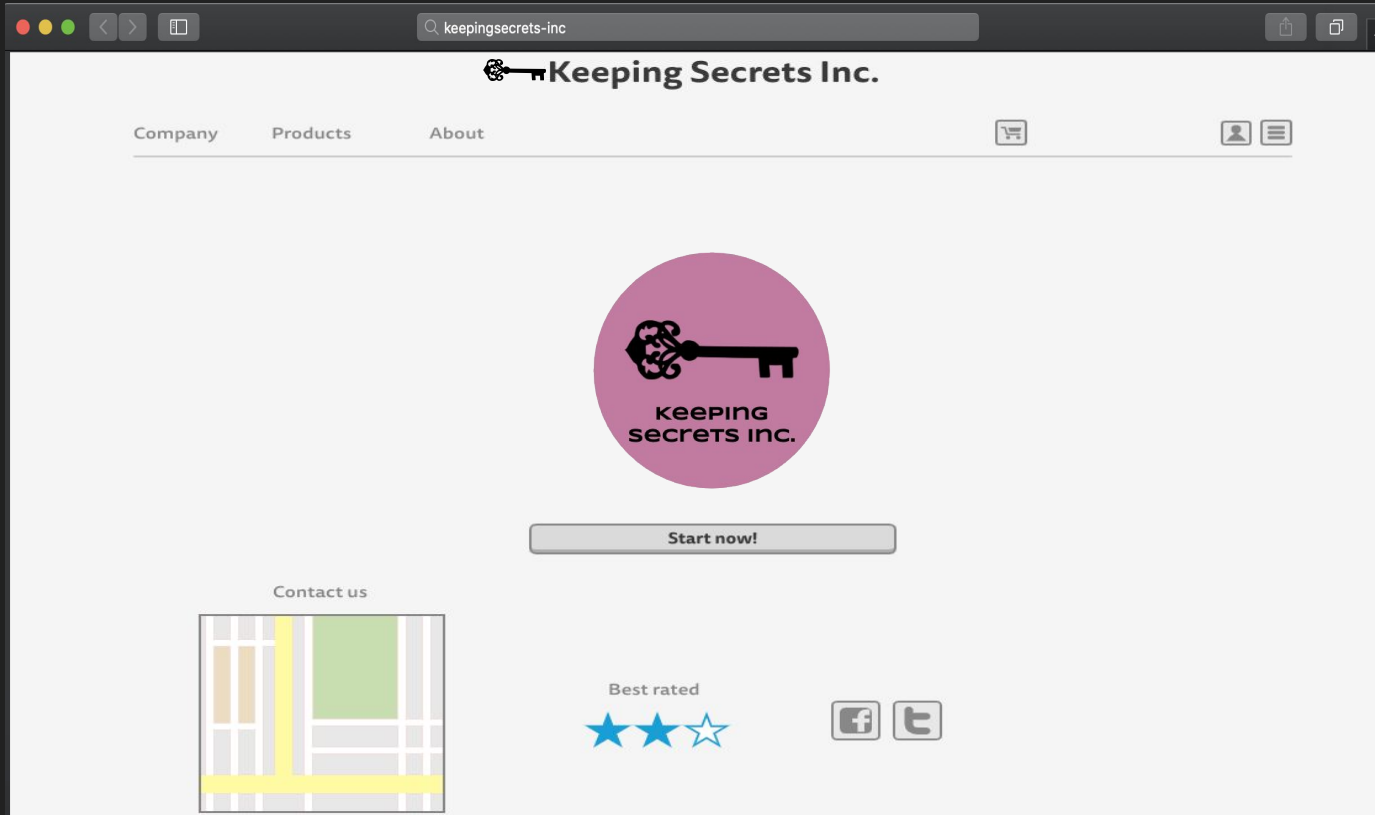
Why phishing beyond emails?

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

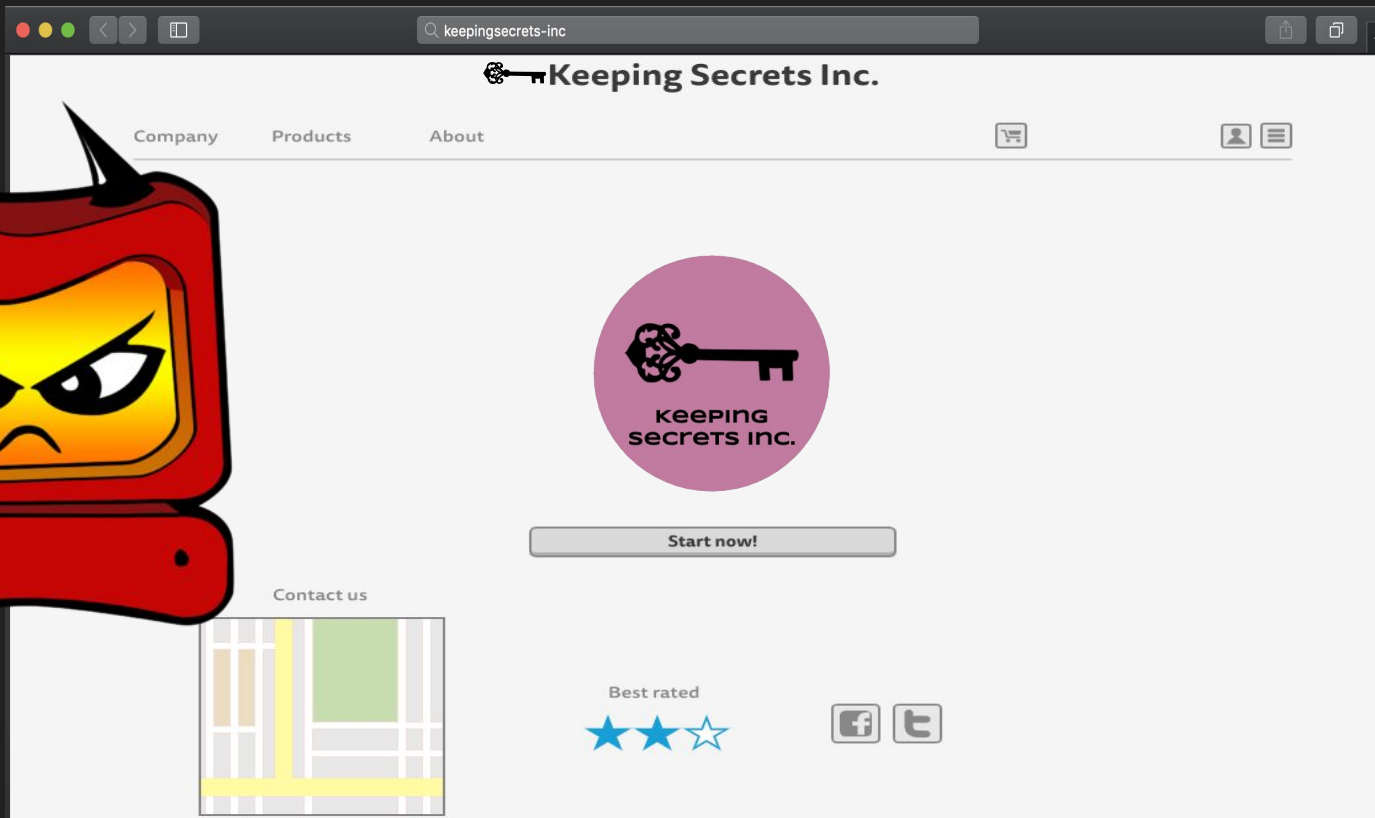
Even the finest sword plunged into salt water will eventually rust
Sun Tzu, The Art of War



The story of Keeping Secrets Inc.



The story of Keeping Secrets Inc.



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

Targets:

INSTALLATION

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

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE

The story of Keeping Secrets Inc.

RECON

- Get prepaid SIM cards (using cash)

WEAPONIZATION

- Set up accounts on target mobile communication Apps

DELIVERY

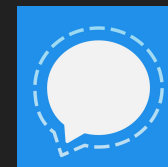
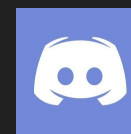
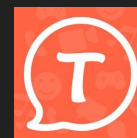
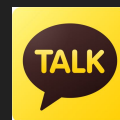
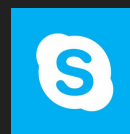
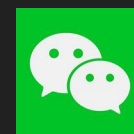
- Standard phishing preparation (domains, social engineering, etc.)

EXPLOITATION

INSTALLATION

COMMAND & CONTROL

ACTIONS ON OBJECTIVE



The story of Keeping Secrets Inc.

RECON

- Standard phishing best practices

WEAPONIZATION

- Get advantage of preview functionality

DELIVERY

- Additional capabilities

EXPLOITATION

- Ability to install mobile malware

INSTALLATION

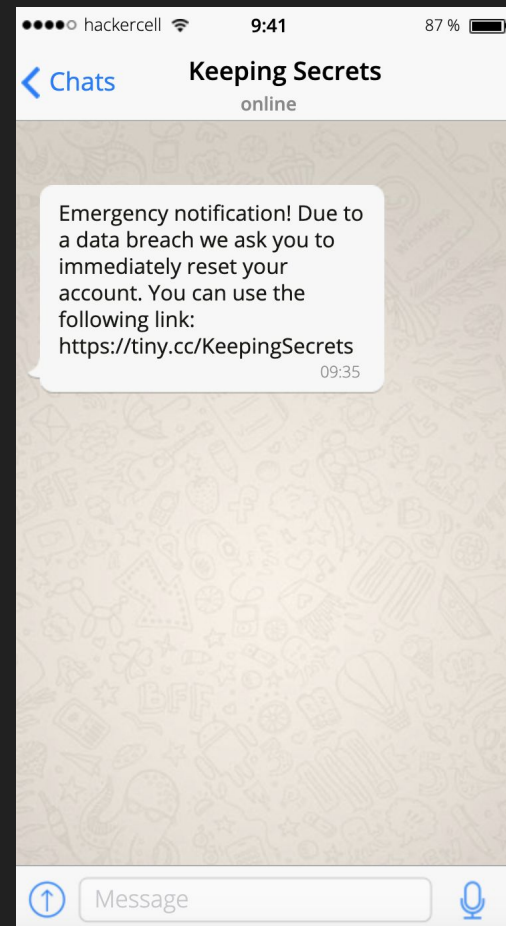
- Steal 2FA tokens

COMMAND &
CONTROL

- Turn the phone to a rogue AP

ACTIONS ON
OBJECTIVE

- 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

EXPLOITATION

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

INSTALLATION

- ✓ Easy way for users to report suspicious activity

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

Targets:

EXPLOITATION

- Credentials
- Communication platforms
- Externally accessible platforms

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE

The story of Keeping Secrets Inc.

RECON

- Accessing platforms externally

WEAPONIZATION

- Credential stuffing attacks

DELIVERY

- Standard phishing preparation (domains, social engineering, etc.)

EXPLOITATION

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE



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:

- Social media
- Forums
- Blogs
- News websites

WEAPONIZATION

DELIVERY

EXPLOITATION

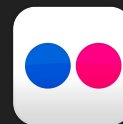
INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE



twitter



The story of Keeping Secrets Inc.

RECON

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

WEAPONIZATION

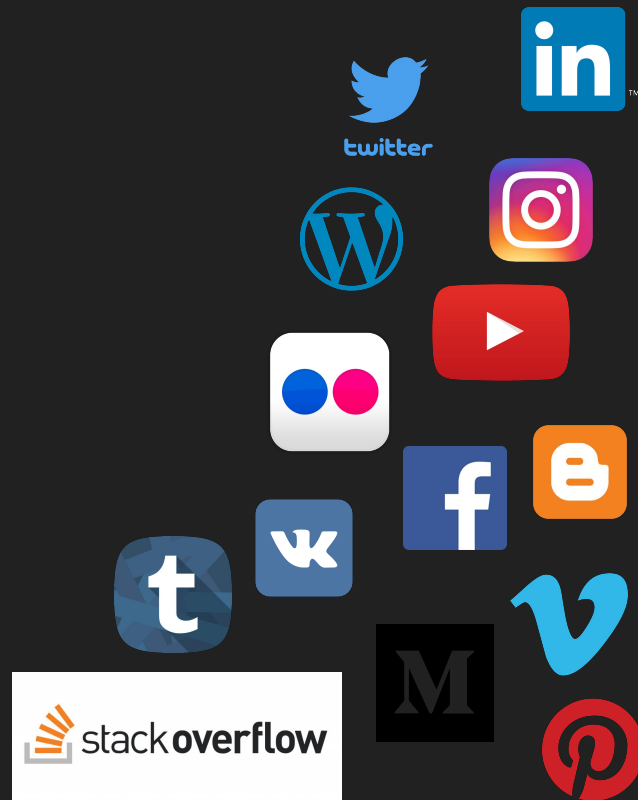
DELIVERY

EXPLOITATION

INSTALLATION

COMMANDS
CONTROL

ACTIONS ON
OBJECTIVE



The story of Keeping Secrets Inc.

RECON

- Standard phishing best practices

WEAPONIZATION

- Additional capabilities

DELIVERY

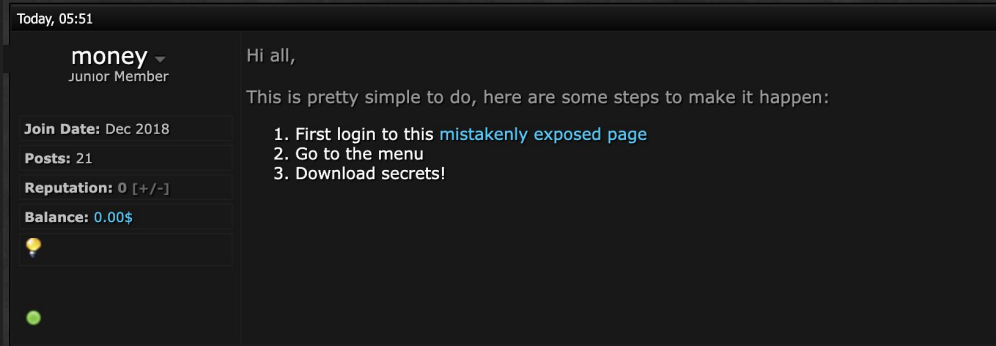
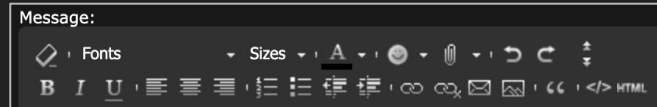
EXPLOITATION

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE

- 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.



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



The story of Keeping Secrets Inc.

RECON

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE



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

- Create GMail accounts/personas

WEAPONIZATION

- Standard phishing preparation (domains, social engineering, etc.)

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE

The story of Keeping Secrets Inc.

RECON

- Standard phishing best practices

WEAPONIZATION

- Additional capabilities

DELIVERY

- 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.

EXPLOITATION

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE

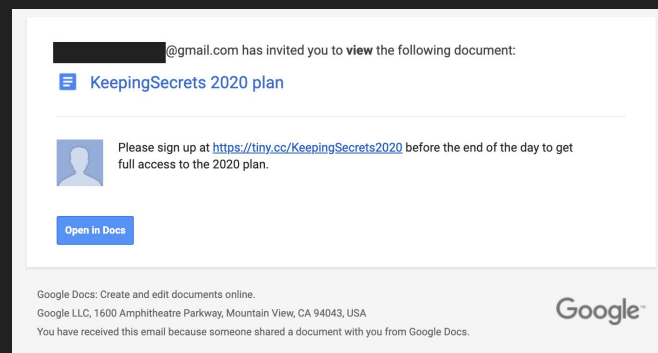
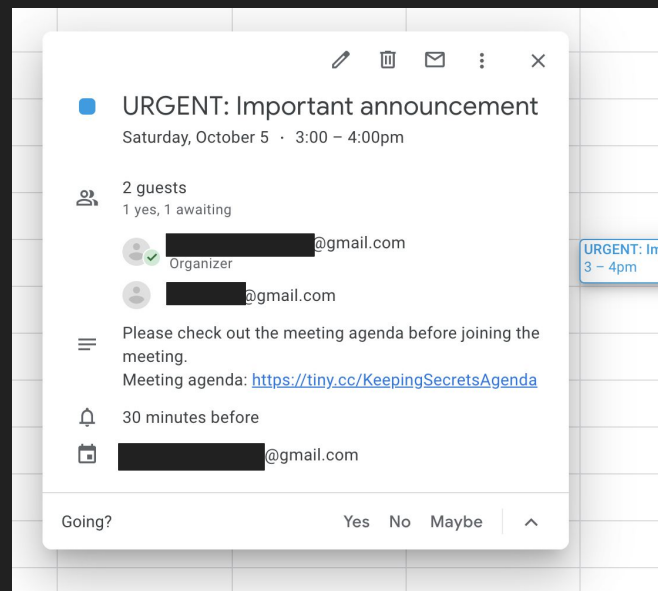
Would you like to send invitation emails to Google Calendar guests?



Dismiss

Don't send

Send



The story of Keeping Secrets Inc.



The story of Keeping Secrets Inc.

RECON

Keeping Secrets Inc. nailed it!

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE

- ✓ 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

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

WEAPONIZATION

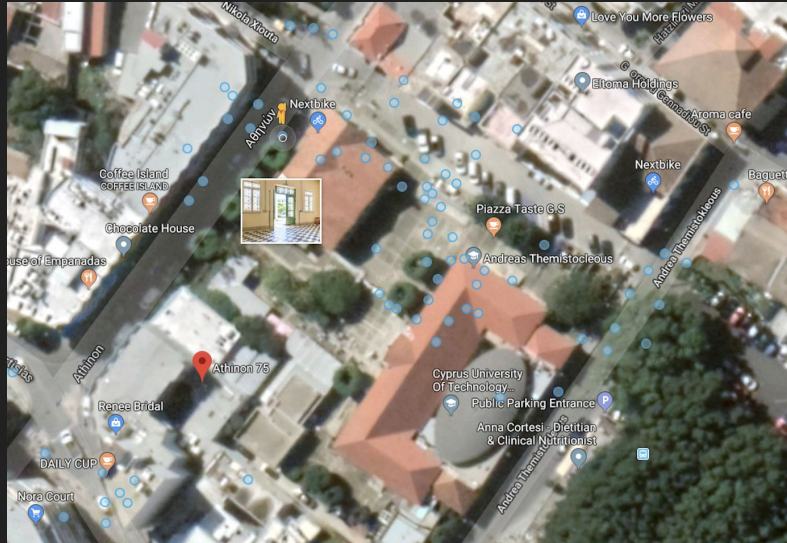
DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE



The story of Keeping Secrets Inc.

RECON

- 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.)

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE



The story of Keeping Secrets Inc.

RECON

- Standard phishing best practices

WEAPONIZATION

- Additional capabilities

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE

- 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

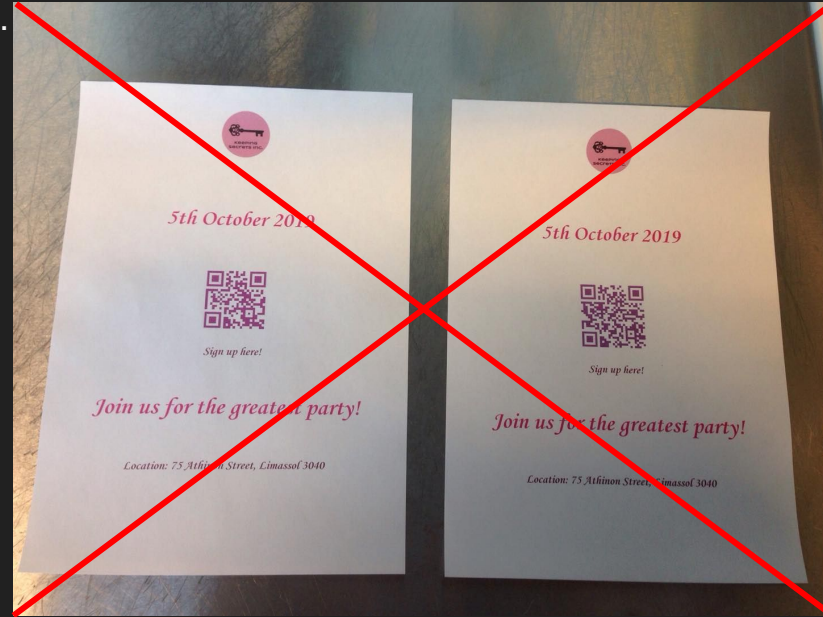
INSTALLATION

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

- Create anonymous accounts/personas

WEAPONIZATION

- Get gift cards (pay cash) to buy online advertisements

DELIVERY

- Tweak ad settings to target Keeping Secrets Inc.

EXPLOITATION

- Standard phishing preparation (domains, social engineering, etc.)

INSTALLATION

COMMAND &
CONTROL

ACTIONS ON
OBJECTIVE

[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

WEAPONIZATION

- Take advantage of the preview functionality

DELIVERY

- Additional capabilities

EXPLOITATION

- You can see how many clicked it

INSTALLATION


- You can remove it/hide your tracks

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?

